Not Invented Here: Power and Politics in Public Key Infrastructure (PKI) institutionalisation at two global organisations

Frederick Wamala
Department of Information Systems

A dissertation submitted to **the London School of Economics and Political Science**
as a partial requirement for the award of a **Doctor of Philosophy degree in Information Systems**
of the University of London.

Dedication

To all the people who helped me in return for nothing!

Abstract

This dissertation explores the impact of power and politics in Public Key Infrastructure (PKI) institutionalisation. We argue that this process can be understood in power and politics terms because the infrastructure skews the control of organisational action in favour of dominant individuals and groups. Indeed, as our case studies show, shifting power balances is not only a desired outcome of PKI deployment, power drives institutionalisation. Therefore, despite the rational goals of improving security and reducing the total cost of ownership for IT, the PKIs in our field organisations have actually been catalysts for power and politics.

Although current research focuses on external technical interoperation, we believe emphasis should be on the interaction between the at once restrictive and flexible PKI technical features, organisational structures, goals of sponsors and potential user resistance. We use the Circuits of Power (CoP) framework to explain how a PKI conditions and is conditioned by power and politics. Drawing on the concepts of infrastructure and institution, we submit that PKIs are politically explosive in pluralistic, distributed global organisations because by limiting freedom of action in favour of stability and security, they set a stage for disaffection.

The result of antipathy towards the infrastructure would not be a major concern if public key cryptography, which underpins PKI, had a centralised mechanism for enforcing the user discipline it relies on to work properly. However, since this discipline is not automatic, a PKI bereft of support from existing power arrangements faces considerable institutionalisation challenges. We assess these ideas in two case studies in London and Switzerland. In London, we explain how an oil company used its institutional structures to implement PKI as part of a desktop standard covering 105,000 employees. In Zurich and London, we give a power analysis of attempts by a global financial services firm to roll out PKI to over 70,000 users.

Our dissertation makes an important contribution by showing that where PKI supporters engage in a shrewdly orchestrated campaign to knit the infrastructure with the existing institutional order, it becomes an accepted part of organisational life without much ceremony. In sum, we both fill gaps in information security literature and extend knowledge on the efficacy of the Circuits of Power framework in conducting IS institutionalisation studies.

Acknowledgements

The journey to this PhD has been a very difficult one. I have weathered a fair amount of storms. However, it would have been impossible without the support of many individuals and institutions. Let me take this opportunity to express my gratitude for this support.

First, I would like to thank the LSE Information Systems Department for paying most of my tuition for the PhD and all my fees for the MSc ADMIS course. The Department also covered some of my living expenses. I also thank the Commonwealth Secretariat for their Academic Exchange Fellowship that supported my data collection exercise. I specifically thank Mr Rogers W'O Okot-Uma for his help in securing the funding from the Commonwealth.

I would like to thank my supervisor, Dr. James Backhouse, for reading my draft chapters with a critical eye. I am also sincerely thankful to the following people in the Information Systems Department who took special interest in my welfare. I am grateful to Dr Steve Smithson, Dr Jonathan Liebenau, Dr Shirin Madon and Dr Carsten Sørensen for giving me personal support. I also appreciate the help I received from Professor Bob Galliers, Dr Tony Cornford and Dr Edgar Whitley regarding extra funding. Furthermore, I thank Sarah Emery and Prodromos Tsiavos for their help. I also appreciate the support of my two "brothers in arms" Daniel Osei-Joehene and Gamel Wiredu with whom we shared the dream.

Outside the IS Department, I would like to thank Yvonne Ward, my colleague at the LSE IT Help Desk, for always wishing me well. I also appreciate the support of Mr Joel Kibazo and his wife Jay. I further thank Mr Peter Wren at the LSE for his help. Lastly, I thank my old friends Mr Bakulumpagi Lwanga, JJ Otim "Mukwaya" Lucima and Robert Mudhasi for supporting me. For all those I have mentioned and the rest, let me repeat, thanks very much!

Table of Contents

List of figures

CHAPTER 1:
RESEARCH ISSUES

Introduction

Information Systems are essential for the coordination (Earl and Feeny 1994, Nutt *et al.* 2000) and control of activity (Ciborra 2000, Meyer and Rowan 1991) in formal organisations (Morgan 1997, Pfeffer 1992). As such, complex networks of computer-based information systems (IS) are the engine of large modern organisations. The technologies both improve communication potential and modify its patterns. A key attraction is that, "Because technology reduces the cost and unreliability of relaying orders, management can tighten control (Hinds and Kiesler 1999)." Thus, because IT is immensely transformative (Kling 1990, Kling and Iacono 1984, Kling and Jewett 1994), management should carefully consider the social, economic and organisation implications of new systems (Angell 2000). However, fashion and fads drive innumerable IS projects (Abrahamson 1991). Kling (1990) traces the syndrome to early days of computing. He argues,

> "Early computer enthusiasts were excited or awed by the prospects of a transformative technology. ...although much of the managerial and academic world has become sceptical of exaggerated claims and **hyper-hype** ...which are part of the official story of computerisation -- pushed by the marketing arms of computer vendors, futurists like Tofler and Naisbitt, and sympathetically amplified by journalists."

Likewise, Abrahamson (1991) argues that innovation literature is interspersed with beliefs that innovations, and their diffusion, naturally benefit adopters. However, astute marketing often leads organisations into deploying fashionable technologies (Buchanan and Boddy 1983, Ciborra 2000, Swanson and Ramiller 1997) without considering critical issues such as technical efficiency, organisational desirability, political and cultural feasibility (Checkland 1981, Checkland and Scholes 1990). To Abrahamson, fads may lead to the rejection of useful technologies because they discourage their careful and sustained implementation. He says,

> "Fads or fashions cause organisations to leap rapidly from one technology to the next, so that no technology has enough time to work ... managers jump rapidly from one problem to the next, so that technologies do not solve problems because the **problems go out of fashion** before technologies can solve them (Abrahamson 1991)."

However, Swanson and Ramiller (1997) argue that despite the zest with which the business-oriented media proclaims IT advances, experts now greet the declarations with as much doubt as affirmation because buzzwords are often "signals of din and confusion."

E-Commerce Security

The foregoing debate directly applies to Electronic Commerce[1] and the fledgling attempts to secure it (Jøsang *et al.* 2001) because it, too, is shrouded in hype. E-commerce makes it possible for parties who are not in direct contact to enter into, undertake and perform entire contracts within the bounds of cyberspace. This is irrespective of whether they had a pre-established business relationship or not. This faceless commerce opens up copious business opportunities but also comes saddled with risks (Bhimani 1996, El-Ata *et al.* 2002). Because of concerns about confidentiality, authentication, non-repudiation and authorisation, e-commerce has not taken off as widely as predicted (Levitt 1999, Schneier 2000).

As a result, e-commerce security is widely associated or even synonymous with cryptography (Blaze *et al.* 1996, Diffie and Hellman 1976, Gollmann 2000a, Singh 1999) because it buys confidence in an uncertain world (Garfinkel and Spafford 1997). Global political fights over export control (Gollmann 2000a) and key escrow (Ganesan 1996, Whitley and Hosein 2001) underlined the role of cryptography as a premier control measure for e-commerce and other aspects of modern computing (Wood 1996). The general sentiment is that without cryptography e-commerce could never have become mainstream business (Blanchette 2000, Clarke 2001). Cryptography is divided into secret key and public key or asymmetric cryptography. The next chapter discusses the two types of cryptography in detail. Of the two branches, public key cryptography (Jøsang *et al.* 2001) and its technological realisation in the electronic world, namely Public Key Infrastructure (PKI) (Blanchette 2000), are hot e-security topics because of their ability to enforce real-time contracts between potentially distrusting parties across distances.

However, PKI deployments have to date been driven by fads and hype. This is little wonder. The digital security sector has traditionally thrived on the pursuit of technical fixes (Dhillon and Backhouse 2000, Hitchings 1995, Smith 1993, Wood 2000) because security is "very, very difficult to do (Schwartau 1998)." Due to the prevalence of the PKI fad Gartner Group,

[1] **Electronic Commerce** here refers to Internet-based buying and selling of information, products and services.

an IT research and consulting firm, developed a "PKI Hype Cycle" to show the stages of PKI development. The cycle has five stages as illustrated below.

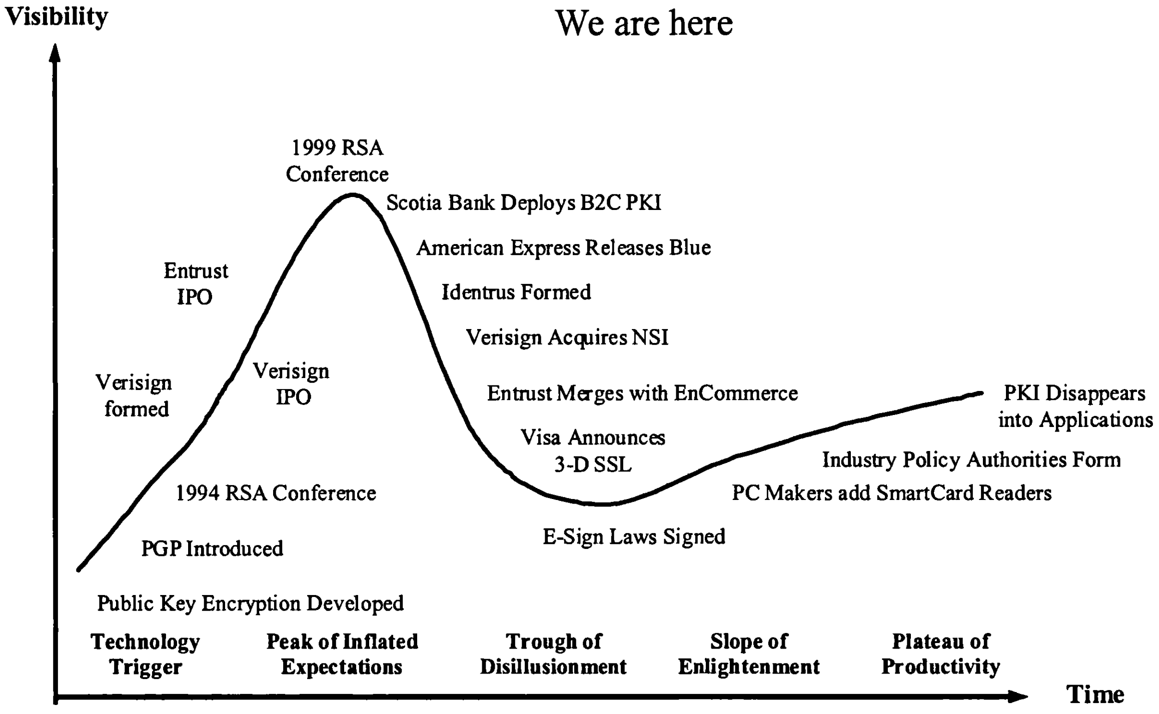


Figure 1 – The Gartner PKI Hype Cycle

PKI hype coincides with the "Peak of inflated expectations." The phase saw over-enthusiastic projections about the technology with conference organisers and magazine publishers the main beneficiaries. Therefore, the craze simply replayed the long established 'year of the...' syndrome (Ellison and Schneier 2000) in the security sector. To Ellison and Schneier first it was "firewalls, then intrusion detection systems, then VPNs (Virtual Private Networks) and now certification authorities (CAs) and public key infrastructure (PKI)." The mantra goes, "if you buy X, then you will be secure (Ellison and Schneier 2000)." However, there were more pilot projects and failures than successes as vendors pushed PKI to its limits leading the press to abandon it. The result was the current "trough of disillusionment."

This was predictable because, as Abrahamson argues, deploying systems based on fashion disadvantages technically efficient technologies because they often need more time to tailor to specific organisational needs than what the craze permits. Indeed, Gartner warned that, "Infrastructure investments like PKI frequently take time to show benefits (Wheatman and Pescatore 2001)." Gartner expected substantial value in two to three years. However, fashion is not the only concern about PKI. Claiming that sometimes the importance of cryptography to web security is often embellished, Gollmann (2000) warns that uninformed use of the technology may cause problems because it was designed for communication not internet security. He insists that although,

> "Some issues in web security are typical communications security problems, there are also scenarios where there **are no longer 'trusting' parties wishing to communicate securely in a 'hostile' environment, but 'hostile' parties needing a 'trusted' environment to communicate** (Gollmann 2000a)."

Consequently, using cryptography on the mistaken assumption that it enforces the same policies and addresses the same threats as in communication security is risky. Thus, PKI is in crisis. On the one hand, PKI is clearly vital for secure e-commerce, e-government and digital democracy. A clamorous example is the UK Inland Revenue system that was "suspended when users reported seeing snippets of other people's information" (BBC 2002, BBC 2002a). However, other commentators have doubted the usefulness of PKI in secure e-commerce. For instance, in a sweeping broadside at the technology, Clarke (2001) insists that PKIX has been, and will remain a failure because it makes wrong assumptions about organisational structures and key usage. We continue this debate in Chapter 2.

We believe PKI is at crossroads because current research almost exclusively considers technical features and ignores views like power and politics that are relevant in explaining institutionalisation. Our research highlights this oversight and explores the usefulness of a power angle in explaining how a PKI is taken for granted (Kling and Iacono 1984). We believe useful PKIs must become acceptable in the private cultural and political spaces (Silverstone and Haddon 1996) of the host organisations because new technologies are often incompatible with workflows (Ciborra 2000). In sum, we hope the insights from our thesis can augment the technical literature and help provide a better PKI institutionalisation picture.

The rest of the chapter proceeds as follows. The first part summarises our main arguments and sets the tone for the dissertation. We introduce the debates here to take the readers, many unfamiliar with subject, directly to the subject matter. The approach is useful because it,

> "Not only piques their curiosity ...but also provides them with an orienting glimpse into the storyline that will be developed (Golden-Biddle and Locke 1997)."

The early depiction of the debates is crucial "in the establishment of rapport between the work and its readers (Golden-Biddle and Locke 1997)." Therefore, we provide a research 'sneak preview' that initiates the storylines that we discuss later in the dissertation. Next, we explain the purpose of the dissertation including the motivation and scope of the study. The research questions follow. Thereafter we justify our research and general approach. We end with a summary and the structure of the dissertation.

Purpose of the study

In light of the foregoing remarks, this dissertation investigates the impact of power relations in the PKI institutionalisation process. We examine the effect of the PKI on two organisations that are deploying it, exploring its effects on power and responsibility structures. We emphasise process here because, as Monteiro and Hepsø (1998) contend, institutionalisation is but shorthand for an ongoing socio-technical negotiation. Indeed, as other studies (Hanseth and Monteiro 1998, Hanseth *et al.* 1996) indicate, it takes hard work and luck to mobilise sufficient support (Monteiro and Hepsø 1998) for complex information infrastructures. We hoped to assess whether deploying a PKI is a clear-cut process as the technology white papers and general management literature claim (Ciborra 2000). However, we find that PKI institutionalisation is a long-term process fraught with technical, legal and regulatory challenges and a minefield of political machinations dressed up in cosmetic arguments about security and Total Cost of Ownership reduction (Hoffman 2002, Pratt 2002).

Motivation of research

This research stems from our general interest in large information infrastructures and their impacts on managerial and decision-making structures of global organisations. The sheer reach of these technologies inevitably has security and political implications in pluralistic organisations. Since conventional infrastructural research focuses on technological issues, our understanding of social and organisational issues is limited. We believe security directors should look beyond the current focus on implementing the available technologies to address the complex task of incorporating these products into business governance processes. Thus, following (Markus and Pfeffer 1983, Silva 1997, Silva and Backhouse 2003), this study explores the importance of power and politics in PKI institutionalisation. First, we demonstrate that a PKI becomes 'part of the furniture' (Silva and Backhouse 1997) if it positively reinforces power sources and structures of the host organisation[2]. Second, because specific business divisions or country offices spearhead PKI projects, the infrastructures incorporate values, beliefs and agendas that may conflict with the culture of either the wider organisation or substantial constituencies within it (Markus and Pfeffer 1983). Thus, the infrastructure faces challenges because "counterimplementation is most likely to occur when

[2] We use the word to cover both the intra and interorganisational use of PKI.

outsiders bring in threatening new technologies (Keen 1981)." Public key infrastructures perfectly fit the bill because they are panoptic.

But what makes this dissertation unique? First, it focuses on the internal impact of the PKI as opposed to the interoperability issues that have dominated research on the technology to date. We assess how the PKI is interwoven into political and institutional spaces of our case studies and how it simultaneously becomes the support and physical manifestation of the security objectives and regime. As a result, we shift attention from the current fascination with keys to encapsulate a process for the creation of a functional security infrastructure. Second, contrary to views in the besotted trade press (Kling 1990), this dissertation illustrates that public key infrastructures are never passive security systems because they skew the control of organisational action in favour of powerful individuals and groups.

Put another way, the greater security supported by the PKI imposes arduous rigidities on the routines of daily work (Ciborra 2000, Keen 1981) that may either become taken for granted or rejected. A useful PKI should ensure an effortless repetition of security behaviour, which over time leads to a security culture (Hitchings 1995). If this behaviour becomes 'the expected way of doing things', it initiates the institutionalisation process. Therefore, we strongly argue that PKI institutionalisation depends, less on the technical brilliance of the underlying algorithms and key lengths and, more on efforts to blend it with the existing power and responsibility arrangements of the host organisation.

We show that a PKI has better chances of institutionalisation if it positively reinforces an organisation's (BSI 1999, Finne 1996, Nosworthy 2000, Wood 1997) institutional order by building on current structures. We argue that a key reason why about 70% of PKI deployments are at pilot stage (Townsend 2001) and others have failed (Clarke 2001) is because the native X.509 design attempts to create rival structures and power centres either on top of or in competition with the existing organisational order (Gutmann 2002). The problem is that PKIX architectures have sought to superimpose hierarchical and authoritarian structures onto organisations that largely have decentralised authority arrangements (Clarke 2001, Markus 1983). Therefore, many public key infrastructures have faced resistance from stakeholders worried about the loss of autonomy and flexibility.

Apart from issues with the PKIX model, computer security has traditionally been seen as a superfluous impediment (Parker 1997, Schwartau 1998) to getting work done. Therefore, an institutionalised PKI is beneficial because it becomes invisible, freeing employees from decision-making and enables them to dedicate more time to doing innovative activities (Berger and Luckmann 1967). Put simply, when a PKI becomes an expected component of organisational life, users no longer regard it as an impediment to work.

Yet despite hackneyed phrases, the current literature has encouraged the view of PKI as one of those products that could act as a "kind of magic security dust that they could sprinkle over their software and make it secure (Schneier 2000)." The literature offers little advice on how to address the sensitive power issues caused by the implementation of public key infrastructures in large organisations. For instance, a PKI enables managers to compel relying parties to achieve desired outcomes through its supervision, monitoring and surveillance abilities. As such, PKI institutionalisation could encounter political problems. Actually, the majority of PKI literature came out at the "peak of inflated expectations" in the hype cycle.

Our thesis highlights the gaps in the literature and introduces insights from power and politics that we believe offer a more comprehensive explanation of PKI institutionalisation. This is a good contribution because, as Pfeffer (1992) argues, although power and influence have negative connotations, they are "not the organisation's last dirty secret, but the secret of success for both individuals and their organisations" and their mastery is vital for the success of innovation and organisational change (Markus and Pfeffer 1983).

To build our case, we explored the concerns of stakeholders about possible loss of power, forms of interference and intervention because these fears sow seeds of resistance against any innovations in IS. We also examined the exercise of power and the imposition of discipline and control over employees faced with new methods of working because this affects organisational politics. The two case studies allowed us to explore these developments at different stages in the change life cycle, resulting in good insights into how organisations can set firm foundations for PKI acceptance. Institutionalisation is vital because PKI is not only a complex, all-pervasive (Adams and Lloyd 1999) and an expensive technology, it can hamper organisational flexibility (Barber 2000) and even reduce security (Newman 2001, Schneier 1999a) if not properly implemented. Levitt (1999) warns that a PKI "reaches deep into enterprise IT infrastructure and must function reliably, or the results could be disastrous."

Moreover, as Star and Ruhleder (1994) were to argue, simpler systems are often "picked up much more quickly and interfere less with other work habits than those which require substantial investment in changing habits and infrastructure."

Scope: Boundaries of Thesis

We should mention that although institutionalisation studies can take many perspectives, this dissertation does not look at the following areas. First, we do not see PKI as an independent actor. Writers like (Ciborra 2000, Hanseth 2000a, Hanseth and Monteiro 1998, Hanseth *et al.* 1996, Monteiro and Hepsø 1998) have discussed this view of infrastructure extensively. These studies talk about the infrastructure 'hijacking' the process of its institutionalisation and hence drifting. As Markus (1983) puts it tongue-in-cheek, this is a case of a system running people rather than people utilising it.

Second, we did not study power relations between stakeholders in the PKI interorganisational networks such as Certification Authorities, Registration Authorities, Verification Authorities and standards bodies notably the Internet Engineering Task Force (IETF) and the PKI Forum. In the first place, it was not practical to study all these organisations and be able to finish the PhD in good time because they are simply too many. Important too is our realisation, early on in the study, that such a line of investigation would not be feasible for a PhD, because these structures are in flux and could have changed beyond recognition by the time we got ready to write the dissertation. A common thread of research around these institutions deals with PKI interoperability and interoperation from technical and legal angles. PKI *interoperability* refers to the *capability*, and PKI *interoperation* refers to the *effect*, of logically linking multiple PKIs to form a larger PKI supporting a wider community of users (Baum and Ford 1998). While these are interesting areas, we believe the interoperability debate grossly underestimates the significance of organisational power plays in the success of, even the most well-intentioned and comprehensive, technical standards.

Third, our study of power relations in PKI institutionalisation does not focus on individual attributes. Authors like Agarwal and Prasad (1999) claim, "individuals' perceptions about using an innovation are posited to influence adoption behaviour." They attribute successful computer use to 'some kind of natural affinity' (Star and Ruhleder 1996). These authors, for instance, explain resistance in terms of the personality traits of the resistors who are seen as 'troublemakers' (Markus 1983) that resist new IS because of factors internal to them. The approach explains resistance with ideas such as people resist all change, people with cognitive styles accept systems, while intuitive thinkers resist them. This view is problematic because by claiming ability to catalogue traits (Hofstede 1993) in diverse global organisations, it trivialises institutionalisation. Critically, the uncertain benefits of examining personal traits may outweigh the costs of doing so (Markus 1983). At worst, this is a cynical attempt to explain away the failures of system designers.

Lastly, this dissertation excludes detailed mathematical accounts because these have already been covered (Menezes *et al.* 1996, Piper and Murphy 2002, Schneier 1996a). Instead, after Star and Ruhleder (1996), we argue that understanding context is critical for successful PKI institutionalisation because the technology only becomes an infrastructure for someone, when connected to a particular activity in a given cultural context. However, since technology is society made durable (Latour 1991) we cover the PKI technical features in detail to understand the interests inscribed into the IT artefact (Orlikowski and Iacono 2001).

Research questions

This study has a major research question and several sub-questions.

Major question

What is the role of power and politics in PKI institutionalisation?

Sub Questions

The sub-questions include:

(a) Does the implementation of a PKI disturb organisational power balances?

(b) What is the role of managerial and decision-making structures in the process?

(c) Is security enough reason to institutionalise a PKI in distributed organisations?

Justification of study

Cryptography is not just critical for internet security (Blanchette 2000). It also underpins security in applications that range from automatic teller machines, pay-per-view TV, cellular networks, the hapless digital cash and pre-pay utility meters (Anderson and Needham 1995, Schneier 1997). Therefore, ensuring PKI institutionalisation is of paramount importance for security in a networked world. Mathematicians, engineers and computer scientists, who honed their skills in the above-mentioned applications, currently dominate organisational PKI deployments. Thus, it is little wonder that issues surrounding key lengths and management, algorithms, ciphers and the design of dependable systems (Anderson 1994, Anderson 2001) still dominate literature in this field. The literature depicts PKI as a detached technical artefact that is impervious to the conditions surrounding its development and use (Star and Ruhleder 1994). This mindset is problematic in security practice because it wantonly extends the idealistic engineering roots of cryptography (Anderson 1994), which assume a logical world (Schneier 2000). Actually, the concept of Satan's Computer was introduced by (Anderson and Needham 1995) and adopted by (Schneier 1999b) to accentuate the difficulty of programming a secure computer as compared to – a general purpose – one designed to withstand Murphy's Law[3] (Anderson 2001). Unlike general-purpose computers, designers of secure systems need a detailed understanding of the potential threats the systems may face in use. However, because adversaries and their tools and techniques of attack constantly evolve,

> "Security engineering is different from any other type of engineering. ... **security features within products, are useful precisely because of what they don't allow to be done.** Most engineering involves making things work. ... Security engineering involves making sure things don't fail in the presence of an intelligent and malicious adversary who forces faults at precisely the worst time and in precisely the worst way. (Thus) security engineering involves programming Satan's computer (Schneier 1999b)."

Since much of this security depends on cryptology and Schneier (1997) argues, "With cryptography, what you see isn't what you get. Subtle flaws can render any security system vulnerable to attack" then the engineering logic is not sufficient on its own.

As we discuss elsewhere, X.509, the most widely used certificate standard, was a solution in search of the problem before the Internet. In the same vein, Davis (1996) eloquently explains why the very design of public key cryptography (PKC) systems, like PKI, makes unrealistic assumptions (Clarke 2001) about the ability and willingness of users to meticulously validate

[3] Murphy's Law (**"If anything can go wrong, it will"**) was named after US Capt. Edward A. Murphy.

other people's public keys and keep their own private keys secure (Schneier 2000). In practice, users are either unable or unwilling to manage keys diligently, and the underlying technology does not rectify this weakness (Davis 1996). Thus, we believe the success of a PKI depends on its association with power structures in the host organisation.

We draw parallels between current PKI research and trends in Electronic Mail (e-mail) research. Early e-mail studies focused on the technological constraints of its design and attempted to improve its friendliness and to make "it more accessible, reliable and flexible (Romm *et al.* 1996)." Later research, however, covered non-technical organisational aspects. Similarly, this dissertation transcends the PKI research focused on improving reliability and flexibility to address the fiddly organisational issues. We believe this is a beneficial research direction because since computer scientists, engineers and mathematicians publish most PKI literature, non-technical issues like power and politics are not a priority. Yet a vital reason why large infrastructural systems, like PKIs, are resisted and subsequently fail is the,

> "Fear of undesirable effects on the organisational structure, **power distribution** or the possibility of cultural conflict between the system and the organisation in which it is to be implemented ... Individuals are likely to consider systems more or less appropriate if they feel that they might gain or lose power due to the implementation of the system (Romm *et al.* 1996)."

A system stands a risk of rejection if powerful actors view its implementation as a threat to the current structural characteristics of the organisation. This is because large information infrastructures affect organisational norms and values through their modification of the techniques of production, discipline and surveillance. Romm *et al* argue that before institutionalisation takes place, management and employees need to understand the political aspects of a technology. Otherwise, success at the early stages can culminate in devastating political side effects at the later stages of implementation. They lament that when power and politics are mentioned, many people regard them as detrimental to the institutionalisation of an IS and hence suggest their elimination (Pfeffer 1992).

The empirical nature of our research fills a gap in PKIX knowledge because we assess the use of the infrastructure in real life settings. This is unlike many of the critics who, because of their own commercial agendas, only give information to promote their wares. An example will suffice. Schneier makes a risible point by warning that "with cryptography, what you see isn't what you get" but shortly after he states that his company "Counterpane Systems has the expertise you need to make sure your system is as secure as it looks (Schneier 1997)." In another paper, he claims Counterpane offers "leading-edge expertise in the fields of intrusion detection and prevention (Ellison and Schneier 2000)." We are not picking on Schneier *per se* but only showing that the lack of adherence to PKI standards has forced different vendors into "territory grabbing." We extend this debate in the next chapter.

Since technological innovation is not just a matter of engineering but IS are social products (Silverstone and Haddon 1996), our socio-technical study informed by the Circuits of Power (CoP) framework (Clegg 1989) addresses more issues than purely technical approaches. As a renowned computer scientist astonishingly warned, "organisational issues are not just a contributory factor in security failure ... They can often be primary causes (Anderson 2001)." Our two case studies show that shifting power balances is not only the desired outcome of deploying a PKI but power and politics are essentially the means of facilitating this institutionalisation. We use the CoP framework, adapted from social and political science theory (Clegg 1989) by Silva (1997), to account for these forces because it shows how power circulates through the technological component of information systems as well as norms, techniques of production and discipline. Briefly put, the main contribution of this dissertation is to apply conceptions of power and politics to an empirical analysis of a hitherto natural science dominated area of information security.

Chapter summary

The Chapter covers the purpose of the dissertation, justifies it, and outlines the research questions and our contribution to knowledge. We also place this research within the IS and information security domains. We analyse these changes through the theoretical lenses provided by previous research on institutionalisation notably (Silva 1997, Silva and Backhouse 1997) and (Introna 1997) encapsulated in the CoP framework. However, unlike (Silva 1997, Silva and Backhouse 2003) our research objective was not to "offer a theoretical framework" because the CoP is already available. We set out to extend these works by exploring the CoP's viability as a methodology for large IS empirical studies. We focused on how the framework can help identify elements to focus on during empirical work. For instance, we found that researchers should cautiously use the native CoP terms such as "power and politics" because they are so emotive. The dissertation takes a similar approach.

Organisation of the Dissertation

The rest of the dissertation proceeds as follows. In Chapter 2, we critically review the relevant literature on PKI and other themes of the dissertation namely: infrastructure and organisational politics. We broadly argue that PKI is yet to become a pervasive security substrate because organisations have been unable to appreciate the capricious interaction between its at once restrictive and flexible technical features, organisational structures, goals of sponsors and potential user resistance. By focusing on technical aspects, current research downplays the role of context and its attendant political encumbrances in institutionalisation. Chapter 3 offers the theoretical foundations of our thesis with the evaluation of the debates surrounding the concept of power. We survey the considerable literature on the different views of power and their influence on IS research. Thereafter we focus on the Circuits of Power framework.

Chapter 4 deals with research design. We discuss the philosophical foundations of our methodological approach and place them within the IS research tradition. We also provide the rationale for a case study research strategy, the selection of the two field studies, data sources and the role of the CoP framework as data collection and analytical tool for this research. We also give a background to our research decisions. In chapters 5 and 6, we present the findings from our two case studies Oilcom and Bankrecht respectively. The chapters include a reflection on the political, social and historical background of the research settings. Since we also used the CoP to direct our research (methodology) we present the findings from the two cases based on the framework. However, we do not follow the traditional CoP elements but the themes we developed during our research to overcome the repetitions in the circuits.

In Chapter 7, we bring together the findings from both case studies and analyse them using the CoP framework lenses. We assess whether the CoP framework explains our evidence or if it leaves big questions unanswered. We use the answers to these questions to evaluate the usefulness of the CoP in explaining events in the real world. Finally, Chapter 8 summarises the dissertation, discusses our contributions to theory, methodology and practice. The chapter ends by outlining the limitations of the research and suggests directions for future research.

CHAPTER 2:
LITERATURE REVIEW

Introduction

This chapter provides the underlying rationale for our research by discussing the main themes namely organisational power and politics, technical security and infrastructure. We justify the themes in terms of current literature and the gaps that exist within it. The focus on the gaps gives us the justification from the literature for our study. This gap-driven review has the added benefit of focusing our debate.

The literature we consider is divided into technical and social approaches. Technical security covers a range of sub-disciplines such as computer and network security and specific techniques like cryptography, devices and tools. The literature avers that organisations can avoid or reduce security threats by using the 'right' tools and preventative measures. On the contrary, the social side addresses issues of power and politics and appreciates the role of people, policies, procedures and processes in information systems use. We combine both approaches because we believe it is vital to understand the effect of context on security products and approaches. Hence, our research transcends the artificial divisions that dominate PKI literature and security practice. The chapter is organised as follows. First, we discuss power and politics in IS adoption. Next, we survey the technical security literature with a focus on cryptography. To assess how a PKI becomes a catalyst for power and politics and bridge the artificial gap in the literature, we use the concept of infrastructure as a thread of logic to tie the study together. We conclude that an infrastructure is institutionalised when it effortlessly supports and is an integral part of work practices.

IT and quest for control

Transaction cost theorists claim organisations primarily exist as institutional, contractual arrangements to govern transactions among individuals faced with complex environments (Ciborra 1993). Thus, the key job of managers is to control (Ciborra and Hanseth 2000, Markus and Pfeffer 1983) and maintain these contractual arrangements (Ciborra 1993) in a milieu of cooperation and conflict. However, control is elusive because rapid technological innovation, changing markets, dynamic regulatory environments and new organisational forms (Bjørn-Andersen and Turner 1998, Truex *et al.* 1999) have conspired to create a sweeping wave of change. Stability is reportedly out, change is in (Orlikowski 1996) and gurus advise organisations to transform themselves rather than merely execute routines (Ciborra 1993). Putting it flamboyantly, Handy avers,

> "We are now entering an Age of Unreason, when the future, in so many areas, is there to be shaped, by us and for us – **a time when the only prediction that will hold true is that no predictions will hold true**; a time, therefore, for bold imaginings in private life as well as public, for thinking the unlikely and doing the unreasonable (Handy 1990)."

Handy links the discontinuity with a hurried wave of innovation in technology and economics notably information technology and biotechnology. Ironically, he also sees the same technologies as vital for shaping the "Age of Unreason." A subtext of Handy's work is that, "if management uses the new powerful tools 'properly' it will be in control (Ciborra 2000)." Indeed, Kling (1980) argues managers chiefly deploy information systems to direct resources and control the activities of subordinates. As such, it has been widely claimed that IS can radically increase the control managers (Earl and Feeny 1994) exercise over subordinates by providing them with "fine grained, timely and accurate information about the activities within their administrative domains (Kling 1980)."

The foregoing remarks support the *technological imperative* standpoint that sees IT as the prime and relatively autonomous driver of organisational change (Avgerou 2001, Orlikowski 1996). Information systems reputedly trigger sweeping changes in organisational structures, work routines, information flows (Ciborra 1993, Kling and Iacono 1984, Orlikowski 1996) and enhance performance (Ackoff 1967). However, technological determinism (Knights and Murray 1994) ignores the interaction of people with technology in social contexts and instead focuses on the capabilities of IT in representing, manipulating, retrieving and transmitting information (Orlikowski and Iacono 2001). This rational view of IS also assumes that actors have common goals (Ciborra 1993, Keen 1981). However, as Kling (1980) argues, only ardent determinists would claim that the effects of computer use depend exclusively on the technical features of the model adopted. For example, after Burns (1969), Knights and Murray (1994) argue that career and political objectives of individuals often contradict official organisational goals. As such, we embrace the political (Knights and Murray 1994, Markus 1983) or strategic rationality (Ciborra 1993) view, which,

> "Assumes that different individuals or subgroups … have different objectives depending upon their location in the hierarchy and that, in general, they can be expected to **achieve these local goals rather than global organisational goals whenever differences exist** (Markus 1983)."

To Knights and Murray (1994) this revelation underscores the need for understanding sub-unit competition and political dynamics because they illuminate the broader organisational struggles and conflicts characterised by individuals jockeying for position.

Power and Politics in Information Systems

In view of the foregoing remarks, IS are vital for the acquisition and exercise of power because they reconfigure the face of decision-making, organisational performance and legitimacy. To Kraemer and Dutton (1982) computing entails power shifts because it improves the decision-making effectiveness of some actors at the expense of others. The frequency and magnitude of power shifts depend on the extent and ways in which different actors use computers. Thus, IS are products of conflict, domination, sabotage or compromise because real organisations are federations of groups (Kling and Iacono 1984) with overlapping but often conflicting interests, objectives and values (Kling 1980).

According to Saunders *et al.,* the past two decades have seen regular, albeit peripheral, coverage of the impact of power on IT in the management and information systems literature. The studies see power as encompassing topics of politics, authority, influence, participation in decision-making, decision rights and centralisation or decentralisation (Saunders *et al.* 2000). However, since these views of power include many levels of analysis, it is up to the readers to discern the element under discussion. For instance, to French and Raven (1959), individuals accumulate power from rewards, punishments, legitimacy, expertise and reference. Pfeffer and Salancik (1978) focus on organisational or intraorganisational bases of power like resource provision. As such, Saunders *et al.* advise researchers to state their view of power and indicate the unit of analysis because this influences the theoretic outlook.

Markus and Pfeffer (1983) argue that power mainly derives from the ability to influence substantive outcomes through impacts on organisational action. However, it can also stem from shaping attitudes and beliefs about the legitimacy and rationality of decisions and actions without actually using the control system. They describe this as an organisation's paradigm. It includes values such as language and symbolic content. If an IS openly conflicts with the dominant organisational paradigm and culture, more resistance and instances of systems failure (Keil 1995) would be expected (Markus and Pfeffer 1983). This is because language and symbols are used politically to mobilise support and quieten opposition (Kling and Iacono 1984). Thus, regardless of the motive, controlling an information system is intensely political as well as technical (Keen 1981, Markus 1983). We agree that,

> "Rather than considering politics as an impediment ... we look at it as an important and potentially beneficial factor in successful organisational learning. (Indeed) understanding the political implications of a new technology **may be one of the most important lessons an organisation learns** during the process of institutionalisation (Romm *et al.* 1996)."

To Dutton and Danziger although research on technology and politics is extensive, a focus on factors that shape IT use and effects on the environment unifies the literature. The literature has three angles. First, the adoption and use of technology unfolds through an ongoing socio-political process in which the environment constrains the artefact (Avgerou 2001, Hanseth and Monteiro 1998, Kraemer and Dutton 1982). Second, technology affects its environment causing intended and unintended effects (Hanseth and Braa 1998). Third, because a technology is an interdependent system of people, equipment and technique, changes in one element affects other parts (Angell and Smithson 1991). We explore all three approaches.

Control of information

According to Keen (1981) information is a central political resource because of the close relationship between its ownership and autonomy (Clegg 1989). Similarly, Kraemer and Dutton (1982) view information as a political resource within organisations, just as expertise, status or position authority. Information systems affect information flows because they can modify the speed, direction, content, and its patterns of circulation. Therefore, an IS becomes contentious if it gives some actors access to more information (Keen 1981, Markus and Pfeffer 1983) than their rivals. However,

> "Access to information is probably less important as a basis of power than is the **ability to control access to information or to define what information will be kept and manipulated in what ways.** When a system centralises control over data, the individual or subunit who gains the control is likely to accept the

> system readily, while those units losing control are likely to resist, even if they receive access to larger amount of data in return (Markus 1983)."

Dutton and Danziger (1982) believe that the study of the politics of computing should cover the relative influence of various groups over decisions about the use of computer resources and the interests served by the system. While IS generally increase efficiency, the systems that affect power balances enable actors to,

> "**Manage** – control events by getting rapid and correct feedback about operations in progress; **Plan** – anticipate future uncontrollable events by getting analyses of current trends and predictions; **Persuade or coerce** – control decision situations by getting superior or sensitive information which is perceived as compelling (Kraemer and Dutton 1982)."

Keen (1981) argues that when an IS redistributes data this acts as a spur for redesigning the organisation, disrupting patterns of communication and reallocating authority. The impact depends on whether the system aims to simply improve operations or significantly change the social structure (Markus 1983, Markus and Pfeffer 1983). We are interested in the latter case where the new system acts as a vehicle for substantially modifying organisational practices and structures. However, using an IS to cause revolutionary change (Hanseth and Braa 1998, Markus and Pfeffer 1983) increases the risk for conflict, resistance and system failure (Markus 1983, Markus and Pfeffer 1983) because by directly affecting power relations (Keen 1981) the system creates many losers. Yet PKI causes big changes by underpinning new security practices often in conflict with existing power structures.

This study calls for the wider understanding of the role of contextual factors (Avgerou 2001, Orlikowski 1996) such as power distribution and organisational culture (Markus and Pfeffer 1983) in PKI institutionalisation. We see parallels between PKI and the acceptance of infrastructures intended as coupling devices to coordinate planning and improve management control. Infrastructures have been problematic (Hanseth and Braa 1998) because in a quest to make management win, system sponsors largely ignore the concerns of other agencies about the loss of power, interference and other forms of intervention. This sows seeds of resistance that may lead to either the overhaul (Markus 1983) or abandonment of expensively assembled information systems (Keil 1995, Markus and Keil 1994).

IS implementation motives

IS literature has two broad diverse views on the origins of technological solutions. The most prevalent view is systems rationalism (Kling 1980) that has functionalist roots (Knights and Murray 1994). Its proponents believe that rational considerations solely drive IS deployment. Segmented institutionalism counters that organisations may adopt systems for subjective reasons such as politics.

Systems rationalism

This perspective of IS adoption emphasises the positive role that technology plays in organisational and social life (Kling 1980). This view is rooted in the functionalist paradigm that provides rational explanation to social affairs (Burrell and Morgan 1979). Rationalists believe that features of the capitalist world, notably the profit motive and capital accumulation, shape innovation processes (Alchian and Demsetz 1972, McLoughlin and Harris 1997). Thus, organisations ostensibly adopt IS to increase efficiency (Earl and Feeny 1994), improve information flows (Ackoff 1967, Zuboff 1988), cut coordination costs (Malone *et al.* 1987) and generally boost competitiveness (Ives and Learmonth 1984, Porter and Millar 1985, Venkatraman 1991). These ideas are linked with Frederick W. Taylor's scientific management and the Henry Ford automation vision. Since, Fordist ideas remain prevalent in the assumptions of production engineers, managers, systems analysts and work-study experts (McLoughlin and Harris 1997),

> "The overarching assumptions underlying systems development has been that problems, such as they exist, **are technical, not social or organisational, in nature.** As a consequence, organisations are treated like machines: once the technology is functioning properly, the organisation is presumed to transmit its contents unproblematically (Knights and Murray 1994)."

Franz and Robey (1984) agree. They argue that research frequently depicts system development activities as rational events, undertaken to improve the effectiveness of an operation. As a result, many commentators (Gottschalk 1999, Hammer 1990, Hammer and Champy 1993, Porter and Millar 1985) claim that the only useful IS are those adopted after a 'rational' task-technology fit evaluation (Karahanna *et al.* 1999, Venkatraman 1991). There is also a belief in a marked consensus on the major social goals relating to the usage of computer systems (Kling 1980). *The* reason for IS adoption, so goes the story, is to enable an organisation maintain its competitive edge (Ives and Learmonth 1984, Venkatraman 1991) and deliver returns to its shareholders. Thus,

> "Technology is the instrument of change rather than its product. Because **value-consensus** underlies the functionalist paradigm, in normal circumstances conflict or resistance to the progress of technology does not occur. But where there is evidence of political conflict, it is presumed to be pathological or deviant and must be purged much like a virus in piece of computer software, lest it contaminates the whole system (Knights and Murray 1994)."

However, Taylorism is accused of an authoritarian bias (Hirschheim and Klein 1994).

Segmented institutionalism

McLoughlin and Harris (1997) see a common feature of Fordist and post-Fordist models of technology as the belief that change is essentially, an "adaptive activity dictated by broader economic and technological factors." However, insisting that value-consensus is a myth in social life (Knights and Murray 1994), segmented institutionalists see technology as having both 'legitimate' and 'illegitimate' consequences on social life (Kling 1980). They observe,

> "Participants in organisations **adopt computing to enhance their personal status or credibility** ... they identify as dominant values the sovereignty of individuals and groups over critical aspects of their lives, the integrity of individuals, and social equity; **economic or organisational efficiency is subservient to these values** (Kling 1980)."

In reality intergroup conflict is as likely as cooperation because stakeholders have overlapping but conflicting interests (Keen 1981, Kling 1980). Therefore, political struggles and conflict are common in organisational and social life (Knights and Murray 1994). Kling (1980) reveals that actors with a segmented institutionalist approach understand conflicting interests and develop plans to work around them. This could involve demanding different and potentially incompatible technological platforms or even none at all (Kling 1980). However, the outcome of this jostling for position is that big organisations rarely accept universal solutions because the *zero-sum nature of technical artefacts* ensures that the inclusion of given features leaves out preferences of other stakeholders.

Indeed, Kling and Iacono (1984) argue that information systems do not always enhance efficiency as widely claimed but ambitious players use this language as a façade to push the system in a direction that consolidates their power and control over organisational action.

Therefore, IS institutionalisation depends on how well this apparent subjectivity can be dressed up into an objective reality seemingly devoid of political calculation.

Problematic nature of technology

Dutton and Danziger (1982) argue that computer systems usually exist at the periphery of public attention because most observers do not appreciate their social costs and benefits. "And when people do think of computing, it is usually as either **a minor convenience or as an annoying inconvenience** (Dutton and Danziger 1982)." They reveal that a growing body of literature posits that computer systems have major consequences for the sociology and politics of organisations and broader society. In addition, contrary to common logic IT rarely contributes to the allocations of resources and control of diverse activities (Hinds and Kiesler 1999) because of its contradictory attributes. This is because,

> "People who study how technology affects organisational transformation increasingly recognise its dual, paradoxical natural. It is both an engine and barrier for change; both customisable and rigid; both inside and outside organisational practices. It is product and process. Some authors have analysed this seeming paradox as structuration ... **technological rigidity gives rise to adaptations, which in turn require calibration and standardisation** (Star and Ruhleder 1996)."

Kling (1980) argues that managing an IS gets more complicated if it critically depends on people's skills and cooperation because organisational actors normally have conflicting goals. He warns that when there are conflicts over the control of critical resources, information systems may simply be used as "political instruments by the contenders and fought as political intrusions." As such, different groups may see a new IS as a chance to enshrine a reporting structure that minimises their accountability but maximises its visibility and control over opponents (Kling 1980). Interests groups are vital in the institutionalisation of IS because their rules of meaning and membership shape the attitudes of members towards the new system (Karahanna *et al.* 1999). However, the wrangles may be useful. Markus (1983) believes disagreements may prevent the implementation of undesirable IS because some,

> "Are dumb ideas. Others threaten the interests of individuals and groups by intruding in on their territory, limiting their autonomy, reducing their influence or adding to their workload. **While we all may try to act in the 'corporate' interest, we often have very different definitions of exactly what that is** (Keen 1981)."

Since IS can affect power relations when utilised in unpoliticised arenas, Kling (1980) warns that their consequences are more profound when participants consciously set out to increase and exercise their power. Nevertheless, he claims that information systems reinforce the structure of power in organisations more frequently than not because computer-based systems are generally expensive to develop and use. He claims it explains why managers and accountants (Markus 1983, Markus and Pfeffer 1983) often gain power from IS deployments because they authorise the big expenditures and ensure that the systems serve their interests. In other words, information systems act as "political, power-reinforcing instruments (Kling 1980, Torvinen and Jalonen 2000)" that increase managerial control interests by fragmenting and deskilling jobs (Kling 1990). However, Dutton and Danziger (1982) claim Kling's view smacks of managerial rationalism. In this arrangement, authoritative top managers who use extensive, high quality information employ techniques such as cost-benefit analysis to control organisations. It is claimed managers make the major decisions because IS serve wider organisational interests. However, Dutton and Danziger insist information systems are highly malleable and can serve a variety of interests.

To Kraemer and Dutton (1982) while computers are a malleable technology, they are certainly not apolitical (Knights and Murray 1994) because they often serve the interests of actors who control the organisation. It was partly the fear that computers would extend the lives of outdated organisational and societal structures (Angell and Smithson 1991, Weizenbaum 1984) that inspired business process reengineering proponents to coin pithy statements such as 'don't automate, obliterate' (Hammer 1990, Hammer and Champy 1993, Venkatraman 1991). Thus, despite all the revolutionary credentials ascribed to computers (Zuboff 1988), they are not always tools of reform since systems largely automate or even exaggerate existing biases and inequalities of influence (Kraemer and Dutton 1982)." This is due to the complexity of IS that makes it hard for outsiders to oppose actors using the systems to support their own interests and values (Kraemer and Dutton 1982, Markus and Bjørn-Andersen 1987).

However, the power shifts caused by IS, "tend to be subtle, limited, and complex in their patterns (Kraemer and Dutton 1982)." Kling believes it is vital to understand the political context and the technical features of the IS to have a reasonable picture of their probable uses and impacts. Therefore, the political-technical nature of IS (Karahanna *et al.* 1999, Keen 1981, Markus 1983) undermines the sufficiency of formulations that emphasise technical features and downplay the organisational political dynamics in which the systems are utilised. After all,

> "**Computers by themselves 'do' nothing to anybody**. ... (Since) there is sufficient evidence, that computing use is purposive and varies between social settings; little causal power can be attributed to computers themselves. ...and speaking about the 'impacts of technology' often distracts attention from the social processes by which they are developed, adopted and used (Kling 1980)."

Even the phrase 'computer impacts' is deterministic (Knights and Murray 1994) for it attributes power to technology (Hanseth and Braa 1998) yet most social changes linked to IS result from managerial action after the implementation of a system (Kling 1990).

Technical Security

Technical security relies on an array of techniques and devices to constrain the range of activities permissible for organisational members. Therefore, just like rationalistic approaches such as scientific management (Taylor 1911) before them, security techniques such as cryptography attempt to buy certainty and reduce risks in an uncertain world (Garfinkel and Spafford 1997). Cryptography achieves certainty by shaping organisational action through limiting the autonomy of individuals. Thus, to become infrastructural, security technologies need to engender a security culture. Success in this quest relies on their acceptance as part of the routines, values, practices and policies of real organisations.

Old techniques, new risks

Austin (2001) argues that information assets such as customer and employee databases represent a significant share of the overall value of modern organisations. In an effort to increase market share and profitability, organisations have come under pressure to provide their digital assets over the internet (Austin 2001, Klang 2001). However, being a public channel, the security of the internet is inadequate for the needs of all its users (Bumgarner 2001, Diffie and Hellman 1976, Schwartau 1998). With more business transactions conducted online, digital security has become a prerequisite rather than a speciality for high-end users (Fernandes 2001). Yet internet security is a difficult subject because many organisations lack a holistic approach to security (Wood 1997, Wood 2000). However, a number of factors are forcing them to take heed (BBC 2002a, Russell and Gangemi Sr 1991). For instance, in their recent fight against terrorism, governments demand effective security safeguards for critical electronic infrastructure (Pounder 2002).

Changed Security Paradigm

With its global reach, the internet opens up numerous business opportunities. Indeed, at the height of the dotcom boom it was widely predicted that e-commerce would surpass offline business (Singh 1999) in a couple of years (Datamonitor 2000, Forrester 2000, Jupiter 2000a, Jupiter 2000e). However, the predictions underrated the refractory nature of the risks (Bhimani 1996) associated with e-business referred to as "trust." Although the physical world grapples with similar issues, the anonymity of cyberspace exacerbates the risks (Ba 2001, Schneier 2000). To Klang (2001) security issues are inherent in the nature of this medium because the whole concept of the internet relies upon the impossibility of control (Jøsang *et al.* 2001). "This design has the effect of making any attempts of regulation seem a task comparable to Sisyphus[4] (Klang 2001 329)."

Worse still, the new security paradigm has rewritten assumptions and eroded confidence in tried and trusted controls. For instance, computer security has traditionally enforced a fortress mentality (Lindup 1996, Shain 1991). Despite the perilous effects of the mentality in military and corporate history (Schwartau 1998), the practice lives on. To Nash *et al.* (2001) demilitarised zones (DMZs) distinguish resources available to external users (bastion hosts); firewalls limit damage by separating the internal network from public ones and authentication products restrict access. In addition, intrusion detection systems (battlements) and security-hardened operating systems help defend the inner corporate stronghold (Day *et al.* 1999). Inside the fortress is trusted and information resources are availed but anything outside the perimeter is assumed non-trusted until proven otherwise (RSA 1999). However, the,

> "Security challenges are now significantly different. Networking has moved from its medieval roots to a renaissance period. The massive adoption of the Internet as a basis for electronic commerce has moved the whole security model from one of a small community huddling within a medieval keep to a walled city with an open marketplace. ... **Yesterday, security was primarily about how to limit access. Today, it is about how to maximise access – to the right people** (Nash *et al.* 2001)."

Thus, the fortress mentality impedes the very idea of an open global e-marketplace. Yet,

> "We now face a new security paradigm very different from the old paradigm of communications security. Distrusting parties need a trusted environment to conduct a business transaction. ... **The adversary is no longer an intruder but a fraudulent insider, and the third party guarantees rather than compromises security** (Gollmann 2000a)."

E-commerce has also changed attitudes and meaning of key concepts like confidentiality, integrity and availability. Gollmann (2000a) argues that while intruders will find it harder to tamper with orders, the focus of integrity now shifts to ensuring that customers or merchants do not make fraudulent changes (Ba 2001). Parties are less interested in establishing the identity of counterpart than in the validity of the transaction.

[4] A cruel king of Corinth sentenced by Pluto to forever roll a huge stone up a hill in Hades only to have it roll down again on nearing the top.

To conclude, secure e-commerce requires robust measures against fraud (Gollmann 2000a, Schneier 2000, Sherif 2000). To Tan and Thoen (2000) an agent's trust depends on both their confidence in the counterpart and an expectation of effective anti-fraud controls. The distinction is vital in international B2B e-commerce, where partners may not have established trading relationships. With a strong control mechanism, trust arises not because a party has any specific reason to believe the other's trustworthiness but because the system stops deceit (Blaze *et al.* 1996, Tan and Thoen 2000). Cryptography engenders this confidence (Wood 1996) in online interactions.

Cryptography and Web Security

Web security is a complex topic that covers diverse topics such as computer and network security, firewall configuration, authentication services and privacy (Jøsang *et al.* 2001). Cryptography is vital for web security because it offers a control mechanism that enables parties to transact even though they do not trust each other (Adams and Lloyd 1999, Ba 2001). The benefit is mutual because the internet actually resuscitated cryptography. Whereas governments widely used the technology,

> **"The phenomenal growth of the Internet — along with its perceived insecurity — has transformed a relatively obscure and esoteric science into a key link to the promises of the New Economy**: as the current wisdom goes, e-commerce will not flourish until the public gains sufficient confidence that electronic transactions are secure. 'Security', in this context, is generally equated with the ability to exchange information confidentially.., using cryptology-based technologies (Blanchette 2000)."

While most commentators consider cryptography a military technology, civilians (Diffie and Hellman 1976, Gardner 1977, Rivest *et al.* 1978) invented (rather re-invented) nearly all the strongest cryptosystems. For instance, cryptography was a hobby for Victorian 'gentlemen.' Charles Babbage admits, 'Deciphering, is in my opinion, one of the most fascinating arts …and I fear I have wasted upon it more time than it deserves (Standage 1999).' Cryptography has a military association because nearly all its examples are stories of armies and spies using cryptosystems to shield messages (Cohen 1995, Kahn 1996).

Approaches to cryptography

Chen *et al.* (1999) describe encryption as "the transformation of data into a form that is practically close to being impossible to read without certain appropriate knowledge." Encryption maintains privacy because even if a third party intercepts the data the message remains gibberish. The transformation of normal text (*plaintext*) into gibberish (*ciphertext*) can be performed by either symmetric (*secret key*) or asymmetric (*public key*) ciphers (Adams and Lloyd 1999, Chen *et al.* 1999, Schneier 1996a).

Symmetric cryptography

To Singh (1999) under symmetric ciphers, the unscrambling process is simply the opposite of scrambling (Garfinkel and Spafford 1997). Symmetric ciphers rely on the principle that only the sender and recipient have a common key before the transmission of the message (Adams and Lloyd 1999, Nash *et al.* 2001). Symmetric key algorithms are either block or stream (Garfinkel and Spafford 1997, Schneier 1996a, Singh 1999). *Block algorithms* such as DES, Blowfish, RC2[5] and RC5 encrypt data a block at a time. In contrast, *stream algorithms,* like RC4, encrypt data byte by byte. However, symmetric ciphers are problematic in e-commerce because they require a secure out-band channel to exchange the key before communication occurs. This causes key management issues (Blaze *et al.* 1996, Price 1999). As a result,

> "Cryptography has been a derivative security measure. Once a secure channel exists along which keys can be transmitted, the security can be extended to other channels ... **The effect has been to limit the use of cryptography to communications among people who have made prior preparation for cryptographic security.** In order to develop large, secure, telecommunications systems, this must be changed. A large number of users *n* results in an even larger number, $(n^2-n)/2$ potential pairs who may wish to communicate privately from all others. It is unrealistic ... (Diffie and Hellman 1976)."

Despite key exchange problems, symmetric ciphers are fixtures in modern cryptographic systems. This is because they are quicker, offer a large number of possible keys and are easier to implement than public key algorithms. Indeed, "The best symmetric key algorithms offer near-perfect secrecy: once data is encrypted with a given key, there is no way to decrypt the data without possessing the same key (Garfinkel and Spafford 1997)."

Asymmetric cryptography

Unlike symmetric ciphers that rely on a shared secret, public key cryptography (PKC) uses separate keys for encryption (public key) and decryption (private key) (Singh 1999, van Krugten and Hoogenboom 2000). PKC features suit e-commerce because its objective is to enable real time transactions even between strangers. Indeed, PKC arose out of a fear by Whitfield Diffie that the key distribution problem under symmetric ciphers, that had troubled governments and large corporations for ages, would simply prevent the public from taking advantage of cryptography. Singh elegantly summarises the quandary.

> "The whole problem of key distribution is a classic catch-22 situation. If two people want to exchange a secret message over the phone, the sender must encrypt it. To encrypt the secret message the sender must use a key, which is itself a secret, so **there is the problem of transmitting the secret key to the receiver in order to transmit the secret message** (Singh 1999)."

[5] RC stands for Ron's code. Ronald Rivest developed RC2, RC4, a stream cipher and RC5, a block cipher at RSA Security and kept them trade secrets. They were exposed through anonymous postings in Usenet groups in 1994 (RC4 and RC5) and in 1996 (RC2).

Diffie and Martin Hellman (1976) introduced the twin concepts of public cryptosystem and public key distribution systems in their seminal paper "*New Directions in Cryptography.*" Declaring that the world was on the threshold of a cryptography revolution, they underlined the "need for new types of cryptographic systems, which minimise the need for secure key distribution channels and supply the equivalent of a written signature." This heralded an approach where parties communicating solely over a public channel with known techniques were able to create secure communication channels. This was a momentous discovery as the following paragraph reveals.

> "Is it possible to devise a cipher that can be rapidly encoded and decoded by computer, can be used repeatedly without changing the key and is unbreakable by sophisticated cryptanalysis? The surprising answer is yes. **The breakthrough is scarcely two years old, yet it bids fair to revolutionise the entire field of secret communication**. Indeed, it is so revolutionary that all previous ciphers, together with the techniques for cracking them, may soon fade into oblivion (Gardner 1977)."

However, recent research has suggested that Diffie and Hellman were not, after all, the first people to invent PKC concepts. The accolades should have gone to a trio of security agents at the Government Communications Headquarters (GCHQ) in Cheltenham, a top-secret British establishment (Schneier 2000, Singh 1999). James Ellis, Clifford Cocks and Malcolm J. Williamson discovered the same concepts as RSA and Diffie-Hellman but the innovations remained secret. By 1969, Ellis was at the same stage as what the Stanford trio of Diffie, Hellmann and Ralph Merkle were to reach in 1975. He later invited Cocks to put his principles of "non-secret encryption" principles into practice. The outcome was a system similar to RSA asymmetric cipher. Williamson pushed this work forward by discovering the Diffie-Hellman-Merkle key exchange scheme at about the same time as the Stanford trio. By 1975, the agents had discovered all the fundamental aspects of PKC (Singh 1999).

However, since 1976 few PKC algorithms have proved both secure and practical. Many algorithms are impractical because either the key is too large or the ciphertext is much larger than the plaintext. For instance, RSA, the best PKC cipher, is about 1000 and 100 times slower than DES in hardware and software respectively (Schneier 1996a). Thus, nobody directly uses PKC to encrypt messages. Most systems using PGP, PEM and S/MIME employ hybrid cryptosystems where a random key from a symmetric algorithm encrypts the message and after that, the random key is itself encrypted with the recipient's public key (Schneier 1996a, Schneier 2000, Singh 1999).

The crypto arms race

RSA derives its strength from the difficulty of factoring large numbers (Schneier 1996a). Theoretically, this takes millions of years to accomplish (Gardner 1977) because it involves the factorisation of a very large number. Singh (1999) believes that since cryptographers are always fearful of somebody breaking their code, they normally choose prime numbers as big as 10^{130} a figure that would take a hundred million PCs to crack. Singh believes that with suitably large prime numbers, *p* and *q,* RSA is unbreakable for it is virtually impossible to deduce these figures from their product *N.* Announcing the invention of RSA Gardner mockingly writes,

> "All over the world, there are clever men and women, some of them geniuses, who have devoted their lives to the mastery of modern cryptanalysis. Since World War II, even those government and military ciphers that are not one-time pads have become so difficult to break that the talents of these experts have gradually become less useful. **Now these people are standing on trapdoors that are about to spring open and drop them completely from sight** (Gardner 1977)."

However, the battle for supremacy between codemakers and codebreakers is far from over (Kahn 1996). For instance, Singh warns that quantum computing could render RSA and other modern PKC ciphers useless because it simplifies number factoring (Landau 2000, Schneier 1996). In turn, codemakers are looking to quantum cryptography to stay ahead. Singh claims quantum cryptography "is not just effectively unbreakable, it is absolutely unbreakable. Quantum theory ... means that it is impossible for Eve to intercept accurately the one-time pad key established between Alice and Bob."

Public Key Infrastructure (PKI)

In this study, we define a PKI as a *pervasive security substrate* (Adams and Lloyd 1999) that facilitates the implementation of PKC applications. To Hunt (2001) a PKI provides the core framework for a wide variety of components, applications, policies and practices to support organisational security goals (Baltimore 2000). Likewise, Fernandes (2000) sees a PKI as the computer programs and protocols needed to exchange public keys to help associate a person's electronic and physical identities (Baum 1999, NIST 1997).

However, Austin (2000) regards the PKI acronym as a *misnomer* since its reference to PKC conceals the fact that both asymmetric and symmetric cryptography work together in the infrastructure to provide overall security (Schneier 2000, Singh 1999, Zimmermann 1998). PKI is the most promising technology for facilitating digital security because it provides a trusted environment for real time transactions between strangers (Baum 1999, Gollmann 2000a). Nash *et al.* (2001) argue that PKI has caused considerable excitement (Wheatman and Pescatore 2001) because of its immense ability to create and manage a vastly scalable set of digital identities. Indeed,

> "The main impact of cryptology might not lie so much in its ability to provide confidentiality to the masses, but rather in the way it has come to define authenticity of electronic transactions (identification of parties + non-repudiation) and its technological realisation in the electronic world (PKIs) (Blanchette 2000)."

Commentators link PKI with the emergence of internet technologies and e-commerce (Radicati 1998) because these innovations exposed glaring gaps in digital security mechanisms (Adams 2000, Schneier 2000). Organisations originally adopted PKI with applications focused on cost cutting and streamlining business processes and practices (Levitt 1999). The re-engineering hoped to transform social relations, increase employee commitment and thus efficiency (McCabe *et al.* 1998). However, the association with efforts to reconfigure power relations inevitably exposed PKI to the tensions touched off by the exercises. This is the main theme of subsequent chapters. PKI later graduated from a specialised security component of the restructuring exercise into a core IS component (Radicati 1998). In the literature, conventional PKI actually refers to the X.509v3-based architecture or PKIX (Clarke 2001).

PKIX Standards

PKIX standards define the use of X.509 certificates and the accompanying protocols for creating, publishing and fetching certificates as well as the schemes for the generation and distribution of key material (Sun 1998). PKIX was initially a single Internet Draft but has since been broken into six parts that are themselves split into smaller components (Hughes 1998b). We briefly highlight these areas.

Part 1 – Certificate and CRL profile

The section describes the basic certificate fields and the extensions supported for X.509v3 Public Key Certificates and X.509v2 Certificate Revocation Lists (Hughes 1998b, Xenitellis 2000). The part profiles the format and semantics of certificates and CRLs using Abstract Syntax Notation 1 (ASN.1). It also includes the encoding rules for popular cryptographic algorithms such as RSA, Diffie-Hellman and Digital Signature Algorithm (Hughes 1998b).

Part 2 – Operational Controls

This part discusses ways of accessing certificate and CRL repositories using Lightweight Directory Access Protocol (LDAP) version 2 (Austin 2001, Hughes 1998b, Xenitellis 2000). It permits End Entities (EE) such as machines, users and CAs to retrieve certificates and CRLs. It further authorises CAs to populate certificates and CRLs. The document also defines how EEs and CAs using FTP and HTTP can obtain certificates and CRLs from repositories. The part also covers Online Certificate Status Protocol (OCSP) that enables EEs to ascertain the validity of certificates without needing to read lengthy CRLs (Hughes 1998b).

Part 3 – Certificate Management Protocols

This document defines the management side of the PKI model by identifying the entities involved such as CAs, EEs, Repository and optionally Registration Authorities (RAs). The document introduces notions of Personal Security Environment (PSE) like smart cards and Proof of Possession (POP) of the private key. POP mandates EEs to show the RA/CA that they hold the private key corresponding to the public key for which the certificate is required (Austin 2001, Hughes 1998b). It also defines a simple protocol for transporting PKI messages between entities (Xenitellis 2000) as illustrated next.

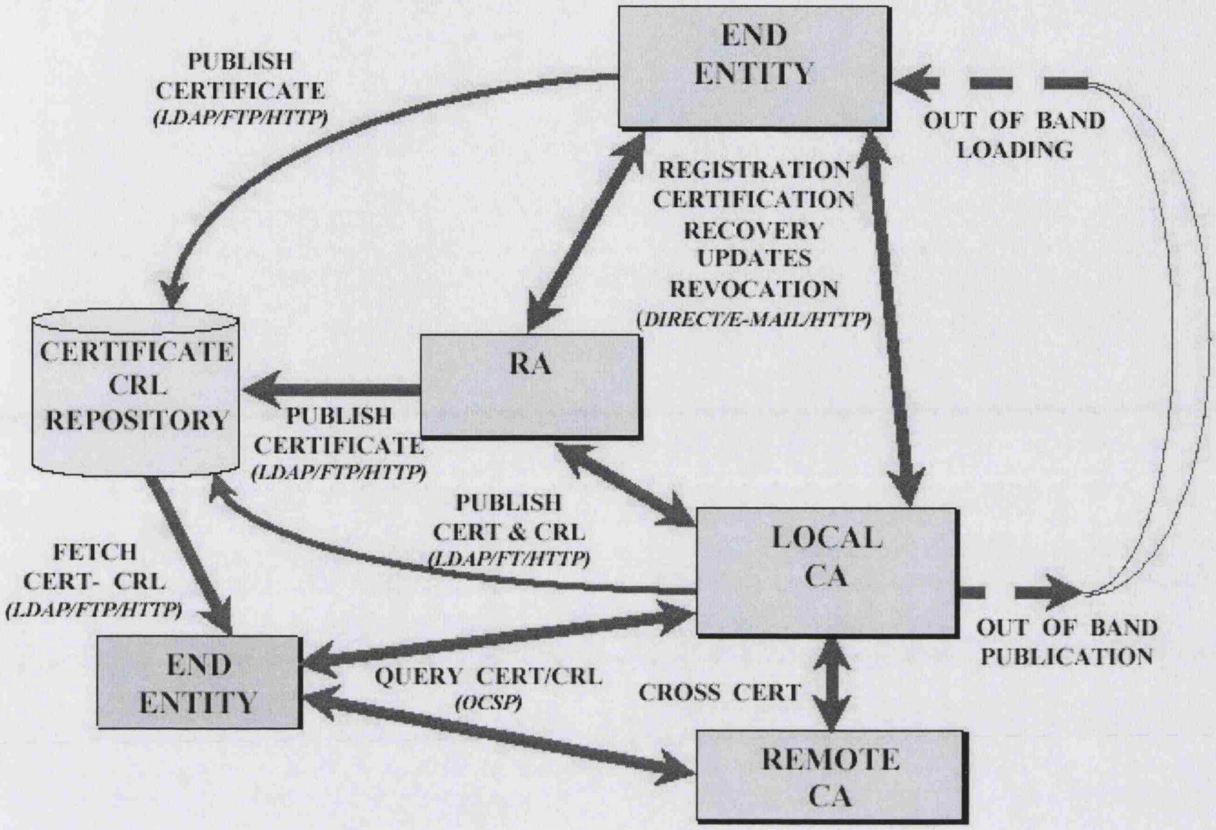


Figure 2 – General PKIX model (Hughes 1998b)

Part 4 – Certificate Policy and CPS Framework

A CPS is a statement of practices that a CA employs in issuing certificates to subscribers (AICPA and CICA 2000, Hughes 1998b, Hunt 2001). Subscribers and relying parties depend on CPSs to ascertain the trustworthiness of the PKI for transactions and interconnection with their own infrastructures (AICPA and CICA 2000, Backhouse 2002). The CPS also covers the certificate and CRL profiles used. The document further establishes the relationship between certificate policies and CPSs.

Part 5 – Time Stamp Protocols

To Austin (2001) time stamps provide control and evidentiary standing for transaction audit. This document describes a protocol between requesting entities and a Time Stamp Authority (TSA). The time stamping services define a trusted third party that creates time stamp tokens in order to indicate that a datum existed at a particular point in time (Xenitellis 2000). In e-business, time stamps secure data transactions and perform a vital piece of assurance of data integrity (Nash *et al.* 2001). Therefore, the time stamp's data structure must itself be cryptographically sound (Adams and Lloyd 1999).

Part 6 – Notary Protocols

The part defines a notary service between requesting entities and a special type of Trusted Third Party called a Notary Authority (Hughes 1998a, Hughes 1998b). The Authority verifies the submitted data for its correctness with a view of building non-repudiation information and creates a Notary Token (Hughes 1998b). Nevertheless, the meaning of "correctness" depends on the type of data certified (Adams and Lloyd 1999).

The primary reason for defining PKIX profiles is to maximise interoperability between different components of a PKI (Baum and Ford 1998, CygnaCom 1995, Fratto 2000, Williams and Zunic 2000). However, since PKIX offers many options, end-users and system integrators face the problem of defining a framework that sets a stage for various PKI entities to communicate with each other (Hughes 1998b, Hunt 2001).

Digital Certificate

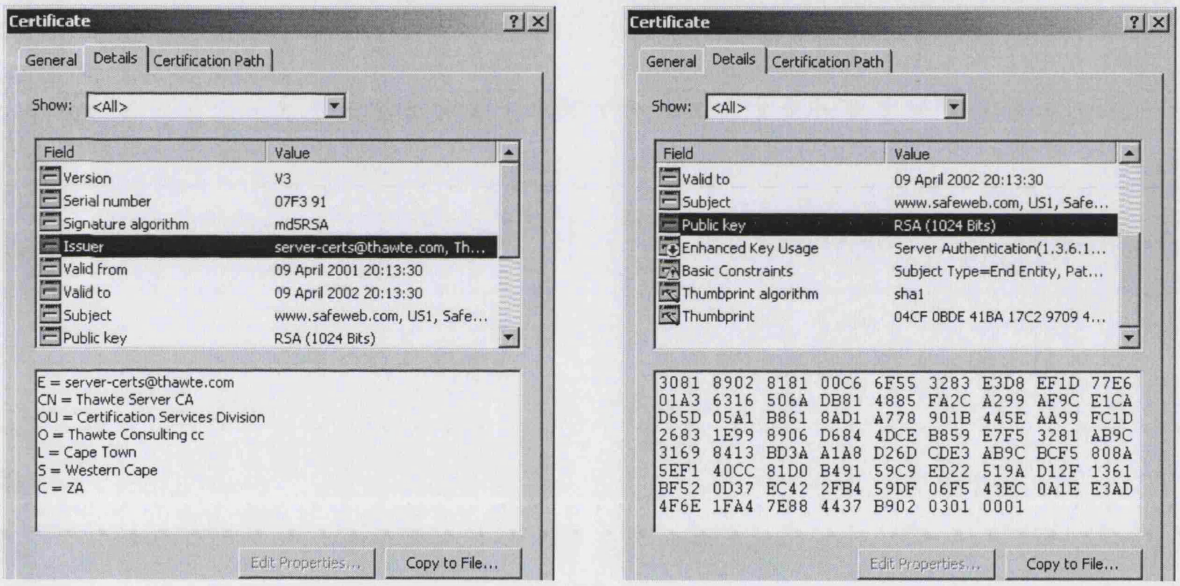
Chokhani and Ford (1999) regard a certificate[6] as a means of binding a public key value to a set of information that identifies an entity such as a person or account associated with a corresponding private key. This entity is the *subject.* The certificate provides assurance that the public key belongs to the subscriber (Austin 2001) by binding it to their digital signature (Hunt 2001). To Austin (2001) it is vital that a CA signs the certificate because although if Bob signed his own certificate it would provide data integrity, Alice has no assurance that the public key belongs to him (Baum 1994, Puhakainen 2000). Self-signed certificates also do not confirm that Bob actually holds the private key to published public key.

X.509 Recommendation

X.509, the oldest standard certificate form, underpins most digital certificates (Ellison 1997). According to Hunt (2001), X.509 provides a useful basis for defining data formats and procedures for the distribution of public keys via certificates digitally signed by CAs. It is an

[6] also called public key certificate

authentication framework designed to support the X.500 directory access standard proposed by ISO and ITU (Ellison 1997, Forné and Castro 1999). While the goal of X.500 was to create a global directory of named persons and things, X.509 provides a PKI framework for authenticating X.500 services by defining the structure of certificates and any optional extensions. X.509 is at version 3 (X.509v3). It supports PKI interoperation and defines extensions used to customise the infrastructure to specific business needs (NIST 1997). However, the flexibility of the extensions allow too often turns into a hotbed of interoperability problems (Baum and Ford 1998, Hunt 2001). The following figure shows the common fields of an X.509v3 certificate presented in Internet Explorer version 6.



Field	Value
Version	V3
Serial number	07F3 91
Signature algorithm	md5RSA
Issuer	server-certs@thawte.com, Th...
Valid from	09 April 2001 20:13:30
Valid to	09 April 2002 20:13:30
Subject	www.safeweb.com, US1, Safe...
Public key	RSA (1024 Bits)

E = server-certs@thawte.com
CN = Thawte Server CA
OU = Certification Services Division
O = Thawte Consulting cc
L = Cape Town
S = Western Cape
C = ZA

Field	Value
Valid to	09 April 2002 20:13:30
Subject	www.safeweb.com, US1, Safe...
Public key	RSA (1024 Bits)
Enhanced Key Usage	Server Authentication(1.3.6.1...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint algorithm	sha1
Thumbprint	04CF 0BDE 41BA 17C2 9709 4...

```
3081 8902 8181 00C6 6F55 3283 E3D8 EF1D 77E6
01A3 6316 506A DB81 4885 FA2C A299 AF9C E1CA
D65D 05A1 B861 8AD1 A778 901B 445E AA99 FC1D
2683 1E99 8906 D684 4DCE B859 E7F5 3281 AB9C
3169 8413 BD3A A1A8 D26D CDE3 AB9C BCF5 808A
5EF1 40CC 81D0 B491 59C9 ED22 519A D12F 1361
BF52 0D37 EC42 2FB4 59DF 06F5 43EC 0A1E E3AD
4F6E 1FA4 7E88 4437 B902 0301 0001
```

Figure 3 – Fields of an X.509 certificate for Safeweb.com

We explore the X.509 certificate further with a simplified version on the next page.

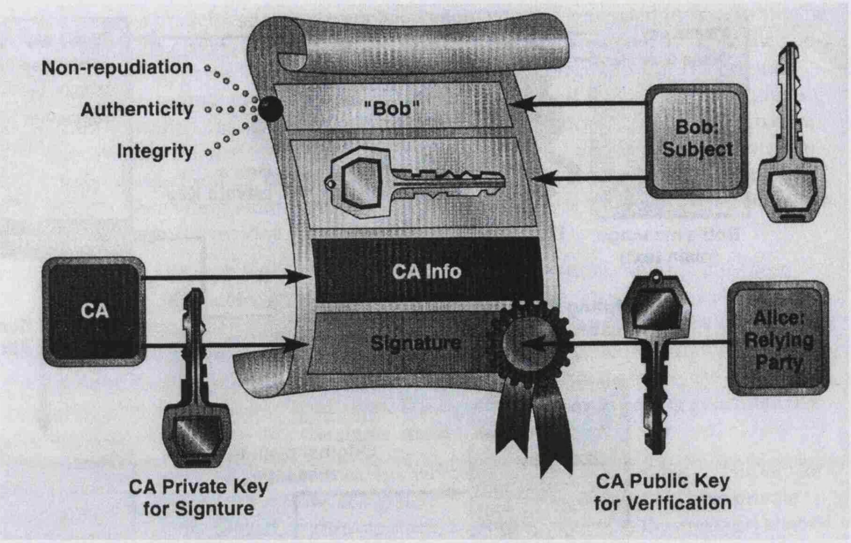


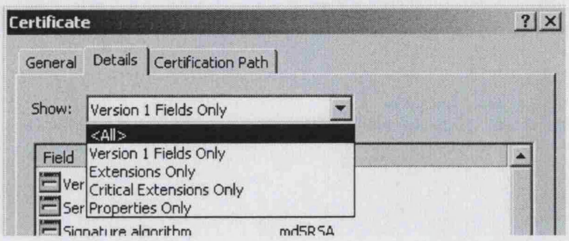
Figure 4 – An illustration of a digital certificate (Austin 2001)

The *Subject* area shows Bob's identity and public key. The CA adds information such as the issuance date, the validity period, its own identity, among other necessary details. The CA hashes the three elements and uses its private key to generate a digital signature, the fourth element of the certificate (Chokhani and Ford 1999). This certificate digital signature supports data integrity, authenticates the CA, and offers non-repudiation to *relying parties* (Austin 2001, Chokhani and Ford 1999).

X.509 Certificate Versions

The X.509 standard not only defines the information that is included on the certificate it also prescribes the order of its presentation (Chadwick 2002, Chokhani and Ford 1999, Gutmann 1999a, Myers *et al.* 1999, Puhakainen 2000). The uniformity is both regarded as vital for setting the stage for interoperation (Baum and Ford 1998) and a key reason why X.509 based infrastructures are regarded as hierarchical and authoritarian (Clarke 2001).

X.509 has gone through numerous revisions to accommodate the changing needs of the security community with Version 1 published in 1988 the most generic. Version 2 introduced *Subject* and *Issuer* identifiers to handle the possibility of reusing subject and/or issuer names (Sun 1998). However, because certificate profile documents strongly warn against the reuse of names and unique identifiers, X.509v2 certificates are not widely deployed. Hence, the most widely used PKIX certificate is X.509v3 issued in 1996. This version supports the notion of *Extensions*, which allows organisations to define additional certificate identifiers as illustrated below (Hunt 2001).



Show: Version 1 Fields Only

Signature algorithm md5RSA

Figure 5 - An illustration of a certificate listing most of the fields in X.509 Version 3

The most common extension is *KeyUsage,* which can limit key use to specific purposes say signing (AICPA and CICA 2000). Another popular extension is *AlternativeNames* that allows other identities such as DNS (Domain Name System) names, Email addresses and IP addresses to be associated with a public key. In some cases, an extension can be marked *critical* to inform *relying parties* that it needs proper checking, enforcement or use. However, the extensions are problematic because while,

> "X.509v3 certificates .... offer a variety of extensions which can take on a wide range of options. This provides considerable flexibility, which allows the X.509v3 certificate format to be used in many applications. Unfortunately, this same flexibility makes **it extremely difficult to produce independent implementations that will actually inter-operate** (Hunt 2001)."

Indeed, different vendor interpretations or 'improvements' to the X.509v3 format have caused untold interoperability problems (Baum and Ford 1998, CygnaCom 1995, Fratto 2000, Williams and Zunic 2000). We are not discussing interoperation problems in detail because they are outside the scope of this dissertation. However, we should state that since technical artefacts have a zero-sum character where the inclusion of certain features excludes preferences of others, X.509 extensions often fuel organisational power struggles.

A summary of PKI debates

Most commentators (Adams and Lloyd 1999, Austin 2001, Barber 2000, Baum and Ford 1998, Nash *et al.* 2001, Ortiz 2000, Rivest *et al.* 1978, Schneier 1996a, Singh 1999, Zimits and Montano 1998, Zimmermann 1998), believe that strong cryptography as personified in PKIs is critical for the privacy and security of online transactions. However, recent literature has robustly questioned the apparent coronation of PKI as the backbone of e-security. The sentiments are summarised in a maverick question: Do we even need a PKI for e-commerce? While the trade press claims,

> "PKI is desperately needed for e-commerce to flourish. This statement is patently false. E-commerce is already flourishing, and there is no such PKI. Web sites are happy to take your order, whether or not you have a certificate. Still, as with many other false statements, there is a related true statement: commercial PKI desperately needs ecommerce in order to flourish. In other words, PKI startups need the claim of being essential to e-commerce in order to get investors (Ellison and Schneier 2000)."

A major point advanced by critics of the "PKI for everything" bandwagon (Barber 2000) is that, "prior to the internet; public-key cryptography was a **solution in search of a problem** (Blanchette 2000)." Because,

> "When the oldest standard certificate form, X.509, was created in the 1980's it was part of a larger project X.500, which was to be a distributed global directory of named persons (and other things). The notion that such a directory will come about has persisted and is even present in some plans today. ... What was forgotten in those plans was that most companies and agencies consider their employee lists to be proprietary...(Thus), **the X.500 dream has effectively died but the X.509 certificate has lived on** (Ellison 1997)."

Similarly, Clarke (2001) describes X.509 as the "the hammer that came to hand when the nail was discovered." The critics have argued that PKI has remained alive despite its failure to become a pervasive security infrastructure because of a powerful alliance of forces determined not to see it fail. Blanchette (2000) argues,

> "Public calls to foster 'public trust' in e-commerce highlight how the development of secure transactions is, by and large, a symbolic process. **Whether solutions are actually secure is not so relevant, in as much as secure solutions have to exist**. In a way, the incredible success of cryptological technologies can be explained not so much by some innate superiority, but by a collective process of willing them into existence (Blanchette 2000)."

Klang (2001) agrees. He argues that most e-commerce security efforts still focus on the development of technological mechanisms for secure payment and identification. He contends that although stronger encryption does make information safer, on its own it cannot create a secure business environment because administrative routines address identity concerns better (Ba 2001). Indeed, as Garfinkel and Spafford were to argue,

> "If key length were the only factor determining the security of a cipher, everyone interested in exchanging secret messages would simply use codes with 128-bit keys, and all cryptanalysts would have to find new jobs. Cryptography would be a solved branch of mathematics, like simple addition. What keeps cryptography interesting is the fact that **most encryption algorithms do not live up to our expectations**. Key search attacks are seldom required to divulge the contents of an encrypted message. ... messages can be deciphered without knowing the key (Garfinkel and Spafford 1997)."

Another deeply contested issue in the PKI literature concerns Certification Authorities (CAs). The concept arose out of efforts to modify a telephone book to create publicly accessible certificate directories (Blanchette 2000, Diffie and Hellman 1976). Clarke argues that PKIX has been, and will remain a failure because of *"its inherently hierarchical and authoritarian nature, its unreasonable assumptions about the security of private keys, a range of other technical and implementation defects* (Clarke 2001)." The need for CAs within the PKIX model causes most of these problems. As we see elsewhere, the hierarchical PKIX model causes acute political problems in distributed organisations.

To Blanchette the PKI model and the technology itself are still evolving. For instance, he wonders whether certificates should bind public keys to identities or roles. Also "despite the fact that PKI technology has yet to evolve beyond the poster application, to be tested within any kind of large-scale, intensive setting," companies are already fighting for the market. While Entrust and VeriSign have dominated commercial PKI, Radicati (1998) foresaw the arrival of Microsoft, IBM and Netscape (Austin 2001, Lowe-Norris 2000, Microsoft 2002, Microsoft 2002b).

As a conclusion to this review of power, politics and technical security debates and a prelude to the next section, we would like to point out that the institutionalisation of cryptographic systems takes more effort that many people anticipate because of the "Not Invented Here" tag. Cryptology has not only moved from the military to the public sphere (Chen *et al.* 1999, Cohen 1995, Singh 1999), but also from the exclusive concerns with confidentiality (Coppersmith 2000, Ritter 1999, Schneier 1996). Blanchette argues the shift is significant enough to warrant the redefinition of cryptology from a 'science of information secrecy' to a 'science of information integrity'. However, it is difficult to shed the "invader" tag because the use of cryptography in global public organisations is worlds away from the intended user groups in the scientific, military and diplomatic communities. The transition is hard because,

> "Design can be seen as having three interrelated dimensions, each of which is a necessary but insufficient precondition for making sense of innovation as a dynamic process. The first dimension, and the most obvious, is that of *creating the artefact*. ... The second dimension is ... ***constructing the user***. .. images of eventual users are incorporated into the fabric of the object, but at the same time users are designed themselves – as ideal or as necessary to complete both the function and vision embodied in the artefact. The third dimension of design involves *catching the customer* (Silverstone and Haddon 1996)."

Therefore, appropriating an artefact implies taking it into private cultural spaces and making it familiar (Silverstone and Haddon 1996). As we discuss elsewhere, the appropriation of PKC systems largely depends on user discipline. However, since users face significant barriers in "hooking up" (Star and Ruhleder 1994) and the system lacks a mechanism for ensuring its incorporation into actual living and breathing organisational contexts, the results have been disappointing. Indeed, Hunt (2001) concludes that although PKI solves many security problems, there are still several concerns and risks associated with its use coupled with organisational, and management issues for which solutions are still evolving (Clark 2000, Schultz 2002). However,

> "It may well turn out that PKI technology meshes wonderfully well with user expectations, business practices and day-to-day usage, and ushers us into being a new golden age of consumerism. Unfortunately, the future may not be so rosy… **the relationship between the cryptographic key and the individual cannot be established mathematically (it is procedural)**, is highly complex and worse, easily compromises the mathematical security of the whole (Blanchette 2000)."

Ross Anderson has catalogued crypto failures (Anderson 1994). He believes that while the security discipline has largely sorted out technical issues, "system aspects, where most things actually fail, aren't being worked on anywhere near as much (Heiser 2002)."

Infrastructure: Bridging the social-technical gap

This dissertation uses the concept of infrastructure to tie together the supposedly disparate fields of cryptography, power and politics. We say supposedly, because cryptography is but a blatant attempt at maintaining power and political structures by reducing uncertainty in organisational interactions. Thus, the separation of the two fields is artificial because useful PKIs rely on the support of power and political structures to provide a context (Star and Ruhleder 1994, Star and Ruhleder 1996) for the performance of security practices (Anderson 2001, Camp 1999, Jøsang *et al.* 2001).

Rationale for infrastructures

To Ciborra (2000) the role of infrastructures was originally to standardise systems and reconcile centralised IS departments and distributed information resources (Angell and Smithson 1991, Williams 1997). This stems, in turn, from the Fordist rationalisation drive, which demanded uniform solutions (McLoughlin and Harris 1997, Rolland and Monteiro

2002). As such, organisations sought IT systems that offered tools for automating work activities based on 'universal' mathematical principles with applicability across the widest array of firms and occupations (Williams 1997).

Sawyer (2000) argues that the vitality of infrastructures to organisational success is steadily increasing (Byrd and Turner 2000) for two reasons. First, infrastructures are embedded in work (Star and Bowker 1995). Each infrastructure "is unique since common technical components are woven into an organisation's administrative and social fabric (Sawyer 2000)." Indeed, Star and Bowker (1995) argue that the adoption of any system simultaneously relies on its intellectual value and organisational fit. However, the organisational side is decisive. Second, infrastructures are vital in the formulation and execution of strategy (Ives and Learmonth 1984, Porter and Millar 1985, Venkatraman 1991) and maintaining organisational flexibility (Clegg and Wilson 1991, Hanseth *et al.* 1996, Nelson and Ghods 1998).

Associating infrastructures with management models transformed them from "a thrown-together institutional backbone to a value generating, integrated set of technologies, applications and process (Ciborra and Hanseth 2000)." The ability to maintain control and coherence to the different contexts (Rolland and Monteiro 2002) is the key selling point for infrastructures. Indeed, Ciborra and Hanseth (2000) assert that most technologies and organisational forms aim to advance control over processes in society and nature (Smithson 1994). Yates (1989) claims that this is paramount because managerial control enables organisations to coordinate their operations and achieve desired goals. She contends that communication systems exist to coordinate large, multinational firms efficiently.

However, companies rarely follow their blueprints (Meyer and Rowan 1991). Indeed, Sawyer (2000) warns that the contribution of an infrastructure to organisational success is difficult to ascertain (Ciborra 2000) for two reasons. First, most organisations have limited understanding (Ciborra 2000) of the effects of infrastructures on work (Star and Bowker 1995, Williams 1997). This chiefly stems from their context-dependent nature, their pervasiveness, and the unpredictable and varied nature of their effects at multiple levels of the organisation. Second, the rate of change of the core IT is so rapid that organisations rarely get enough time to use any technology properly (Abrahamson 1991, Ciborra 2000). To Sawyer (2000) this rapid change ensures that at any given time several parts of the infrastructure are in flux (Truex *et al.* 1999). Ciborra and Hanseth (2000) also warn that while infrastructures help control global phenomena, they are themselves difficult to control. They claim infrastructures may curb governance capabilities as much as they enhance them because, "infrastructures tend to '**drift**' i.e. they deviate from their planned purpose for a variety of reasons often outside anyone's influence."

What (or when) is an infrastructure?

Adams and Lloyd (1999) argue that a *pervasive substrate* is a foundation for a large environment such as a corporate organisation. As such, they regard an infrastructure as a pervasive substrate because it exists such that disparate entities can "tap into it" and use it on an as-needed basis (Armstrong and Sambamurthy 1999). Similarly, Hanseth (2000) sees the critical feature of an infrastructure as its support or enabling function. To Sawyer (2000) infrastructures constitute hardware and software, administrative roles and rules that support that collection, and the informal norms and behaviours that grow around the IT and the rules for governing its use. Broadly put,

> "An infrastructure can be thought of as a platform for implementation that, without interfering with the details, offers the foundation and service needed by the various applications for production, distribution and recreation. But an infrastructure can also be a regulating skeleton, providing framework and guidelines for activity. The infrastructure provides **stability and security rather than liberty of action** (Dahlbom 2000)."

To Star and Ruhleder (1994, 1996) common infrastructural metaphors are those of substrate or something upon which something else 'runs' or 'operates.' From this view, infrastructures are passive physical artefacts (Star and Ruhleder 1994). Talking about the belief that useful infrastructures are invisible, Dahlbom (2000) claims,

> "Infrastructure .... is subterranean and out of sight, and preferably not only below but also beyond our consciousness. When you are reminded of the infrastructure, it tends to make you nervous: there is something down there making everyday activities possible, but you do not really know what it is, where it is, or how it works, and what will happen, **come to think of it, if it breaks down.**"

However, Star and Ruhleder (1996) sharply dismiss the ready-to-hand view. They claim that such a metaphor is neither useful nor accurate in understanding the relationship between work/practice and technology because it fails to capture the ambiguities of infrastructure usage. It could also lead to *de facto* standardisation of a single, powerful group's agenda (Dutton and Danziger 1982, Kling 1980, Kraemer and Dutton 1982, Meyer and Rowan 1991, Star and Bowker 1995). Likewise, to Williams (1997) any functioning system has multiple meanings of usage assigned to it because while a large community shares the single object, it may appear differently to each group (Hanseth 2000). It is, therefore, impossible to have 'universal niches' because "one person's standard is in fact another's chaos." Therefore, the infrastructure becomes transparent or as part of the furniture (Silva and Backhouse 1997) *when* local variations are folded into organisational changes.

After Jewett and Kling (1991), Star and Ruhleder (1996), hold that infrastructure is fundamentally a *relational* concept because no artefact, computer-based or otherwise, is a discrete entity, a standalone thing. It becomes infrastructure in relation to organised practices or a given cultural context. They further argue that an infrastructure, like other tools, is not just a *thing* with pre-given attributes frozen in time – but becomes a tool in practice, for someone, when connected to some particular activity. Thus, studies of infrastructure should cover "a relationship or an infinite regress of relationships, never a 'thing' – stripped of use – because infrastructure emerges for people in practice, connected to activities and structures (Star and Ruhleder 1994, Star and Ruhleder 1996)." As such, the valid question is *when* – not *what* – is an infrastructure. Dahlbom argues,

> "It is important to see that these systems are not just technical systems, but rather socio-technical. ...Once we begin to slide down this slope, we will see more and more examples of things to include in the infrastructure. ... All this **makes infrastructure a somewhat slippery notion**. Perhaps we should only use it a relative sense: X is an infrastructure relative to Y, meaning that Y depends for its operation on X, and X is somehow more stable and basic than Y (Dahlbom 2000)."

These views stress the heterogeneous nature of infrastructure as represented by the notion of embeddedness and its socio-technical nature due to links with conventions of practice (Ciborra 2000, Hanseth 2000). This echoes the sociology of technology and science works that reject a 'great divide' between nature and artifice, human and non-human, technology and society (Ciborra and Hanseth 2000, Latour 1991, Walsham 1997). Thus, since useful PKIs are both catalysts and products of power, the technology becomes an infrastructure once it supports organisational processes.

From infrastructures to institutions

To conclude this Chapter, we link the concepts of infrastructure and institutionalisation. We saw that infrastructures are regulating skeletons, which provide more security and stability than liberty of action (Dahlbom 2000). Actually, Ciborra (2000), after Star and Ruhleder (1996), argues that infrastructures are institutions, norms and conventions that provide the often-implicit context for the performances of practices. Therefore, we argue that a technical artefact connected to an organisational context is an infrastructure. However, infrastructures become institutions when they typify specific work practices.

Politics of work practices

Williams (1997) argues that workplace technologies are no longer just an external force transforming work but are part of work and develop in tandem with it. This close relationship calls for IT to embed visions of work transformation (Latour 1991). As such, system development needs good techniques for understanding, representing and modelling work practices and processes (Bannon 1995) because designers often make wrong assumptions about how tasks are performed (Suchman 1995). Unearthing the underlying work practices makes it possible to embed the 'correct' procedures into the IS and ensure that routines are reproduced with economy of effort (Silva and Backhouse 1997). However, this talk discounts the contentious nature of work (Bannon 1995, Suchman 1995). It is difficult to capture the practices because,

> "**Representing work is difficult, messy, complex, and often politically touchy**. To capture (or classify) is to cut off, simplify, in some direction; work is notoriously slippery and situated. Whose voice, whose version will hold? Who benefits from which standards? One person's infrastructure may be another's barrier (Star and Bowker 1995)."

Apart from the mysterious nature of work (Suchman 1995), creating useful specifications is further complicated by the rapid change in work practices, decision process, roles and responsibilities (Handy 1990, Kettinger and Lee 2002, Salmela 1993, Salmela *et al.* 2000, Truex *et al.* 1999). The problems are more evident with systems designed for environments different to the host organisation. For instance, many cryptographic products either started as sensitive military applications (Blanchette 2000, Kahn 1996, Piper and Murphy 2002) or assumed hierarchical organisational structures. However, different uses demand the re-invention of universal solutions to avoid tensions with local arrangements.

Institutions and institutionalisation

According to Stinchcombe (1968), "By an 'institution' I mean a structure in which powerful people are committed to some value or interest. The key to institutionalising a value is to concentrate power in the hands of those who believe in that value." Jepperson (1991) argues that institution and institutionalisation are core concepts in sociology and connotes the presence of authoritative rules or binding organisation. He defines an institution as an organised, established procedure represented as the constituent rules of society. To Zucker (1991) the only idea common to all usages of the term 'institution' is the establishment of relative permanence of a clearly social sort.

Berger and Luckmann (1967) argue that although habitualised actions retain their meaningful character for the individual (Suchman 1995), organisations prefer the routinisation of the meanings in the general stock of knowledge (Rod 2000, Walsham 1993) to support future projects. The milieu of stable practices opens a foreground for deliberation and innovation, processes that precede institutionalisation for it allows the anticipation of activity and alternatives. Therefore, institutionalisation occurs whenever there is a reciprocal typification of habitualised actions by other types of actors. "Put differently, any such typification is an institution. ...The institution posits that actions of type X will be performed by actors of type X (Berger and Luckmann 1967)."

To Avgerou (2000) organisational IT institutionalisation is a product of the need to increase the efficiency and strength of the control and coordination mechanisms of the bureaucracy (Yates 1989, Zuboff 1988). She claims that the institutional elements of IT include the established view on the value of technology and knowledge, a network of industries supporting IT, professional expertise, regulations for development and IT use and professional societies. Jepperson (1991) argues that while many scholars regard institutionalisation as either equivalent to, or a form of, stability or survival, this identification is inaccurate. He claims that institutionalisation is a relative property because we decide whether to consider an object to be an institution depending upon analytical context because "institution is relative to centrality." However, institutions,

> "By the very fact of their existence, **control human conduct by setting up predefined patterns of conduct, which channel it in one direction as against the many other directions that would theoretically be possible**. It is important to stress that this controlling character is inherent in

> institutionalisation as such, prior to or apart from any mechanisms of sanctions specifically set up to support an institution (Berger and Luckmann 1967)."

Although mechanisms of control exist in many institutions, their controlling efficacy is only of a supplementary kind because the primary power lies in the mere existence of the institution. "To say that a segment of human activity has been institutionalised is already to say that this segment of human activity has been subsumed under social control." Institutions are powerful in their own right because,

> "As historical and objective facilities, confront the individual as undeniable facts. The **institutions are there, external to him, persistent in their reality, whether he likes it or not.** He cannot wish them away. They resist attempts to change or evade them. They have coercive power over him, both in themselves, by the sheer force of their facility, and through the control mechanisms that are usually attached to the most important of them. The objective reality of institutions is not diminished if the individual does not understand their purpose or their mode of operation (Berger and Luckmann 1967)."

Jepperson (1991) agrees. He argues that although persons may not comprehend an institution, they typically have ready access to some functional or historical account of why the practice exists. He adds that institutions are not just constraint structures because they simultaneously empower and control. Like infrastructures, institutions present a constraint-freedom duality for they are vehicles for activity within constraints (Jepperson 1991).

Legitimation of institutions

According to Berger and Luckmann (1967), a key feature in sustaining any institution is legitimation, which constitutes ways used to 'explain' and justify it (Stinchcombe 1968). To Stinchcombe legitimacy creates a readiness in other centres of power to support the actions of a person with a certain right. Likewise, Meyer and Rowan (1991) reveal the legitimacy of bureaucratic organisations rests on the norms of rationality.

Berger and Luckmann (1967) claim legitimation is unnecessary in the first institutionalisation phase because the institution is self-evident for all concerned. The need for justification arises when there is need to transmit the institutional order to either a new generation or a group that has no individual recollection of the institution. "Legitimation not only tells the individual why he *should* perform one action and not the other, it also tells him why things *are* what they are." That these ideas are strikingly similar to the concept of legitimation introduced in Structuration Theory (Giddens 1984, Jones 1999, Walsham 1993) is no accident because the theory traces its origins to Berger and Luckmann's concept of the mutual constitution of society and individuals (Jones 1999). Therefore, creating a "corresponding canopy of legitimations" is no admission that the institution is less real but it ensures that its relevance is associated with concrete social processes (Berger and Luckmann 1967). Stinchcombe (1968) argues that the best way of legitimating an institution is making it useful. Deviance visits institutions without legitimacy because people generally reject routines dictated by others more than ones they personally helped establish.

Roles, responsibility and structures

Jepperson (1991) regards institutions as socially constructed, routine-reproduced, program or rule systems. A common way of ensuring adherence to an institutional order is attaching it to roles (Ba 2001, Backhouse and Dhillon 1996). This is a critical area because,

> "The origins of roles lie in the same fundamental process of habitualisation and objectivation as the origins of institutions. ...**All institutionalised conduct involves roles**. Thus, roles share in the controlling character of institutionalisation. As soon as actors are typified as role performers, their conduct is *ipso facto* susceptible to enforcement. Compliance and non-compliance with socially defined role standards cease to be optional, though, of course, the severity of sanctions may vary from case to case (Berger and Luckmann 1967)."

Thus, understanding the nature of roles and responsibilities is vital because they both represent and constitute institutions. The scope of institutionalisation depends on the generality of *relevance structures*. Organisations that share only a few of these structures normally have a narrow scope for institutionalisation. Indeed, they also incur a risk "that the institutional order will be highly fragmented, as certain relevance structures are shared by groups within the society but not by the society as a whole (Berger and Luckmann 1967)." In conclusion, institutionalisation occurs when,

> "The interaction ... becomes predictable. The 'There he goes again' becomes a 'There we go again'. ... the institutions are now experienced as possessing a reality of their own, a reality that confronts the individual as an external and coercive fact... 'There we go again' now becomes '**This is how these things are done**'. A world so regarded attains a firmness in consciousness; it becomes real in an ever more massive way and it can no longer be changed so readily (Berger and Luckmann 1967)."

Zucker (1991) agrees. She argues that for highly institutionalised acts it is sufficient for one person simply to tell another that this how things are done (Jepperson 1991). "Each individual is motivated to comply because otherwise his actions and those of others in the system cannot be understood (Zucker 1991)."

Chapter summary

We argued that the main cause of PKI interoperability problems is the failure to appreciate the interaction between its at once restrictive and flexible technical features, organisational structures, the goals of its sponsors and potential user resistance. Drawing on the concepts of infrastructure and institution, we submit that PKIs are politically explosive technologies because by limiting liberty of action in favour of stability and security, in pluralistic organisations, they risk backlashes. This should not have been a concern if public key cryptography, the underlying PKI technology, had a centralised mechanism of enforcing the user discipline it relies on to work successfully. However, users are either unable or unwilling to rigorously validate others' public keys and securely manage their own private keys. Hence, we argue that without the support of power structures PKI institutionalisation is difficult.

CHAPTER 3:
THEORETICAL FRAMEWORK

Introduction

This chapter extends our coverage of power and politics in IS management introduced in Chapter 2. We started the discussion of power in Chapter 2 in an effort to introduce the deeper theoretical aspects of the research gradually. A considerable body of literature exists on the diverse views of power and their influence on IS research. We build on these works notably (Introna 1997, Silva 1997, Silva and Backhouse 1997, Silva and Backhouse 2003). Silva (1997) adapts the Circuits of Power (CoP) framework for information systems research from Clegg (1989). He presents the CoP as a theoretical framework that accounts for power and politics in IS institutionalisation. Power being a universally disputed concept, the CoP framework is efficacious because it "encompasses different approaches to power that far from being contradictory are complementary."

We begin with a discussion of how to gain, lose and manage with power. While we do not fully discuss the structuration framework, we include the insights it provides to the study of power. We also left out a detailed description of Actor Network Theory because, since like the CoP framework, it originates in the sociology of science, we cover similar concepts. We conclude with the key concepts of our chosen theoretical framework, the Circuits of Power.

Power and Politics

Although political theory is entirely concerned with the conundrum of power (Ransom 1997), it remains an elusive (Bachrach and Baratz 1962) and heavily contested concept (Keen 1981, Law 1991b, Saunders *et al.* 2000). To Clegg (1989), the disagreements are so numerous that even the best books on the subject cannot transcend the transitory nature of the debates. For instance, Lukes characterises power as "ineradicably evaluative and 'essentially contested' (Lukes 1974)." Power debates have been multidisciplinary because although the concept originated in political theory and political philosophy, it later became part of political sociology and is now a central concept of most social and human sciences (Clegg 1989 268, Giddens 1984, Ransom 1997, Said 1986). However, because the different disciplines espouse contradictory underlying values and beliefs,

> "**Power has always been one of those words that everybody uses without necessary being able to define satisfactorily**. It is treated both as a quality or attribute possessed by individuals, groups, or larger social structures and as an indicator of an active or interactive process or relation between individual or collective actors. Moreover, it also applied to physical phenomena and processes (Wrong 1995)."

Consequently, commentators have warned that no commonly accepted or even preferred meaning of power is feasible if "people differ on normative issues as they are likely to do indefinitely, if not forever (Wrong 1995)." Thus, Hoy (1986) concedes power has been and would probably always be a contested concept. Wrong (1995) argues that unlike inherently normative concepts such as 'justice' and 'democracy', power resembles other fiercely contested but not naturally normative and value-laden concepts such as inequality.

Bachrach and Baratz (1975) claim every human institution has a "power structure" that is an integral part and the mirror image of its stratification. However, pluralists reject this view stressing that, "Power may be tied to issues, and issues can be fleeting or persistent, provoking coalitions among interested groups and citizens, ranging in their duration from momentary to semi-permanent." We follow the lead of researchers like (Barnes 1986, Silva 1997, Silva and Backhouse 1997, Silva and Backhouse 2003) to underline the difficulty of coining an acceptable definition for the concept of power. We believe that although,

> "**Matters of precise verbal definition are not of great significance in the social sciences; an exaggerated importance is often attributed to them**. ... But surely all they can actually do is inhibit specific ways of using particular words, and require the use of other words instead. This, at any rate, is why I regard problems of verbal definition ...as small problems, and why I see only very limited possibilities of gain from the criticism of definitions (Barnes 1986)."

However, since even Barnes agrees, "it is necessary to offer some simple image of the nature of power in society, because there is no widely accepted account or image", we select the definition of the concept provided by Wrong (1995) for this dissertation. Viewing power as a human or social phenomenon, he regards it as "*the capacity of some persons to produce intended and foreseen effects on others.*"

Ransom (1997) argues that scholars of power need to ask two questions. First, how does it function? He sees the 'how to' question as key to Foucault's work (Foucault 1980, Foucault

1986) because it focuses on power, its sources, strategies and tactics for its use and loss (Pfeffer 1992). Traditional political theorists such as Locke, Hobbes, Rousseau, Rawls and Habermas raise the second question about what makes a power structure legitimate (Foucault 1982). Supporting the relational view of power, Ransom reiterates the definition of power as the ability of individual A to make individual B to do something they would otherwise not have done (Bachrach and Baratz 1962, Debnam 1975). However, he cautions against Wrong's claim that power produces foreseen effects on others saying, "It turns out, on closer inspection, that this process is anything but straightforward and there are all sorts of strange and unexpected ways in which individuals exercise power over others (Ransom 1997)."

Debnam (1975) agrees. He argues that to understand an outcome of power we must first identify two parties to the interaction to ascertain a change of position by either participant, attributable to efforts of the other. This means understanding the dynamics of a concretely verifiable relationship. However, he warns that while this may be the ideal situation, "one can never demonstrate conclusively in the social sciences that any given factor is both necessary and sufficient for the production of any given effect (Debnam 1975)." Debnam also dismisses the claim of Bachrach and Baratz (1962) that a researcher can understand power by asking 'strategically' placed individuals for opinion about who is powerful. He believes the approach could be misleading because it does not separate hearsay from fact. Indeed, as Barnes (1986) argues, it is always expedient in explicit discourse for powerful people to represent themselves as mere authorities without discretion. This dampens efforts to persuade, pressurise or influence their judgement.

Wrong (1995) observes that a key cause of disagreement in the conventional definition of power is the aspect of intentionality (Bachrach and Baratz 1975, Debnam 1975). He recognises that many critics believe his definition of power is incomplete because it apparently ignores the unintended and unanticipated effects of decisions and actions of the powerful. He is sympathetic to critics who label his definition as a brazen attempt to downplay the role of unintended consequences in assessing the role of power in society. He insists, however, that for power to have unintended consequences it must usually first be exercised in a social relation in which an actor produces an intended effect. Bachrach and Baratz (1975) agree. To them power is operative even when A unconsciously exercises it or when he is aware of exercising it and produces unintended effects.

Dark side of power

Wrong (1995) contends that the use of power as a near-synonym of influence, control, rule and domination results in its sharing of the many shades of meaning of these terms. He insists that to treat 'power' and 'influence' as synonyms is to make the exercise of power equivalent to any social effect. He represents the impact of "unintended influence" and identifies two forms of influence, unintended and intended (power) as illustrated.

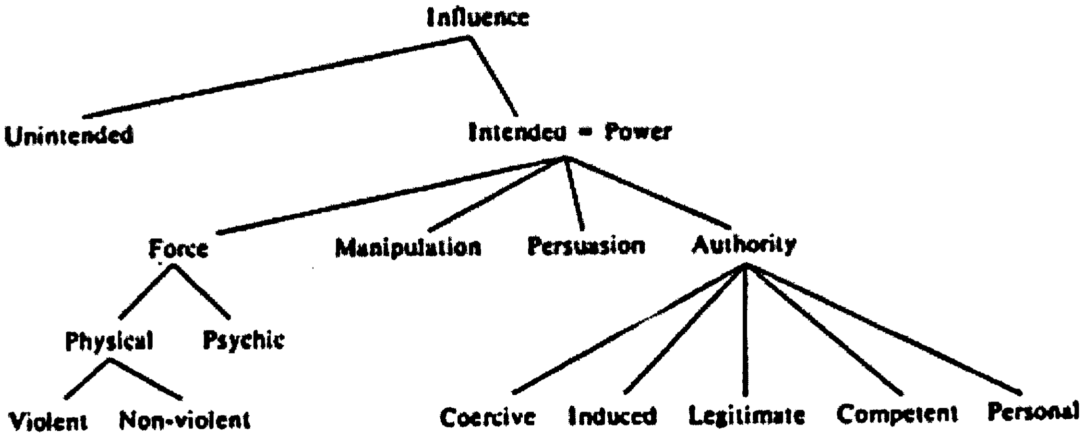


Figure 6 – Categorisation of power (Wrong 1995).

According to Wrong (1995) a key difference between power and influence is that the former continues to possess overtones of coercion even among writers who do not define it as so (Pfeffer 1992). For instance, Weber defines power as achieving ends 'even against the resistance of others who are participating in the action.' Thus, Wrong argues that the term retains something of a malign, sinister, even demonic aura. To Debnam (1975a) power attains a sinister face when, "the purpose is hidden, not necessarily the action which embodies the purpose." Even the traditional definition of power implies coercion because A achieves outcomes against the wishes of B (Debnam 1975).

Wrong (1995) argues that the negative connotations are amplified when power is treated as the cardinal motive for human striving as in familiar allusion to 'will to power,' or 'lust for power.' Scholars widely associate power with all human relations and social structures through the claim that it is the basic object of human striving (Machiavelli 1997, Nietzsche 1968). Wrong asserts that because unequal distribution of power is prevalent among groups and social categories, humans invariably seek to dominate and impose their will on others (Debnam 1975a). As laconically put,

> "**This world is the will to power – and nothing besides!** And you yourselves are also this will to power – and nothing besides! (Nietzsche 1968)."

For instance, Machiavelli's view of power as a play of strategic forces (Introna 1997) has attracted wide criticism for being an unprincipled pursuit of power bereft of religious and ethical sense (Machiavelli 1997). Advising princes to gain and retain supreme power by ruthless and amoral means if necessary, he states,

> "For a man who, in all respects, will carry out only his professions of good, will be apt to be ruined amongst so many who are evil. A prince therefore who desires to maintain himself must **learn to be not always good, but to be so or not as necessity may require**. ... For all things considered ... some things that seem like virtue will lead you to ruin if you follow them; whilst others, that apparently are vices, will, if followed, result in your safety and well-being (Machiavelli 1997)."

However, Wrong argues that Nietzsche and his disciples like Foucault (Foucault 1980, Foucault 1986), classified as cynics, define power in a neutral way regarding its malign and benign uses. For instance, the original meaning of the widely derided 'will to power' characterisation dealt with the force to preserve and enhance the vitality of an organism and its control over the environment (Wrong 1995). Hirschheim and Klein (1994) blame distortions about power for creating anxiety and causing people to distort or withhold information to protect themselves. However,

> "**Some doubted that any hidden or obscured phenomenon lurked in the dark, outside of the empiricist gaze.** If something such as the second face of power could not be seen, they argued, what proof could there possibly be that it existed? ...Either things were real and could be clearly seen or they were not real at all, except in what was taken to be a hothouse imagination of left-wing zealots (Clegg 1989)."

Bachrach and Baratz advance the concept of "Non-decision" making to explain decisions that result in the suppression or thwarting of a latent or manifest challenge to the interests of the decision maker. They claim this explains the consequences of covert control and mobilisation of bias (Debnam 1975). Non-decision presupposes that political consensus commonly arises when actors mobilise resources to prevent challenges to their values and interests (Bachrach and Baratz 1975). However, Debnam disagrees. He claims that people are largely "apolitical, strongly influenced by inertia, habit, unexamined loyalties, personal attachment, emotions, transient impulses." He believes neither frustration nor inequality is automatically the work of a hidden hand as implied (Debnam 1975).

Conceptions of Power

To reiterate, power is a disputed concept. Nowhere is the metaphorical rancour more clamorous than the internecine split between sociologists and political scientists. Sociologically oriented researchers – *elitists* – see power as highly centralised while political scientists – *pluralists* – largely regard power as widely diffused (Bachrach and Baratz 1962, Debnam 1975). Pluralists focus not upon the sources of power but its existence. Therefore,

> "Power to them means 'participation in decision-making' and can be analysed only after 'careful examination of a series of concrete decisions.' ... **the pluralist researcher is uninterested in the reputedly powerful.** His concerns instead are to (a) select for study a number of 'key' as opposed to 'routine' political decisions, (b) identify the people who took an active part in the decision making process, (c) obtain a full account of their actual behaviour and (d) determine and analyse the specific outcome of the conflict (Bachrach and Baratz 1962)."

This is the exact opposite of what elitists do (Introna 1997). While praising the approach over the elitists, Bachrach and Baratz (1962) point out two basic flaws in the pluralist perspective. First, pluralists ignore the fact that the exercise of power may be, and is often, confined to relatively 'safe' issues. Second, the model provides no 'objective' criteria for distinguishing between 'important' and 'unimportant' issues in the political arena. Undeniably power is not only exercised when A participates in decisions that affect B but also, "To the extent that A succeeds in doing this, B is prevented, for all practical purposes, from bringing to the fore any issues that might in their resolution be seriously detrimental to A's set of preferences (Bachrach and Baratz 1962)."

Bachrach and Baratz, state, "All forms of political organisation have a bias in favour of the exploitation of some kinds of conflict and the suppression of others because *organisation is the mobilisation of bias*. Some issues are organised into politics while others are organised out." They attack pluralists for assuming "erroneously" that only concrete decisions reflect power because this ignores the fact that some groups prevent contests from arising in the first place. Thus, they assert, "there are *two faces of power*, neither of which sociologists see and only one of which political scientists see." Debnam (1975) sharply disagrees. He claims that Bachrach and Baratz's research strategy offers no means of gauging the import of mobilisation of bias. He insists research should neither be started from the premise of the sociologist who ask, “Who rules?” nor from pluralism where the query is, “Does anyone have power?” but by investigating the particular “mobilisation of bias” in the institution under scrutiny (Debnam 1975).

Barnes (1986) also accuses sociologists of insistently proceeding as positivists instead of realists in their treatment of power. Clegg (1989) concurs. He argues that early writers on power saw it in a mechanical, modernist spirit under which it “was to be conceived in positivist terms as something directly observable and measurable.” The metaphor is rooted in classical political theory associated with Thomas Hobbes. Power is, “A locus of will, as a supreme agency to which other wills will bend, as prohibitory; the classic conception of power as zero-sum; in short, power as a negation of the power of others.” The model includes a centrally located sovereign to which all activities of power are traceable (Introna 1997, Ransom 1997). Because Hobbes was interested in understanding power and ways of using it to right, the sovereign is accountable for its effects (Introna 1997, Ransom 1997).

What sort of capacity is power?

Although power is often thought of as the capacity to enforce one’s will (Barnes 1986, Ransom 1997), to get things done (Pfeffer 1992), the literature is largely silent about the characteristics of this capacity. To Debnam (1975a) the frequent use of the term power denotes a facility, which is neither authoritative nor coercive. Likewise, Clegg (1989) sees power as a ‘capacity’ premised on resource control. Barnes (1986) calls for an explanation of how an agent or role with power differs from one lacking it. He argues that although,

> “There is a great deal on how to define power, how to detect its presence, how to measure it through empirical indicators and visible correlates, how to identify its material effects; **but there is next to nothing upon what power is ‘in itself’ as it were** (Barnes 1986).”

He believes that to explain away this gap in knowledge, authors routinely link power with authority. For instance, Zuboff (1988) claims authority is the spiritual dimension of power because agencies need a degree of shared faith in the values that determine rank. To Weber (1964) authority means the probability of power targets obeying a specific command. Identifying the types as legal[7], traditional[8] and charismatic[9], he claims that stable power

[7] Legal authority rests on enactment with its purest type represented by bureaucracy.

[8] Traditional authority depends on the belief in the sacredness of the social order and its prerogatives, as they have existed for a long time. The purest form is the patriarchal authority.

structures rely on the belief that they are 'legitimate' by right (Weber 1964). To Debnam (1975a) the difference between authority and coercion describes the limits of legitimate and illegitimate action. However, Barnes (1986) sees total disarray in attempts to establish whether power or authority is superior. He avers that while in the sociological tradition the received view is that authority is power plus consent, legitimacy or institutionalisation, there is controversy about what to add to transform power into authority. We continue this debate under the "power discretion" notion of power.

Law's notions of power

Power is such an omnipresent facet of social life that even a failure to refer to it "points to '*silences in the text*' that are held to reveal a presence confirmed by its very absence (Wrong 1995)." Cataloguing the experience of sociology, Law (1991b) rages that because power is, "Used, re-used, and endlessly abused, it is unsurprising that they are many who believe that it should be dropped altogether from the vocabulary of the discipline." To Callon (1986) this is little wonder because sociologists rarely, if at all, agree about anything. Likewise, Hoy (1986) suggests that since, "social philosophers may be fated to perpetual quarrelling, social scientists should be able to either define univocally central theoretical concepts like power or dismiss such concepts if they continue to elude quantifiable refinement." He stresses that a decision needs to be taken because if the concept of power is not understood, we risk failing to grasp the character of society as well (Hoy 1986).

Against this background, Law (1991b) believes he can extricate a useful notion of power from the "shipwreck of sociology". He suggests four themes in the sociology of power: 'Power to', 'power over', 'power storage' and 'power discretion.' Law argues that 'power to' and 'power over' can under specific circumstances be stored and used in a discretionary and calculative manner. Each power form is relational because its deployment affects the environment and causes change (Wrong 1995). Although he dodges the question of how these relations are stabilised, Law asserts that the power networks are never purely social because they are a product of a fabric that integrates social relations and technical, architectural, textual and natural non-human actors (Latour 1991). Thus, he writes,

[9] Based on the affectual and personal devotion of the follower to the lord and his gifts of grace (charisma). The unheard of and the emotional rapture from it are sources of personal devotion (Weber 1964).

> "To understand the social and, more particularly, to understand what it is that stabilises social relations to generate power effects we have, I suggest, to make sense of the way in which the 'social' interacts with and is constituted by these other materials. And, in particular, we have to explore the way in which discursive ordering strategies (in part) shape, and are embodied in a range of different materials (Law 1991b)."

This view is relevant to us because even the reference to information systems as social systems (Angell and Smithson 1991) implies a heterogeneous sociotechnical network (Law 1991b) under which power relations are rooted (Foucault 1982). Eschewing what he calls sociologism and technologism, Latour (1991) claims we never face objects or social relations, but chains, which are associations of humans and non-human agents. "No one has ever seen a social relation by itself ... nor a technical relation." Hence, understanding the material heterogeneity of arrangements is critical (Law 1991b, Star 1991) because, "whenever we discover a stable social relation, it is the introduction of some non-humans that accounts for this relative durability (Latour 1991)."

Power to

This notion represents the productive and enabling character of power. Several authors have commented about this form of power (Barnes 1986, Barnes 1988, Foucault 1982, Wrong 1995). For instance, Barnes (1986) argues that this power is the capacity to enforce one's will even against opposition. Likewise, Giddens' definition of power as the capacity to achieve outcomes also supports this notion. He identifies a two-way relationship between power and human agency because without power there is no agency (Giddens 1984). Using the terms agency and actor interchangeably, Law seeks to bridge the legendary agency/structure dualism by presenting an actor as a set of relations. A key difference between Law and Giddens is that to the former, "Agents are not co-terminous with people" because other entities can too be agents (Clegg 1989). Barnes (1986) appreciates the unequal distribution of this added capacity to perform in society. However, he sees this power as a non zero-sum social property (Law 1991b).

Wrong (1995) argues that most of the confusion surrounding the concept of power has been caused by the conflation or at least a slurring of the difference between "power to," the more general category, and "power over." He defines 'power to' as the capacity of individuals to satisfy their wants. He argues that this distinction remains crucial because conflation of the two senses of power is the source of many ambiguities, conceptual and rhetorical, that cling to the power concept (Wrong 1995). In common with Barnes, he regards power to as "obviously relational" which implies that the whole is greater than the sum of its parts (Law 1991b). Wrong adds that power as the capacity to produce effects may be imputed to the agency as a dispositional property even when the capacity is not manifest in action. To Law's surprise Foucault too espouses this concept of power as an enabling phenomenon and eschews the zero-sum conception.

Power over

This has traditionally been the most dominant theme of power among social theorists. For instance, Foucault (1982) claims, "let us not deceive ourselves; if we speak of the structures or the mechanisms of power, it is only insofar as we suppose that certain persons exercise power over others." According to Law (1991b), most of these theorists adopt, whether expressly or not, a zero-sum view of power, which implies a relative empowerment, and disempowerment of agencies in a relational field (Clegg 1989). Lukes (1974) is a key advocate of this notion. He asserts that, "A exercises power over B when A affects B in a manner contrary to B's interests." He raps proponents of the 'power to' notion arguing,

> "They focus on the locution 'power to', ignoring 'power over'. Thus power indicates a 'capacity', a 'facility', an 'ability', not a relationship. Accordingly, the conflictual aspect of power – the fact that it is **exercised *over* people – disappears altogether from view** (Lukes 1974). "

Law sympathises with Lukes' claim that many theorists, notably Parsons[10], in their desire to understand the social system fail to see that such a system may be a product of conflict between parties with different interests and degrees of power. Lukes (1974) labels the generic concept of power as 'power over' and influence as 'power to'. He subsequently focuses on the former claiming this is to maintain focus on the relational and contested character of power relations. However, Law (1991b) rejects Lukes' assertion that the central definition of power relates to 'power over'. He depicts it as an example of the "insularity of social theory and its ignorance to both natural scientific thought and dictionary definitions (Law 1991b)." Like Barnes (1986, 1988), he sees no reason why concern with 'power to' should automatically eliminate interest in 'power over' because relations and capacities are indissolubly linked.

[10] To Lukes, Parsons seeks to "treat power as a *specific* mechanism operating to bring about changes in the action of other units, individuals or collective, in the process of social interaction." However, he wonders what is specific about this mechanism to distinguish it as 'power'.

Power storage

According to Law (1991b), the conjoined character of 'power to' and 'power over' raises a further question of whether or not agents are able to store up 'power to' or 'power over.' For instance, he wonders what it means when Lukes says some agents *are* more powerful than others. In attacking power reductionism, which treats everything as an expression of power and describes phenomenon as a social relation in which some persons possess and exercise power over others, Wrong (1995) provides a good definition for power storage. This notion of power is associated with social stratification where people have access to unequal power, income and other resources. The beneficiaries of this unequal distribution or "haves" then attain and maintain their favoured position by means of the power they exercise over the underprivileged "have-nots." Thus, the notion of power storage relies on the inseverable nature of power relations and capacities.

Law exemplifies power storage through a case study of a formal organisation. He argues that managers assume that they have a 'store' of power to act. This normally takes the form of money because its liquidity enables 'powers' conveniently to convert it into a variety of actions, which are also accumulated, deployed and further converted. "Money is thus a relationally derived store of power to act and (accordingly) power over certain others." However, Law cautions that money is not the only store of the capacity to act because achieving outcomes of power involves a heterogeneous network of social-technical elements. After Giddens (1984), Wrong claims we should regard power itself as a resource. He argues this is because power results from the mobilisation of resources such as wealth, knowledge and skills to produce effects. This view supports Foucault's claim that power is an achievement and is not normally stored (Law 1991b). He argues,

> "**Power is exercised rather than possessed; it is not a 'privilege', acquired or preserved,** of the dominant class, but the overall effect of its strategic positions – an effect that is manifested and sometimes extended by the position of those who are dominated (Foucault 1979)."

However, Law (1991b) finds Foucault too restrictive because he presents an either-or situation. From the advice, we *either* have a unity of domination *or* conflicting strategies of power. Law claims society routinely assumes that both 'power over' and 'power to' can indeed be stored. However, the methods of storage are never fail-safe. Law gets support from the concept of 'structural power'. It deals with a "set of (prior) reproduced asymmetric social relations between groups based on the possession of, and restriction of access to, certain resources (Layder 1996)." The prior arrangements constrain the exercise of power by both individuals and collectivities within and outside the structure. In sum, Law submits that 'power to' and 'power over' may be stored on condition we remember they, "are also an effect, a product of a set of more or less precariously structured relations."

Power discretion

Law terms this notion as the 'power not to' act or power/discretion. He argues that once power is 'stored', this notion explains when to exercise this capacity over other actors. The inference is that an agent can switch potential 'power to' and 'power over' on and off. Thus, they have discretion. Barnes (1986, 1988) provides the link between power and discretion by arguing that 'real' power not only has capacity for action but also discretion in its use. He insists,

> "Authority should be thought of as **power minus**, that to possess power is more expedient and advantageous than to possess authority ... power directs a routine with discretion, an authority directs it without discretion. ...But they do in response to external indications; the basic pattern of their actions is entirely the product of external constraint. **Authority then, is power minus discretion** (Barnes 1986)."

Thus, maximising power is about retaining as much discretion over strategic routines as possible. "The problem of the power holder in this context is to create passive agents and prevent their metamorphosis into active agents (Barnes 1986)." Law (1991b) hails the distinction between powers and authorities because it fits with routine distinctions between representatives and delegates, or policy makers and mere functionaries. However, Law is uncomfortable with the authority and power dichotomy especially what it means to have discretion. He regards the solution offered by Barnes as simplificatory because authorities are not always 'mere relays' and powers calculative mobilisers of routines, due to overlaps. He believes we should treat the distinction as a continuum of (relational) powers and authorities. Most would lie "between the two, borrowing and so embodying more or less explicit strategies of calculation (Law 1991b)."

Consequently, unlike authors who restrict themselves to one view of power (Lukes 1974, Wrong 1995), the four notions give a more comprehensive picture of how relations are stabilised for long enough to generate the effects and conditions of power (Law 1991b). As

Law observes, we need to understand 'power to' and 'power over', their storage and deployment while appreciating they are precarious relational and transformational effects (Clegg 1989). Law believes the character of 'power to' and 'power over' is a function of a socio-technical network of relations in which an actor is implicated, explained, "Perhaps (by) the 'circuits of power' to use Stewart Clegg's felicitous phrase." We discuss the CoP next.

The Circuits of Power framework

Stewart R. Clegg (1989) concedes power is the most contested of concepts. As such, there is no single all-embracing concept of power *per se* (Hoy 1986, Wrong 1995). He identifies at least three groupings clustered around loci of dispositional, agency and facilitative concepts of power. In the dispositional conception advanced by Wrong, power is equated to a set of capacities (Law 1991b). The facilitative conception of Parsons sees power in terms of its ability to achieve goals. This was an effort to stress the positive aspects of power to mitigate its dark side (Pfeffer 1992, Wrong 1995). However, Clegg claims, "None of these conceptions easily fitted into a narrative structure constructed around a single, essentially contested conception of power."

Therefore, Clegg introduces the Circuits of Power (CoP) as a tool to unravel and make sense of this dynamic by providing a central tradition of power that incorporates different debates and explains well-grounded alternative conceptions. Clegg argues,

> "Irrespective of mode of analysis, **an adequate framework of power should enable us to sketch a plausible narrative**, where plausibility is not brought into question by recourse to devices such as analytical prime movers, or hidden and inexplicable mechanisms of thought control."

The CoP framework draws on advances in the sociology of science (Callon 1986, Latour 1991) and the sociology of organisations (DiMaggio and Powell 1991, Jepperson 1991, Meyer and Rowan 1991). According to Introna (1997), the framework provides specific language for visualising and thinking through the material nature of power in everyday organisational relations. Appropriate language is critical because, as Silva (Silva 1997, Silva and Backhouse 1997) argues, answering obstinate questions about what power is and how to study it in information systems needs a theory of power. Thus, the framework is an apt choice because of its origins in political and organisational theories.

The framework explains how organisations achieve specific outcomes and more critically how these outcomes are stabilised for long enough to generate effects and hence the conditions of power (Law 1991b). The crux of Clegg's argument outlined in his book *Frameworks of Power (*1989) is that to achieve outcomes of power agencies need to make alliances, control resources and translate rules that govern meaning and membership in organisations (Clegg 1989).

As stated previously, we build on the works of other IS researchers who have used this framework in our discipline. However, there are two differences between those studies and our dissertation. First, with the exception of sections of (Silva 1997), these works rely on secondary data from the London Ambulance Service information systems failure (Introna 1997, Silva and Backhouse 1997) to test the framework. In contrast, we present a more detailed appraisal of framework's utility in explaining the relationship between power and institutionalisation. The framework guides our interview design, data collection and analysis. Second, the previous studies cover relatively conventional IS aimed at internal efficiency. Although these systems also attempted to change work habits, a PKI is both more pervasive internally and opens up the organisation to the unpredictable outside world. Apart from their scope, PKIs are difficult to stabilise because they focus on security - a "moving target."

Next, we present a substantive discussion of the CoP Framework. We start by outlining Clegg's notion of power and the evolution of the framework. Following that section is coverage of the main CoP elements. The discussion is vital because we not only drew on the framework for theoretical concepts as ways of viewing elements in the real world but it also showed us the elements to trace in empirical work (Walsham 1997).

Clegg's Notion of Power

Clegg believes the terminology of power originates from Weber's (1978) discussions of how his three pure types of legitimate authority – rational, traditional and charismatic – differed from other forms of domination[11] (*Herrschaft*), and subsequently how domination varies from other forms of power (*Macht*) (Weber 1964). He argues that domination becomes authority when institutionalised through the circuit of dispositional power as a substantive modality of rule such as legal rationality.

Clegg agrees that the key elements of power systems are agencies and events that interest them. However, he rejects explanations focusing on dominant ideologies, real interests or three dimensions (Lukes 1974) widely associated with Marxist authors. These authors place the problems of conflict and change at the forefront of power analysis (Burrell and Morgan 1979). In IS Marxist authors believe that information systems always aim to deskill workers and increase monitoring (Knights and Murray 1994) for the benefit of the dominant managerial interests (Markus 1983, Markus and Pfeffer 1983). Clegg argues that understanding interests should not focus on the "individual actor's reason to act" because agencies may represent other interests because of a process of 'translation' (Callon 1986). Thus, "reference to interests in this schema is not to be taken as referring either to individual agent's 'reasons' or to their unknown but 'real' interests (Clegg 1989)."

Clegg also compares the sovereign view of power in what he calls the 'fiction' of *Leviathan* (Hobbes 1968) to Machiavelli's imprecise, contingent and strategic vision. The strategic perception is associated with post-structuralism (Nietzsche 1968, Wrong 1995), which stands against the notion of sovereign power traceable to a central source (Introna 1997, Ransom 1997). Like Machiavelli, Foucault focuses on how power achieves strategic effects through its disciplinary character (Foucault 1979, Introna 1997, Ransom 1997). However, Foucault claims, "it is not power, but the subject, which is the general theme," of his research (Foucault 1982).

Introna (1997) argues that while Hobbes focuses on what *power is* or should be, Machiavelli writes about what *power does*. Likewise, Clegg contends that the Machiavelli project

[11] **Domination** is the likelihood that a given group will obey a command with a specific content.

represents a "full blown, if somewhat marginalised, way of seeing power." Machiavelli sees power as significant in the way it manifests itself in shaping and reshaping relations in everyday practice – power as strategic force relations (Introna 1997, Machiavelli 1997). His disciples de-emphasise the total score and focus on the more contingent and local interpretation. They share "an analytical focus on and fascination for shifting, unstable alliances, a concern for military strategy and a disinclination to believe in any single, originating and decisive centre of power (Clegg 1989)." Clegg believes Machiavellian insights are more relevant in postmodern times compared to the victorious project of Hobbes spurred by "that mythical, heroic, modernist law bringer."

The Circuits of Power

The framework considers power to be circulating through the episodic, social integration and system integration circuits of power. Clegg christened the framework a 'Circuits' of Power to indicate the relational nature of power (Bachrach and Baratz 1962, Debnam 1975, Wrong 1995) that implies at least two agencies. It also shows that power should not only be seen as a 'thing' that can be owned (Foucault 1979). Instead, he regards power as a phenomenon whose outcomes keep circulating in organisations through norms, rules and values (social integration) and their relationships to techniques of discipline, surveillance and supervision (system integration). He contends that,

> "**In the circuits framework, power is multifarious**: it is episodic power; it is also the circuit of power through rules and domination, as well as the overall empirical articulation which configures the theoretical circuits in any application of the model."

Why does Clegg insist on three circuits? He believes that to sketch a plausible narrative, a satisfactory framework should cover the diverse conceptions of power as represented in the three circuits. The episodic circuit is vital because it illuminates how agents struggle to achieve their desired outcomes. However, to produce intended and foreseen effects on others, agents depend on rules and pre-configured standing conditions or capacities explained under social and system integration circuits. Therefore, the three circuits give a full picture of how agencies exercise power over others and how to embed these outcomes into the fabric of actual breathing organisations.

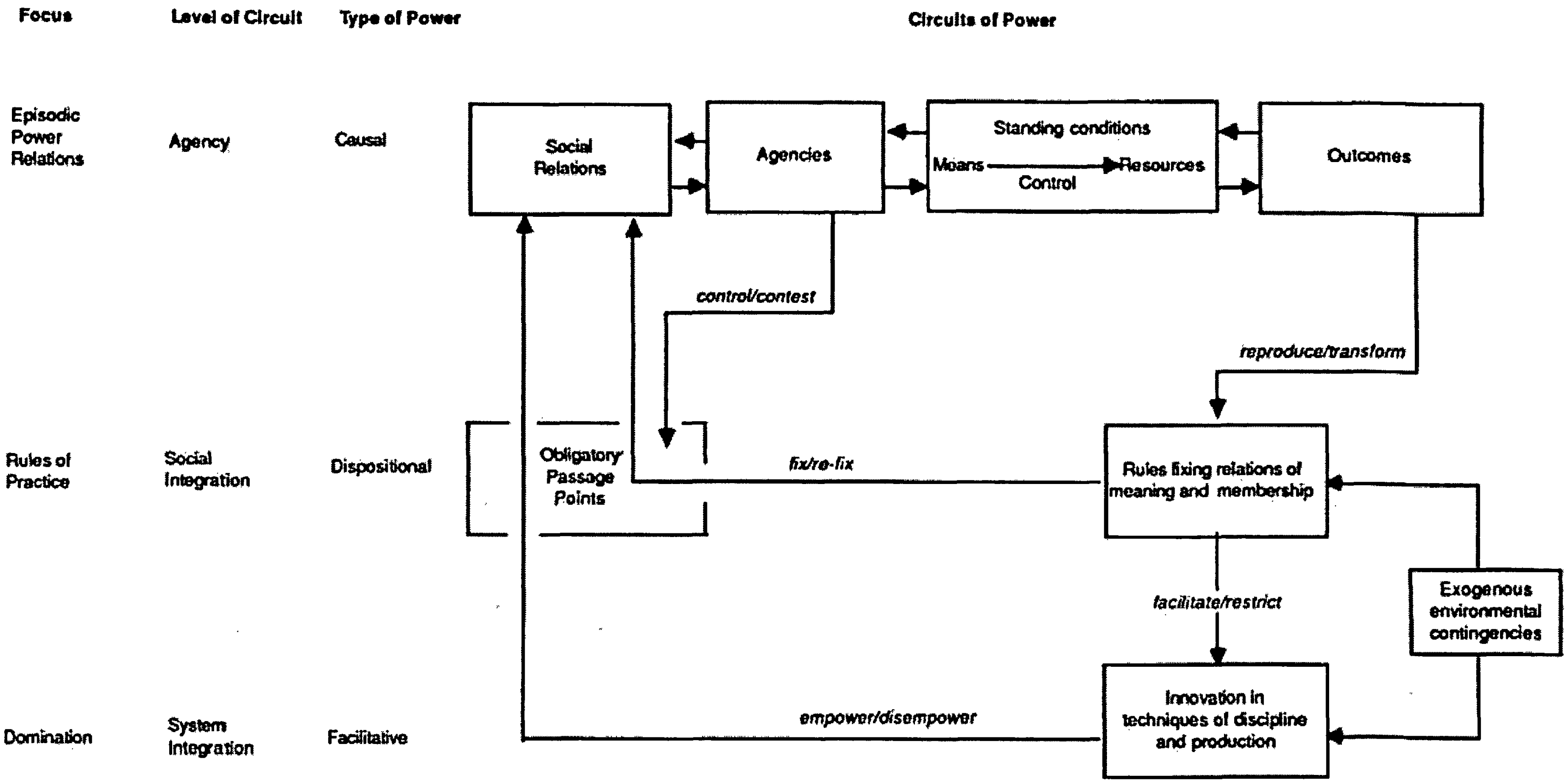


Figure 7 - The circuits of power framework (Clegg 1989)

The circuits diagram is composed of nodes and subways. The nodes represent the main elements of each circuit while the pathways stand for 'fields of force' embodied in the organisation. Although Clegg views the terms 'field of force' and the 'actor network[12]' perspective in Actor Network Theory (Walsham 1997) as similar, he opts for the former. He argues this is because apart from the human subject, agency may be vested in,

> "Non-human entities as diverse as machines, germs, animals and natural disasters. ...Organisations may constitute a form of collective agency and there is no reason to make **this a second-rate form of agency compared to that of the problematic human subject**. Where organisation achieves agency it is an accomplishment, just as it is for the individual but more so, because it involves the stabilisation of power relations across an organisational field of action, and thus between many subjectivities, rather than simply within one embodied locus of subjectivities (Clegg 1989)."

The organisational field of action is analogous to the Foucauldian field of force concept. Referring to agency instead of actors, Clegg argues, "Such fields exist only to the extent that they are an achievement of episodic power in the institutional field, stabilising relations of power between organisational agencies A, B... N." He rejects accusations that the CoP is too complex by borrowing the law of 'requisite variety' to claim, "The complexity of the phenomenon is mirrored in its representation." Let us now discuss the main CoP elements.

Episodic Circuit

This is the most obvious circuit because the exercise of power under it ideally produces tangible and foreseen effects on others. Agents manifest episodic power by mobilising resources and alliances to produce intended outcomes. The circuit represents power and resistance because politics includes both a struggle for power and attempts to limit, resist and escape from its exercise (Clegg 1989). Lukes (1974) also sees social systems as products of conflict between parties with different interests and degrees of power (Ransom 1997).

Law (1991) links episodic power with 'power over.' It is relational power (Lukes 1974), which "trades off some extant 'fixing' of facilitative and dispositional power (Clegg 1989)." By including standing conditions and showing that episodic power relies on other circuits, Clegg claims to have solved the structure-power quandary without using the duality of

[12] He defines an 'Actor Network' as an interrelated set of entities successfully translated by an actor.

structure[13] concept (Giddens 1984) or focus on real interests (Lukes 1974). Critics have accused Giddens of conflation (Barley and Tolbert 1997) and ignoring enduring relations (Introna 1997) for claiming that institutions only exist as memory traces and are only instantiated when drawn on social in action. Therefore, episodic power relies on the capacities of agents grounded in resource control to achieve outcomes. Agencies activate resources in power struggles hence those with more resources have a stronger power base.

The episodic circuit is both coherent and important in its own right because power can either flow within it alone or encompass the other circuits. However, power restricted to this circuit automatically reproduces existing configurations of rules and domination. Since, it neither tests the social integration nor system integration circuit it cannot innovate. Consequently, outcomes of economy power are rarely enduring because by failing to reshape rules of practice there is no *power storage* to maintain these effects. To understand how the episodic circuit stabilises social relations to generate power effects, we assess its constituent features.

Social Relations and Agency

To Clegg it is difficult to have a complete view of power unless we identify both agents and their associated social relations. The relations are significant because their long-term stability is pivotal to the generation of power effects. In the framework, social relations constitute the identity of agencies that are the collective loci of decision-making and action. To understand the relations, we need to analyse the political landscape to ascertain the political subdivisions that characterise an organisation (Pfeffer 1992). This reveals the conditions that pre-configure[14] power relations and hence explains what constitutes effective *agency*, especially the organisational type. The analysis covers the wider relational field of force for power configuration in which social relations constitute agency. Social relations also give insights into reification – the greatest achievement of power. Reification is associated with power storage (Law 1991b) and occurs,

> "**When power is regarded as thing-like, as something solid, real and material**, as something an agent has, then it represents power in its most pervasive and concrete mode. It is securely fixed in its representations (Clegg 1989)."

[13] Giddens argues that the basic domain of social science study is neither the experience of the individual actor nor the existence of any form of social totality, but social practices ordered across time and space.

[14] A major criticism of the structuration framework is that it fails to appreciate that prior inequalities of power derive from the reproduced relations of domination and subordination of the groups to which specific individuals belong or represent (Layder 1996).

Reification is close to power storage because to store power or have discretion over its development is to enjoy or suffer from the effects of a stable network. The reification of relational conditions occurs through the fixing of their obligatory passage points. However, control is precarious because, "It will be open to erosion and undercutting by the active, embodied agency of those people who are its object (Clegg 1989)." Put differently, "those who command and those who obey are locked in a mutual dependency that is infused with shared meaning. Command is ever vulnerable to the vagaries of changing values, conflicting experiences, and diverse interests (Zuboff 1988)."

Resistance: Control/contest

In practice, reified power rarely, if ever, occurs entirely without resistance. Thus, contrary to common assumptions, power is seldom the complete reification. Although all forms of agency – human and organisational – are an "achievement of control produced by discipline" it is difficult to get obedience and compliance (Foucault 1979, Ransom 1997). Clegg argues that by definition, wholly effective discipline admits no breach, no 'disobedience' and total rule-boundedness. Since Machiavelli observes that organisations are, "locales in which negotiation, contestation and struggle between organisationally divided and linked agencies is a routine occurrence (Clegg 1989)," resistance goes together with the exercise of power.

Episodic power causes resistance because of the power/knowledge nature of agency (Foucault 1980). Clegg claims that power and resistance are inseparable because some conceptions of resistance are over-extensions of a sweeping concept of power itself. Indeed, resistance indicates power exercise. Thus, an analysis of episodic power should appreciate that relationships between agencies are unequal because of the identities conferred by social relations and access to resources (Law 1991b, Layder 1996, Wrong 1995).

Success in mobilising resources depends on the ability of agents to interpret standing conditions and use the available means. Clegg argues that agencies operate in a highly complex arena of standing conditions because they not only coexist with others with conflicting interests but they also attempt to exercise 'power over' each other. Hence, we should do the following to study the standing conditions of episodic power. First, we need to identify the agencies trying to exercise 'power over' others. Second, establish the scope of the action of the involved agencies. Third, identify the means available to each agent to activate their desired resources. Lastly, researchers should characterise the resources that underpin the capabilities of each agency. Clegg believes he enriches the usual view of episodic power by showing standing conditions as essential for achieving varied outcomes.

Outcomes

Within the episodic circuit, the *Outcomes* quadrant reflects the objectives and intentions of agents as enshrined in dominant discourses. Researchers assess outcomes by exploring intentional actions undertaken by agencies and their interpretation of others' actions. Clegg distances himself from Lukes (1974) definition of power, which assigns putative interests to agents. He argues that intention is not synonymous with something interior to private mental states of persons or even equivalent to what people claim comprises their private mental states. Clegg focuses on the intentional actions and interests of agencies to ascertain whether they have been realised or not.

However, he warns we cannot simply assume power as the realisation of outcomes from capacities. Indeed, in many social relations an agent's power is less than the capacities they mobilise to achieve a specific outcome. Clegg believes this is because 'social games' rarely correspond to the idealised conditions of pure games that have clear rules of engagement. These rules are, "more fragile, ambiguous, unclear, dependent upon interpretation, and subject either to reproduction or transformation depending on the outcome of struggles to keep them the same or to change them this way or that." Powerful actors both have greater scope in their permissible actions and authoritatively reinterpret what the rules mean because,

> "The concept of rules also relates to that of intention. ...In regarding a behaviour as a specific type of social action, which can be said to have been intended to be such and such an action, we ... make reference to our interpretations of social actions by reference to social rules (Clegg 1989)."

The interaction between capacities and resistance and in the 'social games' ensures that agencies seldom achieve all their intended outcomes. Thus, to achieve outcomes of power agencies have to overcome resistance posed by the causal powers of competitors.

Aggregate effect of episodic circuit

While episodic instances of agency power are the most apparent, Clegg (1989) warns that an exclusive concern with this circuit fails to address the phenomena adequately (Law 1991b). This is because the episodic circuit cannot stabilise social relations on its own. As such, episodic power needs to move through the other two circuits to allow the translation, fixing and either reproduction or transformation of rules, relations and resources. Thus, these circuits provide the field of force for the articulation of episodic agency conceptions of power. Indeed, in the long term agencies seek power to reproduce the 'substantively rational' conditions that enable the strategies espoused in the episodic circuit to make contextual good sense. These conditions provide a foundation for institutionalisation because they make routinised actions retain their meaningful character (Suchman 1995) in the general stock of knowledge (Berger and Luckmann 1967).

Obligatory Passage Points (OPP)

The concept of Obligatory Passage Points is central to the circuits of power analysis. To Introna (1997), OPP is a rhetorical device that presents the solution to a problem in terms of the resources of the agent proposing it. The premise is that since innovations disturb the social integration circuit by introducing new meanings, their survival hinges on attaining stability, "in rules of practice as an obligatory passage point through which an agency's reproduction must pass (Clegg 1989)." OPPs enrol interests of different agencies into stable representations to form an organisational field. In turn, the field allows the creation of alliances necessary for achieving outcomes of power.

The OPP concept has roots in the sociology of translation (Callon 1986, Latour 1991) and Actor Network Theory (ANT). Callon introduces the sociology of translation or enrolment to explain the role played by science and technology in structuring power relationships (Callon 1986). He defines translation as the *mechanism by which the social and natural worlds progressively take form resulting in certain entities controlling others*. Like Foucault, Callon is a disciple of Machiavelli. He offers three methodological principles for the sociology translation namely agnosticism, generalised symmetry and free association. *Agnosticism* dictates impartiality when faced with actors engaged in controversy. Observers should both be impartial towards the scientific and technological arguments used by the protagonists and avoid censoring actors as they speak about themselves and the social environment.

Generalised symmetry demands both a commitment to explaining conflicting viewpoints in the same terms and that the observer uses a "single repertoire" after the description. Lastly, *free association* requires the observer to abandon all a *priori* distinctions between natural and social events. "These divisions are considered to be conflictual, for they are the result of analysis rather than its points of departure (Callon 1986)."

The principles attempt to provide a broad view of power because, "understanding of what sociologists generally call power relationships means describing the way in which actors are defined, associated and simultaneously obliged to remain faithful to their alliances (Callon 1986, Latour 1991)." Callon (1986) explains that for actors to impose their definition of the situation on others, they must go through four 'moments' of translation. These are problematisation, interessement, enrolment and mobilisation.

Problematisation is the 'moment' where the actor attempting to become a spokesperson defines the nature of the problem to others and suggests ways of resolving it. However, the actor presents the solution in terms of their resources, inevitably establishing themselves as an obligatory passage point in the network of relationships they are building. The actors attempt to become an indispensable part of the network of alliances or associations between entities they helped define and create.

Interessement encompasses actions by which an entity attempts to impose and stabilise the identity of the other actors defined through problematisation. This 'moment' is "founded on a certain interpretation of what the yet to be enrolled actors are and want as well as what entities these actors are associated with. The devices of interessement create a favourable balance of power (Callon 1986)." Interessement serves to impede rival alliances or interferences that might question the legitimacy of the proposed OPP and attempts to get members to confirm the selected passage. The success of this 'moment' confirms the validity of problematisation.

Enrolment is a critical stage because it consummates alliances. For as Callon argues, no matter how convincing the argument, there is no guarantee of success until we reach a stage where interrelated roles are defined and attributed to actors who hopefully accept them. This is the stage where the "multilateral negotiations, trials of strength and tricks that accompany interessement" succeed or fail. Ideally, actors consolidate alliances through bargaining and mutual concessions.

Mobilisation is the final 'moment'. It deals with ways of determining the legitimacy of the spokesperson. Success at this stage depends on answering the prime question of who speaks or represents whom. The spokesperson is like a macro-actor who successfully translates other actors' wishes into a single will for which they speak (Callon and Latour 1981). Enrolment creates a single voice which is "extremely powerful because of the forces on which it relies." Therefore, translation explains how a few represent many silent actors of the social and natural worlds that they have mobilised because to translate is to,

> "**Express in one's own language what others say and want**, why they act in the way they do and how they associate with each other: it is to establish oneself as a spokesman. At the end of the process, if it is successful, only voices speaking in unison will be heard (Callon 1986)."

The notion of translation emphasises the continuity of displacements and transformations at each stage in terms of goals, interests, devices and human actors. When it occurs, power is exercised because some displacements play a more strategic role than others do.

The Circuit of Social Integration

Clegg conceives of social integration or dispositional power in terms of the relation between the rules governing meaning and membership. To Wrong (1995) dispositional power is the capacity of agencies to produce intended and foreseen effects on others even though they may not manifest this potential in action. According to Introna (1997), the analysis of this circuit identifies both legitimate and illegitimate power. Introna believes that the recognition of illegitimate power is fundamental in a complete political appraisal because a key reason for IS failure is the, "lack of fit between the meanings arising from the information system, and the prevailing organisational rules and norms."

We saw elsewhere that 'power over' trades off some extant 'fixing' of facilitative and dispositional power. To Clegg indexicality is the reason why a change in rules governing meaning is always contentious. Indexicality implies that the meaning of speech and language depends on the specific features of the context of their use such as personal, temporal or location. Thus, attempts to deploy new material conditions such as technology, techniques and methods of production, run into trouble if they demand significant changes to the rules governing meaning and membership.

Introna (1997) argues the acceptance of new material conditions largely depends on their integration with the institutionalised organisational order as encapsulated by norms, beliefs and values. He warns that where there is a lack of fit, material conditions may engender social relationships and practices that can threaten the organisation's very existence. Clegg (1989) observes that issues of social integration, achieved through fixing rules governing relations of meaning and membership, become important within both organisations and organisation fields as they age. This is because while all norms are temporal, older organisations experience greater structural inertia that slows innovation down. Older organisations are slow innovators because their membership and meaning characteristics like personnel, formal structure, culture and goals tend towards homology. Inertia is remarkably destructive where information is not merely an intellectual commodity but a political resource, whose redistribution through a new IS, affects the interests of particular groups

(Keen 1981). Organisational outflanking[15] thwarts radical social change because the absence of collective organisation to do otherwise premises compliance.

Silva (1997) warns that because of the structural nature of dispositional power, elements of the circuit are probably the most elusive in research. Unlike episodic power, especially when seen through positivist eyes (Hofstede 1993) as something directly observable and measurable (Barnes 1986, Clegg 1989), dispositional power is embedded in social practices, rules and norms making it less obvious. Therefore, researchers must rely on their understanding of the organisational context built through data collection to discern the elements. Since Clegg identifies organisational age as a factor in institutionalisation, it is vital to reconstruct the history of the case studies to understand how members value innovations.

Exogenous Contingencies

In the CoP framework the arrow between the 'exogenous environmental contingencies' quadrant and the rules of meaning and membership highlights the link between institutional isomorphism and the social integration circuit (Silva 1997). Exogenous contingencies represent coercive pressures from agencies with authority in an organisational field that transform or reinforce the rules of meaning and membership. The CoP draws on concepts of institutional isomorphism to explain how organisations adopt innovations and how the innovations become stable in organisational fields (Meyer and Rowan 1991). To DiMaggio and Powell (1991) an *organisational field* represents those organisations that in aggregate constitute a recognised area of institutional life. These include key suppliers, resource and product consumers, regulatory agencies and competitors.

Isomorphism explains a constraining process that forces one unit to resemble others faced with similar environmental conditions. Isomorphism is both competitive and institutional (DiMaggio and Powell 1991). *Competitive isomorphism* is the purer type and assumes a system rationality emphasising competition, niche change, and fitness measures in competitive markets. *Institutional isomorphism* considers other firms because organisations compete not just for resources and customers but also political power and legitimacy. Institutional isomorphism can be coercive, mimetic or normative.

[15] Under "organisational outflanking" resistance may "consolidate itself as a new power and thus constitute a new fixity in the representation of power, with a relational field of force altogether."

The *coercive isomorphism* emanates from political influence and the problem of legitimacy where centrally configured agencies use existing configurations of episodic power to demand specific actions from dependent relations in the network. These pressures could be forceful, persuasive or "invitations to join in collusion." *Mimetic* processes rely on the power of uncertainty to create imitation. Organisations may model themselves on others when knowledge of technologies is low, goals are ambiguous or when the environment creates symbolic uncertainty. The dominance of the technically inferior QWERTY over Dvorak keyboards shows the power of uncertainty (Rogers 1983). The *normative* type stems from professionalisation or a collective struggle by members of an occupation to define conditions and methods of their work. The goal is to create a cognitive base and legitimation for autonomy. Overall, isomorphism leads to homogenisation even of new entrants once the organisational field is established (DiMaggio and Powell 1991).

However, to Clegg institutional theory is not concerned with the nature or source of innovation itself. The institutional perspective focuses on the 'politics' and 'ceremony', which the CoP framework represents as rules of practice. Social change is the interest of the circuit of facilitative power through system integration.

The Circuit of System Integration

This circuit deals with 'material conditions' of techniques of production and discipline. After Lockwood (1964), Clegg states that material conditions include the technological means of control over the physical and social environment and the skills associated with these means. The circuit deals with facilitative power because material conditions of production either empower or disempower agencies in their productive activities. Facilitative power is associated with the ability to produce and achieve collective objectives as we saw under the 'power to' notion. Because some agencies have capacity to define collective objectives, this circuit explains why organisational members work together and extends the notion of power beyond concern with conflict. Thus, systemic integration deals with the coordination of working practices. Both discipline and production are in this circuit to amplify the productive angle of power since *A* draws on these mechanisms and techniques to ensure *B*'s compliance.

System integration concerns the CoP through techniques of domination because the facilitative conception of power sees the episodic exercise of power as always beginning from conditions. Although this frequently occurs through a 'zero-sum conflict', Clegg believes it is not automatic because in a relational field the empowerment of relatively more powerful and weaker agencies may simultaneously occur. Having discipline and production in one circuit also recognises that methods of production entail methods of discipline (Foucault 1979, Ransom 1997). Discipline normally attempts to achieve the subordination of individual agencies to collective objectives. Disciplinary practices rely on the surveillance of organisational members through the collection, recording and comparison of data about their activities (Keen 1981, Markus and Pfeffer 1983). To Clegg these 'disciplinary practices' are micro-techniques of power meant to inscribe and normalise not only individuals but also collective, organised bodies because,

> "Surveillance, whether personal, technical, bureaucratic or legal, is the (central power) issue. Its types may range through forms of, for instance, supervision, routinisation, formalisation, mechanisation and legislation, which seek to effect increasing control of employees' behaviour, dispositions and embodiment, precisely because they are organisation members (Clegg 1989)."

Apart from direct control, surveillance can take forms like cultural practices of moral endorsement, enablement and suasion to more formalised technical knowledge. Clegg's notion of discipline encompasses Foucault's ideas of hierarchical observations, normalising judgements and examinations and views focusing on rationalised obedience in form of authority (Weber 1964).

Therefore, system integration is vital circuit because it is a source of resources for power, subject to competitive pressure. Competition depends on passage ways made obligatory by the fixing of rules of practice at the facilitative core of power. The circuit focuses on the empowerment and disempowerment of the capacities of agencies, whose strategic value relies on changes in techniques of production and discipline. However, to Clegg the process is double-edged. Although it is oriented towards environmental resources, their retention relies on stabilisation in rules of practice as an obligatory passage point through which an agent's reproduction must pass in the social integration circuit. By affecting the capacities of agencies, system integration introduces potent uncertainty and dynamism in power relations via innovation in techniques of production and discipline. This presents opportunities for challenging established episodic power configurations because it generates competitive pressures through new techniques and forms of discipline. After Lockwood (1964), Clegg writes transformation,

> 'Of an existing configuration of power ...will ... arise "from a '**lack of fit**" between its core institutional order and its material substructure", and "will be characterised by a typical form of 'strain' arising from the functional incompatibility between its institutional order and material base".'

Contrary to Marxist and functionalist perspectives, these processes are not automatic. The outcome depends on whether agencies can take control of the 'nodal' or OPPs enabled by the system and social integration circuits or not. The agencies need to establish networks and alliances of control to use the techniques of production and discipline as pathways for ushering in new standing conditions. Eventually the agencies need to translate the new rules and norms implied by an information system into discourses that other agencies can understand and accept as ready-to-hand (Introna 1997).

Like social integration, changes in the system integration circuit are either endogenous or exogenous. The former are a result of episodic power outcomes that may enhance innovation in techniques of production and discipline. However, exogenous changes result from environmental contingencies, which may interrupt the fields of force in the system integration circuit. Clegg cautions that whereas circuits as terms are 'integrative' they can as well be disintegrative particularly where exogenous sources of change are involved. The receptivity of exogenous factors relies on OPPs and rule fixing.

Chapter summary

Scholars agree that power is probably the most fiercely contested concept. Some have suggested that since there is bound to be perpetual disagreement, social science should simply discard the elusive concept. The discord has roots in the different worldviews pursued by scholars of power. For instance, while positivists regard power as directly observable and measurable other scholars simply regard it is as property of relations.

Wary of calls for the banishment of the power concept, we followed the lead of other IS researchers and adopted the Circuits of Power framework because it provides a central tradition of power that incorporates different debates and offers well-grounded alternative conceptions. The framework does not advocate a single sovereign power conception but distinct circuits. Each circuit relies on effective organisation whose form is subject to pressures of reproduction and transformation in each of the circuits of social and system integration. Whether system disintegration or contradiction leads to transformation and new rules depends on the network of power and passage points achieved through episodic power's configuration of the organisational field at the social organisation level.

CHAPTER 4: RESEARCH DESIGN

Introduction

This Chapter discusses the philosophical underpinning of our methodological approach and places our work within the wider IS research traditions. We highlight the theoretical concepts upon which our research is based because behind every method lies a belief about the nature of the world and knowledge (Mingers 2001). We cannot overstate the value of providing the supporting theory of reality for such a contested concept like power. As discussed previously, we adopted the Circuits of Power (CoP) framework because it provides a central tradition of power that incorporates different debates and alternative conceptions.

The chapter is organised as follows. First, we present the philosophical underpinnings of information systems research covering the positivist, interpretive, and critical stances. We focus on the interpretivist approach because it best grasps the elusive and contested essence of power and politics. The next section examines the case study research strategy. We thereafter reflect on our rationale for selecting the two field studies, the data sources and the role of the CoP framework as data collection and analytical tool for this research.

Philosophical assumptions

Zuboff (1988) argues that behind every method lies a belief about the nature of the world and knowledge (Mingers 2001) because researchers pursue different worldviews (Creswell 1994). She believes researchers should state their theory of reality and how that reality surrenders itself to knowledge seeking efforts (Zuboff 1988). To Creswell (1994) the assumptions cover the nature of reality (ontological); relationship between the researcher and subject (epistemological); role of values (axiological); the language of research (rhetorical) and the process of research (methodological) (Burrell and Morgan 1979). The assumptions jointly form a paradigm because they are constructs of thought about the social world (Creswell 1994, Mingers 2001). We focus on epistemological assumptions because this chapter discusses our research decisions.

Epistemology

Epistemology deals with assumptions about the grounds of knowledge. It focuses on ways of understanding the world and communicating this as knowledge to other human beings (Burrell and Morgan 1979). Epistemology defines obtainable forms of knowledge and ways of ensuring that it is 'true' or appropriate evidence and its character. Knowledge could be real and transmittable in a tangible form. Alternatively, it could be of "a softer, more subjective, spiritual or even transcendental kind, based on experience and insight of a unique and essentially personal nature (Burrell and Morgan 1979)." The assumptions enable researchers to ascertain what constitutes good evidence and ways of gathering it properly. However, to Zuboff, epistemological basics are subject to debate but not to ultimate proof. She adds,

> "Each epistemology implies a set of methods uniquely suited to it, and these methods will render the qualities of data that reflect a researcher's assessment of what is vital. I believe that **researchers ought to indicate something about their beliefs, so that readers can have access to the intellectual choices** that are embedded in the research effort (Zuboff 1988)."

Likewise, Burrell and Morgan (1979) believe the failure to broach underlying viewpoints about the social world often sows doubts about the credibility of research findings. The widely used classification of IS research epistemologies into positivist, interpretive, and critical stances (Klein and Myers 1999, Orlikowski and Baroudi 1991) follow the work of Wai Fong Chua in the Accounting discipline. She argues that Accounting research traditionally emphasised, "physical realism, hypothetico-deductivism, the natural tendency toward social order, and a 'value-free' position in terms of the relationship between theory and practice." Highlighting the severe limitations of this mainstream theory, she calls for the appreciation of the role and meaning of accounting data in action (Chua 1986). Next, we discuss the underlying beliefs of the three approaches.

Positivism

Positivists believe that "objective" data can be collected from "out there" independent of researcher preconceptions and can be used to test prior hypothesis or theories (Creswell 1994, Klein and Myers 1999, Walsham 1995a). From this view, the world is characterised by order rather than discord. The "social structures of reality are 'found', 'observed' or 'modelled' rather than 'interpreted' or 're-created' (Torvinen and Jalonen 2000)." Positivism views the social world as a hard, external and an objective reality. Hence, researchers analyse the relationships and regularities between various elements.

Lee (1991) associates positivist research with inferential statistics, hypothesis testing, mathematical analysis and experimental and quasi-experimental design. To Orlikowski and Baroudi (1991) the paradigm is part of the scientific or empirical-analytical tradition characterised by formal propositions, quantifiable measure of variables, hypothesis testing and drawing of inferences about a phenomenon from the sample to a stated population (Galliers 1991). Positivism is also deterministic. Individuals respond in a mechanistic fashion to situations they encounter in the external world (Burrell and Morgan 1979). Thus, individuals and their experiences are "products of the environment; one in which humans are conditioned by their external circumstances." After Bleicher (1982), Galliers (1991) argues that positivists insist,

> "The empirical-analytical method is the **only valid approach to improve human knowledge**. What can't be investigated using this approach can't be investigated at all scientifically. Such research must be banned from the domain of science as 'unresearchable.'

Methodologically, the focus is on the concepts themselves, their measurement and the identification of underlying themes (Burrell and Morgan 1979, Walsham 1993). Creswell (1994) links the positivist paradigm to quantitative studies that statistically test theory to determine whether predictive generalisations hold true.

An extensive study of IS literature by Orlikowski and Baroudi (1991) revealed that although there was no theoretical or topic congruence among researchers, positivism was the most dominant philosophical worldview (Galliers and Land 1987, Lee 1991). To Walsham (1995a) positivism has the status of tacit knowledge in mainstream IS literature because it needs less or no argument to support it. When effort is concentrated in a limited area of theoretical assumptions, it generates orthodoxy so dominant that,

> "Its adherents often take it for granted as right and self-evident. Rival perspectives within the same paradigm or outside its bounds appear as satellites defining alternative points of view. Their impact upon the orthodoxy, however, is rarely very significant. They are seldom strong enough to establish themselves as anything more than a somewhat deviant set of approaches. As a result, **the possibilities which they offer are rarely explored, let alone understood** (Burrell and Morgan 1979)."

The authors claim they developed their feted "Four Sociological Paradigms" out of concern, "about *academic sectarianism* reflected at various times in open hostility, ostrich-like indifference and generally poor quality dialogue and debate between essentially related schools of thought." Our research follows the interpretive tradition.

Interpretivism

The growing criticism of positivism and the quest for alternative epistemological and methodological foundations has increased the appeal of interpretive research (Bryman 1988). Indeed, the claim of interpretivism as a valid approach of inquiry has penetrated mainstream IS to an extent that it is taken seriously, at least in methodology research literature (Walsham 1995a). Lee (1991) believes the interpretive approach has gained attention as an alternative to positivist research because natural science does not effectively handle social reality. However, hurdles remain because, "It is safer for authors to stick to positivist orthodoxy (Walsham 1995a)."

Lee (1991) associates interpretivism with procedures such as ethnography, hermeneutics, phenomenology and case studies. Interpretivism is linked with voluntarism because it,

> "Attributes to human beings a much more creative role: with a perspective where 'free will' occupies the centre of the stage; where **man is regarded as the creator of his environment**, the controller as opposed to the controlled, the master rather than the marionette (Burrell and Morgan 1979)."

Voluntarism prizes the subjective experience of individuals in creating, modifying and interpreting their social world. Therefore, interpretivism assumes that people create and associate their own subjective and intersubjective meanings as they interact with the world around them (Orlikowski and Baroudi 1991). Lee (1991) insists the adjective 'subjective' is not a synonym for 'biased', 'opinionated' or 'untestable' but refers to the meaning held by the observed human subject. To Orlikowski and Baroudi (1991) interpretive studies reject the notion of "objective" or "factual" actual accounts of events and situations and instead seek relativistic, albeit shared, understanding of phenomena (Burrell and Morgan 1979). As such, multiple realities exist in any given situation because the researcher, the subject and study readers have different views (Creswell 1994, Mumford 1985, Walsham 1995a). Interpretivists focus on the complexity of human sense making as the situation emerges and attempt to understand phenomena through the meanings that people assign to them (Giddens 1984, Jones 1999, Walsham 1993). In general,

> "Interpretivists argue that organisations are not static and that the relationships between people, organisations and technology are not fixed but **constantly changing**. As a consequence, interpretive research seeks to understand a moving target (Klein and Myers 1999)."

To Walsham (1995a) value-free data is unobtainable in interpretive studies because inquirers use their own notions to guide the study (Mingers 2001). Hence, there is no objective reality to discover and replicate because theories of reality are just ways of making sense of the world (Walsham 1993, Zuboff 1988). To Orlikowski and Baroudi (1991) interpretivism does not seek generalisations about a population but attempts to understand the deeper structure of a phenomenon with the belief that this can inform other settings (Kettinger and Lee 2002, Markus 1983). Thus, interpretive research takes,

> "A nondeterministic perspective where the intent of the research was to increase the understanding of the phenomena within cultural and contextual situations; where the **phenomenon of interest was examined in its natural settings** and from the perspective of the participants and where researchers did not impose their outsiders' *a priori* understanding of the situation (Orlikowski and Baroudi 1991)."

Therefore, the researcher is able to represent 'reality' from the voices and interpretations of the informants (Creswell 1994, Galliers 1991). Klein and Myers (1999) believe interpretive research can produce deep insights into IS phenomena because it focuses on human thought and action in organisational settings. To Galliers (1991) this follows an in-depth self-validating process, in which the continual questioning of the presuppositions leads to a better understanding of the phenomena under study.

Qualitative methods

Klein and Myers (1999) argue that while interpretive research does "not subscribe to the idea that a pre-determined set of criteria can be applied in a mechanistic way, it does not follow that there are no standards at all" to judge it (Buchanan *et al.* 1988). The paradigm is often associated with qualitative studies or,

> "An inquiry process of understanding a social or human problem based on **building a complex, holistic picture**, formed with words, reporting detailed views of informants, and conducted in a natural setting (Creswell 1994)."

The rising interest in qualitative research is a product of dissatisfaction with quantitative techniques. To Benbasat *et al,* (1987) the concern stems from the complexity of multivariate research methods, the distribution restrictions, large sample sizes and the sheer difficulty of understanding the results. Franz and Robey (1984) state that because rational and non-rational or political myths coexist and complement each other during IS implementation, qualitative research best captures the two sets of stories.

Silverman (1998) believes the major attraction of qualitative research is its ability to reveal how humans interact. Qualitative research has the "ability to focus on actual practice *in situ*, looking at how organisations are routinely enacted (Silverman 1998)." However, Silverman rejects the "fashionable identification of qualitative method with an analysis of how people 'see things', preferring to focus instead on how people 'do things' (Bryman 1988)." He insists researchers should question the belief that the qualitative approach is only 'exploratory' or 'anecdotal'. He believes case study methods can examine large datasets with standard issues of 'reliability' addressed through systematic transcription of data.

However, to Klein and Myers (1999) the word interpretive is not always a synonym for qualitative because, depending upon on the underlying philosophical assumptions of the researcher, qualitative research may or may not be interpretive. Similarly, Walsham (1995a) argues that the interpretivist school is not homogeneous in its knowledge claims. Carroll and Swatman (2000) agree. They argue that qualitative research covers a plurality of research paradigms - positivist, interpretive and critical - with which there are many research methods – case studies, field studies, ethnography and action research – processes and techniques. They stress that while there is no agreed doctrine underlying all qualitative social research (Markus and Lee 1999, Silverman 1998), it is generally the collection of data in the form of words and images, which is analysed by methods that do not include statistics or quantification (Carroll and Swatman 2000).

Markus and Lee (1999) also argue that what researchers often refer to, as qualitative or interpretive research is not one method, but many methods, each with its own appropriate and different criteria of evaluation. Consequently, they coin the term "intensive research" to describe qualitative research to signal the variety of methods in this field (Markus and Lee 1999). Since, interpretivism is not a dominant approach in IS research (Orlikowski and Baroudi 1991, Walsham 1995a), the tendency to lump dissimilar methods into a collective term tempts journal editors, reviewers and readers to apply a single criteria inappropriately to all studies under the label. However, the lack of understanding is mutual because,

> "While intensive researchers have been, unfortunately, habituated to the application of inappropriate criteria to intensive research by some colleagues who specialise in quantitative methods (a practice that, fortunately, has been lessening recently), we have been shocked and dismayed by a similar lack of **'professional courtesy'** by intensive research specialists (Markus and Lee 1999)."

However, Carroll and Swatman (2000) warn that this array of research approaches poses theoretical and practical problems for researchers. A cardinal theoretical concern is the difficulty of assuring the quality of qualitative IS research. Even the choice of the 'best' paradigm and method does not guarantee good qualitative research because success largely hinges on the experience and sensitivity of the researcher. For instance, Silverman (1998) reveals that while many qualitative researchers see their aim as being able to 'see through the eyes' of subjects, others would see this aim as 'subjectivist' and even 'journalistic.' The scientific school also dismisses claims that open-ended, qualitative interviews give direct access to 'experience' insisting that common-sense reasoning influences what this means (Galliers 1991, Silverman 1998).

Critical perspective

According to Orlikowski and Baroudi (1991), this stance questions the status quo through the exposure of deep-seated, structural contradictions within social systems. The purpose of this critique is to identify and fight restrictive social conditions. Likewise, Klein and Myers (1999) argue that research takes a critical stance if it brings to light restrictive and alienating conditions. To Orlikowski and Baroudi (1991) these are taken-for-granted assumptions about organisations and information systems. The goal of the research is to provide a dialectical analysis that reveals the historical, ideological, and contradictory nature of existing social structures (Orlikowski and Baroudi 1991).

Klein and Myers (1999) regard critical research as emancipatory because it attempts to eliminate the causes of unwarranted alienation and domination and hence enhance the opportunities for realising human potential. Critical theorists assume that agencies can consciously act to change their social and economic conditions. However, the theorists "recognise that human ability to improve their conditions is constrained by various forms of social, cultural and political domination as well as natural laws and resource limitations (Klein and Myers 1999)."

Plurality of perspectives

From the ontological assumption of multiple interpretations for any social phenomena (Creswell 1994, Galliers 1991, Walsham 1995a), interpretivists believe that the positivist claim of being the only valid approach for improving human knowledge is injudicious. Interpretivists argue that in its broadest definition information systems is essentially a pluralistic field that draws on and provides a nexus for many diverse research fields and disciplines (Dahlbom 1997, Mingers 2001). Interpretivists have also challenged basic aspects of positivism. For instance, Silverman criticises the 'objectivity' claims of surveys and other quantitative research methods. He insists that while 'properly' designed questionnaires appear to deliver valid and reliable quantifiable information,

> "Respondents' **answers to survey questions are inevitably abstracted from the day-to-day business of actually operating the system**. Thus, there may be a world of difference between the contingencies of working with a given piece of IT and responding to a questionnaire about one's 'attitudes' towards the system (Silverman 1998)."

Silverman claims surveys depend upon a 'positivistic' model, which assumes that 'tools are discrete entities' (King 1996). However, since artefacts only become tools in practice (Star and Ruhleder 1996) this view is problematic. Orlikowski and Baroudi (1991) add that if we agree that IS are complex (Kling and Dutton 1982, Newell *et al.* 2000, Rolland and Monteiro 2002, Star and Ruhleder 1994), then multiple perspectives allow the exploration of the phenomena from diverse angles. For instance, while qualitative methods describe well the socially constructed world (Walsham 1993, Walsham 1995a), quantitative research has better tools for defining, counting and analysing variables (Creswell 1994). Hence, a plurality of views should enrich IS research (DeSanctis 1993, Markus and Lee 1999, Mingers 2001).

Markus and Lee (1991) call for the clarification of evaluation criteria for intensive methods to improve acceptance and appreciation of diversity within the community and across the intensive/quantitative divide (Walsham 1995a). Since the polarities between qualitative and quantitative research largely serve didactic purposes,

> "It is inaccurate to assume that quantitative and qualitative research are polar opposites. ...For, of course, there are no principled grounds to be either qualitative or quantitative in approach. **It all depends upon what you are trying to do**. ...Indeed, often one will want to combine both approaches ...just as quantitative researchers would resist the charge that they are all 'positivists' ... there is no agreed doctrine underlying all qualitative social research (Silverman 1998)."

Burrell and Morgan (1979) claim, "To understand a new paradigm one has to explore it from the inside, in terms of its own distinctive problematic." Lee (1991) also dismisses the belief that the approaches are opposed and irreconcilable. He offers a framework to show that the approaches can be mutually supportive rather than exclusive. However, Walsham (1995a) warns that interpretivists would strongly oppose Lee's views because they confuse and conflate contradictory epistemological positions. In conclusion, Markus and Lee (1999) call an end to these "paradigm wars" arguing that methodologies in themselves, like algebraic symbols, are formalisms, devoid of empirical content.

Information Security philosophical roots

Galliers (1991) writes that after positivistic claims that if a phenomena cannot be investigated by empirical-analytical methods it can never be studied scientifically, a number of IS researchers have been led into 'illogical' conclusions that,

> "1. Every real phenomenon can be measured
> 2. If it can't be measured, it's not real
> 3. If it can be measured, it is real."

Galliers and Land (1987) also express concern about the primacy within IS of traditional, empirical research more suited to the natural sciences to a near exclusion of different research perspectives that nevertheless make good contribution to knowledge (Mumford 1985, Orlikowski and Baroudi 1991). Nowhere in IS are these practices more prevalent than information security research. A brief background will suffice. Computer security, as a discipline, originated from research laboratories of computer manufacturers and the mathematics departments of universities (Dorey 1991). As these roots suggest, methods of information security implementation have relied on the traditional approach to systems analysis also known as hard systems thinking (Hitchings 1995). Hard systems thinking starts from the premise of a carefully defined objective that systems engineers take as given (Hirschheim and Klein 1989, Hirschheim and Klein 1994). However, this approach is problematic in "messy, changing, ill-defined problem situations" (Checkland 1981, Checkland 1989, Checkland and Scholes 1990) that characterise organisational life.

Hitchings (1995) argues that despite the recent barrage of criticism directed at hard systems thinking in systems design (Mathiassen and Stage 1992), security methods still rely on this approach. The approach originates in the functionalist paradigm (Burrell and Morgan 1979, Knights and Murray 1994). Put briefly, functionalists rely on objective and empirical scientific methods to discover binding laws of causality for establishing cohesive and stable social structures (Burrell and Morgan 1979, Dhillon and Backhouse 2001, Latour 1991) like infrastructures. Similarly, technical security attempts to eradicate uncertainty in work routines by reducing exceptions (Stinchcombe 1968).

From a value-consensus standpoint, rationalists believe the suppression of exceptions is a legitimate pursuit because they expect all organisational actors to contribute to common objectives (Etzioni 1964). Organisations use infrastructures because managers view exceptions as illegitimate, disruptive and costly activities (Knights and Murray 1994, Romm and Pliskin 1997). Technical security as encapsulated in the CIA (confidentiality, integrity and availability) model also supports the value consensus view. Because by stopping the unauthorised disclosure, modification and withholding of information, the model focuses employees on their assigned tasks in support of common organisational objectives. However, compliance is difficult to achieve because as segmented institutionalists argue, individuals and subgroups have conflicting goals leading some to view security as a hindrance to getting work done (Parker 1997, Schwartau 1998).

Objective social science known as 'sociological positivism' (Dhillon and Backhouse 2001) informs most information security work. The approach applies models and methods derived from natural science to study human affairs. However,

> "**Critics point to the futile search for the same type of knowledge as found in nature science,** which can be characterised as analytical and value free and with only occasional efforts that consider the subjectivism of the applications (Dhillon and Backhouse 2001)."

Because this literature relies on a value consensus proposition, it sees security problems as purely technical not social or organisational (Knights and Murray 1994). The mixed interest nature of organisations links conflict, power and politics to security practice (Hirschheim and Klein 1989). Besides, since systems succeed or fail on their ability to transcend these problems, the natural scientific approach is problematic because,

> "**Science ...does not inquire after the motives of an action,** as if these have been present in consciousness before the action; but it first breaks up the action into a group of mechanistic phenomena and seeks the previous history of this mechanistic motion – but it does not seek it in feeling, sensation, thinking. It can never take the explanation from this quarter: sensation is precisely the material that is to be explained (Nietzsche 1968)."

The literature reliant on functionalist views is not useful in understanding power because it ignores the telling impact of people (Backhouse 1997, Hitchings 1995) in security practice. Consequently, in a departure from security orthodoxy, we adopted an interpretive approach to underpin our study of the role of power and politics in PKI institutionalisation. We believe we can understand organisational power plays better if we appreciate the assumptions and intersubjectively shared meanings that people assign to events and actions. Using interactive interpretive techniques, chiefly interviews, we assess both the formal power structures and politics (Pfeffer 1992, Silva 1997). Next, we consider the assumptions behind methodologies.

Research Strategy

Burrell and Morgan (1979) argue that ontological and epistemological assumptions about the relationship between human beings and their environment have direct methodological implications. They propose *nomothetic* and *ideographic* approaches as two broad methodological choices. The *nomothetic* view is associated with the objective dimension of social science and stresses the role of systematic protocols and techniques. Like natural science, nomothetic approaches focus on rigorous hypothesis testing using quantitative techniques such as surveys, questionnaires and personality tests (Burrell and Morgan 1979, Creswell 1994, Galliers 1991). This approach seeks general laws and restricts itself to procedures acceptable to exact science (Luthans and Davis 1982). Until recently, IS research in a "rush for scientific respectability" had opted for this approach leading to the shunning of approaches such as traditional case studies because they were deemed not 'scientific enough' (Franz and Robey 1984, Luthans and Davis 1982).

The *ideographic* perspective is associated with the subjective dimension. The main emphasis is that researchers can only properly understand the social world by obtaining first-hand knowledge of the subjects under investigation (Burrell and Morgan 1979). Research includes detailed explorations of the background and life history of the subject. The findings give researchers insights into the life of the subject revealed in impressionistic accounts. Overall, "the ideographic method stresses the importance of letting one's subject unfold its nature and characteristics during the process of investigation (Burrell and Morgan 1979)."

The dichotomy is largely artificial because the two approaches overlap and can profitably be combined to enrich IS knowledge (Luthans and Davis 1982). However, Franz and Robey (1984) argue that because of threats to internal validity and the virtual impossibility of experiment control, it is questionable whether "many scientifically-based conclusions can be drawn from IS implementation in the real world." They believe that other than using control groups, researchers can address threats to validity with intense data collection using a variety of measurements. Thus, Franz and Robey (1984) advocate the ideographic approach in IS research because it provides more in-depth explanation (Luthans and Davis 1982) of particular events and their context (Benbasat *et al.* 1987) than the nomothetic approach.

Rationale for Case Study strategy

Our methodological stance follows the *ideographic* approach. Although some scholars see power as directly measurable and hence observable through scientific study, we believe the subjective orientation of the ideographic approach better informs research of this fundamentally disputed concept. Since, we do not regard power as a 'thing' but as a relational concept manifest in outcomes, we required a research strategy that could elicit the intersubjectively shared meanings that agencies assign to outcomes of power. We chose a case study approach. Next, we discuss the key features of case study research and its efficacy in illuminating socially constructed reality.

Benbasat *et al,* (1987) argue that there is no standard definition of a case study (Cavaye 1996). Likewise, to Yin (1994) the most commonly encountered definitions of case studies merely repeat the types of topics researched with the strategy. He believes the citing of topics such as 'organisations', decisions' and 'processes' is insufficient for establishing the needed definition for a case study. Yin reveals that most social science textbooks completely disregard the case study as a formal research strategy because scholars consider it an exploratory stage for other research strategies. However, to Benbasat *et al,* (1987) the unique feature of case studies is that they examine a phenomenon in its natural setting, employing multiple methods to gather information from entities such as people, groups or organisations. This is similar to the definition of interpretive research (Orlikowski and Baroudi 1991).

Yin (1994) argues that the choice of a research strategy depends on the type of research questions, the control an investigator has over the actual behavioural events and the focus on contemporary as opposed to historical phenomena. He believes case studies uniquely contribute to knowledge of individual, organisational, social and political phenomena because they allow an investigation to retain the holistic and meaningful characteristics of real life events. He believes case studies are desirable when, "a 'how' or 'why' question is being asked about a contemporary set of events over which the investigator has little or no control (Yin 1994)." This is because these explanatory questions deal with operational links and require tracing over time rather than assessment of mere frequencies or incidence. Benbasat *et al,* (1987) also emphasise the emerging nature of case study strategy by arguing that, to a degree, researchers have a little a *priori* knowledge about key issues and their handling.

We chose this strategy because we asked 'how' and 'why' questions, expected little control over the research environment and we focus on contemporary phenomenon within real-life contexts. This strategy is appropriate because our focus is on how power and politics enable public key infrastructures to become part of real-life contexts (Benbasat *et al.* 1987). Indeed, PKI institutionalisation occurs when the "boundaries between phenomenon and context are not clearly evident (Yin 1994)."

Although some authors associate this strategy with the scientific research tradition (Checkland 1981, Galliers 1991, Lee 1989), case studies are a preferred strategy for interpretivist research (Benbasat *et al.* 1987). Walsham (1993) claims, "The most appropriate method for conducting empirical research in the interpretive tradition is the in-depth case study." However, authors like (Cavaye 1996, Eisenhardt 1989, Galliers 1991) disregard the appropriation of the strategy by either positivist or interpretivist researchers and stress that case studies can be of either tradition. This is because case study research,

> "Can be a highly structured, positivist, deductive investigation of multiple cases; it can also be unstructured, interpretative, inductive investigation of one case; lastly, it can be anything in between these two extremes in almost any combination (Cavaye 1996)."

She believes the versatile and pluralistic nature of the strategy has led to confusion because authors only present specific variations. She is concerned that while researchers such as (Lee 1989, Walsham 1995) acknowledge other types of case research, others such as (Benbasat *et al.* 1987) present their own versions as if they were the only type. Cavaye (1996) insists there is no one 'best way' of conducting case research and all variations are legitimate uses of the strategy. Lee (1989) argues that efforts to clarify the methodological basis for conducting case studies continue in reaction to accusations that they are not 'scientific enough' (Franz and Robey 1984, Luthans and Davis 1982). He claims that although natural scientists are the loudest critics of this strategy, a scientific methodology actually complements and supports the methods traditionally associated with the case study.

The failure by researchers to decide whether case research represents a strategy or just a method also causes confusion. After Weick (1984), Galliers (1991) describes methods as ways of systematising observation. We believe a research strategy is a synonym of what Galliers calls an approach because it defines a way of going about one's research (Yin 1993, Yin 1994). Like strategies, approaches are more generic than methods because they may embody a particular style and employ different methods or techniques (Galliers 1991). Indeed, Yin (1994) stresses that the case study is neither a data collection tactic nor merely a design feature but a complete research strategy.

In line with the ideographic approach, Galliers (1991) sees case studies as common strategies for studying 'real world' situations in information systems. A key strength of the strategy is its ability to facilitate the understanding of complex 'reality' in considerably more detail than most other approaches. This is because case studies draw on a wide array of techniques. For instance, while a case study may rely on similar techniques as a history,

> "It adds two sources of evidence not usually included in the historian's repertoire: direct observation and systematic interviewing. ...**the case study's strength is its ability to deal with a full variety of evidence – documents, artefacts, interviews, and observations – beyond what might be available in the conventional history study** (Yin 1994)."

Benbasat *et al.* (1987) see three fundamental reasons for the value of case research in information systems. First, researchers study IS in their natural settings and learn about the state of the art from which they can generate theories for improving practice. Second, as Yin (1994) argues, case studies are suited for answering 'how' and 'why' questions, which are invaluable in explaining the complexity of IS implementation. Lastly, case studies are suited for studying phenomena with little previous information. This applies to most IS because the rapid rate of innovation brings new twists even to established technologies that could generate valuable insights for building theories (Eisenhardt 1989).

Case study types

From a theoretical standpoint, Yin (1993) identifies three types of case studies. They are, causal, exploratory and descriptive. *Causal* case studies focus on cause and effect relationships in a study situation. This search generates causal relationships and explanatory theories of phenomena. *Exploratory* case studies represent the traditional type of case studies, which were normally part of other research strategies. Data collection occurs before the formulation of theories or specific research questions (Yin 1993). Yin (1994) believes this application of case studies is a major reason why many social science textbooks disregard the approach as a formal research strategy (Walsham 1995a). This research adopted the descriptive case study. *Descriptive* case studies require the selection of a theory in advance of research design and data collection and use it to guide the two research stages. As such,

> "This theory should be openly stated ahead of time, should be subject of review and debate, and will later serve as the 'design' for a descriptive case study. The more thoughtful the theory, the better the descriptive case study will be (Yin 1993)."

Case study designs

Yin (1994) regards a case study design as the logical sequence that connects the empirical data to a study's initial research questions and, ultimately, to its conclusions. "The main purpose of the design is to help to avoid the situation in which the evidence does not address the initial research questions. In this sense, a research design deals with a logical problem and not a logistical problem." The designs can either be *single* or *multi-case* studies. Within the two types there can also be unitary or multiple units of analysis. Therefore, Yin proposes four types of designs namely: single-case (holistic); single-case (embedded); multi-case (holistic) and multi-case (embedded).

Single-case study is appropriate under several conditions. First, when it represents a critical case in testing a well formulated theory. Second, this design is useful if a case represents an extreme or unique case. A third rationale is revelatory when the case offers the researcher an opportunity to observe and analyse phenomena previously inaccessible to scientific investigation. A key risk with this design though is that the case may not turn out as unique or revelatory as expected (Lee 1989). Single-case (embedded) studies are one where the same case involves more than one unit of analysis. However, a case is single (holistic) if it covers a whole organisation or program.

We adopted the *multiple-case* design. Yin argues that the evidence from multiple cases is more compelling and scholars believe the overall study is more robust. Besides the rationale for single-case studies is hard to support because, "the unusual or rare case, the critical case, and the revelatory case are all likely to involve only single cases, by definition (Yin 1994)." However, we admit the multi-case design, "is resource intensive, intellectually challenging and highly demanding of the social and political skills (Pettigrew 1990)" of the researcher.

Like experiments, multiple case designs follow 'replication' instead of "sampling" logic. Sampling involves enumerating an entire universe of respondents and selecting a subset of it deemed representative of the entire pool. Yin believes applying a sampling logic to case studies would be misplaced for the following reasons. First, case studies are generally not appropriate for assessing the incidence of phenomena. Second, since case studies cover both the phenomenon and its context, they normally yield many potentially relevant variables. Third, a sampling logic could make the empirical research of vital topics impossible because some generate too many variables. After Yin, we selected the two cases to assess whether they produced similar results (literal replication) or gave contrasting results but for a predictable reason (theoretical replication). We took each case as a 'whole' study and sought convergent evidence and conclusions from it, which we compare with the second case.

Case Study research controversies

To Yin (1994), perhaps the greatest concern over case study is the claimed lack of rigour. He argues, "Too many times, the case study investigator has been sloppy and has allowed unequivocal evidence or biased views to influence the direction of the findings and conclusions." He believes the biggest obstacle to wider case study application is the limited codification of its research designs. Thus, researchers need to report all evidence fairly.

Positivist researchers identify an additional limitation of case studies as, "the lack of control of individual variables – and hence the difficulties in distinguishing between cause and effect (Galliers 1991)." The problem associated with distinguishing between cause and effect, are, to a degree, circumvented by undertaking longitudinal case studies (Romm and Pliskin 1997). To Pettigrew (1990) the longitudinal case method provides the opportunity to examine continuous processes in context and draw in the significance of various interconnected levels of analysis. Similarly, Franz and Robey (1984) argue that longitudinal data collection improves the measurement validity and offers alternative interpretations for events. Validity improves because data collection occurs as events occur. Different interpretations are easy to seek because activities ostensibly undertaken for rational reasons, to say deliver a better system, may also serve political interests of the actors. Thus, by recording activities as they happen with the respondents' interpretations, longitudinal studies elucidate both the cause and effect of the events.

Critics see the assignment of different interpretations to observations by stakeholders as problematic because of bias concerns. However, Yin (1994) believes the accusation is unfair. He insists bias can also enter into the conduct of experiments and the use of other research strategies such as designing questionnaires for surveys or conducting historical research. However, he concedes that case studies are more prone to risks of bias because not all researchers adequately overcome the problems.

Yin (1994) reveals critics have also downplayed the usefulness of case studies because they reportedly take too long, generating a daunting mass of unreadable documents. He claims that while past procedures may have justified this, recent innovations in case research, including his book, would lead to change. He argues that the belief that case research necessarily takes time is borne out of a perception that wrongly confuses the strategy with specific data collection methods like ethnography and participant observation. Case studies do not solely depend on these methods. Indeed, Yin (1994) believes that depending on the topic, one could conduct a valid study without even leaving the library and telephone.

Selection of case study organisations

Huang (1997) argues that the selection of field studies depends on relevance and purpose. On relevance, the selection depends on the potential to "replicate or extend an emergent theory" (Eisenhardt 1989) from a substantive area. Regarding purpose, the number of field studies is a trade-off between theoretical understanding and generalisation (Huang 1997). Huang goes on to claim, "The greater the number of varied studies, the greater the possibility of generalisation achieved." However, this view perpetuates a sampling logic (Yin 1994). Together with controversies we discussed above, critics claim case studies have limited application because they are usually restricted to a single event or organisation, which makes it difficult to acquire "similar data from a statistically meaningful number of similar organisations (Galliers 1991)." The criticism is invalid because case studies are generalisable to theoretical propositions not universes (Yin 1994). The goal is "to do a 'generalising' and not a 'particularising' analysis," according to Yin.

Walsham (1993) believes the view of generalisation depends on the epistemology. He argues that statistical generalisability is vital under a positivist stance. However, for interpretivists, "the validity of an extrapolation from an individual case or cases depends not on the representativeness of such cases in a statistical sense, but on the *plausibility and cogency of the logical reasoning used in describing the results from the cases*, and in drawing conclusions from them (Walsham 1993)."

Bryman (1988) also insists inductive case studies are capable of addressing generality as long as it means theoretical rather than statistical aspects. He believes the problem of case study generalisation is not as recalcitrant as its traditional depiction implies. He draws on Glaser and Strauss (1967) whose notion of 'grounded theory' offered an alternative framework for generalisation different from that associated with the statistical criteria. He contends, "Case study researchers have often been very apologetic about the external validity of their findings, but there is a growing view that such diffidence may be unwarranted (Bryman 1988)." Next, we discuss our research decisions.

Background to research decisions

We regard this section as an important part of the dissertation because it explains our research decisions. This is vital because the decisions determined the data we gathered and the insights we drew from it. Pettigrew (1990) asserts that researchers should codify and organise the tacit knowledge acquired through empirical work for the benefit of scholars conducting similar studies. Hence, we support a call on researchers to state their epistemological stances because behind every method lies a belief (Mingers 2001, Zuboff 1988).

Buchanan *et al.* (1988) argue that while conventional textbooks gloss over the 'darker' realities of research, they are central to success in field studies. They claim it is common knowledge that "accounts in academic journals depart considerably from the research practices of their authors." Indeed, a growing body of IS literature takes a 'confessional' approach to illuminate actual research practices (Schultze 2000, Scott 2000). Scott (2000) coins the notion of 'Lived methodology' to encapsulate a situation where researchers appropriate methodologies and continually interpret them. She adds, these,

> "Abstract interpretive principles intensify into experience, and we are confronted by the dilemmas of **lived methodology**: the particular people, places and times that promise to condition the practice of one's IS research methodology (Scott 2000)."

Scott asserts that greater methodological openness would both reflect a growing self-confidence among IS researchers and support further development and understanding of interpretive research (Pettigrew 1990). Similarly, Schultze (2000) argues that if researchers render their actions, failings, motivations and assumptions open to scrutiny and critique, they put themselves on a par with their 'subjects' of study who feel exposed. Consequently, the deconstruction of the rigid dichotomy between theory and practice improves the expertise of IS researchers (Scott 2000).

To reiterate, we adopted the *multiple-case* study design. Since multiple case studies are useful for comparison purposes (Walsham 1993), this approach satisfied our goal of expanding and generalising theory and obtain insights to inform security practice. We looked for two global organisations that we could contrast in terms of structure and business because operational differences create varying security needs and hence PKI uses.

From the outset, we knew that relevance and purpose are key factors in deciding our candidate study organisations. An equally important driver was the possibility of gaining access. Why? In the first place, it is extremely difficult to gain academic research access (Huang 1997) because the deluge of requests makes many organisations feel over-researched (Buchanan *et al.* 1988). Second, we conducted our research during a global economic downturn during which academic research was not a prime concern for managers. Hence, the conditions demanded innovative responses to concerns about research disrupting work and commercial confidentiality (Buchanan *et al.* 1988).

A further issue was that we focused on an information security infrastructure. Public key infrastructures are restricted systems because computer security has traditionally been synonymous with secrecy (Russell and Gangemi Sr 1991). As if a security focus was not problematic enough, the subject matter of our study is power and politics. Within organisations, workers fear discussing politics because they suspect researchers could inform rivals (Buchanan *et al.* 1988). This owes to the semiotic nature of agency where agencies are both executors of action and carriers and creators of meaning (Clegg 1989, Silva 1997).

As such, we employed a "pragmatic, almost opportunistic approach" to getting access (Buchanan *et al.* 1988). To Buchanan *et al,* (1988) whatever well constructed views a researcher has about issues such as the nature of social research and data collection methods, this vision is constantly challenged by the practical realities, opportunities and constraints of conducting research. Zuboff (1988) advocates a similar approach when she states, "As a field researcher, I understood the importance of opportunism and serendipity." A realistic approach was helpful because organisations are bounded institutions to which one must seek, negotiate and gain access (Bulmer 1988).

Buchanan *et al.* (1988) advise researchers to "use non-threatening language when explaining the nature and purpose" of their studies. For instance, the terms 'research' and 'interview' have strong negative connotations. Therefore, our first measure was to use the words "power and politics" sparingly because they are so emotive. During our research requests, we stated that we were interested in the "Organisational and management implications of introducing a PKI." We hoped to explore the impact of the PKI on organisational roles and responsibility, procedures and rules for information access. We also focused on the benefits or problems different groups may have experienced with the infrastructure. The "high level" phrases actually add up to the main thesis of the CoP framework – how agencies achieve outcomes of power and how these relations are stabilised long enough to generate the effects and conditions of power (Law 1991b). We should stress that we did not follow,

> "A 'free for all' or 'anything goes' approach to data collection, in which you get what evidence you can anyway you can ... The claim for research as an art of the possible and the plea for opportunism do not therefore rule out the need for controlled, systematic, morally justifiable methods and scientific rigour (Buchanan *et al.* 1988)."

We selected the pragmatic approach because of its effectiveness in opening doors to the few organisations that had been able to implement this novel and sensitive technology on a large scale. The strategy did not divert us from the professional duty of writing an account that is plausible and interesting (Klein and Myers 1999). As subsequent chapters show, the 'high level' terms were so successful that respondents readily volunteered to discuss power and politics. We summarise the contributions of the approach in Chapter 8.

Procedure for getting case studies

Buchanan *et al,* (1988) warn that negotiating access to organisations, for the purpose of research, is a game of chance not skill. They insist that there is no conventional way to gain research access but suggest two ideas. First, they advise researchers to use friends and relatives, where possible, to gain access. Second, their talk of access being a game of chance, not skill, actually refers to serendipity (Zuboff 1988). Let us explain.

We hoped to research at two large global organisations, preferably engaged in different sectors, to contrast PKI usage and impacts. Although our focus was on big and important users of PKI, size was not an overriding factor because of the degree of novelty attached to using this technology on any scale at all (Radicati 1998). The Gartner Group reported in December 2000 that about 80% of available products and services were still restricted to pilot projects (Townsend 2001). Thus, while it was pleasing to get big PKI projects, novelty meant we would have been happy enough to get any good sized but operational project. Through contacts and serendipity, we gained access to two large and important PKI global deployments. We briefly reconstruct the story as follows.

We contacted candidate organisations in late 2000 after establishing the macro-criteria. We used the social, business and academic networks of the Computer Security Research Centre

(CSRC) and the Information Systems Department at the LSE to identify the candidates. At the time, the CSRC was engaged in a number of projects with commercial and government organisations in the United Kingdom, Switzerland and Italy that had big PKI projects. We did not make much progress due to the novelty and secrecy surrounding the PKI projects.

Our research breakthrough came in November 2000 and combined serendipity and the use of contacts. A fellow PhD student passed on an invitation to Infosecurity Europe at Olympia, London. The exhibition also hosts conferences. We attended a workshop organised by the European Electronic Messaging Association (EEMA). The association opened doors to organisations, offered tutorials, actual empirical data and the current thinking of leading PKI vendors. For instance, a flagship EEMA project, under its objective to promote global interoperation in an open environment, is the PKI Challenge (pkiC). The CSRC is a registered member of EEMA. We shall explore the EEMA contribution more under the data collection techniques. Next, we give a brief background of the organisations we studied.

Comparing the two organisations

This dissertation presents accounts of two global organisations that have implemented PKI on a large, albeit chaotic, scale. These firms belong to the energy and financial services sectors. We believed the different sectors would contrast PKI use and adoption process. However, the organisations also have common features. First, both are large businesses with offices in over a thousand global locations. For instance, the oil company has many people with important responsibilities away from the head office. The employees generate intellectual property that needs secure transmission. The firm also has numerous e-business ventures that have opened its network to external partners. Similarly, in response to internet pressures on margins, the Swiss bank provides banking "at any time, in any place, by any device." Thus, PKI is vital for the success of both organisations.

Second, the two sectors face some of the most stringent regulations in the world. The energy industry is subject to tough health and safety regulations. Companies must demonstrate good practice or risk heavy fines and/or damage to their brands. Likewise, the financial sector has suffered from tough regulations because of fears that alternative banking channels may siphon money value from the regulated banking industry. Regulators fear the money would go into the 'underground' economy undetected leading to money laundering (Comrie 1998, Gilmore 1993, Gilmore 1999, Hance and Balz 1996, Morgan 1998, Smith 1996). The noose is tighter because of recent corporate scandals and the so-called 'global war against terrorism.' The bank is also a leading player in wealth management in Switzerland where secrecy is vital. Thus, the bank needed a security system to support record keeping, detection and reporting of suspicious transactions and maintain an audit trail.

Because these are ongoing PKI projects, one of the conditions of access was that we conceal the real identities of our field organisations. Therefore, we refer to the oil company as Oilcom and the financial institution as Bankrecht. However, people familiar with both sectors may be able to individuate the organisations. We briefly outline how we got permission to research.

Oilcom

We first got a contact for Oilcom at an EEMA meeting organised at De La Rue offices in Basingstoke in February 2001. We got into conversation with a London-based Oilcom senior Security Consultant who was interested in our research topic. Fortunately, the consultant was an old friend of Dr James Backhouse, our supervisor. From his work with PKI at Oilcom, he agreed with our assertion that addressing the organisational impacts of this infrastructure remained the biggest challenge. He promised to help if we sent him a 'decent' proposal.

We later fortuitously discovered that a student who had taken the Security option on the MSc ADMIS course at the LSE, also worked on the same team at Oilcom as the senior Security Consultant. These two contacts initiated the access process after we sent them the research proposal. We met the second contact soon afterwards and conducted an impromptu interview that generated excellent insights into the objectives of the Oilcom PKI project. However, the research did not proceed as quickly as anticipated because the contact had global security responsibilities that frequently took him away from London. With hindsight, this was a good development because we used the period off-site to clarify our questions and during that time, the PKI project progressed and raised even bigger questions. During this period, we negotiated with Oilcom managers about time, confidentiality and the benefit the company would derive from the research. We largely used the strategy offered by Buchanan *et al,* (1988) where a researcher provides pre-emptive answers to these common concerns.

We made real progress when we found yet another ADMIS alumnus from the 2000/2001 class employed as a business consultant. We had attended the same 'Interpretation of Information' classes as part of the MPhil/PhD programme. Because the second gatekeeper was busy, the business consultant agreed to organise the interviews for us. This involved booking a meeting room – a contested commodity at Oilcom – and fetching more interviewees at the appropriate time. The research proper started in May 2001.

Bankrecht

Apart from the importance of security, another reason for targeting the financial services sector was a pragmatic one. The CSRC and the IS Department have extensive links with the City of London and the global financial community. Thus, we had a rich background and support network for research in this sector. Through our links with EEMA and the LSE, we contacted several members of Indentrus[16] LLC, a network of about 60 financial institutions worldwide that act as Identrus Certificate Authorities. We got good feedback.

While waiting for responses we serendipitously got permission to research at Bankrecht headquarters in Zurich and its London offices. In late 2001, we subscribed to *Information Security*, a good US trade publication. We liked the sceptical tone of a correspondent who said he worked for a large financial institution in London. For instance, to typify the farcical vendor hype which classifies every product as 'best in class' and 'leader', he hilariously rewrote his own profile to state he "is a *leading* infosec specialist and *leading* author who works for a *leading* bank in a *leading* European country." He supported the CSRC view that a purely technical logic cannot actually give security because at the end of any technical fix there is a person and a social system (Backhouse 1999).

In March 2002, he revealed that Bankrecht had a PKI project in Switzerland and promised to inquire about research access. In May, we got the contact of the Bankrecht IT Security Director and sent a proposal that pre-emptively answered concerns about time and confidentiality. We promised Bankrecht AG a quick report of our findings. In late May, Bankrecht granted us access on condition that we allowed the IT Security Director to conduct the interviews and return consolidated answers. The bank later allowed us to conduct all

[16] ABN AMRO, Bank of America, Bankers Trust (since acquired by Deutsche Bank), Barclays, Chase Manhattan, Citigroup, Deutsche Bank and HypoVereinsbank founded Identrus™ LLC.

interviews in Zurich on 23rd July 2002. We kept in touch with the respondents and got updates on the PKI project. From the Zurich discussions, we got contacts for PKI engineers at Bankrecht's investment division in London whom we interviewed in August 2002.

In brief, our research access resulted from a creative use of informal contacts and luck. Apart from the severe time constraints imposed for the interviews, both organisations allowed us to use the findings as we saw fit. This was on condition that we disguised the identities of the organisations in any subsequent writing. The anonymity guarantees were vital because,

> "Members of organisations speak from positions of comparative power, influence and vulnerability, and the researcher may seek information that could potentially compromise those positions (Buchanan *et al.* 1988)."

Since, our research was about power and politics, anonymity helped us elicit personal and sensitive information. Buchanan *et al* classify this as 'Getting on', which involves negotiating access to the lives and experiences of respondents. It depends on confidence that the researcher is trustworthy, non-partisan and is genuinely listening to respondents.

Data Collection Techniques

A key tenet of the interpretive paradigm is that since knowledge of reality is a social construction, multiple realities exist in any given situation. Therefore, to access the different meanings participants assign to the same phenomenon, action or event it is vital to employ the principle of triangulation. Triangulation can be of theory, personnel and method. We focus on method here. To Zuboff (1988) it involves, "a continual juxtaposition and comparison of data culled from different sources that purport to describe the same phenomena." Likewise, for Trauth and O'Connor (1991) triangulation refers to checking inferences drawn from one set of data sources by collecting data from other sources. However, multiple data sources do not necessarily result in convergent data but deepen the understanding of apparently contradictory data (Trauth and O'Connor 1991).

We used the techniques usually associated with interpretive research in information systems: semi-structured interviews and analysis of documents. We explored personal, group and divisional perceptions of and reactions to the PKI through interviews and assessed long-term patterns through documentary analysis (Buchanan *et al.* 1988). As discussed elsewhere, a key strength of the case study research strategy is the unique ability to deal with a wide variety of evidence (Yin 1994).

Interviews

To Walsham (1995a) interviews are the main source of data for interpretive case studies because they capture the respondent's interpretation of action and events, as well as their beliefs and aspirations. Therefore, our primary source of data was interviews. We interviewed people with significant influence on the PKI project and any frequent users of PKI-enabled applications. They included managers, system architects, designers, internal security and business consultants, project leaders and users. We specifically sought people with experience in different roles, departments and levels of the organisational hierarchy to help us document the multiple viewpoints about the PKI deployment.

We captured the official agenda, workforce views and the technical environment. From these findings, we built an understanding of the role of power in the contextual conditions pertinent to PKI institutionalisation. We relied on gatekeepers to identify interviewees. We sought information about the emergence of the PKI project especially about how and why top managers were convinced that this is *the* technology to solve the identified security problems. This analysis helped outline the key events in the PKI lifecycle and summarised the desired and real outcomes from the perspectives of different agencies.

Being semi-structured, we prepared interview guides that corresponded to the CoP framework. Although we prepared the questions in advance, we rarely followed them to the end because the interaction with the interviewees brought up leads to information that our fixed list could not accommodate. We followed the advice of Buchanan *et al,* (1988) that, "The researcher has to be attentive and ready to put the interview guide aside," when respondents make seemingly trivial but potent remarks. We also changed the tone of the questions to reflect the status and experience of the respondent. We divided the respondents into managerial, security, IT consulting, general user and vendor categories. For managers we targeted those with powers to determine budgets, hire staff, evaluate projects, resolve conflicts, appraise staff, select and purchase materials and equipment.

We corroborated controversial information by anonymously printing out views from previous interviews for the comment of other respondents. This was a priceless technique because it removed the research abstraction and convinced cagey respondents to give refreshingly robust answers. With the exception of a section of one interview, we digitally recorded and fully transcribed all our discussions. Gatekeepers also gave us fascinating pieces of information during coffee breaks and on our way out of buildings.

In addition to the interviews with agencies within the two organisations, we interviewed some leading vendors. At Oilcom, PKI is part of a Windows 2000 deployment that also includes smart cards and thin clients, which rely on the operating system's native security features. Bankrecht Investment also has a Microsoft PKI deployment with clients running Windows 2000 and XP. Hence, we interviewed Mr Stuart Okin, Chief Security Officer, Microsoft UK and Mr Tony Rice, the Head of Business Critical Consulting in November 2002. We had a discussion earlier with Mr Steve Adler, Microsoft Product Manager, Europe Middle East and Africa after his presentation on Active Directory and Windows .NET at an EEMA meeting.

SchlumbergerSema provides the smart card solution at Oilcom. We held a brief discussion with the manager responsible for PKI and smart cards at an "Executive Briefing" organised by Entrust in May 2002. Schlumberger has also published their experiences at Oilcom in a case study for the Smart Card Alliance. Siemens provides the smart cards at Bankrecht. We gathered enough information about these cards from Bankrecht AG and the five EEMA presentations between November 2000 and September 2002 from a senior member of the UK Siemens Business Consulting division.

Documentary Analysis

The documents we analysed covered the whole PKI lifecycle. We hoped to ascertain why and how the organisation chose a PKI as the security infrastructure. From the documents, we hoped to identify the PKI sponsors and their attempts to convince other agencies to 'buy into' the solution. As stated above, we used interviews to gather some of this information because they have the advantage of capturing current events. However, retrospective documentary analysis helped trace 'objective' arguments advanced to support PKI at different stages.

The documents included the IT Strategy; IT Security Policy; Practices and Procedures; Infrastructure standards; Internet strategy; Cryptography guidelines; Certificate Policy and Certificate Practice Statements; Project plan/timetable; Documents about the selection, implementation of PKI; project announcements and internal IT/IT security magazine. We also explored documents that contained information about evaluation and co-ordination of the PKI, announcements and training documents, organisational charts and corporate annual reports. We also used newspaper and magazine articles and e-mail communications between the respondents and other PKI stakeholders. E-mail as a source had rich information because it was a vital tool for negotiating access and allaying fears about the research process.

We obtained interesting information and tips from vendor case studies of PKI projects in our study organisations. Because of the novelty of PKI deployment, vendors like Schlumberger used the 'case studies' to advertise their expertise. While the documents contain informative technical details, they looked too sanitised to be true. However, they were good for triangulation and generating questions for interviews.

Also because of the novelty, we attended an EEMA event organised under the UK Electronic Business Users Forum (UKEBUF) at which Oilcom managers discussed the PKI project. UKEBUF frequently covers security issues notably PKI and directory services. It was an excellent opportunity to learn about the project because the presentation was subject to extensive peer review. Since technical managers and staff attend EEMA events, participants expressed frustration with organisational politics. Although we were active participants, we switched to an observer capacity during the discussion of the Oilcom project. We recorded the discussion and received soft copies of the presentation.

We also used studies and white papers published by Microsoft, Schlumberger, Entrust and Siemens. They provide good technical detail on PKI and smart card deployment. We classified and interpreted these documents using the Circuits of Power framework. Given that they were marketing pitches, some parts sounded too sanguine about specific PKI products.

The Circuits of Power in Data Collection

As a prelude to discussing our contribution in Chapter 8, we reveal that we encountered numerous problems in our use of the CoP framework for data collection. One of our intended theoretical contributions was to extend previous research on the CoP (Introna 1997, Silva 1997) by exploring its methodological viability in IS empirical studies. We focused on the language and other aspects that could help researchers conduct empirical studies using this framework. As such, we assessed the usefulness of a list of questions suggested by Silva for guiding research (Silva 1997, Silva and Backhouse 1997, Silva and Backhouse 2003). However, we encountered problems with the list.

To Buchanan *et al.* (1988) the quantity and quality of data collected during research greatly depends on the investigator's ability to win and retain the trust of the respondents. Success largely depends on the personality of the researcher. However, trust is jeopardised when the researcher is suspected to be disorganised, sloppy and not in command of the subject. In sum, a poor interview schedule can be a recipe for disaster.

We got this impression from the interview that entirely used Silva's questions. Although this respondent at Oilcom was a good friend, he kept saying, "Not sure what you are asking here" and "haven't we answered that question already?" The problems arise from the very nature of the framework. The CoP signifies that outcomes of power keep circulating in organisations through rules and their relationships to techniques of discipline and production. While at the theoretical level the 'circulating' conception is fine, it creates a bewildering number of repetitions between the circuits in interview schedules. Thus, wholesale conversions of the CoP concepts into an interview schedule could make a researcher look amateurish.

Data collection themes

Therefore, for two obvious reasons we promptly grouped the CoP concepts into business environment, technology adoption process and social aspects of the organisation themes. First, Silva's list retained much of the awe in the original CoP. Hence, to avoid threatening language, we left out loaded terms such as episodic power relations, domination and standing conditions. Second, the list was impractical because it repeated the same themes across the three circuits, OPP and exogenous contingencies. As we were to learn, the overlaps were detrimental to a smooth interview because asking similar questions every ten minutes to a busy security manager risked shattering the hard-earned rapport. Put briefly, the questions were inelegantly repetitive and retained ominous language. The themes are as follows.

Business environment

This theme coincides with exogenous contingencies in the CoP. These represent coercive pressures from agencies with authority in an organisational field that transform or reinforce the rules of meaning and membership. An organisational field includes key suppliers, resource and product consumers, competitors and regulatory agencies. The CoP draws on concepts of institutional isomorphism to explain how organisations adopt innovations and how they become stable in organisational fields. We gathered data about the history and operational conditions of our study organisations under this theme. We also sought data about organisations and conditions that influence technology adoption.

Social aspects of the organisation

The theme is close to the episodic circuit because it gives a snapshot of the organisational political landscape. We used the theme to identify the different political subdivisions within the organisations. It also shed light on the material resources, techniques and skills required to perform tasks (standing conditions). The identification of the different agencies/groups engaged in organisational action actually justifies this theme because it highlights the link between the three circuits of power. Episodic power both depends on rules of meaning and membership and on techniques of discipline and production. Consequently, the theme explains the conditions that enable the exercise of episodic power.

Technology adoption process

The theme unifies issues surrounding the use of technology in organisations because of overlaps between OPP, system integration and episodic circuits. Since agencies could resist a new system because of the physical characteristics of the system and resistance is associated with both circuits, a single theme makes sense. We discuss these issues in detail in the concluding chapter to amplify our contribution.

Data Analysis

For data analysis, we relied on the same approach used by (Silva 1997, Silva and Backhouse 2003). From the broad CoP lenses, these works applied an iterative approach to data analysis characterised as *telling-showing-telling*. According to Golden-Biddle and Locke (1997), the concept underscores the relationship between depicting data and conveying its theoretical meaning. They attribute the distinction between 'showing' and 'telling' to the 1961 work of literary critic Wayne Booth. He explains that accurately observed details do not hold readers' attention for long unless 'if the details are made to tell, only if they are weighted with a significance.' Presenting data both looks backward to the forms and process of organisational life and forward to the theoretical points for resolving gaps in the literature. As such,

> "**We both show data and tell their significance**. ... (Hence) we couple the fragments of organisational life with our theoretical points and commentaries. The life we portray always is theorised as, reciprocally, the theory that we develop always is contextualised (Golden-Biddle and Locke 1997)."

The *telling-showing-telling* characterisation is the absolute version of this interactive model. To Golden-Biddle and Locke in this sandwich structure, the first 'telling' explains how the theoretical point is manifest in the subsequent data. 'Showing' means the presentation of data. It is an aspect structuring a story in a way that bridges the worlds of the readers and the field. The second, 'telling' connects the presented data with the theoretical concepts to explain or tell what the data showed. We use the model as follows.

We present the theoretical concepts in Chapter 3, where we explain how the concept of power is manifest in empirical research. We present the CoP as the tool for visualising power in terms of outcomes, standing conditions, techniques of control and discipline. We suggest the CoP because of the realisation of numerous problems in the literature regarding the visualisation or even mere explanation of power. This Chapter extends the theoretical points made in Chapter 2 about the complex character of power. To resolve this problem, we explore the philosophical underpinnings of IS research. In Chapter 4, we select the ideographic approach, as personified in interpretive research, because its subjective orientation is most effective for studying the disputed concept of power.

Chapters 5 and 6 show the data. Our goal is to 'take' readers to our field studies through conveying the elements of power in the fragments of the organisational life we present. Golden-Biddle and Locke argue that to transport readers into the field, researchers should portray first-hand experience with the subjects' world. "However, efforts to take the readers into the field are, at the same time, pointing to the readers' world and to the theoretical points being advanced (Golden-Biddle and Locke 1997)." Therefore, having drawn attention to this data, we tell the readers what it showed through our analysis of the findings in Chapter 7. The depiction of power in the two cases supports our theoretical propositions by concretising them in living organisational contexts. Thus, we spread the *telling-showing-telling* concept over several chapters. This dynamic approach conforms to our descriptive case study approach by showing the connection between the case, the framework and our interpretation. In sum, the "interlocking of data and theory reinforces the coherence of our storylines, giving them the quality of straightness (Golden-Biddle and Locke 1997)."

Chapter summary

This Chapter presents the philosophical underpinnings of our methodological approach and places it within the broader IS traditions. Having surveyed the different approaches, we highlight and justify our choice of the interpretive tradition. We further undertake an extensive discussion of our research strategy and show how it supports our theoretical agenda. We reveal the rationale for selecting the two studies and give the reasons behind our research decisions. We thereafter discuss our data collection techniques and the role of the CoP framework in data collection and analysis. We link this discussion to previous and subsequent chapters and highlight issues for further discussion.

CHAPTER 5: 'STEALTH' PKI AT OILCOM

Introduction

This chapter and Chapter 6 *show* data by conveying elements of power in our field studies. Since we used the Circuits of Power (CoP) framework to direct our research (methodology), we present the findings from the two cases based on the framework. However, the presentation follows the three themes we developed during empirical research to overcome repetitions and tone down ominous language. The themes cover the business environment, technology adoption and social aspects. We re-introduce the native CoP concepts in Chapter 7. The rest of this chapter is organised as follows. In the business environment theme, we discuss the history and current governance structures of Oilcom. The governance structures link the business environment to the social aspects. Technology adoption starts with the mandatory PC standard named Group Infrastructure-Desktop (GID) because it both supports and relies on the public key infrastructure. The discussion is vital because while this study is about PKI, GID provides a context for its usage and explains its success.

PKI and Desktop standard

As stated in Chapter 4, a major reason for selecting Oilcom and Bankrecht was that the organisations are pioneers of large-scale PKI use. However, PKI use is currently restricted to user authentication. These two cases are actually typical of global organisations that run diversified businesses in numerous jurisdictions under localised organisational structures. We conducted 20 interviews at Oilcom each lasting about an hour. Our respondents included the Director of Global IT projects, Principal Architect, Team leaders, Principal Security consultant, security and business consultants and users with both "User standard mode" and "developer" machines. The respondents have worked at Oilcom for between one and twenty five years. We also interviewed senior Security managers at Microsoft – EMEA and UK – and attended a SchlumbergerSema briefing at an Entrust workshop for security managers.

Business Environment

Oilcom is a large and diverse global energy and petrochemicals company that is among the world's top three biggest oil companies. The Group claims competitive leadership in oil products, deep-water production, Liquefied Natural Gas (LNG) and polyolefins. Oilcom had market capitalisation of $149 billion in 2000 and aims to lead its sector globally. While most people identify Oilcom with service stations, global oil and gas exploration and production, it also delivers energy solutions and petrochemicals. These include transporting and trading oil and gas, marketing natural gas, producing and selling fuel for ships and planes, generating electricity and providing energy efficiency advice. Oilcom also produces and markets petrochemical inputs for plastics, coatings and detergents. The Group has also invested in renewable and lower-carbon energy sources but it does not process coal and nuclear power.

Nature of business

Naturally, energy services companies jealously guard the intellectual property generated in course of their work because it provides the ingredients for innovation. Oilcom channels much of this data through its research centres on which it spends over US $1 billion annually. The centres develop new products and processes. For instance, in 2001 Oilcom released a 'revolutionary' type of unleaded fuel developed at its UK global innovations centre. The centres also research in applied science and technology, which leads to new business opportunities. In 1998, the Group created a Technology Ventures division to liaise with the service industry to develop and market its proprietary technologies. The technologies include logging and drilling equipment, production enhancement devices and natural gas processing units. Oilcom claims its intellectual property extends beyond oil and gas to new energy utilisation devices, manufacturing processes and environmental remediation.

Therefore, the value of the intellectual property and the hazardous location of oil wells make the protection of information a critical success factor. Oilcom also prizes security because its employees have recently become targets of kidnappings in trouble spots across the world. Threats to staff and oil well accidents have emphasised the need to protect information from unauthorised access by third parties such as competitors and pressure groups.

History of Oilcom

Oilcom is one of the oldest energy services companies in Europe. The Group grew out of a London shop in the first half of the nineteenth century that later became a successful import-export venture. Oilcom later moved into the oil sector exporting lamp and cooking oil to the Far East. In early twentieth century, the firm merged with a European competitor to form one of the largest global commercial enterprises. The Group expanded with acquisitions in Europe, Africa and the Americas throughout the twentieth century. The period coincided with mass production of cars. Oilcom's growth shuddered to a halt in the First World War because several governments confiscated its assets and/or closed them down. However, Oilcom received a massive sales boost in 1919 with the opening of non-stop trans-Atlantic flights.

The Group also lost assets in World War II. It later invested in newer production, transport and refining facilities. This investment boosted output and sales to an extent that throughout the 1950s and 1960s Oilcom supplied almost one-seventh of the world's oil products. The period also saw the development of natural gas as an alternative source of energy. Oilcom benefited because it had made major oil & gas discoveries in the North Sea.

However, an economic recession combined with a steep rise in the price of crude oil had a serious impact on the overall oil business. The illustration on the next page originally published by the US Department of Energy's Office of the Strategic Petroleum Reserve, Analysis Division, summarises the World Oil market and prices during 1970-2002. The Energy Information Administration updated the figures for 1995-2002.

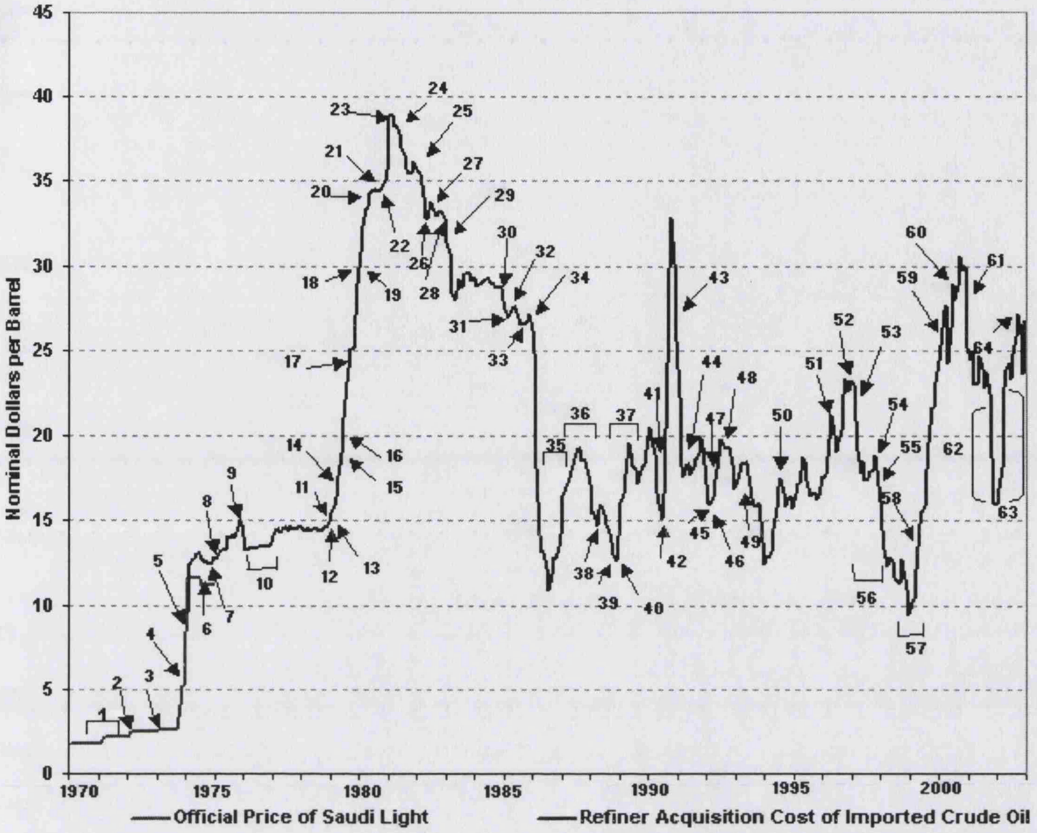


Figure 8 - World Oil Market and Oil Price chronologies from 1970 - 2002

The chart shows the crises that sparked huge rises in crude oil prices. Point 9 saw a huge rise after OPEC announced a 15% revenue increase effective October 1, 1975. Other crucial points are 23 when the first major fighting in Iran-Iraq War occurred; point 42, showing the Iraq invasion of Kuwait and 59 after OPEC oil production cutbacks. The oil prices tripled between January 1999 and September 2000 because of weather and low oil stock levels. Oilcom attributes its long-term survival to 'scenario planning'. Writing in a 1988 issue of the Harvard Business Review, a senior Oilcom manager claims,

> "The key to corporate longevity and success is the ability to adopt a survival mode when the business environment is turbulent and to switch to a self-development mode when the pace of change is slow. ... A very effective learning tool, which can be described as a form of **game playing, is developing "what if" scenarios and planning responses to them**."

Oilcom claims to have used scenario planning in the 1980s to weather a huge drop in the oil price from $28 to a measly $16 a barrel. Despite new investments, Oilcom believes the oil, gas and chemicals businesses are central to its mission of delivering high shareholder value.

Governance structures

Official documents reveal that administration at Oilcom rests with a board of management consisting of at least two managing directors (MDs). The MDs hold office until retirement unless removed earlier. A supervisory board in turn oversees the policies of the MDs and general business direction. The Board appoints one of the MDs President, who thereafter determines the division of responsibilities among fellow MDs. Since Oilcom has two holding companies, MDs of each organisation are also part of the "Presidium of the Board of Directors" also commonly known as Group Managing Directors. The MDs are also members of a joint team known as the Committee of Managing Directors (CMD). The CMD is the supreme Board. It develops long-term plans and reviews key investment decisions.

This structure is obviously complex. To add more intricacy, the two holding companies are separate legal entities that, as public companies, observe laws and corporate practices of their respective countries of incorporation. As we see later, these differences make any global IT implementation at Oilcom a complex socio-technical negotiation.

Service and Operating Companies

The holding companies do not directly engage in operational activities. This is the job of Operating Companies (OCs) based in 145 countries with over 115,000 employees. The management of each company is responsible for the profitable and viable operation of its business. OCs share global experiences and are associated with the holding companies through two Service Companies (SCs). We based our research at the London offices of one of the SCs. Admitting that, "Oilcom is not an easy company to understand," a Team leader argues that SCs exist to provide general and specific services to OCs that are largely organised on a country-basis. Similarly, the Chairman of the CMD argues,

> "Our business model is of strong, locally-rooted companies – harnessing the capabilities of focused global businesses ... global efficiency with local effectiveness. International mobility helps cohesion, as well as sharing experience. **It is increasingly supported by electronic interaction.**"

The Group claimed 6% of its employees worked abroad in 2001. The service companies also provide the rules under which the local companies must operate. For instance, SCs stipulate and enforce minimum health and safety standard for all OCs. To a senior SC consultant,

> "This is a very heavily regulated industry. Our businesses are regulated in several ways. There are health and safety implications, brand value implications, good practice and legislative implications that we have to demonstrate that we meet. If we do not do these things properly then we are in trouble and **we lose the value that we have built up over a hundred years**. It is not something that we really want to take blame for, OK, and the businesses don't want to take blame either, OK?"

Business structure

The business sits on top of the Group physical structure discussed above. Oilcom operates six global business divisions: Exploration and Production (E&P); Downstream Gas and Power; Oil Products; Chemicals, and Renewables. Recently the Group added the "Other Activities" division that is split into customer, hydrogen and trading. A small team of about eight people called the Executive Committee (Excom) heads each of the business divisions. An Excom recruits a team of about a hundred or two hundred people, which directly reports to it, to help run the business. The Excom sets the overall strategy for the business division and targets for operating companies. Some employees report to the local company and the Excom.

However, not all companies have the six business divisions although most have Oil products, the signature service. The only divisions with exploration, production, refining, marketing for oil products, downstream natural gas and power generation, chemicals and Renewables are in the UK, Germany, Netherlands, USA and Philippines. As we shall see with GID and PKI, these operating companies are powerful because they control enormous resources. The gas and power division is unusual because Oilcom typically runs the holdings in joint ventures especially in Asia. The Group teams up with other oil companies, specialist operators or even governments who directly run these businesses. Oilcom takes shareholdings that range between 20% and 50%. However, the ventures have complicated network administration and the deployment of tools that help establish control over IT such as public key infrastructures.

Social aspects of Oilcom

Dues to its size and diversity of operations, Oilcom relies on a huge pool of professional skills that include the following. In E&P, the Group employs geologists and geophysicists for exploration. Production employs chemical, mining and mechanical engineers. After this stage, the next processes are manufacturing, supply and distribution. Processing requires the skills of chemical and mechanical engineers. Lastly, the key skills for Oil products are marketing, distribution and expertise in refinery technology.

Employment is conditional on the acceptance and continual adherence to nine principles that apply to all business affairs and describe the behaviour expected of every employee. The principles cover objectives of operating companies; responsibilities; economic principles; business integrity; political activities; healthy, safety and the environment; the community; competition and communication. They are contained in a "Statement of General Business Principles" that governs how each company conducts its affairs. The guidelines stem from the principles of honesty, integrity and respect for people first printed in 1976.

Oilcom requires chief executives of all companies and businesses to report on the application and success of the principles throughout their organisations annually. However, despite these efforts, the distributed structure has traditionally encouraged the proliferation of groups narrowly focused on their trade. Some of our respondents blame the fiefdoms for the political paralysis at Oilcom. Consultants are responsible for increasing cooperation within the Group. Next, we explore the consultancy role and its vitality to IT deployment.

Consultants

Oilcom uses consultants with different skill sets. For instance, Technology Consultancy and Research Services demands expertise in geosciences, engineering and pure sciences. The team we interacted with most sits within an area called Information Technology International (ITI). The division has consultants specialising in organisational architecture, IT, information security and business processes. Other consultants work in contracting and procurement, legal services, intellectual property, finance and treasury, among other areas. Consultants act as flexible resources because local companies cannot afford to keep a team of people with all the necessary expertise all the time. Business divisions such as Oil products may retain their own teams of internal consultants. However, the majority of consultants work for Service Companies (SCs) making them central to Group-wide information systems deployment and knowledge sharing. However, to a Team leader this role is controversial because,

> "**Often you are seen as somebody who is interfering with their work or as a spy from central office**. I think that is actually less true in smaller operating companies because they know they cannot possibly have all the expertise. ...Where it is a big issue is with larger OCs, say Oilcom UK. They employ several thousand people and have many senior people with lots of knowledge and lots of experience and **they would like to think that they can run everything themselves.**"

Since the management of each company is responsible for the long-term viability of their own operations, they decide whether to accept the consultants and their advice or reject it. Indeed, the Director of Global IT Projects stresses,

> "It is their business. The whole purpose of Service Companies is simply offering advice. The responsibility for the business is with the national operating company and with the line of business and it is not up here. So yes, of course they can say '**we don't need these consultants**'."

In practice rejection is rare because either somebody in the company or on the Excom invites the SC consultants. Therefore, they get a mandate from an influential sponsor. However, the local companies retain the veto on how even mandatory standards are implemented. We will see that the companies can use these powers to either block or slow down large infrastructural projects. In our study, the delaying tactics of the OCs have sharply increased the expenditure of the supposedly cost saving GID and may pose enduring risks to PKI interoperability.

Oilcom brand

We previously saw that apart from the two holding companies, Oilcom relies on OCs to run its business in over 145 countries. In addition, a business structure composed of six divisions, run by Excoms, sits on top of the aforementioned physical structure. The Oilcom brand holds together this complex organisational structure. According to a security consultant,

> "Oilcom isn't quite a corporate in the sense that we often get from American economists of a kind of joined together organisation. **It is predominantly a brand,** and people buy into it and the brand does different things. ... It is many different companies but the brand is ultimately the most important thing. It is sacrosanct. If you damage the brand that is the worst thing you can ever do."

Since branding is common to our two case studies, let us briefly discuss its key concepts. According to Interbrand, a global branding firm, a brand represents the relationship between a firm, its employees and customers (Interbrand 2001). Interbrand declares that to reap maximum benefits the organisation should 'align' its internal features such as culture, reward systems, key success activities and structure to its brand. Interbrand claims employees must 'live' the brand and management must show commitment to the values in its behaviour and communications as illustrated below.

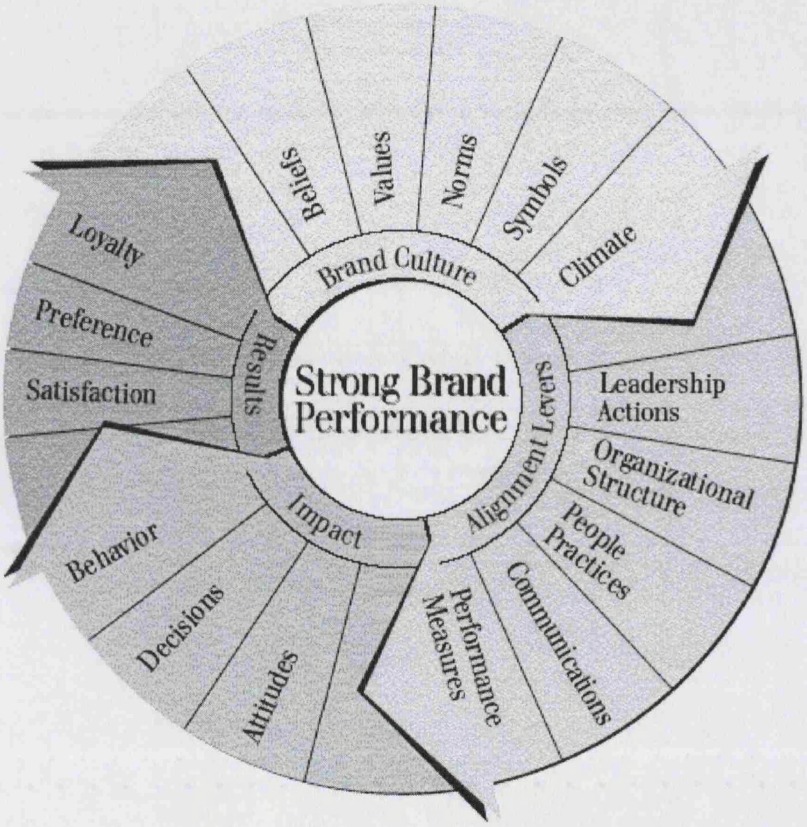


Figure 9 – Brand Culture Align Flow (Interbrand 2001).

The brand culture has an impact on the behaviour, attitudes and decisions of agencies if supported by management actions and the organisational structure.

Technology adoption process

Despite the professed importance of IT in coordinating far-flung activities, until 1988 Oilcom did not drive mandatory infrastructures from the centre. The character of the IT service mirrored the decentralised organisational structure seasoned with splintered and often chaotic arrangements in which each business division and local company runs its own infrastructure. For instance, Oilcom UK had separate IT departments for each business division such as Oil Products and E&P. Other companies replicated this structure. Even small markets like Oilcom Uganda would run their own IT Services. To the Principal Architect[17], "We were repeating many things ... This is obviously a recipe for doing more than you need."

To arrest the mayhem and cut costs, Oilcom launched an IT standardisation drive. First, the Group consolidated the different IT groups across lines of business to create a single IT unit that for instance covered Oilcom UK. After this success, Oilcom consolidated all the IT services for the companies into a global service. IT became part of Services International (SI) in 1997. SI expedited efforts to centralise the provision of computers, servers and network administration. However, the evolution of SI into an institute covering the whole services area created immediate disaffection. According, to a Team leader,

> "It has been very difficult to make theses things happen ... Because local OCs originally hired most IT people, many wanted to work for Oilcom in their home country where they had national identity. ...now suddenly you are being told you are no longer part of Oilcom France but part of SI or whatever. People didn't like that. **In practice their job probably didn't change very much but just that move of parentage,** if you like, ownership led to many people leaving the company."

To the Director of Global IT projects, the problems emanated from poor knowledge of local businesses by SCs. However, a Team leader blames 'governance issues'. He argues that,

> "One of the difficulties is that Oilcom has always been **a very distributed company**. ...the advantage of a centrally directed company is that **if a man on the top says 'do this' it ripples down and gets done**. In Oilcom, it really doesn't work like that at all. The centre only sets the strategy, principles and general direction. ...the way those are implemented is at the **discretion of local management**. Hence, **it is very difficult for IT to be provided in a common way across the whole business.**"

Oilcom later removed IT from Services International and created an independent division entitled Information Technology International (ITI). In 2000, as part of GI standardisation

[17] He is an Enterprise Architect and focuses on IT strategies and decisions that support business needs.

drive, the Committee of Managing Directors (CMD) appointed ITI as the sole supplier of IT to all companies. We shall focus on the centrally managed desktop otherwise called GI-Desktop (GID) and its relationship with PKI after a brief discussion of Group Infrastructure.

Group Infrastructure (GI)

Oilcom has a long history of standardising desktops with GI the fourth cycle of this process. The first attempt was with the MS DOS era where service companies recommended hardware configurations, suppliers and software choices. The phases failed because the companies or Operating Units (OUs) ignored the optional advice leading to software incompatibility. For instance, the Director projects reveals that in 1992 a central office in Europe,

> "**Employed about 3,500 people who had 29 different word processing packages in that office.** ... each of our Managing Directors' secretary had their own particular word processing product so that when they were away nobody else could produce any typed documents for their particular MD."

After 1992, the Group signed a software contract with Microsoft and standardised on MS Office. At the end of this licence, Oilcom provided standardised pre-configured Windows 95 desktop images and subsequently pre-configured NT Servers. The Group still run the infrastructure through local delivery organisations. However, according to a Business Consultant, many teething problems remained at this stage. He reveals,

> "Apart from the E-mail system that was common, I could not take files around OCs because of version issues. You frequently had different upgrades across the desktop applications. For instance, I could send somebody an Office 97 document not realising they only had Office 95. Thus, you had to save it to the lowest common denominator. **It was such silly issues like that getting in the way.**"

The Director Global IT projects reveals the failure to respect hardware and maintenance structures created extraordinary IT management complexity justifying GI. Discussions on the Group Infrastructure (GI) started at a CMD meeting in late 1998. The committee endorsed GI on 19th October 1999. To the Director, GI involved,

> "Moving from a Windows 95 distributed management infrastructure to one where we had a single management framework overseeing the **complete re-implementation of the entire desktop and server infrastructure and all the supporting services behind them such as mail and directories.**"

Group Infrastructure Desktop (GID)

This is the desktop component of the GI set of standards. According to the Principal Architect, GID involved the migration of all desktops and related servers to Windows 2000 and Office 2000. The servers and desktop devices were sourced from Compaq through a Group procurement agreement. Oilcom loaded the laptops and PCs with a limited matrix of standard applications. Wherever possible, Oilcom configured desktops to run the "User standard mode". According to the GI proposal, in this locked-down mode,

> "**Changes to core desktop software will be strictly controlled from centralised Service Centres.** This will allow (the IT division) to manage and automatically upgrade software via the network, thus obviating expensive individual visits to upgrade each device, and **guaranteeing that standardisation is maintained.**"

Most users are unable to change small things like wallpaper and screen savers on the PC. In the "User" mode, all new software requires scripting for GID in Malaysia. However, a limited number of advanced users such as technical consultants have unlocked "Developer machines." Oilcom claims GI is an attempt to learn from 'world-class peer' organisations such as IBM, Nestle and Unilever that manage their infrastructures with a focus on costs that sharply rise with mobile working. The 'peer' firms have implemented strict standardisation and simplified their demand, supply and support systems. Likewise, the GI proposal states,

> "Group Infrastructure involves a managed transition to **a centrally controlled and rigorously enforced technology platform** that is implemented Group wide. ... The ability of the project to deliver the anticipated benefits will depend upon a standardised approach being adopted in all OUs with **only limited flexibility to accommodate OU specific requirements.**"

The Principal Architect claims GI exists primarily to reduce the Total Cost of Ownership (TCO) for IT. For instance, based on the Gartner model with 1998 actuals, the Oilcom average direct TCO per annum was at least US$3,600. The cost varied between US$2,000 and $9,000 across the Group. The IT division blamed the rising costs on customisation and independent adoption of software, which led to fragmentation, high support complexity and delays in the implementation of software and functionality. Cross-business technology 'fixes' to enable connectivity and information sharing proved unreliable. Oilcom expected to standardise unit costs at $2,500 by the end of 2001. The Group targeted 10% year-on-year reductions to stay ahead of industry benchmarks. The Director of IT projects argues that cost was a major driver of GI because the oil price was low at the time of its inception. Therefore, there were cost-cutting pressures on the businesses. However, he admits,

> "In fact, I think the value of what we have done is much more in terms of **a business enabler than a cost reduction.**"

The Principal Architect agrees. He argues that standardising on Windows 2000 would have had very little impact on the cost without changes in the support organisation. The changes saw the number of PCs under ITI control increase from 69% to 94% by the end of 2001. For instance, twelve companies classified as 'large' sites lost control of over 19,000 machines to ITI. Western Europe companies liked the changes because to a Business Consultant,

> "Some of the bigger, more powerful, more established operating companies were the ones that would have more sway when GI was being designed in the first place. **So I would imagine that they would have got pretty much what they expected.**"

Indeed, the GI proposal suggests sampling a "small number of archetype companies, which will serve as a template to judge OU requests." However, companies in poorer countries, notably in the Far East were dismayed because GID was more expensive than local sourcing arrangements. A Team leader agrees. He argues that,

> **"While the cost associated with this desktop is quite reasonable in Northern Europe, the same cost applies for instance, in Uganda too and there it is quite a high cost.** We are saying to the Ugandan company, 'you must have this' and they say 'we don't have any money, how can we have it?'"

The Director IT admits cost overruns. ITI started with a budget of US$1000 for each GID client but spent $1900 in the first phase. The project had a budget of $70m to $100m for 65,000 units at its launch in November 1999. However, by April 2001 the cost stood at $110m. Eventually, the project team discovered in July 2001 that it probably needed about $170m. He blames the cost overruns on failure to anticipate delays and poor information about the number of PCs at Oilcom. Other respondents attribute the delays and cost overruns to the political fires that GI stoked. We discuss the power issues after the coverage of PKI. To maintain the standard GI client, Oilcom relies on PKI and its support features like Active Directory. Next, we discuss e-business activities and their influence on PKI deployment.

Focus on E-Business

One of the "Value Benefits" of the Group Infrastructure (GI) proposal is that it was a "pre-requisite for effective use of e-commerce and rapid uptake of business-to-business commerce" at Oilcom. With the blessing of the CMD, the rollout of GI saw a rapid launch of e-commerce projects across various business divisions starting in 2000. The Group sought major cost improvements in oil drilling, finding, development and production and saw the internet as a useful medium especially in procurement. By the end of 2000, Oilcom had e-procurement sites at eighteen locations in North America, Europe, Asia-Pacific and Africa. Signing the e-commerce projects off, the CMD Chairman argues that,

> "To continue our history of continuous profitable growth, **we must respond to a range of issues that define the context in which we do business**. These include globalisation, liberalisation of political systems and markets, and the effects of new technologies such as the **internet**."

Oilcom launched the savings drive through a number of extranets for customers and suppliers. The Group also co-founded or participated in nine business-to-businesses (B2B) marketplaces and exchanges. Oilcom Trading spearheads the exchanges. A key example is Trade-Ranger, an energy and petrochemical B2B exchange. Launched in July 2000, Trade-Ranger is an independent initiative built with the support of the world's 15 foremost energy and petrochemical companies. The founding members include ENI, Mitsubishi Corporation, Repsol YPF, Royal Dutch/Shell, Statoil, Total, Unocal and British Petroleum. Trade-Ranger delivers the cost savings sought by the Group.

The Group also extended the internet into business-to-consumer (B2C) transactions. Oilcom claims to use the "internet to extend and deepen relationships with customers." Customer-focused initiatives have included integrated energy services for households, differentiated motor fuels and financial products for motorists. Oilcom launched several internet-enabled insurance products in 2000. The Group also changed its internal business practices. The focus "has been on digitising the business, and on the cost reductions and process efficiencies which this brings." As we see next, ventures with competitors and customers have totally changed the Oilcom network administration and security paradigm.

GID and Information Security

While the internet enables low cost transactions, the medium lacks the traditional identity, commitment, evidence and trust safeguards. A key implication of this change is that security is no longer primarily about limiting access but maximising it to the right people. Thus, internet security focuses not on intruders but on potentially fraudulent insiders and business partners. This is what forays into e-commerce made Oilcom realise.

Security regime

Another reason we selected Oilcom is its security reputation. For instance, the Group actively participated in the development of BS7799 that formed the basis for ISO 17799. Indeed, many of its former employees have top security jobs in public organisations in the City of London. We saw that security is critical to Oilcom because it generates trade secrets from the over a billion dollar research budget. Good security also assures health and safety regulators and environmentalists that it takes due care. While most SCs advice is optional for operating companies, security has always been mandatory. Oilcom outlines its security regime in documents that include "Porcupine"[18] or the Seven Point Plan, Business Communication Principles and Trust Domain. They are part of a security initiative launched in 1997/98. The principles guide the creation of all documents and hence minimise legal and security risks.

Trust Domain

The goal of Trust Domain is to create a Group-wide, trusted network environment to support global business applications and information sharing. The CMD made the adoption of Trust Domain and its related standards and controls mandatory. Trust Domain requires companies to implement minimum-security standards, independent of technology, but consistent with BS7799. The GI proposal states,

> "The remote access solutions (e.g. dial in, mobile office) will also be implemented in a **Trust Domain compliant manner**. 'Strong authentication' will be incorporated. This will provide the ability to authenticate the remote users securely and control their access to resources on the Group's network. The new infrastructure will allow 'On-site' partners, 3rd parties and JVs to have controlled access to the required parts of the Group's network using similar degrees of authentication."

[18] The Group argues that aggressors find it difficult to attack a porcupine because an impenetrable defence of sharp points protects it. Oilcom hoped to use the same principle for its own Information Security.

Trust Domain supported the CMD effort to increase information flow within the Group and with its business partners, customers and suppliers. As BS7799 recommends, Trust Domain relies on independent certification to confirm the compliance of counterparties. Indeed, even when an operating company outsourced IT, the company remained responsible for ensuring that contractors comply with Trust Domain. In brief, Trust Domain launched the concept of an open internal network, which Oilcom only selectively closed. The Group later extended this fundamental shift to transactions between itself and the outside world.

Public Key Infrastructure (PKI)

We previously saw that Oilcom believed Group Infrastructure (GI) was a precondition for its e-business drive. This was because GI enables common global processes and practices, easier mobile working and enforcement of business discipline. The GI proposal further envisages, "greatly increased data and information security." GI also allows users to "log on anytime, anywhere, on any Group desktop" because all data and applications are stored on network drives. However, this change in the network access logic made password-based authentication inadequate. Therefore, instead of investing all resources on defeating intruders, Oilcom sought robust measures to protect against fraudulent behaviour by parties accessing its network. The Group believes cryptography is an appropriate tool for this job.

Oilcom has used cryptography for over 20 years. However, because these products were largely proprietary, over time they became very expensive to maintain. With e-business at full speed in the late 1990s, the Group decided to replace these special security features and products with off-the-shelf products. GI offered the platform for new cryptosystems. While GI-Desktop (GID) provides the context for the use of PKI, cryptography underpins both GI's enabling (roaming) and restrictive infrastructure (locked down PC) features. Thus, Oilcom aligned PKI with efforts to standardise desktops and rationalise IT services. The result is a symbiotic relationship, which makes it difficult to extricate PKI from GID fortunes and troubles. The GI proposal stresses the importance of cryptography to GID by stating that,

> "**Various forms of encryption will be offered as a service in the new environment**, e.g. secure (encrypted and/or digitally signed) e-mail. For secure communication over un-trusted networks, such as the Internet, Virtual Private Networks (VPNs) will be set up using encryption."

The proposal stipulates that security efforts must build on activities already underway in the Group and be compliant with Trust Domain, US Export (Cryptography & Data) and European Privacy Export regulations. According to a security consultant, PKI is associated with GID because the latter is a Windows 2000 solution that relies on its core component Active Directory to handle certificates and smartcards. Thus, GID gives the backbone for using certificates. The Principal Architect agrees. He argues,

> "PKI is a technology component within the infrastructure which allows things like SSO. ... PKI is an essential component for using smartcards. .... The main reason for having a smartcard is to do the

> authentication of users to the desktop and the server so that you no longer need to have a password in that circumstance. It also gives you the ability to roam around anywhere. ... However, smartcards are not useful on their own without PKI because the latter enables us to benefit from the security strengths of smartcards such as a tamper resistance. **So PKI, smartcards and other supporting technologies are tied together to provide a service delivered to users via a GI-Desktop.**"

PKI is part of the eArchitecture initiative launched by a new Chief Information Officer in 2000. He raised funding from business divisions to pull together disparate projects into fewer strategic e-business initiatives. The initiative broadly assessed the potential of e-business and e-commerce in boosting profits and cutting costs. In June 2000, the CIO and representatives of the businesses agreed that the infrastructure should be "common user, generic and capable of adoption by any piece of the business and could be mixed and matched." Oilcom created an e-business security work stream within eArchitecture and divided it into Trust Confidence Services, eDirectory and eRegistration projects. PKI belongs to the e-security stream run by a global team with representatives from the UK and other rich countries.

Rationale for PKI

Oilcom hoped to increase security and reduce password management costs through the adoption of PKI, smart cards and thin clients integrated with Windows 2000 native security features. The Group believed PKI would provide better trust and confidence in transactions. A security consultant revealed that,

> "We had accepted that passwords were expensive to support. If you lose your password, you have to wait for an amount of time before the situation is rectified. This means that you do not make a good use of your time. This is an obvious business case. **So we justified the use of PKI and the corporate badge by also looking at the password problem in our changed network access logic.** Smart cards could also save time for the employees because they combined logical and physical security."

The Group also sought an infrastructure that could assure shareholders, regulators and auditors that Oilcom had proper controls around its business applications. As we previously saw, energy companies constantly reaffirm their controls because of the severe brand value and regulatory implications of negligence. The senior Security Consultant argues Oilcom selected PKI because it suited it changed network administration paradigm. He states,

> "The reason we needed to do this is that Oilcom has completely moved its basic network controls or user administrative network controls. Once upon a time Oilcom in common with other big companies we had a closed network, which was opened selectively under very strict controls. **What we now have is an open network, which we selectively close....**One method of selectively closing this network is providing strong authentication, identification, non-repudiation and all these good things which you get from PKI – if you do it properly."

The consultant argues that PKI was an easy choice because, "there is no other alternative at this moment." He adds that Oilcom selected PKI because a number of regulations across the world have made it difficult to resist legally acceptable and binding signatures. These include the UNICITRAL Uniform Rules on Electronic Signatures, the Utah Digital Signature Act, UK Electronic Communications Act, EU Electronic Signature Directive and the US Health Insurance Portability and Accountability Act (HIPAA).

The consultant argues that because the legal and regulatory framework was still in flux, Oilcom sought to understand these laws to control its legal liability and exposures effectively (Oilcom 1997). However, liability and concerns about operability, cost and convenience led Oilcom to reject the idea of acting as a Certification Authority (CA) for the outside world. According to the senior Consultant the major advantage is,

> "You don't carry any liability whatsoever. You wash your hands. You say 'we don't do this, therefore if you need an external certificate this is where you go.' The nature of Oilcom's business is such that we are used to controlling our own liabilities. ... **What we are not good at, and there isn't a company alive that is, I suspect, is managing unknown risks.** Issuing out a certificate to a third party potentially introduces unknown risk, with it comes unknown liability. We have seen what happens when someone faces unknown liability with Enron and Andersen. It isn't a good idea."

Thus, Oilcom preferred to buy the PKI services on demand. However, the Group initially struggled to find providers who could offer a dependable global service. This was because Oilcom needed support for global services in multi-time zones. The security team also asked for permission to customise the security features of Group Infrastructure (GI). The need to modify the infrastructure arose because consultants discovered that GI security features were only suited for internal use. The senior Security consultant argues,

> **"It isn't a gizmo entirely suitable for e-business applications particularly the PKI component. It is no coincidence that no commercial CA uses Microsoft PKI.** The view is that it simply does not fit requirements of a robust external service solution. There are concerns about a number of the detailed pieces of the implementation, which is to do with the design of the product. We understand that is being recognised by Microsoft. It was essentially a toe-in-water, possibly because they decided or weren't able to buy any pieces of the competition ... **I won't say any more** ..."

In response to this charge, Microsoft has taken two steps. First, they bolstered PKI features since Windows 2000 (Microsoft 2002a). Second, in our interviews with three senior managers, the Corporation claimed customers were misusing its software.

Microsoft PKI direction

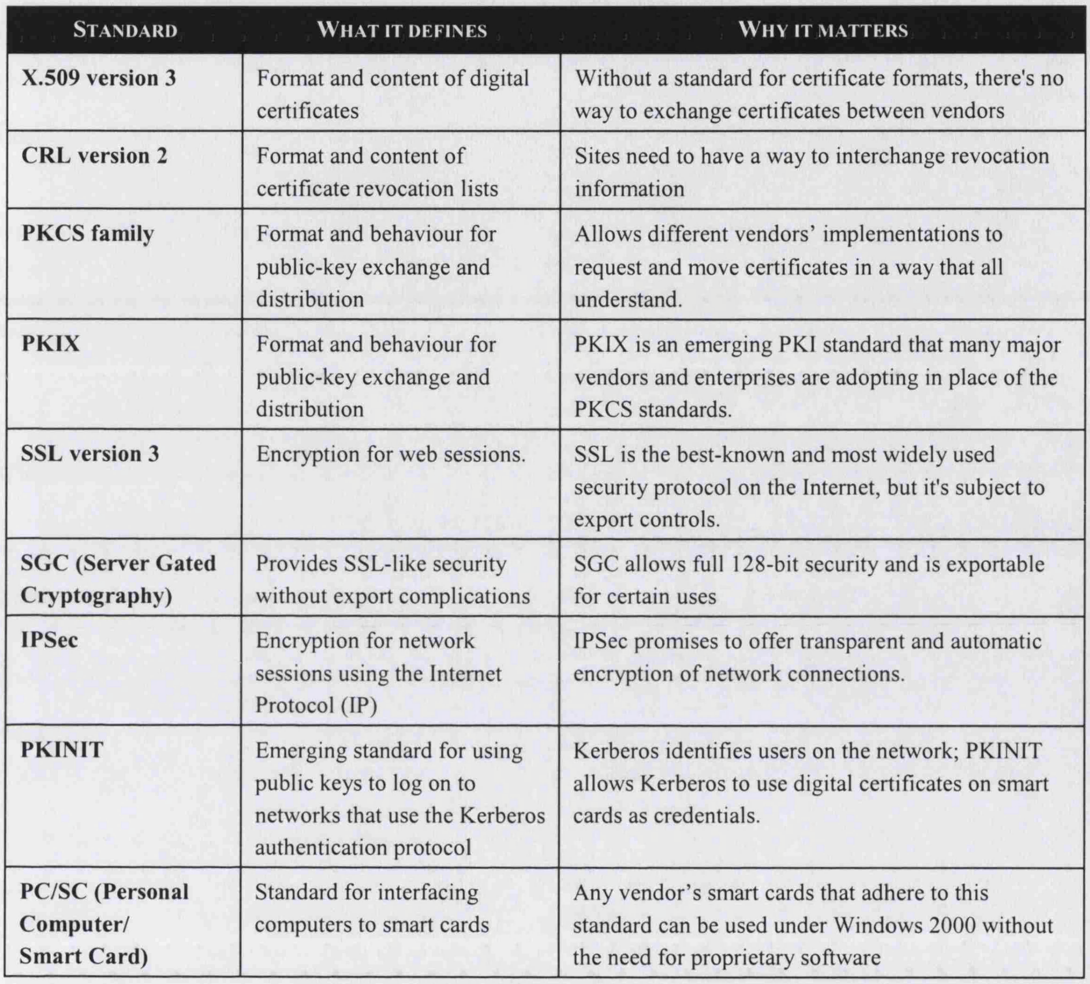
We have seen that the GI proposal explicitly identifies encryption as critical to the success of GID. Therefore, it is impossible to extricate PKI from the problems caused or faced by the GI because cryptography, smart cards and other supporting technologies such as Citrix servers collectively provide a service delivered to users via a GI-Desktop. As we emphasise in Chapters 7 and 8, our discussion of GI dispels a common belief that PKI is an artefact only personified in keys devoid of a context (Microsoft 2002). The technical discussion of Oilcom PKI largely relies on Microsoft's official documents because as a Senior Security Consultant states, "This is a Microsoft shop very much." However, we substantiate this information with comments from our interviews. This section will also be useful for part of our second case study because one protagonist at Bankrecht AG, uses Microsoft PKI. According to Microsoft Corporation a PKI,

> "Is a system of digital certificates, certification authorities (CAs) and other registration authorities (RAs) that verify and authenticate the validity of each party that is involved in an electronic transaction through the use of public key cryptography (Microsoft 2002a)."

Microsoft claims that while it is possible for a single enterprise to use a proprietary vendor solution, open standards lessen the complexities of cross-enterprise exchanges with multiple vendor PKI components. The developers of open PKI standards include the World Wide Web Consortium (W3C), the Internet Engineering Task Force (IETF) and ITU. While admitting that the PKI standards are still evolving, Microsoft claims it,

> "Works closely with these impartial bodies to ensure that its implementation of the standards are correct and fully interoperable. The reason for these standards is simple: **the only way** to achieve true interoperability is through the wide distribution and use of open, vendor-neutral standards. Microsoft has embraced the key PKI security standards and has implemented them (Microsoft 2002)."

To highlight its “openness”, Microsoft enumerates the standards it has adopted.



STANDARD	WHAT IT DEFINES	WHY IT MATTERS
X.509 version 3	Format and content of digital certificates	Without a standard for certificate formats, there's no way to exchange certificates between vendors
CRL version 2	Format and content of certificate revocation lists	Sites need to have a way to interchange revocation information
PKCS family	Format and behaviour for public-key exchange and distribution	Allows different vendors’ implementations to request and move certificates in a way that all understand.
PKIX	Format and behaviour for public-key exchange and distribution	PKIX is an emerging PKI standard that many major vendors and enterprises are adopting in place of the PKCS standards.
SSL version 3	Encryption for web sessions.	SSL is the best-known and most widely used security protocol on the Internet, but it's subject to export controls.
SGC (Server Gated Cryptography)	Provides SSL-like security without export complications	SGC allows full 128-bit security and is exportable for certain uses
IPSec	Encryption for network sessions using the Internet Protocol (IP)	IPSec promises to offer transparent and automatic encryption of network connections.
PKINIT	Emerging standard for using public keys to log on to networks that use the Kerberos authentication protocol	Kerberos identifies users on the network; PKINIT allows Kerberos to use digital certificates on smart cards as credentials.
PC/SC (Personal Computer/ Smart Card)	Standard for interfacing computers to smart cards	Any vendor’s smart cards that adhere to this standard can be used under Windows 2000 without the need for proprietary software

Figure 10 – PKI standards supported by Windows 2000 (Microsoft 2002).

Microsoft claims the use of the open standards developed by security-reliant computing, banking and financial services, legal and governments sectors makes its PKI dependable. The firm claims the ultimate test of the security of an algorithm or protocol is the length of time of its success in public use. Microsoft must have learnt this from its own failed attempts to force proprietary protocols. For instance, Schneier raps the Corporation over its covert work on Point-to-Point Tunnelling Protocol (PPTP) to replace IPSec. The company invented its own authentication protocol, hash function and key generation algorithm (Schneier 1999a). However, PPTP failed miserably.

Windows 2000 supports most respected cryptographic algorithms such as RSA and Digital Signature Standard (DSS) for public encryption; MD4[19], MD5 and SHA-1 for hash algorithms; RC2, and RC4 for secret key encryption. Therefore, Microsoft claims that Windows 2000 offers an open security architecture that allows third party applications including PKI, to use its features. Tellingly, the Corporation adds,

> "**The best place to implement a PKI is in the operating system.** Operating systems already provide a number of other infrastructures, like the printing infrastructure ... and file service infrastructure that retrieves files from shared storage. In both cases, the operating system provides a capacity to transparently and easily use a network service, just as PKI does (Microsoft 2002)."

As we shall see, this is a key statement in the tussle between Microsoft and specialist PKI vendors and current market leaders notably Entrust and VeriSign.

Oilcom PKI components

A number of Windows 2000 security functions use public key cryptography. These include Secure/Multipurpose Internet Mail Extensions (S/MIME); digital signatures; communication using Transport Layer Security (TLS) and Secure Sockets Layer (SSL); local and remote network logon; secure logon credentials using smart cards; Encrypting File System (EFS); secure executable code signing and delivery, and IPSec. Oilcom uses PKI for certificate-based smart card logon, S/MIME, SSL and TLS.

Schlumberger Network Solutions Infosec Group designed the integrated PKI solution. The solution covers physical access, thin client and desktop access using smart cards integrated in Windows 2000. The smart card or Corporate Badge project is a central feature of the GID initiative. In 2000, Schlumberger integrated its DeXa.Badge solution with the Windows 2000 PKI to create a comprehensive set of public key cryptography-based security services and technologies. In 1996, Schlumberger joined forces with Groupe Bull, Hewlett-Packard, Microsoft and Siemens Nixdorf to form the PC/SC Workgroup to address smart card interoperation issues. In 2001, Schlumberger strengthened its IT integration and solutions capabilities with the acquisition of IT consultancy Sema Plc to form SchlumbergerSema. The

[19] MD stands for Message Digest. Like other hashing scheme, MD helps transform data into a unique result that is impossible to change back to the original form.

Oilcom solution below resembles any Microsoft PKI. However, we discuss the specific features incorporated by Schlumberger.

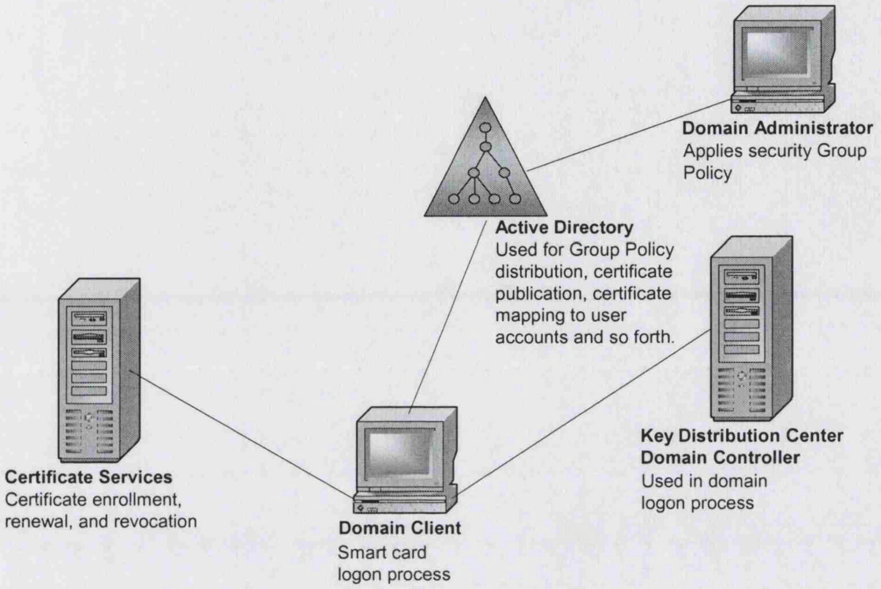

Domain Administrator
Applies security Group Policy
Active Directory
Used for Group Policy distribution, certificate publication, certificate mapping to user accounts and so forth.
Key Distribution Center
Domain Controller
Used in domain logon process
Certificate Services
Certificate enrollment, renewal, and revocation
Domain Client
Smart card logon process

Figure 11 – Windows 2000 Public Key Infrastructure components (Microsoft 2000a).

Certificate Services

Windows 2000 (Win2K) uses X.509v3, the conventional certificate format. Win2K Certificate Services enable an organisation to implement PKI without depending on an external Certification Authority (CA). According to the PKIX Certificate Management Protocols, a CA establishes the identity of certificate holders, revokes suspicious or expired certificates, and publishes a Certificate Revocation List (CRL). In a simple PKI model, an organisation may have one root CA. However, large organisations typically run a number of CAs organised into certification hierarchies (Microsoft 2000a). However, a security consultant claims that Oilcom has not deployed PKI. He states,

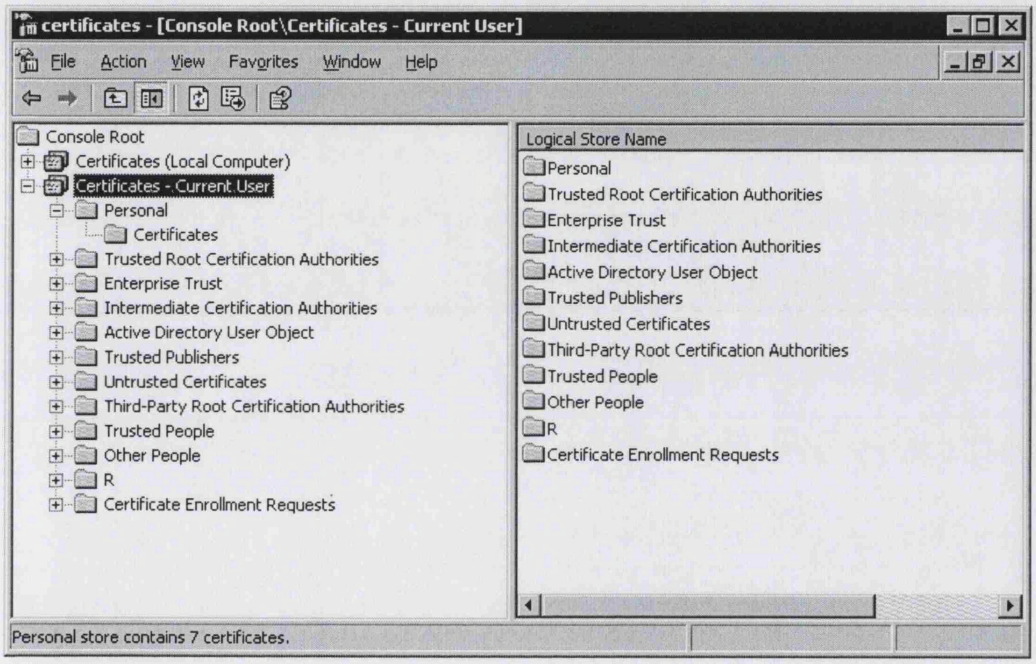
> "We had this conversation before. There is no PKI at Oilcom. They are called certificates and certificates and PKI are very different. PKI constitutes the management processes. It encompasses the understanding that covers the use of these systems. There is no PKI roll out in Oilcom but there is a rollout of internal certificates. We use these certificates internally at Oilcom. These certificates are plugged into Active Directory. …**No and no. No, we are not using Microsoft PKI. We are using Microsoft certificates. There is a distinction.** Are users aware of this? Ninety-five percent do not know and don't understand."

This is startling because, "While public keys are required for PKI-based security, they're usually packaged as digital certificates (Microsoft 2002)." Thus, a certificate is evidence of

PKI. However, certificates only incorporate public key because private keys have to be stored securely for decryption. According to another security consultant,

> "Strictly speaking there is no specific rule that you have to be in the certificate scheme. But the strict answer is that 'yes' you do need to have a certificate. There are circumstances where people are not, currently, on the certificate scheme not because of certificates but other technological reasons. **That again is a reflection that certificates and associated technologies cannot properly accommodate legacy systems and some of the legacy ways we have been doing business.**"

The Microsoft Management Console (MMC) manages all certificates as illustrated.



certificates - [Console Root\Certificates - Current User]

Console Root
- Certificates (Local Computer)
- Certificates - Current User
  - Personal
    - Certificates
  - Trusted Root Certification Authorities
  - Enterprise Trust
  - Intermediate Certification Authorities
  - Active Directory User Object
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification Authorities
  - Trusted People
  - Other People
  - R
  - Certificate Enrollment Requests

Logical Store Name

Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Other People
R
Certificate Enrollment Requests

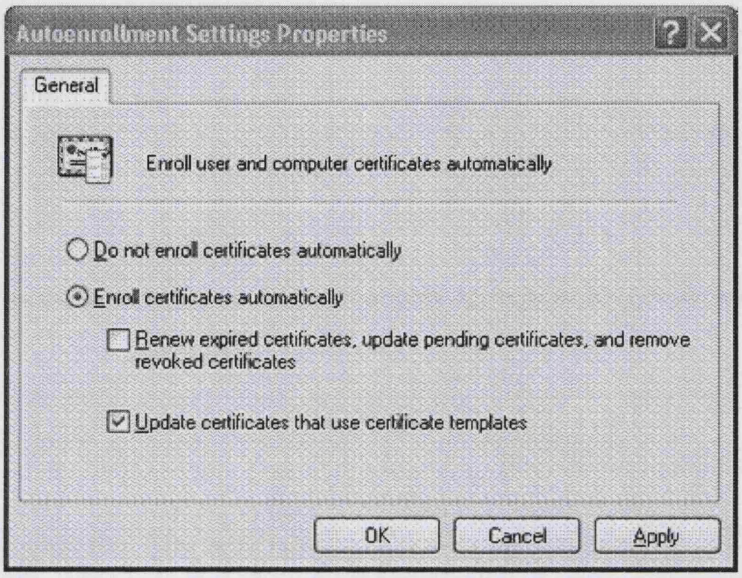
Personal store contains 7 certificates.

Figure 12 – Microsoft Management Console for certificates (Microsoft 2002a).

Windows 2000 removes the need for 'physical' certificate signing because Certificate Services incorporate CA Web enrolment pages that allow the automatic management of certificates. The module installed by default with a Microsoft CA, enables the submission of certificate requests through a browser. Using Active Directory (AD) and Group policies, computers and domain controllers can automatically enrol for machine-type certificates. Machine auto-enrolment facilitates IPSec or L2TP[20]/IPSec VPN connection with Windows 2000 servers (Microsoft 2001). It is also possible to install CA Web pages on Win2K servers

[20] Layer Two Tunneling Protocol (L2TP) is a secure protocol used for connecting Virtual Private Networks over public lines such as the Internet. Practically, L2TP combines two other secure communications protocols namely Point-to-Point Tunneling (PPTP) and Cisco Systems' Layer Two Forwarding (L2F). Microsoft and other firms developed PPTP for secure TCP/IP packet transmission (***Source***: CNET).

that are not running a CA. Windows XP Professional extends auto-enrolment to user certificates as illustrated below.



Enroll user and computer certificates automatically

○ Do not enroll certificates automatically

● Enroll certificates automatically

□ Renew expired certificates, update pending certificates, and remove revoked certificates

☑ Update certificates that use certificate templates

Figure 13 – Auto-enrolment Settings (Microsoft 2001).

User-certificates in Windows XP also rely on Group Policy and certificate templates. Certificates templates are rules and settings applied against incoming certificate requests. Customised templates are stored in Active Directory for use by all CAs in a forest (Microsoft 2002a). With AD, Windows XP automatically enrols for certificates at log on consequently enabling PKI applications like smart card logon, EFS, SSL and S/MIME. Microsoft claims auto-enrolment cuts the PKI total cost of ownership (TCO). We explore the political implications of auto-enrolment, AD and Group Policies in Chapter 7.

Domain Client: Smart Card logon

Oilcom users authenticate to the GID client using smart cards. According to Microsoft (1999a), a smart card is a class of credit card-sized device with varying capabilities that range from stored-value cards, contact-less cards and integrated circuit cards (ICC). Shelfer and Procaccino (2002) believe a ‘true’ smart card has on-board embedded processor or smart chip. Roland Moreno filed the first ICC patents in France in 1975 and the US in 1978. Motorola and Bull produced the first smart card chips in 1977.

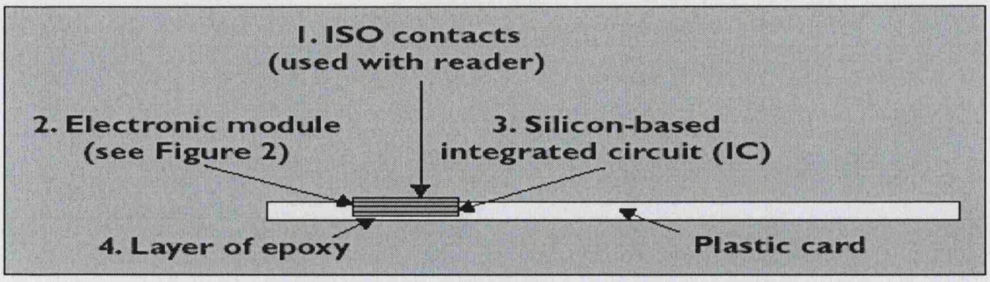

1. ISO contacts (used with reader)
2. Electronic module (see Figure 2)
3. Silicon-based integrated circuit (IC)
4. Layer of epoxy
Plastic card

Figure 14 - Cut away side view of a smart card (Shelfer and Procaccino 2002).

Microsoft (1999a) argues that IC cards are the most useful for network security because they perform sophisticated operations such as digital signature and key exchange.

Smart cards, GID and PKI

Windows 2000 introduced the capability for logging onto workstations and servers with smart cards. The authentication is either interactive, client or remote (Microsoft 1999a). *Interactive login* involves Active Directory, Kerberos v5 and certificates. With *client authentication,* permissions rely on a certificate that matches an account stored in AD. Lastly, *remote logon* involves a certificate with the Extensible Authentication Protocol (EAP) and Transport Layer Security (TLS) to authenticate a remote user to an AD account. Oilcom uses smart cards for interactive and remote logons. We focus on interactive logon and give a detailed account of the procedure under the Key Distribution Centre/Domain Controllers section, which explains the Kerberos Authentication Protocol Version 5.

We saw that Oilcom claims to have deployed smart cards to reduce the costs of passwords, encourage information sharing and improve security. Schlumberger reveals Oilcom hoped to reduce password management costs from the industry estimates of $100 per user annually to $50. As we explain in Chapter 7, smart cards have become at once the primary and yet less threatening personification of PKI at Oilcom. Interviewees largely attributed this success to a long history of badges at Oilcom. In a case study of the Oilcom project for the Smart Card Alliance[21] SchlumbergerSema argues,

> "When used as part of an infrastructure that incorporates public-key cryptography, smart cards can provide tamper-resistant storage for PIN codes, private keys, digital credentials, and other personal information.

[21] The Alliance is a multi-industry association working to accelerate smart card technology application.

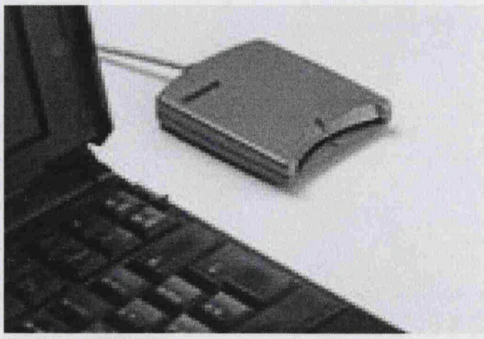
> **Companies can use PKI and smart cards to authenticate users requesting network access, to digitally sign and encrypt documents, and to achieve non-repudiation."**

Apart from the cost issue, smart cards offered Oilcom a simple, user-friendly interface that supported the management committee goal of building e-business capabilities across the Group. The DeXa "corporate badge" solution comprises smart card technology, integration, and program management, and support services. Oilcom choose smart cards for PKI because unlike computer hard disks, they offer secure private key generation, storage and portability (Crossley 2002). A security consultant argues,

> "The medium which we chose was a smartcard and have the certificate on it, on the chip of the smartcard. ...the only way we issue a certificate is by smartcard. I have a certificate because **I have a smartcard and it is part of the GI standard that I have a smartcard.** Thus, the certificate is on the smartcard and the certificate is for authenticating you as you log onto the system."

Oilcom awarded the PKI contract in the winter of 1999. However, the Group fired the vendor in June 2000 for failure to deliver a working solution. Schlumberger won the contract in January 2001 on condition that they met the original schedule. Apart from the restricted time, the number of employees to receive smart cards also increased from 85,000 to 105,000 at 1,200 sites in 145 countries. Oilcom had both underestimated the PCs it owned and acquired new businesses during the project duration.

The DeXa.Badge solution is a centralised credential management system that enables multiple authentication mechanisms like PKI, biometrics and One Time Passwords. The solution also manages building access because of the card's compatibility with most physical access control systems. Schlumberger produces the cards and adds special features on demand. Oilcom uses 16k and 32k Cyberflex Access smart cards that have the Group's colours as background and an image of the cardholder. The card has a return address at the back. However, after corporate advice, the card does not identify Oilcom. The card readers are from the Schlumberger "Reflex" range that supports standard peripheral interfaces such as PCMCIA, USB and Serial, as shown next.



Reflex USB V2

Reflex 20 PCMCIA

Figure 15 – Some of the Schlumberger card readers at Oilcom

The smart card platform includes a Schlumberger Self Service Module centred on a web-based card management system. Developing this web-based, low-overhead system was a huge challenge because nothing comparable existed in the marketplace.

Citrix and Terminal services

Oilcom also asked Schlumberger to design a certificate-based smart card authentication mechanism to a remote MetaFrame server for thin client (Citrix) sessions. No other organisation was using this technology at the time. Citrix enables the deployment of business applications such as Microsoft Office, SAP and Oracle across the network regardless of the client device in use. However, Citrix is more important for retaining centralised IT control. Citrix maintains the locked down PC in association with "Terminal Services" a Windows 2000 feature that allows the creation of independent user profiles in Active Directory. Administrators use the Terminal Services profile to restrict access to applications by removing them from the user's Start Menu (Microsoft 2001a). The same service creates and stores network connections to printers and other resources for user sessions. In Windows 2000, all application execution occurs on the terminal server and only keyboard, mouse and display information moves over the network. Terminal services support the centralised management of applications irrespective of client and network connection.

A Schlumberger add-in enables MetaFrame servers to recognise client card readers as local. DeXa.Badge also runs PKI over Citrix that enables mail signing and encryption, secure web access and high security with two-factor authentication (Crossley 2002). Schlumberger admits these were huge challenges because no organisation had conducted a smart card and Windows 2000 PKI deployment of this scale anywhere in the world. Smart card deployment started in early 2001 with a deadline of the first quarter 2002. However, on 18th October 2002 a senior Security Consultant confirmed the project was still ongoing because implementation problems and acquisitions had increased the workload. Schlumberger claims its solution is flexible because it works with all major PKI vendors. Apart from the initial trouble with printing the cards, a Security Consultant believes the smart card deployment has been smooth. While the success is widely linked to the history of using badges, the new smart card is much more powerful than users realise. The security consultant reveals,

> "This new card has an extra bit on it. It has a 'proximity swipe' on the back, smartcard on the front. **The card gets me my lunch everyday; it gets me into the building and logs me onto my machine.** .... That was quite a conscious thought when they were formulating the smartcard project. ... They did say 'we will consciously put the certificate on the access mechanism to your PC on the same card you get lunch with because in that case you won't forget it'."

As such, contrary to the official IT security line, the DeXa.Badge is revolutionary. The link of the card with the cafeteria was clever because lunch sessions are professional activities at Oilcom. According to a technical consultant project teams use lunch to present reports and share knowledge. She says consultants also use lunch to resolve problems and pitch for future work by highlighting their expertise in specific areas.

However, the combination of functions on the card took time. A security consultant reveals that at the beginning all users had separate cards for physical and network access. He claims this was because of technological and organisational issues that the project initially struggled to overcome. We shall see that Bankrecht AG not only has separate cards for logical and physical security, employees still use cards from two banks that merged in 1998 to create this Group. A senior Security Consultant stresses,

> "We are committed to a single infrastructure across the world which means **I can go to any other office with or without my laptop but certainly with my smart card and my data is there for me**. Certainly, we have a large number of travellers. Some people travel an enormous amount. Others travel infrequently. We must turn our various businesses into single entities across the globe, which they haven't been. They should be able to see exactly the same thing wherever they have their people, which is as it should be. Gone are the days when Oilcom was managed on a country basis."

Therefore, smart cards are cardinal tools in the efforts of Oilcom to establish the identity of users on its gargantuan network, which was proving very difficult with the proliferation of networks, the Internet, thin clients and PCs. In addition, the combination of logical and physical security on one card has not only set a firm foundation for security but is also the mainstay of the efforts to standardise IT provision within the Group.

Active Directory (AD)

Active Directory is at the heart of Windows 2000 PKI (Lowe-Norris 2000, Microsoft 2000a, Microsoft 2001a). Although PKI can function without directories, a combination of the two technologies delivers better business value (Austin 2001). Microsoft enshrined the dependence of its PKI on AD by attaching most of the critical functions for large organisations to the directory. Microsoft reveals,

> "Active Directory is tightly integrated with Windows 2000 security services such as Kerberos authentication protocol, **public key infrastructure**, Encrypting File System (EFS), the Security Configuration Manager, Group Policy and delegated administration. This integration allows Windows applications to take advantage of the existing security infrastructure (Microsoft 2000a)."

Other key features requiring AD are IntelliMirror, a configuration management system and Global Catalog (GC) for unified information view. The Corporation claims that while Windows 2000 Server and Professional individually have security features to protect information stored on individual PCs, "comprehensive, policy-based security that controls access to networked resources" should incorporate AD and enjoy its distributed security features. Microsoft warns that most advanced Windows 2000 security features require Active Directory (Microsoft 2001a). Like other large organisations, Oilcom uses the directory to store information about users, hardware, applications and data on network users. To a senior Security Consultant,

> "We realised that Active Directory is a complex piece of infrastructure. We knew AD was going to be even more critical than the X.500 directory it replaced. We are using it for a whole range of different things, which are not immediately obvious to the users of Microsoft systems. ... **Active Directory is more of what we thought it would always become: a multipurpose animal.** ... It (AD) is an absolutely critical piece of infrastructure because if we cannot find people or certificates in it, we cannot operate this business. As simple as that."

Active Directory is also a focal point for the validation of information on Certificate Revocation Lists (CRLs), facilitates key recovery and storage of encrypted private keys. Microsoft claims that since Windows 2000 uses AD to store public key information, its PKI is easier to manage because there are no new tools to learn, components to install or manage. In contrast, many other PKI products create unique stores for certificate and CRL data and require separate databases for users, computers and PKI data. Critically too, Microsoft claims, "Third-party PKIs must be purchased separately, and require per-certificate *license fees* and increased management tasks (Microsoft 2001)." We return to the certificate fee issue in the Bankrecht case study. The storage of certificates, CRLs and policy details in AD allows the replication of the data using the directory's native features. Microsoft argues,

> "Unlike the flat-file directory used in the Windows NT Server operating system, Windows 2000 Active Directory stores information in **a logical hierarchy that represents your business structure**. This allows for greater growth and simplified management (Microsoft 2000a)."

Active Directory divides the hierarchy into domains, organisational units (OUs) and objects. The hierarchy logic attempts to organise network resources in a way similar to the storage of files and folders on a Windows PC. The AD hierarchical structure looks as follows.

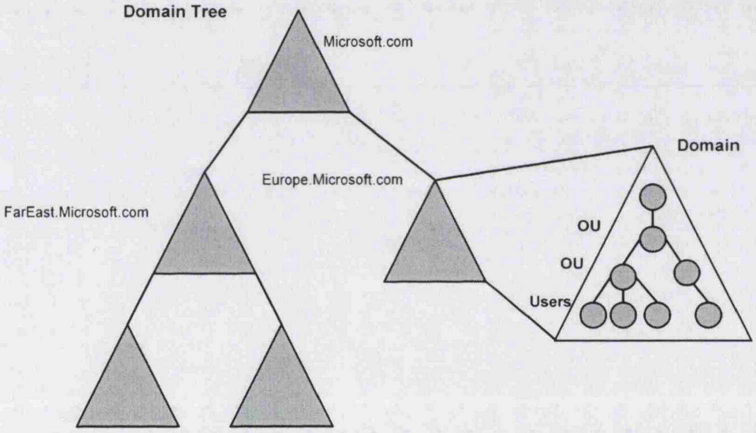


Figure 16 – Hierarchical structure of the Active Directory service (Microsoft 2000a).

A central concept of the logical hierarchy is a domain. Microsoft defines a domain as a collection of network objects such OUs, user accounts, groups and computers that share a common directory database with respect to security (Microsoft 2000a). Domains play a critical role in security because they form the core unit of the logical structure within AD. Grouping objects into domains allows the network to reflect the organisational structure.

As illustrated above, large organisations may contain multiple domains creating a hierarchy named a *Domain Tree*. The *tree* contains multiple domains connected by trust relationships and a common schema, configuration and global catalog (Microsoft 1999a). The first domain under the Tree is a *Root Domain* and all domains beneath it are *Child domains*. Oilcom has largely amalgamated all its domains into one. However, the Service Companies were yet to migrate from the child domains. Domains contain OUs, which are containers for organising objects into logical administrative groups. An OU can include user accounts, groups, computers, printers, files shares and other OUs (Microsoft 2000a). By October 2002, Oilcom had over 100,000 device and 110,000 people records in AD. The Group used AD to populate the global address list within the Exchange infrastructure until the completion of the migration to Exchange 2000. The migration slowed down after the records negatively affected Active Directory's performance.

Group Policy

Active Directory supports fine-grained access controls that allow administrators to specify who can see, change and copy directory information (Microsoft 2002). This feature depends on the ability to group information into domains and OUs enabling administrators to manage security for a collection of objects such as computers rather than each object individually (Microsoft 2000a). This is a function of Group Policy (GP), a primary tool for defining and controlling how programs, networks resources and operating systems function for users and computers (Microsoft 2001a). In brief,

> "**Group Policy is a significant feature of Active Directory because it lets you apply all types of policies to large numbers of computers in a uniform way**. For example, you can use Group Policy to configure security options, manage applications, manage desktop appearance, assign scripts, and redirect folders from local computers to network locations (Microsoft 2000a)."

Group Policy applies to users or devices based on their membership in sites, domains or OUs. The settings apply to computers at boot time and to users at logon. Administrators use Group Policy to define extensive security policies for the domain say defining minimum password length and intervals for their changing. Group Policy can override settings at lower levels.

Active Directory permits administrators to *delegate* responsibility within a forest or domain. Administrators may create OUs and assign control for particular users or groups to someone else. The control covers specific operations such as creating groups, controlling membership lists and adding accounts to the domain. However, "Group Policy settings and user groups let administrators precisely define delegated authority. ... Further, because of fine-grained access control, administrators can narrowly define the scope of the delegated tasks (Microsoft 2000a)." This is a key centralising feature of Active Directory because while support groups have power to undertake some activities, the administrator retains full control over user accounts. Group Policy also controls PKI. For instance,

> "PKI components that integrate with Active Directory **can use its policy mechanisms to control who may request certificates, who may fetch them from the directory, how long certificates remain valid, and so on** (Microsoft 2002)."

Group Policy automatically distributes certificates to users and machines, establishes certificate trust lists and lists of trusted CAs and manages recovery policies for the Encrypting File System (Microsoft 2000a, Microsoft 2002a). Windows 2000 also stores certificate templates in AD. Enterprise CAs use the templates to determine certificate format, key size and the required X.509 extensions (Microsoft 2001).

Key Distribution Centre/Domain Controllers

The KDC/DC is central to the domain logon process. Windows 2000 implements the Key Distribution Centre (KDC) as a domain service which uses Active Directory as its account database (Microsoft 1999a). The KDC is a Kerberos service. The Kerberos Authentication Protocol provides a mechanism for mutual identification between a client and server, or between different servers (Kohl and Neuman 1993, Microsoft 1999a). Kerberos is a product of an MIT project entitled 'Athena' that hoped to stop hackers from capturing network passwords (Bellovin and Merritt 1991, Neuman and Ts'o 1994).

Kerberos Version 5 (v5) relies on the shared secrets authentication technique. A Kerberos client (Windows 2000 workstation) and Kerberos Server use a symmetric cryptographic key to verify one another's identity. Kerberos derives the encryption key from a password (Neuman and Ts'o 1994). This is an improvement on the Windows NT 4.0 proprietary NT LAN Manager (NTLM) Challenge-Response, which requires a separate client authentication for each network resource the user accesses. Kerberos v5 is the primary security protocol for accessing resources in Windows 2000 domains. By default, Kerberos v5 creates a two-way transitive trust relationship between security authorities.

Kerberos authentication depends on *tickets*. The Key Distribution Centre (KDC) provides these tickets through a single process comprising of the Authentication Service (AS) and the Ticket-Granting Service (TGS). The AS issues Ticket Granting Tickets (TGTs) to users, machines and services, or authenticated principals, for admission to the TGS. The TGS issues tickets for admission to other services in the domain or to a TGS in another trusted domain (Microsoft 1999a). Windows 2000-based Domain Controllers (DC) implement Active Directory with an integrated KDC to ensure the storage of information in a single directory.

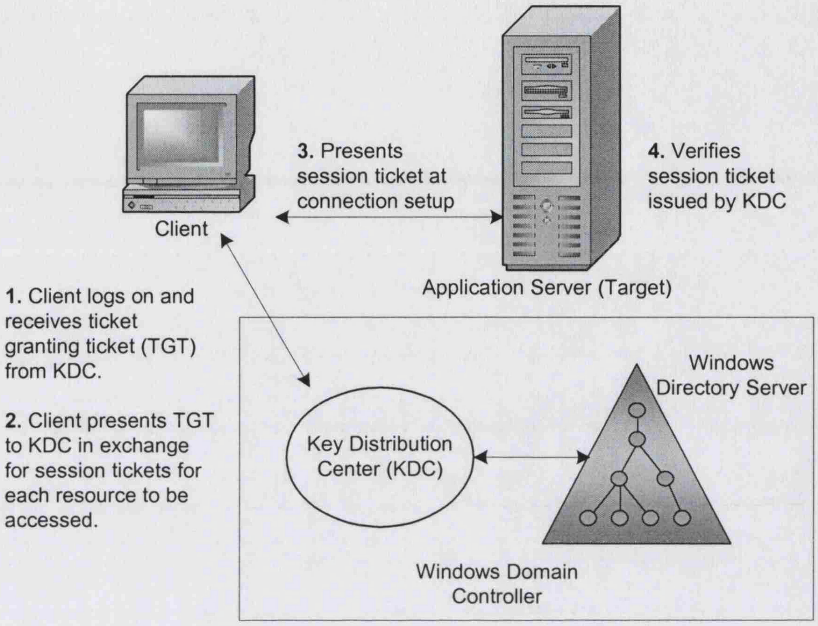

Client
3. Presents session ticket at connection setup
4. Verifies session ticket issued by KDC
Application Server (Target)
1. Client logs on and receives ticket granting ticket (TGT) from KDC.
2. Client presents TGT to KDC in exchange for session tickets for each resource to be accessed.
Windows Directory Server
Key Distribution Center (KDC)
Windows Domain Controller

Figure 17 – The Kerberos authentication process

When a user logs onto a domain, Windows 2000 locates an Active Directory Server and Kerberos authentication service. Smart card authentication uses information encrypted from a private key with its public key registered in AD. The ability to authenticate users initially with public key certificates instead of passwords or shared secrets is an extension to the Kerberos v5 protocol proposed by the IETF called PKINIT. PKINIT is the basis for Windows 2000 smart card logon support. *Interactive* smart card logon begins when a user inserts a smart card into the reader causing the display of the Graphical Identification and Authentication (GINA) component of Windows 2000 logon. This prompts for a Personal Identification Number (PIN) instead of a username, password and domain name. However, the PIN only authenticates users to the smart card not the domain as illustrated.

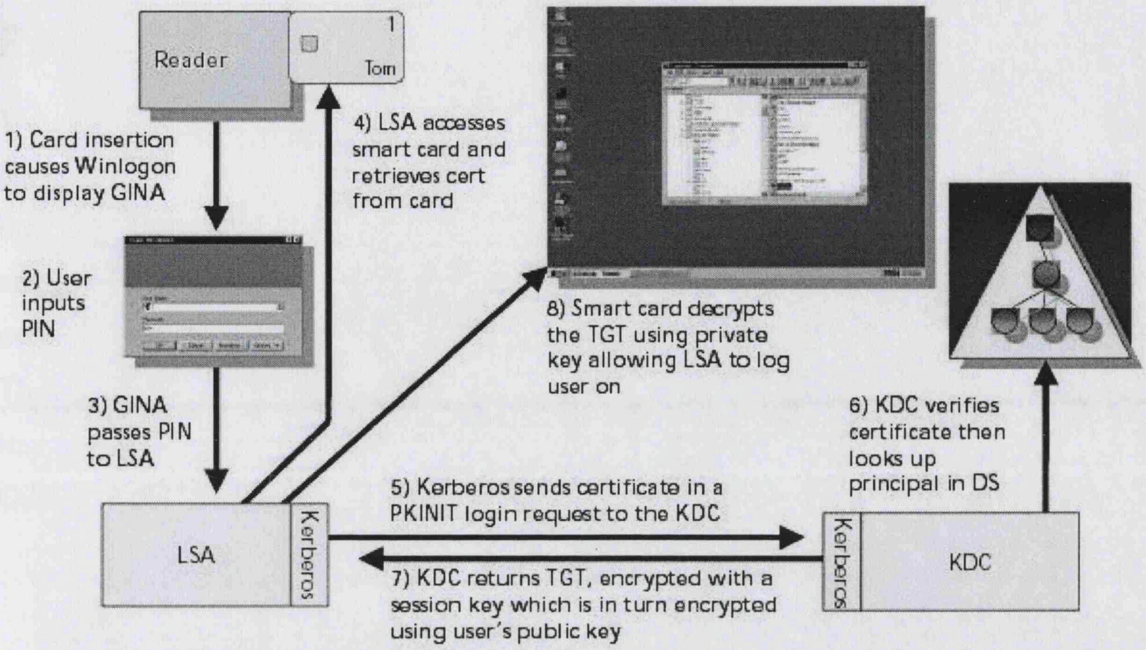

Reader
1
Tom
1) Card insertion causes Winlogon to display GINA
2) User inputs PIN
3) GINA passes PIN to LSA
4) LSA accesses smart card and retrieves cert from card
5) Kerberos sends certificate in a PKINIT login request to the KDC
6) KDC verifies certificate then looks up principal in DS
7) KDC returns TGT, encrypted with a session key which is in turn encrypted using user's public key
8) Smart card decrypts the TGT using private key allowing LSA to log user on
LSA
Kerberos
Kerberos
KDC

Figure 18 – Interactive Logon with certificate in Windows 2000 (iT_SEC 2002).

After the initial stage, Kerberos v5 protocol and its PKINIT extension authenticate the user to the domain using a certificate stored on the card. Windows 2000 uses the PIN and certificate to initiate actions that identify and authenticate the principal. The logon request goes to the Local Security Authority (LSA), which forwards it to the Kerberos authentication package running on the client (Microsoft 1999a). From here, the Kerberos package sends an Authentication Service (AS) request to the KDC service on the Domain Controller asking for authentication and a TGT. The Key Distribution Centre verifies the path of the certificate to ensure that it can be trusted before satisfying the AS request. If the KDC fails to build a valid path, it turns down the request. The KDC also verifies whether the CA is authorised to issue certificates that are a basis for authentication within the domain. Windows 2000 demands that trusted issuing CAs must be of enterprise type published in Active Directory.

Politics of GID and PKI implementation

We previously highlighted the link between PKI and GI-Desktop (GID). This relationship both helped PKI institutionalisation but also exposed it to the problems of GID. This was inevitable because GID drastically reconfigured the support arrangements in favour of the central IT team at the expense of local providers. One of these changes was the creation of a network of international support centres in Malaysia; Texas, US and Manchester, England. The rationalisation led to job losses because the centrally managed infrastructure required less support staff. The GID centralisation drive also clashed with the historically distributed Oilcom organisational structure causing huge resentment. A business consultant reveals,

> "I think the problems we have had implementing GI are symptoms of a wider issue that we have had for decades in Oilcom, which is that **nothing is really ever driven from top-down**. We are not a kind of company where there is a very strong command and control structure. Everything historically has been consensual and operating companies have had a lot of autonomy. So you have got this company that has got a deep culture in history of OCs doing their own thing and then you appoint some poor GI Project Manager and tell him to drive something from top-down when that is just counter to the whole culture of the company. So I don't envy the person who has had to manage GI."

A team leader agrees. He argues that the biggest problem with GID is that it abandoned the traditional approaches to system deployment at Oilcom. All large system deployments normally start with a 'Stakeholder Analysis'. The analysis looks at how an IT system impacts on different people, whether they are ready to change, how much they understand the change and whether they have reached a stage of actively supporting or preventing the system. From the analysis, ITI assigns much of the system responsibility to the user division. To the Team leader, "What we try and avoid is a belief that a bunch of IT people come in from nowhere, put a system in and go away." However, this is exactly what happened with GID because top management directed its swift deployment without consulting operating companies.

The central IT team also lacked control over GI costs because Oilcom raises funds for big projects from business divisions. In return, the divisions demand a comprehensive business case, especially the impact of the new infrastructure on autonomy. A technical consultant believes the GI deployment problems were inevitable because the decentralised Oilcom structure encourages politics. She reveals,

> "It is not as easy to work together through different departments of Oilcom **because of political reasons.** There is a lot of talk about 'stealing' work even internally, which is not a very good situation. .... It doesn't

> always feel like it is one company in that sense because different people and departments have their own goals and they are not always willing to share the knowledge they have throughout the company … **I don't think things are quick enough because of the politics.**"

As part of our triangulation exercise, we showed this view to respondents at various levels of the hierarchy. The statement excited heated debate. For instance, a security consultant totally disagreed with the observation. He insisted,

> "When that person talks about 'because of political reasons' that makes it sound like **there is an undercurrent of Machiavellian people running around the place building empires etcetera**. I do not believe that is the same Oilcom I work for. … departments not working together is common ... However, it is not an inhibitor at Oilcom. **But stealing work? No. Not that I am aware of!**"

The Principal Architect also doubts the statement. He argues politics is a covering word and often an excuse when people fail to achieve their objectives. However, he apparently reveals the political angle of Group Infrastructure (GI) when he says that a key project objective was to support full information access within Oilcom. He states,

> "Interestingly, a key driver of GI is full access to information because now the businesses are too restrictive. … In a way, we are using IT to break through the barriers of people creating their own fiefdoms … The IT would not change people's attitudes, the businesses and the organisations or the people factors, but at least we will make sure that the IT is in support of what we want to achieve. Oilcom is a big company which operates in many cultures and countries around the world, so **the people side of things is probably the bigger challenge facing a new information system.**"

Chapter summary

This Chapter presents the first of our two case studies. We discuss the Oilcom business environment including its history, nature of business and governance structures. The technology adoption process follows. We assess the IT standardisation efforts especially the rigidly enforced GID client that provides a context for PKI usage. Next, we discuss the PKI technical features. We conclude with a focus on the politics of PKI and GI.

CHAPTER 6:
BANKRECHT PKI EFFORTS

Introduction

This chapter *shows* field data by discussing the power issues surrounding PKI at Bankrecht. Despite mergers and acquisitions abroad, Bankrecht is an archetypal security-conscious Swiss bank. Thus, apart from pioneering large-scale PKI use, Bankrecht is an interesting case study because security is vital for its survival. We proceed as follows. First, we summarise the two phases of the study. Next, we describe the business environment and the effects of secrecy laws on governance structures. Under social aspects, we explore the cohesive power of the Bankrecht brand. The technology adoption theme traces the life of the PKI since 1992. The first phase ends in chaos with many independent divisional CAs because Bankrecht failed to mobilise institutional support for the infrastructure. Branding intervenes in the second phase to give wings to the fledgling dream of a centralised PKI.

Pioneering PKI efforts

The PKI project preceded the merger between two Swiss banks that created the current Bankrecht AG. According to an original member of the PKI team, one of the two banks, we refer to as Bankrecht X, decided in 1992 to use X.509 certificates and smart cards. However, unlike Oilcom, that uses smart cards for interactive certificate-based logon, Bankrecht largely employs the card as a password and certificate repository.

We conducted fifteen interviews in both Switzerland and London averaging an hour. Our respondents included a member of the original PKI team who is now a Vice President, the Director IT Security, Associate Director IT Security/PKI Project Leader, a member of the original PKI engineering team and Head of Smart Card Infrastructure (SCI) Project. Others were leader Smart Card Production team, members of the second and first-level User Support teams, an engineer of the PKI/Windows Core Technologies team and several users. We also include data from iT_SEC the integrator of the PKI solution and Entrust. This information covers the first phase of the PKI from 1992 to September 2002.

The second phase starts after a management decision in late 2002 to abolish all subsidiary brands by June 2003. Bankrecht claimed this is "a further evolution of its brand strategy and portfolio." We evaluate a series of lively e-mail exchanges between several parties led by Zurich-based Wealth Management & Business Banking (WM&BB). The PKI became a part of Orlando, the re-branding drive, following Bankrecht Investment's inconsistent naming of its root Certification Authority (CA). In the first phase, Bankrecht Switzerland (BS) claimed BI should adopt the Swiss PKI because they had more experience with large deployments. In contrast, WM&BB promotes centralised PKI by proxy because it focuses on branding.

Like Oilcom, we were obliged to protect the real identity of our study organisation and respondents as a condition for research access and ownership of the data. As the readers will realise, we present controversial information from an on-going project, which may worsen the already frosty relations between the divisions. However, we present enough hints for people conversant with Swiss banking to guess the organisation.

Business Environment

Bankrecht claims to be one of the world's leading financial firms "serving a discerning global client base" with assets worth over £428 billion. Bankrecht AG operates worldwide as an integrated investment services firm with a diversified portfolio ranging from wealth management & business banking, asset management, securities, investment banking and fund management. It has five business divisions. These are Private Banking covering Swiss and international clients; Wealth Management in the US; Investment Banking and Securities under Bankrecht Investment (BI); Institutional Asset Management and Funds and lastly, Retail and Corporate Banking in Switzerland.

Bankrecht claims world leadership in private banking services and a good position in global asset management. Its investment banking division (BI) is also among the pre-eminent global houses especially in Europe. Bankrecht, with a close rival, easily lead corporate and retail banking in their native Switzerland. The firm operates in over 50 countries covering all major international financial centres and employs over 70,000 people. Bankrecht supplements its global physical presence with online services. The Group also has business relationships with more than 3,000 financial institutions.

Nature of business

Bankrecht believes that as an integrated Group, not merely a holding company, it provides a better service to clients by drawing on expertise from its various businesses. It was in pursuance of this "one firm" approach that in late 2002 Bankrecht consolidated its trading into a single brand. We explain the implications of the re-branding drive on PKI later. The bank serves what it terms a 'discerning' global client base of 'high net worth' individuals. As such, Bankrecht focuses on wealth management because,

> "The secular trends affecting the investment world make wealth management the most attractive segment in the financial industry. As individuals continue to increase their reliance on equity investments ... the demand for wealth management products and services will increase. **This growth is expected to be highest among our core affluent target market.**"

Bankrecht already claims leadership in global wealth management. It has over 11,000 client advisors who manage CHF 1.5 trillion of invested assets. Bankrecht runs the operations through a US investment firm, a global private bank, and uses third party banking products and services. The Group insists that private banking is not just a niche within the Group but wealth management is central to overall strategy because,

> "Wealth management is a profitable business, with low capital requirements, **a stable revenue base and high barriers to entry**, thanks to the breadth and depth of products and services that today's demanding clients require."

The products and services range from investment services and portfolio management to comprehensive financial planning, real estate advice, Islamic funds and art banking.

Swiss Banking Secrecy

Probably the biggest reason for the success of Bankrecht and other Swiss banks in wealth management is the country's Banking Secrecy laws. To Schneider (2002) the concept of financial privacy is firmly entrenched in Swiss laws, regulations and culture. He argues that, "In an instance of profile following principle, financial privacy also provides a competitive advantage for Swiss financial institutions (Schneider 2002)." However, the recent storm over the Swiss handling of bank accounts for Jewish holocaust victims showed that secrecy is a subject of impassioned conflicts and debates (Guex 2000, Studer 1997). The Swiss have been accused of other questionable deals like,

> "In the '70s, it was the Wall Street insider traders, in the '80s it was the Pizza connection, a drug ring operating out of US pizzerias and the Lebanon Connection, a Lebanese-Turkish drug operation, and in the '90s came news of Italy's corrupt officials using Swiss bank accounts as a hideaway. Claimants are still fighting over who should get funds deposited in Swiss banks by former Philippine president Ferdinand Marcos (Studer 1997)."

Guex (2000) argues that the maintenance of secrecy has been a major objective of Swiss authorities throughout the twentieth century and exerted a substantial influence on domestic and foreign policy. He contends that Swiss authorities devised their financial system to create conditions for the expansion of secrecy explaining why the policies have been consistent over the years. However, banking secrecy has caused recurrent tensions between Switzerland and other countries notably the USA over Jewish deposits (Guex 2000) and recently the USA Patriot Act[22] (Schneider 2002).

Secrecy has been rooted in Swiss banking activity since the end of the nineteenth century. Guex (2000) argues that the Swiss ruling circles strengthened the law as a business strategy to take advantage of the exorbitant taxes levied by many European countries on the wealthy propertied classes. Recognising that Switzerland could not compete with the commercial power of London, Paris and Berlin, Swiss bankers saw heavy taxation as an opportunity to attract foreign capital (Guex 2000). This was around 1901. However, after a crisis in 1931, farmers and Socialist parties pressured the Federal government to take more control of the banking sector to protect the lower and middle classes. Surprisingly, the Federal Banking law adopted in 1934 reinforced the practice by making,

> **"Violation of banking secrecy subject to criminal law and the possibility of both heavy fines and up to six months' imprisonment.** In principle, such violation had to be automatically prosecuted by the legal authorities, even if the injured party did not sue (Guex 2000)."

What does the history of Swiss banking secrecy have to do with our study? The answer is as follows. Security, or more precisely confidentiality, is a matter of survival for Bankrecht. Good security not only gives the bank competitive advantage in wealth management, it averts the risk of heavy fines and criminal liability. This explains the drive to deploy a centralised PKI and the relative ease of its acceptance in Switzerland. However, the PKI solution run into difficulties abroad especially in London because the foreign divisions are more concerned about availability than confidentiality.

[22] The Act imposes tough sanctions on US and foreign banks that fail to identify sources of foreign assets.

Brief history

Bankrecht AG is a product of a 1998 merger of two Swiss banks. We refer to the bigger of the two banks as Bankrecht X and the other as Bankrecht Y. The new entity created a network of 645 branches in Switzerland and another 159 offices abroad. Unlike many other countries that distinguished between deposit and investment banks in the 1930s, the Swiss 'universal' banking model offered various services under one roof. However, foreign acquisitions transformed the banks from archetypal purveyors of "Swiss universal banking" into global financial groups. We briefly discuss the histories of the two banks.

Bankrecht X was created in 1912 by a merger of two Swiss banks. From its inception, the bank focused on the local market by taking over several banks in Swiss cantons and setting up its own branches. In 1945, Bankrecht X moved its head office to Zurich and acquired a major bank. After years of relentless growth, it became the biggest bank in Switzerland in 1962. Bankrecht only moved abroad after World War II with the opening of a London branch in 1967 and New York in 1975. The bank had acquired a British brokerage firm in 1966. Despite these foreign forays, Bankrecht remained a promoter of the Swiss universal banking concept. By 1998, Bankrecht X had assets of CHF 557.6 billion. The bank managed a Swiss business network of 357 branches and another 82 abroad.

Bankrecht Y was founded in Basel, Switzerland in 1872. From the outset, the bank emphasised foreign operations leading to the opening of its first branch abroad in London in 1898. A New York agency followed in 1939. Bankrecht Y focused on foreign operations to an extent that despite opening branches in other regions of Switzerland at the start of the 20th century, it only made major nationwide expansion in the 1960s. In 1945, Bankrecht Y acquired a big Swiss bank, which improved its local network. In Switzerland, Bankrecht Y applied the universal bank model to corporate and retail accounts but it concentrated mainly on commercial banking for corporate clients abroad.

In the 1990s, Bankrecht Y bolstered its international credentials with major acquisitions. For instance, in 1995 it acquired a venerable investment bank in London. The investment bank became Bankrecht Investment (BI) after the 1998 merger. The independent-minded BI is a major protagonist in PKI institutionalisation fallout at Bankrecht. In the same year, Bankrecht

Y acquired two banks in Chicago, USA and took 90% ownership of an Italian partnership. At merger, the bank was worth CHF 438.9 billion and operated a Swiss network of 288 branches and 77 offices abroad with over 27,000 employees. The merged entity acquired a prominent New York securities firm in 2000.

Governance structures

The top administrative bodies at Bankrecht AG are a Board of Directors and the Group Executive Board. The Board is the supreme body with responsibility for the overall direction of the Group and the supervision of its executive management. A chairman who is responsible for corporate governance, public and political affairs and strengthening corporate culture, heads the Board. The executive board has the management responsibility for the company. It implements strategy, aligns business divisions to the 'integrated model' and exploits synergies within the Group. The board and its head, the President, are answerable to the Chairman. The board performs these functions through the 'Corporate Centre', which ensures that the divisions operate as a coherent and effective whole. Thus, Bankrecht always aspires to carefully plan the portfolio of its businesses and ensure they stick to the overall corporate goals. Bankrecht claims that its organisational structure both creates robust checks and balances and allows management the flexibility to make appropriate decisions.

Social aspects of Bankrecht

Unlike Oilcom, whose Service Companies only perform an advisory role, Bankrecht tightly controls policy from its headquarters in Zurich and Basel. The bank claims that while to the outside world its strength derives from products and technology, it also has powerful intangible features. The bank claims the intangible factors include, "the values we share, our culture, our client relationships and our brands." Bankrecht coined five elements to encompass all the intangibles. The elements are *brand and identity, knowledge and innovation, talent and culture, client relationships and financial intelligence.* To Bankrecht while each element is individually important, they collectively define the personality of the Group. We shall restrict ourselves to brand and identity, talent and culture because they are directly relevant to the PKI project. Bankrecht claims its name is,

> **"A seal of quality guaranteeing trust, dependability and professionalism** ...Its effect is to instil confidence in us from our clients and to act as a unique door-opener, granting all of our business Groups around the world access to new and successful relationships."

The bank declares that a key strength of its culture is the close co-operation between different businesses. It requires all employees to demonstrate its principles and values and act as 'brand ambassadors.' Bankrecht places particular emphasis on the consistency of the brand because of its centrality to business strategy. The Group demands that all advertisements, branch network and publications such as websites consistently reflect the brand. As such, the bank requires all its businesses to show a clear understanding of the brand contours because,

> **"The key is to create a broad brand vision or identity that recognises our brand as something greater than a set of attributes that can be imitated or surpassed.** In particular, a company must consider its brand not just as a product or service, but as a symbol and even a personality."

Bankrecht AG claims the 'brand-as-personality' perspective associates people, culture and values with the brand. The link reportedly strengthens the bank because the outcome is more resistant to imitation than product attributes. Bankrecht further claims a personality makes a brand more memorable and becomes a vehicle for expressing customer identity. However, the bank concedes the challenge of brand consistency is,

> "By no means small when we consider the diversity present within the (Bankrecht) Group. **There are various business groups, each with their own character, spread across six continents, dozens of languages** – and yet there is only one (Bankrecht)."

Bankrecht claims diversity is not an encumbrance since its culture takes the best from all divisions to create a corporate image. The bank argues that from innovation, client focus, global appreciation, client privacy or technological skills, every merger and acquisition contributes to a defining characteristic of the Group. Thus, Bankrecht declares,

> "**We do not pretend to inject a uniform ... culture across all 70,000 staff**. Not only would this be impossible, it would also negate the strength of national and business individuality, and that would be wrong. It is a strength that in Tokyo for example, our local culture will reflect national culture and this will be quite different from the culture we project, say, in Madrid or San Francisco. ...So, our approach to culture in (Bankrecht) is to accept and acknowledge that diversity is a strength."

Thus, despite efforts of the "corporate centre" to control policy, in practice business units operate under localised organisational structures with enormous autonomy from the head offices. However, Bankrecht warns that diversity is not a licence for a free-for-all culture jungle. The bank promotes openness, intellectual honesty and ethical standards as core cultural values common to all divisions. *Openness* deals with acceptance of new ideas and unfettered communication with stakeholders. *Intellectual honesty* focuses on a consistent tone of communication and respect for all views, including controversial ones. The *ethical standards* value rejects all forms of discrimination. However, diversity is wobbly because the Swiss "corporate centre" frequently seeks to dictate organisational culture.

Technology adoption process

Information Technology is a critical resource for all banking services and products. The IT division aims to operate, “a stable, secure, efficient and reliable IT infrastructure at competitive prices.” However, Bankrecht insists, “The aim is always to develop products, services and technology that align the interests of the bank and all its client groups.” The IT division manages all applications throughout their life cycle on behalf of the business divisions, which control the budgets. Despite claims that IT is a “core competency” Bankrecht underlines its support role by arguing that,

> “Technology can help advisors to match their clients with appropriate products and services. **Technology supports but never supplants the client/advisor relationship.**”

However, technology is important. For instance, in private banking a web-based interface allows client advisors to model and demonstrate portfolios and their risk characteristics online. Likewise, the US wealth management division operates a portal that allows clients to access full account information; monitor potential investment with portfolio software and receive stock quotations and news from Reuters. The Group also uses web-enabled proprietary platforms to help financial advisors track clients and markets through up to the minute access to research. In 1996, Bankrecht Investment (BI) launched a web-based instant messaging service, which links the bank and thousands of its customers.

Changed role of IT division

Before the merger Bankrecht X ran a common desktop standard that disabled many user features across Switzerland. The bank designed the system entitled Abacus after a fiasco with a grand mainframe system in 1974. Abacus is a client-server architecture running on Unisys platforms. It gave Bankrecht X huge IT lead over its Swiss rivals who relied on IBM mainframes. However, since the applications resided on several servers, under Abacus the bank lost the single-sign-on feature leading to the proliferation of passwords. This was the first justification of PKI. In contrast to the harmony established by Abacus in Switzerland, the foreign divisions of Bankrecht X operated locally implemented but globally incompatible systems. The bank attempted to end the anarchy with a middle-level system to coordinate its foreign exchange, equities, bonds, derivates and precious metals divisions. However, Bankrecht X discarded the system in the face of stiff resistance from regional managers for Europe, North America, Asia and Japan. The regions virtually run banks within the bank and invidiously guarded their independence. Incompatibility was just a little annoyance until the late 1990s because Switzerland, which still produced 90% of the revenue, had centralised IT.

The same problems befell Abacus after the merger when the Swiss-IT division dominated by former Bankrecht X staff attempted to deploy the solution in global offices. However, the key difference this time was that foreign divisions, especially investment banking, generated a larger proportion of the revenues. We focus on the power struggle between Switzerland and Bankrecht Investment (BI), a former Bankrecht Y division, in London. A support specialist reveals that the IT culture clash was inevitable because,

> "Bankrecht X was much more standardised. ... But Bankrecht Y was different. All the branches in the regions had separate servers. And if you logged into one you could never connect to a server in the next building. ... Bankrecht X had one domain for the whole of Switzerland. So we had a lot of problems with applications after the merger because some could not be easily moved to a single domain. Users ended up having about three different logons depending on where they were."

Even before the merger, the small Bankrecht X business in London rarely listened to their Swiss bosses. The merger worsened the situation because BI took over the profitable capital markets activities. This proud investment house rejected orders from Zurich because it managed the most profitable business. Apart from Abacus, the Bankrecht X IT team also initiated the PKI and smart cards project and spearheaded efforts to export it. However, since most senior management positions in the new bank went to Bankrecht Y executives, the Bankrecht X dominated Swiss-IT team lacked political support for their pet projects. The new bosses also demoted IT to a support role. According to the PKI project leader,

> "**The IT infrastructure is no longer an independent division/entity,** as in pre-merger Bankrecht X, but it is part of the business divisions. ... we have business divisions like Bankrecht Investment, Bankrecht Switzerland, a division in the US and IT is part of these organisations. But in Bankrecht X, IT was on the same level as these business divisions and had the same clout."

Business divisions govern IT because they control money for technology projects and the IT team must obtain their authorisation to work. Since the divisions have different needs, the result is fragmented IT. Apart from network connectivity, which is a Group-wide service, divisions have ad hoc interactions. A PKI engineer at London-based BI reveals,

> "I am not aware of any common IT services. ... **we don't have an IT team within Bankrecht that tries to enforce common practices within the divisions**. It would probably be a good thing but it isn't there. It would probably been cheaper if the finances were from above and resided there. At the moment, it is the business divisions that have the money to pay for IT projects so centralising the service will involve moving the money away from them. I have been in organisations before where they tried to remove the financial control of the people below and this wasn't very easy."

Indeed even Bankrecht Investment has four relatively autonomous IT support centres for the Americas, Europe, Asia-Pacific and Switzerland. The PKI engineer adds, "Switzerland is a division of its own so that tells you a lot!" The clash of cultures between the two banks started soon after the merger. To a support analyst,

> "In the past you used to hear people saying, 'oh, in my old bank this and that was a lot easier. A lot more efficient. A lot whatever.' ... If anything wasn't working this was always the reaction of people. These days I no longer hear people saying that 'I am from or I was in Bankrecht X or Y'."

The charged atmosphere forced Bankrecht AG to create autonomous business divisions. However, this arrangement has implications for services whose benefit derive from scale of use such as PKI. It was in an attempt to reduce conflicts and confusion between divisions that Bankrecht decided to discontinue all subsidiary brands. The branding exercise code-named project 'Orlando' is already forcing divisions to work together.

Security challenges of e-banking

We have seen that Bankrecht businesses widely use the internet in customer dealings. This is because e-commerce drastically reduces the cost of marketing, distributing and servicing financial products (Clemons and Hitt 2000). Bankrecht has deployed alternative services to satisfy customer demands for banking "at any time, in any place, by any device." However, the special features of the new channels have put pressure on the traditional security procedures. According to the Bank for International Settlements (BIS),

> "These characteristics include the unprecedented speed of change related to technological and customer service innovation, the ubiquitous and global nature of open electronic networks, the integration of e-banking applications with legacy computer systems and the increasing dependence of banks on third parties that provide the necessary information technology (BIS 2001)."

BIS argues that while the internet does not inherently create new risks, its features amplify some of the traditional banking issues notably strategic, operational, legal and reputational risks. Bankrecht's expansion beyond Switzerland raised issues about the nature of service provided and its security. For instance, diversification from the Swiss 'universal banking' model forced the bank to cede control to foreign divisions notably the brokerage houses in the US and the UK. Indeed, it was the demands of the new business lines that forced Bankrecht X to supplement its global physical presence with on-line services. We should reiterate that Bankrecht X only opened its first foreign branch in London in 1967. It always attempted to instil Swiss culture in all its businesses. This profile sharply contrasts with the internationalist Bankrecht Y that opened a branch in London in 1898. The bank mirrored US financial houses and did not force its culture on acquisitions.

Therefore, the erosion of the legal and regulatory certainty provided by Switzerland, the increased autonomy of global divisions and the demotion of the IT division to a support role amplified the difficulties of implementing Group wide services. The biggest casualty of the changes was the centralised PKI project. Next, we discuss the technical context; explore the security regime and assess the PKI institutionalisation discourse at Bankrecht.

Bankrecht technical Context

The central Bankrecht applications rely on 15 Unisys ClearPath IX/2200 mainframe systems running Abacus and MAPPER. Abacus is an integrated banking application. After the merger Bankrecht moved the data and applications of the two banks onto the Abacus system. The migration was difficult because the banks used totally different technologies for instance, in account reconciliation. In total, Bankrecht runs over 3,000 servers, which include 1100 Sun Solaris Unix servers, 1100 Novell servers, 850 NT servers and 150 DEC VMS servers. Apart from the core mainframes and application servers, these systems largely serve Switzerland.

Actually, Bankrecht Switzerland (BS) still operates a relatively centralised IT function. The division is composed of two main development teams focusing on banking applications. The Operations team runs all systems on behalf of business divisions. BS also has Support teams one for users and the other covering aspects such as training and client engineering. The client engineering team focuses on the desktop and signs off any application integrated into the client machines. BS runs the so-called "global IntraLAN" that supports Windows NT 4.0 computers. The Switzerland division has enhanced the NT platform with many components and applications. According to a Vice President,

> "We have **a highly standardised end-user platform** and that is rather rigidly enforced. At the end user platform – 40,000 PCs – equalling to 40,000 users they are as much as possible totally the same. Moreover, although users occasionally change the software on their PC, **95% of all users will have a completely and totally similar PC. ... on that type of end user platform it is not very difficult to have a standardised, centralised certificate management in place.**"

The bank named this rigidly defined Windows NT client, End User Platform Domestic (EUPD). Like Oilcom, users cannot install any software on the PC or modify its settings. EUPD users may install software if the PC resides in a relaxed resource domain. This is Resource Domain 3. This covers less than 5% of the bank. BS also has 1,000 Sun Solaris Unix workstations. However, standardisation does not extend beyond Switzerland because according to the VP, "We are not in a position to completely keep all PCs alike."

Bankrecht PKI efforts

We previously saw that by 1901, the Swiss banking circles had transformed secrecy into a potent tool for international competition. In 1934, the Swiss Federal authorities introduced a law that, for the first time, made secrecy violation a criminal offence. The result of the desire to maintain competitive advantage and avoid criminal litigation is that Switzerland is a leading developer of information security products especially cryptography. For example, the country is home to the IBM Zurich Research Laboratory with many cryptographic innovations to its name. IBM credits its Zurich researchers with the invention of the first practical and provably secure public key encryption scheme and crypto tools that power all its Java-based products. Zurich also worked on Secure Electronic Transaction (SET), reputedly the most secure credit-card payment protocol available on the internet.

The excellent International Data Encryption Algorithm (IDEA) was also developed at Eth in Zurich. Bankrecht includes IDEA, a 128-bit block cipher, in its solution. Switzerland is also a player in quantum cryptography research. In 1995, the University of Geneva implemented quantum cryptography in a 23-kilometre fibre optic from Geneva to Nyon (Singh 1999). Bankrecht is reportedly the "biggest software house" in Switzerland because it employs over 3,400 IT professionals. PKI research started in 1992. A PKI engineer on the original team believes this work was revolutionary because,

> "**By 1997 PKI was not even widely written about**. ... most companies did not even know what this was. I was asked to give presentations on what PKI is. Today do see anyone giving presentations on what PKI is? No. Why? Because the fad has died. ... The reason is that they are realising the cost of deploying PKI. The PKI itself is not expensive. It is getting all your applications to work with it. Literally, the cost is not the cash. It is the amount of time necessary to make it work."

The bulk of the original PKI team eventually left Bankrecht. In 1997, the team became a 100% subsidiary of Bankrecht that offered IT security products to the Group and other companies. The subsidiary developed the Bankrecht PKI architecture. However, in 1999 Bankrecht sold the division and it is now a major provider of certificate and smart card based security software products in Switzerland, Germany and Austria.

PKI business requirements

PKI was part of a general drive to provide a cost effective, flexible and responsive IT service to support changing business requirements. The need for different security protocols was in reaction to mergers and acquisitions abroad that exposed the bank to regulatory and other risks. However, the immediate justification for PKI was the desire to arrest the proliferation of passwords that were both causing disenchantment and reducing security. The bank also believed passwords were reducing productivity and increasing help desk support costs. We saw that passwords became widespread at Bankrecht X with the implementation of Abacus, the integrated client-server based system. The Vice President argues that while it was not clear at the time, the mainframe architecture provided Single Sign On (SSO). He adds,

> "In the client server paradigm whenever you moved onto a different server and application resources you had to sign on again. Thus, we had a **tremendous increase of user IDs and passwords**. All of a sudden, a user did not have two or three of passwords; they had 15 or 20 of them. Besides, we did not see anything that would stop the developers from creating more client server applications."

We saw that after the merger Bankrecht X moved the applications and data of its partner from IBM mainframes onto Abacus. Bankrecht AG ended up with 120 heavily used applications. The disempowered IT team came under pressure to avoid the nightmare situation where senior users kept passwords for over 30 applications in a working day. To a PKI engineer a casual survey of office desks showed that users survived the password nightmare by writing them on post-it notes. Of course, this was bad security practice. Bankrecht resolved to re-create SSO without resorting to mainframes first by using scripting solutions. However, the Vice President reveals the bank abandoned scripting because,

> "The solutions were extremely unstable and required extreme administration efforts from the side of the IT to keep them alive. Little things like a vendor changing fields on a sign on mask would make the whole script topple over and not work any more. …. **We concluded in 1992-1993 that we would use a combination of X.509 certificates plus smart cards.**"

A four-man team initiated the PKI project at Bankrecht X. The group included a senior manager in-charge of IT Operations and systems development, our respondent who is now Vice President, a middle manager and a PKI engineer. After restructuring, a team in charge of server platforms added six members to the core PKI group. Server platforms covered mainframes, Unix servers and other new platforms. The server team was a vital addition to the PKI effort because it developed middleware that controlled all IT applications. The joint team took key decisions such as the selection of a smart card infrastructure-based on a

Siemens card. The VP concedes decision-making was easy in this small team. However, the PKI effort ran into trouble after the merger, especially abroad.

Bankrecht PKI components

The PKI uses a combination of X.509 certificates and smart cards with the private key never leaving the card. According to an original PKI engineer on the project,

> "With the PKI our goal was that all communication should be encrypted ...But how do we guarantee that kind of purity, safety and sanctity of the information? We are a networked global organisation that means that you can see our data all over the world. ... The law here (Switzerland) is that you must be physically in the country to access the data. **PKI gives us a way of ensuring that the information is not revealed easily."**

The implementation of the PKI began in earnest in early 1997. This was five years after the research on the PKI began in Bankrecht X. We discuss the reasons for this delay later in this chapter. The solution offers secure Single Sign On (SSO); remote access and communication for file transfer. It also supports secure electronic messaging between servers, key generation and management and certificate-based logon with smart cryptocards. The security framework includes security base services; a distributed smart cryptocard and PKI and operational guidelines incorporating bank-wide security policies and procedures. Below is its illustration.

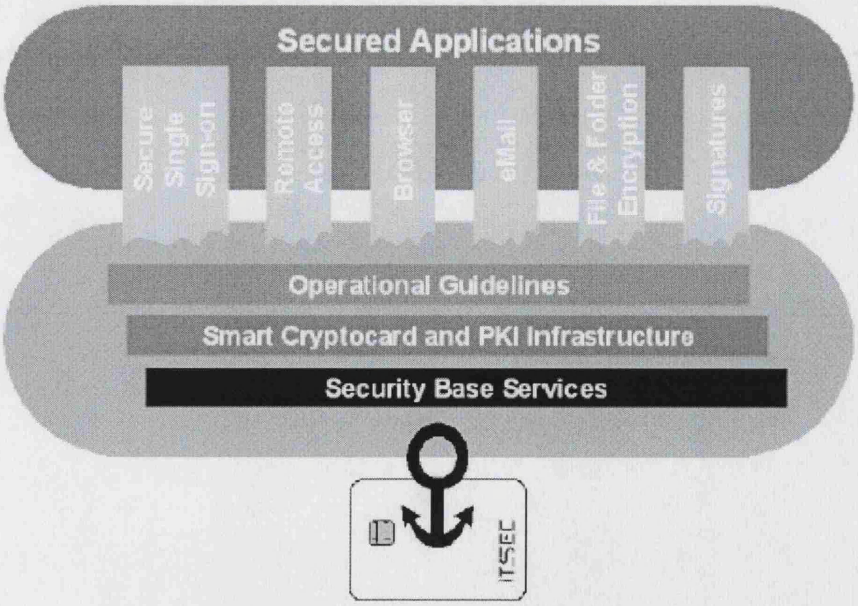


Figure 19 – Bankrecht security solution architecture (iT_SEC 2000)

Security Base Services

This is the foundational layer of the solution. It incorporates cryptographic technologies, open standards and interfaces. The cryptographic technologies include Swiss developed symmetrical IDEA (128-bit), DES (56-bit) and asymmetrical RSA (512-, 1024-bit) cryptographic algorithms. Also included is Secure Sockets Layer (SSL) for browsers, S/MIME and PGP for e-mail, Lightweight Directory Access Protocol (LDAP) for directory access (Chadwick 2002, Wahl 1997) and OCSP for certificate validation services. We discuss the directory later.

The Vice President reveals that the PKI components on the end user PC include a card reader, the card driver and interfaces such as PKCS#11 and Generic Security Services Application Program Interface (GSS-API). The cryptocard reader attaches to workstations via serial ports. The bank uses PC card based readers for laptops. Public Key Cryptography Standards (PKCS#11) specify an API entitled 'Cryptoki' to devices performing cryptographic functions. The layer also incorporates the X.509v3 specification for certificates. Bankrecht is considering replacing PKCS#11 token interfaces with the Microsoft Crypto API/Service Provider interface used at Oilcom. It also wants to replace the expensive PC/SC cryptocard reader interface with OpenCard.

GSS-API provides system-to-system security capabilities in heterogeneous environments. GSS-API defines an interface for the implementation of strong cryptographic authentication and other security services independent of underlying mechanisms. The security services available through GSS-API are compatible with a range of mechanisms based on secret-key and public-key cryptographic technologies (Linn 1997). At Bankrecht, GSS-API authenticates servers and, if required, provides encryption for services such as FTP.

PKI and Smart cryptocard infrastructure

Above "Security Base Services" is the Entrust Intelligent Client. The Entrust PKI is part of the second layer, which also includes the Smart Card Infrastructure (SCI). According to the Vice President, Bankrecht selected Entrust because it was an off-the-shelf, market proven component from an independent vendor. This was because Bankrecht had resolved to adopt open standards and protocols such as TCP/IP, wherever possible. Entrust is popular because independent software vendors offer 'Entrust-ready applications.' However, the choice was controversial. Bankrecht originally ran a home grown CA but a constituency strongly argued for UniCERT, a CA by Baltimore, an Irish company. According to the Vice President,

> "We thought of using Baltimore's CA because the CA is not from the United States and may be a little bit less infamous for being fed with Trojan horses from some American agency. We had a camp that was much in favour of Baltimore. But in the end, we used Entrust because Bankrecht Investment – the other division – big division told us that 'if you go with Entrust we would presumably board your solution'."

We discuss this decision further because it has been a major source of discord between Switzerland and BI. The second layer has two components. To iT_SEC, the PKI interface handles "trust" while the SCI deals with "confidentiality" as illustrated below.

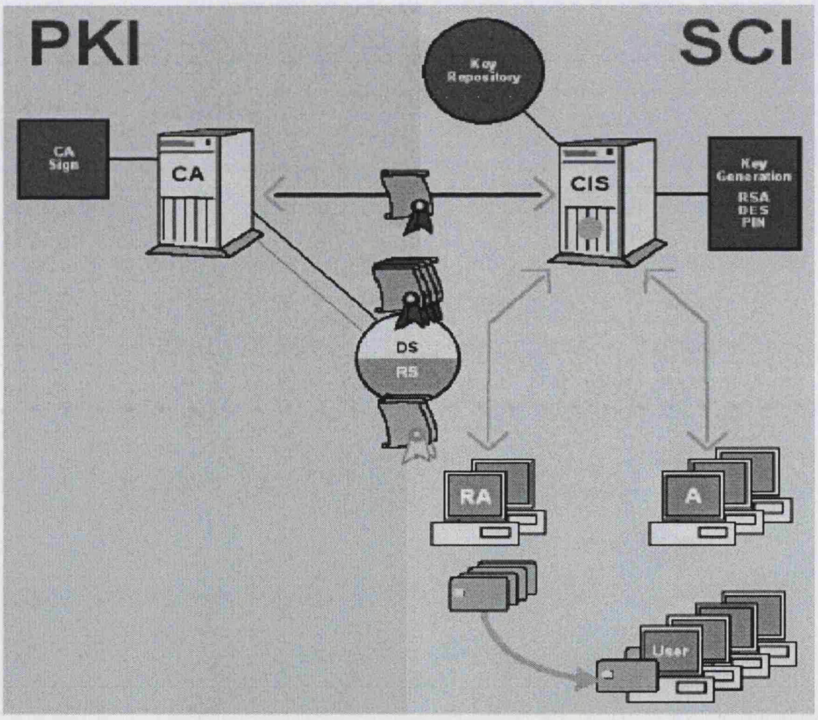


Figure 20 – A combined SCI-PKI at Bankrecht (iT_SEC)

The Smart Card Infrastructure (SCI) is an add-on that manages certificates and private keys on the cryptocard for users. According to a support specialist, the SCI was critical because,

> "You need to help people if their certificate or private key gets destroyed or when they lose or forget the passphrase that opens up the private key that belongs to the public key and the certificate. … you had to

> automatically renew a certificate upon expiration. You have to withdraw the certificate when somebody leaves the enterprise without the end user even knowing anything about it."

The bank's engineering division customised an iT_SEC system to create the SCI. To the VP the modification increased user convenience and helped PKI adoption. He argues,

> "**Most PKIs require end user intervention. We decided very early on that this is going to kill the project, if you need too much end user intervention.** ... Many products that support certificate-based sign on have their own proprietary certificate storage. So you have application proprietary certificate storage and end up with ten certificates, ten private keys and ten passphrases to open up those private keys. So again, the area of SSO is not there. So we agreed on application independent certificate storage on smart card accessed through standard APIs like PKCS #11."

According to iT_SEC, the key components of the combined infrastructure are an Entrust CA server, a Smart Card Information Server (CIS) and a key generator and repository for both the SCI and PKI environments. Other elements are decentralised Registration Authorities (RAs) that request and issue cryptocards. The framework also includes 'security officer level' Assistants (A's) who resolve card problems locally or remotely. The CIS server is vital to SCI operations because it is the centralised infrastructure for smart card creation. The CIS takes requests for card creation and certificate signing from the RA and ships them to the Entrust CA. If satisfied with the request, the CA signs the certificate and publishes it onto an LDAP server. The signed certificate returns to the CIS for onward storage into a local directory that keeps all end user data like encryption certificates and private keys. According to the Vice President,

> "We do not keep the authentication certificate private keys because we create the smart card with two certificates – encryption and authentication certificates. **We keep the private key of the encryption certificate to create a clone at any point in time.** For instance, if you use your encryption certificate for e-mail and you lose your card, you need a new certificate and smartcard to read your mail. It has to be the same encryption private key as the lost one. So you have got to be able to do key recovery in an enterprise unless you sacrifice all your e-mail, which you won't do."

Although Bankrecht actually runs the Entrust CA and CIS on the same server, these are normally separate for security reasons. The CIS keeps an audit trail as it communicates with the CA over the status of keys and certificates on behalf of RAs, Assistants and users. The RA coordinates with the CIS server to produce the smart cards physically. Bankrecht uses standard end user workstations for RAs as well as local and remote Assistants. The RA also incorporates a card printer or coder personalisation device.

Smart cryptocards

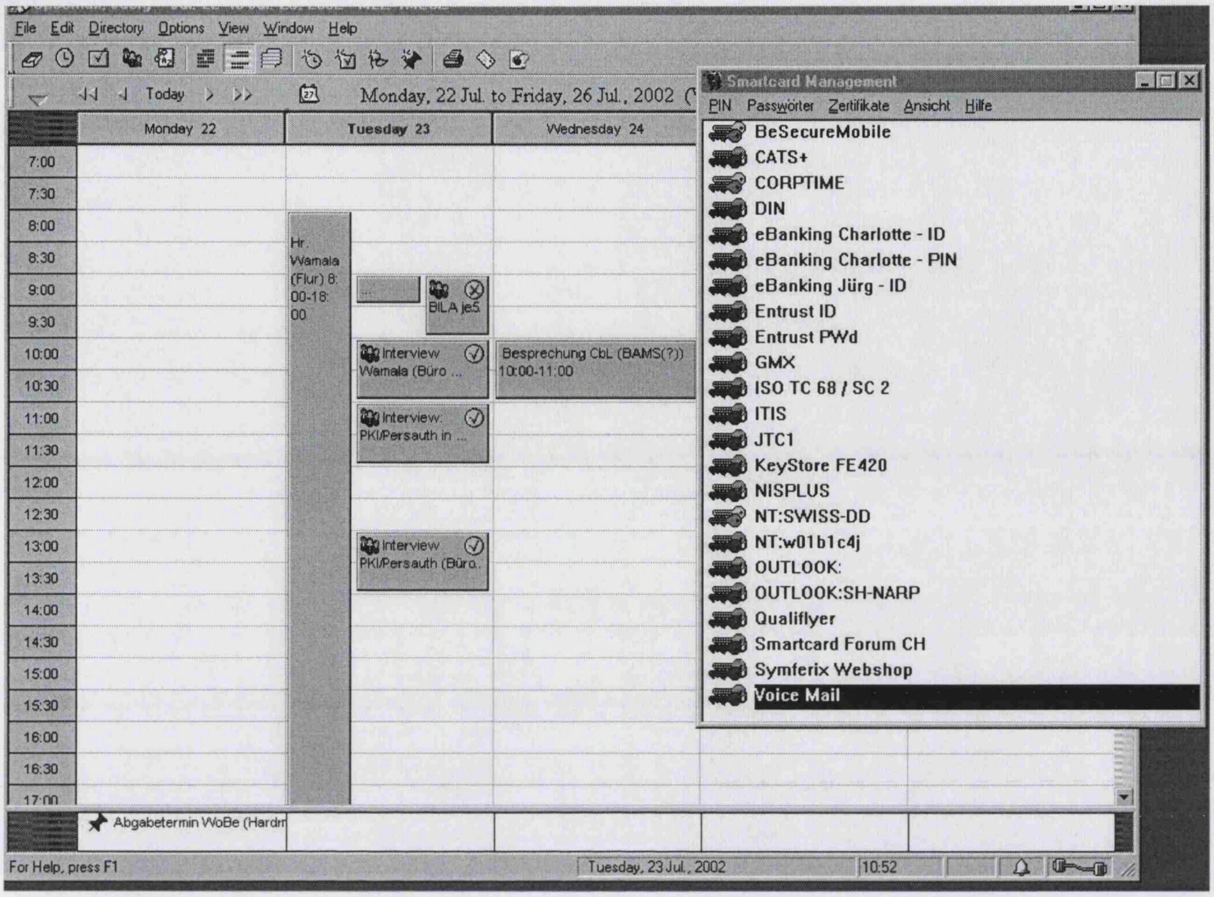
Smart cards are central to the PKI and mandatory desktop at Oilcom. Similarly, smart cryptocards are vital at Bankrecht Switzerland. According to iT_SEC,

> "Anchoring the security framework and the various security applications it supports is the use of 'smart cryptocards' with associated PIN numbers. Each cryptocard can contain and process various encrypted items, for example application log-on passwords. As a result, it is no longer necessary for a user to remember multiple passwords, merely a single PIN number."

The security infrastructure provides mechanisms for retrieving the appropriate password from a cryptocard and passes it to the application. The card also allows users to identify themselves and use any workstation at Bankrecht Switzerland. The card supports strong authentication with certificates and private keys. To a London-based security analyst,

> "We have rolled out something of a PKI in Switzerland, but our other divisions are much more reluctant to start. ... Users authenticate themselves to the card once, and then they have full access to everything they are authorised for. We have full time file encryption, too. The rest of the world has to catch up. ... **Although we do not have a true Single Sign On, the user experiences it as if they were part of such a system.** Users must insert their smart card and authenticate to it before they can use NT. The logins to NT, email, and the file encryption subsystem are actually password based, but login is scripted through a routine in the smart card."

To the Director IT Security, apart from the two certificates, the card stores about twenty four passwords. At logon, the system shows the name and identifier of the application and password and PIN fields. The cards authenticate in three ways. The first type uses a 'scripting engine' that automatically enters, or changes user IDs and passwords upon request. Scripts control this login and require no change to applications like Microsoft Outlook that use it. The second type involves 'drag and drop' facilities that enable the retrieval of passwords from a file on the cryptocard. Users simply select the application name and drop it onto the password request field. The third approach involves an Application Program Interface (API) providing access to passwords stored on the card. Most banking applications authenticate with scripts. Next is a screenshot of one respondent logging on with a scripting engine.


File Edit Directory Options View Window Help
Today
Smartcard Management
PIN Passwörter Zertifikate Ansicht Hilfe
For Help, press F1

Monday, 22 Jul. to Friday, 26 Jul., 2002

	Monday 22	Tuesday 23	Wednesday 24
7:00			
7:30			
8:00		Hr. Wamala (Flur) 8:00-18:00	
8:30			
9:00		BILA jeS	
9:30			
10:00		Interview Wamala (Büro ...	Besprechung CbL (BAMS(?)) 10:00-11:00
10:30			
11:00		Interview: PKI/Persauth in ...	
11:30			
12:00			
12:30			
13:00		Interview PKI/Persauth (Büro.	
13:30			
14:00			
14:30			
15:00			
15:30			
16:00			
16:30			
17:00			
	Abgabetermin WoBe (Hardn		

BeSecureMobile
CATS+
CORPTIME
DIN
eBanking Charlotte - ID
eBanking Charlotte - PIN
eBanking Jürg - ID
Entrust ID
Entrust PWd
GMX
ISO TC 68 / SC 2
ITIS
JTC1
KeyStore FE420
NISPLUS
NT:SWISS-DD
NT:w01b1c4j
OUTLOOK:
OUTLOOK:SH-NARP
Qualiflyer
Smartcard Forum CH
Symferix Webshop
Voice Mail

Tuesday, 23 Jul., 2002 10:52

Figure 21 – Example of automated password entry to a calendar application

The Director adds, "All these passwords are protected on the card, yeah it is not very top protection, but you cannot just read them off like that." According to iT_SEC, the security relies on the personal cryptocard concept where each card contains a 'crypto-processor' that physically protects secret elements, even during cryptographic operations.

However, logging onto applications for the first time is slow. For instance, to get the screenshot above, we waited for about ten minutes for the computer to download the profile. The Director admitted this occurs when a workstation downloads a user's profile for the first time. While the speed improves after the initial logon, he reveals the system is slow for offices far away from Zurich. The Head of the Smart Card Infrastructure argues,

> "The current authentication procedure works. **However, it is primitive**. For example, when I fetch the password from the card management system and drop it into Notepad, you can read it in plaintext! That is not good security really."

While the cryptocard contains authentication and encrypting certificates, the SCI director reveals that only laptop users are required to encrypt their connections and data.

Smart Cryptocard issues

The Associate Director IT Security/PKI Project Leader reveals that despite issuing 35,000 cards to employees in Switzerland, for a long time, only 25% were in use. IT_SEC blames the low uptake on "implementation issues." The company argues that although Switzerland is a small country, Bankrecht divisions exist in regions with different dominant languages, namely German, French and Italian. IT_SEC reveals that the big regional cultural differences demanded the provision of documentation, learning programs and help desk support in the three major languages and English. We return to these issues in Chapter 7. The PKI Project Leader also identifies resistance within the IT division. He states,

> "In principle everybody said it was the right thing to do. However, it was quite difficult for example, to get the developers on-board. They like to do things their way and link from one computer to the other and **were not sure of the benefit of PKI for them**. The same happened with the Support team. The new system gave them more work so they were not happy. It was quite difficult to get the benefits to the end users because those two teams need to be involved. This took a long time to change."

Indeed, iT_SEC reveals problems with attempts to align the project with the organisational structure and implementation practices. The firm says that even pilot projects, "required careful planning and sensitivity to different requirements and priorities in different sections of the bank." To the PKI Project Leader the 'sensitivities' became clearer after the merger because of the move to a divisional structure. He originally worked for the IT Operations division of Bankrecht X. The hierarchical PKIX model was acceptable to this bank because of its centralised IT structure in Switzerland. The Vice President reveals,

> **"When we started with the smart cards, it was very centralised but in the process of trying to deploy it became completely decentralised.** Today the Bank is divisionalised. We have divisions and the divisions are completely on their own. There is no one in the Bank who can give orders that they want this done. So we have no way of ordering anything in the IT area to any of the other divisions. They are autonomous and they do what they want. .... In Switzerland there is a certain amount of centralisation, but other divisions are on their own."

As we see later, Switzerland failed to extend the PKI solution abroad because they lacked power over the autonomous divisions. The Director Security also believes the IT division could not rely on top management support because, "there is a big distance between the very important decision makers and those who really do the job." He argues that because the managers do not really understand what is behind the IT solution, the PKI could only survive if seen as serving the banking activities. Likewise, the Vice President reveals that because management thought in banking terms they asked the PKI team to develop a 'killer application' to encourage cryptocard use. However, the team failed to identify the use because the most vital banking applications did not support certificate-based logon at the time. In 1997, the team 'reinvented' the PKI as a tool for improving user convenience by removing the need for passwords. The Vice President states,

> "Everyone was too cautious and said 'hey, we want to make money' and people are supposed to do their work. Could we then tell them "hey, you are not using your smart card .... Tomorrow you will be forced to use it?'' They won't allow us to do that. They would simply refuse to use the new application. ... So we had no means to make one application that is important to the bank mandatory to use with a smart card. The only way was to make it convenient. **Make it more convenient that not using it** and take care of all the situations that can cause trouble like 'I've forgotten my smart card, I've forgotten my PIN, and I've lost the card.' That is it."

Convenience became such a critical objective because the bank failed to create structures to support the PKI in the face of user resistance. Unlike Oilcom, Bankrecht uses different cards for physical and logical access. The Director IT Security admits, "It is not smart keeping the cards separate. However, this card issue generates endless debate." He sees the cost of designing a custom Bankrecht card and card readers as restrictive. Tellingly, he sees the biggest obstacle to a single access card as the "diverging goals today."

Cryptocard usage in Switzerland received a big boost following the restructuring of IT support. According to the PKI Project Leader, the steps included the rollout of a new standardised NT desktop and the centralisation of IT support. The desktop team moved from general support to IT Consulting. About 150 of the new consultants embarked on an extensive effort to explain cryptocard usage. After this effort, card usage increased from 25% to 87%. The Director IT Security admits the increased uptake was a relief because rivals found it amusing that few employees used the cards. Usage became even more impressive from early 2001 after the bank attached internet access to the cards. To the Vice President,

> "Cards are now used by 97% of all the users in Switzerland completely 'voluntarily'. Not quite. No, no, it is completely voluntarily. **But there is one thing that we made mandatory**. ... If they want to use the Bank to access the internet, they need a smart card."

By making certificate-based internet surfing mandatory the bank forced developers to use the cryptocards. By the time of our research, only 2.5% of employees in Switzerland did not use their cards. The Vice President claims, "I don't care because 2.5% is nothing." Having conquered Switzerland, could the IT team convince other divisions to accept a centralised PKI solution as originally planned? We focus on efforts to deploy the solution at Bankrecht Investment, the London-based investment banking and securities division.

PKI at Bankrecht Investment (BI)

We saw that despite strong support for UniCERT, Bankrecht Switzerland (BS) replaced its 'home grown' Certification Authority (CA) with Entrust because BI promised to adopt the integrated solution. Curiously, BI bought the Entrust CA that BS adopted. According to the Vice President, BI spent $0.5 million to purchase Entrust licenses for all its employees. The deal covered a CA and an Entrust Intelligent Client on each computer. BI later rolled out certificates and Entrust-ready applications. However, the Vice President claims,

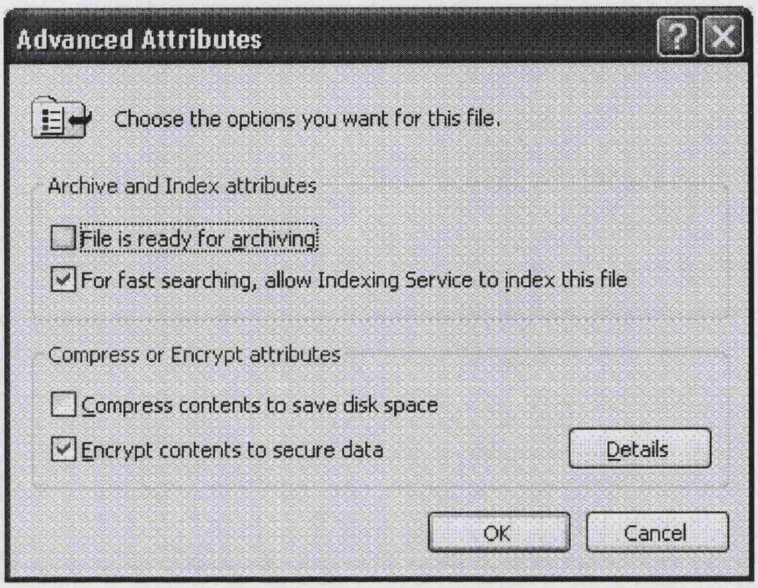
> "After having spent the money they discovered that 'hey spending the money is not having done it.' So you have got work to do! And then they didn't do it. They could not achieve it. **So the money was a total waste. A total waste! And they have nothing.**"

It was after this fiasco that BI convinced BS to integrate the Entrust CA into the SCI-PKI solution. However, after the integration BI rejected the solution and instead opted for a Microsoft CA. Since we extensively discussed Microsoft PKI under the Oilcom case, we only focus on the PKI services deployed at BI, not the infrastructure itself. We interviewed the PKI Engineer responsible for the BI proposal in August 2002. He argues,

> "The general IT direction we are taking is one of use of out-of-box solutions. Bear in mind that we have a worldwide license for Microsoft products. With PKI, the out-of-box Microsoft solution is not that expensive and it is fairly easy to implement. **Alright, it is not the greatest product in the world but it is a product that introduces Microsoft to the market** and we believe subsequent versions are going to be much better. It is a foundation I would say for what we could do in future."

PKI primarily encrypts data on laptops and file servers. The engineer argues that despite the availability of standalone encryption solutions, PKI offers better manageability. It also offers scalability for the deployment of solutions such as secure e-mail signing and encryption and, in the future, smart card logon, digital rights management and services. The division also does code signing to ensure the integrity of its environment. BI hopes to use PKI for workflow controls like certificate-based software issuance. However, the engineer admits that due to the weakness of the business case, the BI team opted to start with Encrypting File

System (EFS) that is free with Windows 2000 and XP (Professional and Server). He believes the EFS product is easy to deploy and manage. The EFS feature in XP look as follows.



Advanced Attributes

Choose the options you want for this file.

Archive and Index attributes

□ File is ready for archiving

☑ For fast searching, allow Indexing Service to index this file

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

Figure 22 – Encryption attributes (Microsoft 2001).

The engineer stresses that Microsoft PKI improves security at little additional expense. Indeed, cost is a source of contention. BI believes it can operate a Microsoft CA at £4 a year per user using a better support model. Although Switzerland is proud of its experience of running an Entrust CA, the managers concede that the cost of £200 a year per user is restrictive. To the Director Security the cost covers certificates, tokens and Entrust support. He admits a lower cost could convince other divisions to adopt the Swiss PKI. However, the Vice President believes BI would have implemented the Swiss solution,

> "Because we know how to use it, **we have deployed it but that would have meant that they would have to live with an application that they did not invent. Everybody has that. I am not blaming them because we all have the same Not Invented Here (NIH) syndrome**. … Therefore, they rejected it. The thing that works they will not use because they did not invent it. It is not theirs. The thing that they could use does not work. …and what they hope is that maybe in five years from now Microsoft will have a CA and a PKI and a working solution not only a toolkit. Today Microsoft has may have a PKI and maybe has a CA but it does not have a working solution that scales well."

Bankrecht Investment (BI) predictably dismissed the BS assertion. The engineer contends BI selected Microsoft PKI because of its superior technical and financial proposition. He claims London conducted a broader PKI requirements analysis than Switzerland. The engineer insists that EFS is apposite for the primary BI requirements of end-to-end security and data encryption. He further sees the major drawback of the Swiss PKI solution as its reliance on cryptocards. He argues that smart card logon at BI "is only on the wish list here" because of the cost of rolling out the cards and readers. Besides, he reveals,

> "**We are not really required by the project to connect with everybody else in the Group**. That is not required. We are just Bankrecht Investment. Of course, we would want to have a solution in place, which allows the Group to function as a Group. However, we are in a tricky position in that we do not have the business driver, remit or financial resources to roll out a Group-wide solution."

However, the Vice President insists Microsoft PKI is not scalable to over 10,000 users. The PKI Project Leader agrees. He argues Microsoft PKI is problematic because it issues application specific certificates that may become too numerous. Because Microsoft PKI issues certificates for different purposes a login certificate is for example different from an EFS certificate. He claims that despite auto-enrolment features, Microsoft certificate life cycle management demands more intervention than Entrust, which he sees as "click and control." A founding PKI engineer in Switzerland also dismisses the cost and technical claims and blames the conflict with BI on politics. He states,

> "London has killed Group wide PKI because of political reasons. ... BI has rejected our Entrust certificates and claims they will use Kerberos instead for Single Sign On, which just makes me laugh. That guy in London making decisions does not really appreciate that some of us had to keep awake until 4am to make the infrastructure work. **They are putting our efforts to waste because of politics.** I hear London has published internal papers declaring our Entrust PKI useless. If they already know the problems why don't they share them and help us to avoid them in the future?"

London-based BI insists its choice of PKI was sound because they are increasingly using Microsoft infrastructural and productivity products. Despite not having a mandatory desktop, the division has upgraded its workstations from Windows NT 4.0 and 2000 to Windows XP. The engineer also questions the technical efficacy of the Swiss PKI solution. He states,

> "The Swiss solution does not actually use the smart card for authentication. They use the card as a password repository. ...in my experience, it is very difficult to enable smart card logon if you don't have Microsoft PKI. .... **Using the smart card as a password repository is one thing. It is easy.** ... However, having the Microsoft authentication process and Domain Controllers work with non-Microsoft certificates is something else. ... I don't think Microsoft officially supports it."

A Bankrecht security analyst in London believes that unlike BI, the Swiss are under more regulatory pressure to implement PKI. However, he believes some personalities have overplayed the differences to achieve political objectives. He states,

> "Due to their Banking regulations the Swiss have to proceed very, very carefully than we do in terms of the requirements for data protection. Their environment affects the type of technology they adopt and its

> shape. It affects you every time you think about the design of anything at all. ... **That is where I think you need to keep a level head but it is so easy to develop a siege mentality.** In my view, political considerations should be left out of technology decision making. There are issues, which are maybe risks, there are manageable risks but can be over-emphasised to achieve political objectives."

Enterprise Active Directory

The Bankrecht SCI-PKI infrastructure supports LDAP directory access and OCSP (Online Certificate Status Protocol) for certificate validation services. Bankrecht uses the directory to keep copies of encryption certificate private keys that support key recovery. BI uses Active Directory (AD) to issue certificates automatically. The division believes AD eradicates costly operational processes since a person receives a certificate with an e-mail account. However, Bankrecht lacks an enterprise directory. The BI engineer argues,

> "The key benefit of our internal PKI is that we can leverage the Microsoft Active Directory. We only issue user and machines certificates. But **we lack a Group wide Active Directory. It was planned but for various political and security reasons we have to divisionalise the directory.** One of the big problems that we come across is that to issue certificates from one division to another in different directories you lose a great deal of that automation. And all of a sudden we have an increase in support requirements and operational processes yet we want to reduce costs."

BI argues that since Switzerland designed the directory and its support model alone there are inevitable administrative strains on a global scene. Different support scenarios are vital because of the global nature of Bankrecht operations and the cultural differences in the divisions. We saw that cultural differences exist even within Switzerland. Inevitably, the differences are sharper across countries. A London-based security analyst claims,

> "**It is very difficult stereotyping an entire nation**, but I think the Swiss have a different mentality to may be the English or the Americans. ... That is my observation and it is probably unfair. ... However, if you are a Risk Analyst and then you had a British hat on you might tend to take a pragmatic view whereas may be the Swiss would have to be satisfied 100%. In reality, you cannot operate a shared network service if you cannot take decisions accordingly. **If we adopt a policy where we accept zero risk then we cannot deploy a shared service and we end up becoming a defence organisation, which we are not.** We are a bank trying to make money."

Active Directory is problematic because it assumes a hierarchical IT structure with one division to enforce standards. Bankrecht lacks this function. AD presumes distinct user groups. However, a founding PKI engineer argues that Bankrecht has numerous intersections of geographical and functional roles. He states,

> "**Bankrecht has six, seven, eight, nine subdivisions? I do not know how many! You see where my problem begins? There are official and non-official subdivisions.** How do you classify those? Because what a PKI can allow you to do is by creating groups, you can make people have access only to

> certain data. If you say everyone is a Bankrecht employee then you do not have that finer granularity that the application offers to have more inbuilt security."

Indeed, because the bank is still integrating newly acquired business in the US and even Switzerland itself, it will take some time to get clearly defined groups. The difficulty of establishing distinct categories afflicts most role-based access control systems. The absence of a central IT function has created interoperability problems because Bankrecht divisions have, for legal, technical and political reasons, implemented either diverse technologies or the same technologies differently. For instance, the BI engineer argues that while services like secure e-mail thrive on a single PKI they are too expensive to deploy and support due to the different platforms. Ironically, he sees the biggest impediment to the "one firm" dream as the failure to create a Group wide directory. He warns,

> **"One of the key things that I think is gonna affect the ability of Bankrecht to function as a Group is the failure to deploy Group wide Active Directory.** Over the future that will be significant. This was because of AD technical issues and political issues. What do I mean by political issues? **Well, a single directory implies, to a degree, a single body of administration**. I know there are delegation capabilities within the product but there is only so far you can go with that. There are certain areas where you want to achieve consistency and that is the goal of a single directory across the Group. But there are different requirements across the Group..."

The absence of an enterprise directory also accentuated the proliferation of PKI islands. At the end of this stage, BI easily won the cost argument because its PKI was obviously cheaper. However, Switzerland insisted they had wider experience and saw the Microsoft CA as a mere toolkit. These disagreements formed the basis for the next phase of the PKI solution.

Branding: Whose domain is it?

In April 2003, we e-mailed the Director IT Security to know whether Bankrecht AG had resolved the conflicts about the PKI management structure. The Director revealed,

> "Yes, the decisions you are referring to have been taken. However, this has **led our management to realise that there may be potential conflicts or at least confusion if we don't coordinate PKI** activities at group level. ....BI has decided it will install and run its own hierarchy of CAs, based on Microsoft's offerings (mainly for financial reasons, **but they are probably not unhappy about the fact that this enables BI to remain independent of Bankrecht Switzerland as regards PKI**). BI has set up a "general purpose" root CA that will then certify the individual CAs issuing end user certificates for particular purposes, the first being EFS (secure e-mail is not actively pushed by BI)."

Running fully independent divisional PKIs seemingly killed the vision of a centralised system based on the Bankrecht X solution. However, an innocuous branding announcement on 12th November 2002 resuscitated the idea. We call this the second phase. The decision led to the abolition of all subsidiary brands in June 2003. Bankrecht claimed simpler branding reflects the 'integrated business model' and the 'one firm' approach. The main casualties were Bankrecht Investment and a US-based Wealth Management division that both lost illustrious non-Bankrecht monikers. However, centralised PKI benefited greatly. The Director IT Security reveals that after the decision to run divisional PKIs,

> "People in BI decided to put just "Bankrecht AG" as company name in their root CA and CA certificates. This has **raised the attention of our branding people** and management in that they realised that PKI naming could not be done randomly by individuals setting up a CA. Thus, we are now trying to set up a coordinating body that will eventually govern not only PKI naming on group level, but also the definition of CA policies and the like."

Switzerland-based Wealth Management & Business Banking (WM&BB) announced the 'coordination' drive on 17 March 2003. The details are in a document entitled, "Request for proposal for centralised 'Bankrecht' Group-wide SSL certificate management for internet-facing websites." WM&BB announced that all internet-facing websites in the Group were to reflect the new brand and move to the bank's main domain by 9th June 2003. The Head WM&BB IT Operations, Security and Contingency argues,

> **"From a legal perspective only the owner of the domain name is entitled to order certificates or assign this task to a third party. This requirement favours centralised management.** ... The operation of the server would remain with the individual divisions, our responsibility would concentrate on the management of the certificates. "

The rebranding activities were coordinated under a project named Orlando. The project started at a workshop on 12-14 March 2003 that resolved to have centralised management of SSL server certificates at internet-facing websites. The import of the decision would be to bring divisional PKI under centralised control. Orlando is a cross-Group IT team with members from all business divisions. As we saw, the actions Bankrecht Investment and its contractor Perot Systems on a new root CA on 6th February 2003 actually spurred Orlando. BI attempted to make their PKI general-purpose to make it useful for other purposes by other projects and/or divisions. However, the "Bankrecht AG" name for the root CA did not reflect the single-brand strategy. Responding to the Orlando proposal, a WM&BB manager argues,

> "The question of having multiple root CAs with the Bankrecht Group is certainly something which needs central coordination and approval by the relevant authorities. It sounds like the 'coordination meeting legal/security/web communications' that you mention would be the ideal place to start."

Interestingly, WM&BB appointed senior BI managers to Orlando coordination positions. For instance, the manager who facilitated the first Orlando workshop is in-charge of renaming domain names, servers and certificates that BI obtained from VeriSign and Thawte to meet rebranding requirements. Another BI manager deals with vendor relationships. The project team also included technical contacts for web applications and certificate management contacts within the business divisions. However, the Orlando workshop appointed WM&BB's IT Operations & Contingency team as the lead support division for the Centralised Certificate Management (CCM) scheme. This is a powerful position because the activities include vendor (CA) contact, initial ordering, receipt of issued certificate and forwarding them to website owners, renewal and revocation.

The Orlando Project set mid-May as the deadline for the completion of the CCM scheme. This required the issuance of new SSL server certificates signed by a commercial CA for about 100 websites across the bank. The project agreed that the 'vendor management' team arranges a Group-wide pricing agreement for certificates with one or two vendors. Orlando suggested a phased expiry of over 100 certificates to avoid their simultaneous expiry in May/June 2004 or 2005. However, the divisions were to manage certificates not associated with the Bankrecht official domain until revocation. We previously saw that BI rejected the Swiss PKI solution because of concerns over support structures. Orlando incorporated the requirement for 24-hour support in the CCM. However, WM&BB expressed concern about this provision because they lacked the funding for the estimated additional 900 person hours per year. Bankrecht Investment (BI) also continued its effort to convince top management that it has a cheaper and more flexible infrastructure than the CCM scheme. Despite these hurdles only six months after the re-branding directive, and two months after the launch of Orlando project, Bankrecht was on the road to a Group-wide PKI. This is a big feat because the Group had, since 1992, tried but failed to establish such an infrastructure.

Chapter summary

This chapter presents PKI institutionalisation efforts at Bankrecht in two phases. The first phase covers the lengthy interaction between the Bankrecht head office in Switzerland and its investment banking division in London. This phase ends in chaos with the main protagonists going separate ways because of disagreements about the cost of the PKI. Switzerland retains the Entrust-based PKI solution and BI opts for a 'cheaper' Microsoft PKI. The second phase follows the abolition of subsidiary brands in June 2003. The phase ends with Switzerland-based WM&BB being appointed lead support division for the centralised certificate management (CCM) scheme. The scheme advances the centralised PKI idea.

CHAPTER 7: ANALYSIS OF FINDINGS

Introduction

The previous chapters depict elements of power and politics in PKI institutionalisation. In line with the *telling-showing-telling* concept, the studies transport us to the two organisations by portraying first-hand experiences of different stakeholders with PKI. The depiction of power concretises our theoretical propositions into living organisational contexts. Having drawn attention to the data, this Chapter *tells* readers what it showed. We use the Circuits of Power (CoP) framework lenses to explore the political undercurrents of the two PKI projects. We base our analysis on the theoretical ideas presented in Chapter 3. Our goal is to ascertain the value of the CoP in explaining the real world events presented in the two case studies.

We organise the chapter as follows. First, we briefly restate the CoP elements. Next, we evaluate the political factors affecting PKI and its proxy GID at Oilcom. The second part focuses on Bankrecht AG. We explore a concerted effort by Switzerland to control its global divisions first with PKI and later branding. We assess how the two strategies attempted to modify the political configurations of the bank and the impact of power on their execution.

The Circuits of Power: Analytical tool

In Chapter 3, we saw that scholars widely see power in terms of dispositional, agency and facilitative concepts. However, Clegg (1989) claims that none of the concepts fits into a narrative structure constructed around a single, essentially contested concept of power. Thus, he introduces the CoP as a tool to unravel the problem. Clegg believes his framework is suited for the role because it incorporates different debates and offers well-grounded alternative power conceptions. With roots in the Sociology of Translation, the CoP provides specific language for visualising and thinking about the material nature of power in everyday organisational relations (Introna 1997). Clegg named it a 'Circuits' framework to signify that power is relational concept and not a 'thing' to be owned.

CASE STUDY ANALYSIS: Oilcom

The PKI at Oilcom is part of Group Infrastructure (GI), a Windows 2000 desktop and server standard. The technical components of the infrastructure include a standard client or GI-Desktop (GID), Microsoft PKI, Active Directory and Exchange 2000. However, GI involves a radical change of the politics, IT support structures and culture of the entire organisation. Oilcom uses X.509v3 certificates. As we saw in Chapter 2, the PKIX standards are offshoots of the X.500 directory access standard proposed by ISO and ITU. X.500 is a command and control standard because it assumes a root entity and dependent roles such as subscribers and relying parties. X.509 offers a framework for authenticating X.500 services by defining the structure of certificates and any optional extensions.

Episodic Circuit

Social theorists traditionally define power as the ability of individual A to make B do something they would otherwise not have done. The definition coincides with the episodic circuit that focuses on the production of tangible and foreseen outcomes. In Chapter 5, we saw that PKI, smart cards and supporting technologies such as Active Directory collectively provide a service delivered to users via a GID client. GID is part of a long-term effort by the Committee of Managing Directors (CMD) to end fragmentation and restrictive business practices within the Group. The CMD argues,

> "It is essential that the (Oilcom) Group becomes faster and more flexible. Free flowing information and making optimum use of our resources helps achieve these objectives. And to maintain a competitive edge we have to share our knowledge and talents globally, both inside the Group and with our business partners, customers and suppliers."

The committee believed these changes would cut costs, increase profitability and respond to challenges such as globalisation. Why then did Oilcom need to become more flexible? In Chapter 5, a technical consultant complained that work was slow because of politics. She claims Oilcom rarely feels like one company because departments often clash owing to contradictory goals and unwillingness to share information. Oilcom has also been criticised by City of London analysts for being slow and reactive to market events. Other respondents believe Oilcom is slow because it relies on committees.

'Management by committee' is a product of the complex Oilcom organisational structure. Oilcom consists of two holding companies that are separate legal entities. Apart from this arrangement, the physical structure of the Group consists of service companies (SCs) and a network of strong, locally rooted operating companies (OCs). Business divisions such chemicals tie the companies together and report to the Excom. The Committee of Managing Directors (CMD)[23] sits above all these entities reviewing long-term plans and key investment decisions. A defining character of the structure is that Oilcom is traditionally a distributed organisation. Oilcom also lacks a strong command and control structure because most decisions are consensual. The only mandatory areas are the brand and business principles.

To transform Oilcom into a more flexible organisation, the CMD mobilised resources and made alliances with various stakeholders. However, changing the character of Group proved complicated. The process saw conflict between parties with different interests and degrees of power. This was little wonder because the episodic circuit represents a struggle for power and attempts to limit or resist and escape its exercise (Clegg 1989). Hence, the committee made GID a key driver of the transformation. GID continues a standardisation effort started in 1988 when SCs recommended hardware and operating software to the OCs. However, because the structure of strong local companies remained intact, the businesses ignored the advice creating massive application diversity.

In 1997, Oilcom created Services International (SI) to change the delivery structures for IT and other services across the Group. SI expedited efforts to centralise and standardise the provision of computers, servers and general network operations. Let us explore the *As* and *Bs* in the power relationship. The committee is obviously the prime *A*. However, SI and Excoms represented it in the direct power exercise. SI became the most prominent player after the 1997 re-organisation of service provision. The division implemented IT systems and services to ensure that all OCs, the *Bs*, complied with the committee goals of increased openness and information sharing. The desired outcome was a flexible organisation with a low cost for IT. This was a contentious issue because the companies traditionally prized their autonomy and

[23] We also refer to the Committee of Managing Directors (CMD) as the committee

had defied earlier attempts to impose similar changes. The standing conditions of the operating companies stem from their management responsibility for local operations. The changes led to departure of employees because of a "move of parentage" after the consolidation exercise. Therefore, despite immense dispositional and facilitative powers, SI failed to realise cost savings because of the resistance of local companies.

After the failure of standardisation to deliver the flexible Oilcom, the committee created Information Technology International (ITI) to focus on IT provision. The standing conditions of ITI derive from their expertise in information technology. The committee legitimated ITI power through documents such as the Seven Point Plan, Business Communication Principles and Trust Domain. The guidelines advocated increased information sharing and security. Trust Domain defines a framework for creating a trusted network environment to support global business applications and information sharing. However, Trust Domain suffered from low uptake because of disparate hardware platforms, support arrangements and IT funding sources. Ironically, the committee also undermined Trust Domain by claiming,

> "It is unrealistic to expect all your Operating Unit services to be inside the Trust Domain. Therefore, **you have to decide which of your global services need to be with the Trust Domain.**"

Allowing companies to select the systems to include in the Trust Domain gave them a good reason for ignoring the measure totally. The result was widespread local customisation and independent adoption of software that exacerbated fragmentation, increased support costs and delayed the implementation of new software and functionality. Consequently, the committee saw GID as a tool for breaking down fiefdoms and supporting full information access. The committee further legitimated the power of ITI in the GI proposal by appointing the division as the sole provider of IT support for all local companies. Unlike previous systems, GID is mandatory. The committee believes GID must remain a "centrally controlled and rigorously enforced" platform to succeed. PKI holds the GID architecture together.

With the technical platform in place, the committee mobilised a field of force to champion its objectives. This was vital because the dispositional and facilitative power of the committee were not decisive due to the lack of a command and control tradition. The committee enlisted ITI, which is part of Service Companies (SCs), to align GID outcomes with its objectives. However, the SCs have an uneasy relationship with operating companies (OCs) especially the big ones. The companies often regard SC consultants as spies from the head office. Therefore, SCs traditionally rely on the goodwill of companies to implement any system or dispense advice because local management is responsible for the profitable and viable operation of businesses.

The large OCs based their resistance on the resources they activated in the struggle with ITI. This is because relative positions of power depend on pre-configured standing conditions under the social and system integration circuits that enable agencies to achieve different outcomes. While ITI had a CMD mandate, the local companies had a stronger power base because they controlled the financial resources. The companies bitterly complained about the loss of flexibility due to the locked down GID client. An ITI team leader admits,

> "**I think there are many human issues around it**. What you are doing is you are taking away from people flexibility they had before. So they don't like that. Maybe it is good for them but they don't like it. If they never had that flexibility, I think new people who joined Oilcom and know nothing but GID don't see a problem, but **if you had the flexibility before and it has been taken away, you see a big problem and you fight against it all the time**. How do you fight GID? By finding things that do not work and by saying 'well this does not work I must have two machines' and things like that."

The resistance of companies led to lengthy delays and cost overruns. It also confirms the power effects of GID. Like earlier IT standardisation drives, GID originally failed to deliver cost savings and improved performance because the large OCs wilfully restricted the power interactions to the episodic circuit. Hence, they reproduced existing configurations of rules and domination. The outcome was unsatisfactory because interactions that produce enduring outcomes must reshape rules of practice to enable *power storage* that maintains these effects.

To remove this power vacuum the committee instructed Excoms to make GID a governance issue. This was a vital decision because Excoms have tactical responsibility for business lines and define performance targets for OCs. With support of Excoms, ITI became the sole provider of "ongoing IT support." Oilcom claims the move aims to leverage buying power and scale, simplify procedures and create a consistent approach to infrastructure installation and maintenance. Thus, the desktops under ITI control increased from 69% to 94% by the end of 2001. The provision of IT as a global service follows similar efforts to streamline Oilcom services. An ITI consultant claimed,

> "What will happen there is that the kit, the people, the infrastructure locally will remain as it is except the fact that who pays the bill at the end of the day is somebody else. The manager of that infrastructure, the

> manager of those people locally changes but in reality nothing has changed nobody changes on the ground, no infrastructure changes just basically it is who pays for it at the end that changes and how to pay for it."

These are contentious changes because they involve control of money and appointment of managers. Law (1991b) argues that managers assume that they have a 'store' of power to act. This normally takes the form of money because its liquidity enables 'powers' to conveniently convert it into a variety of actions, which too are accumulated, deployed and converted. Being a relationally derived store of power money allows 'powers' to exercise episodic power. Therefore, once operating companies allowed ITI to pay for the local IT services and appoint managers, the businesses lost control over the infrastructure.

Obligatory Passage Points (OPP)

The Obligatory Passage Point concept is central to the Circuits of Power analysis. Simply put, when an agency wants to take charge of organisational agenda, they define the existence of a problem and identify solutions for resolving it. However, the agency only presents the solution in terms of the resources they can provide. Thus, OPP covers an array of strategies, resources and artefacts that agencies trying to dominate organisational events claim are indispensable for solving particular problems. An OPP enrols interests of different agencies into stable representations allowing the creation of alliances necessary for achieving outcomes of power. This is the main idea of the CoP framework.

Since innovations disturb the social integration circuit by introducing new meanings, their institutionalisation relies on attaining stability in rules of practice as OPPs. The OPP concept has roots in the sociology of translation that explains the mechanisms by which the social and natural worlds gradually take form resulting into certain entities controlling others. According to Callon (1986), for actors to impose their definition of the situation on others, they must go through four 'moments' of translation namely problematisation, interessement, enrolment and mobilisation. Let us explain how this process unfolded at Oilcom.

Problematisation

This is the 'moment' where an agency attempting to become a spokesperson defines the nature of the problem and suggests ways of resolving it. The IT division and external consultants initiated the 'moment' by referring to reports that showed Oilcom as inflexible and running a high cost for IT. Using a Gartner model and 1998 actuals, Information Technology International (ITI) showed that Oilcom's average direct cost per annum was at least US$3,600. This figure was well above the $2,500 industry average. ITI claimed Oilcom should emulate 'world-class peer' organisations like IBM, Nestle and Unilever that manage their infrastructures with a focus on cost. The alliance presented their problem definition and a ready solution in GI to the committee. The board liked the GI proposal because it promised flexibility, cost reduction and hence improved profitability. Because ITI presented an obvious case for GI, nobody was able to challenge the views at the time. Since Oilcom lacks a command and control structure, even with the backing of the committee it was vital to build a

GI support network. Thus, ITI identified and defined interested agencies in a way that made it central to the network of relationships it created.

Interessement

The episodic circuit discussion identified some of the agencies involved in GI and their interests. The list includes the CMD, Excoms, Service companies, ITI and its expertise, large and small OCs, employees and external players Microsoft, Schlumberger and Gartner. Interessement covers the actions that ITI undertook to impose and stabilise the identity of these agencies. Generally, ITI informed them that participation in the project would improve their standing conditions, cut costs and increase the profitability of the Group.

For instance, ITI invited their old nemesis, the large operating companies, to suggest features to include in GI. This was vital for the success of GI because previous standardisation efforts failed because they alienated these powerful OCs. Thus, ITI forestalled the formation of a unified alliance between the OCs that torpedoed earlier committee endorsed standardisation efforts. However, the interessement was not easy. The Director of the project admits the 'moment' got off to a bad start because ITI wrongly assumed that the committee mandate would automatically cow local companies into accepting the infrastructure. He reveals,

> "We set up a mandatory infrastructure. ...We thought that because the CMD mandated GI, there was no need to sell it. We were wrong! We actually spent more time and effort persuading OCs that they need to take this particular standard. We spent more time on this than on any of the previous standards and initiatives, which were optional. They could choose to take those or not. It was their choice. **This was not their choice**. So they were prepared to spend infinite amount of money and time arguing."

ITI eventually showed these actors that it suited their interests to participate in the project and shape GI rather than use a system imposed without their input. For instance, ITI informed companies that GI would help them reduce costs and meet the CMD requirements for increased profitability. Cost cutting was critical because the oil price was low. ITI got a big boost in its interessement drive when the CMD approved a requirement that, "The GIPT[24] must have the unequivocal backing of the Excoms if the project is to be successful." The CMD asked Excoms to nominate project champions and make GI a governance issue.

[24] Group Infrastructure Project Team

The committee also instructed the Group IT Steering Group (ITSG) to support ITI. Before GI, the ITSG recommended the widely ignored IT infrastructure standards for operating companies (OCs). In addition, the CMD asked Chief Information Officers (CIO) of each business[25] to support GI directly. The local IS departments initially opposed GI because it gave ITI control over their IT. The committee support changed GI from a system prescribed by the corporate centres into a governance issue. However, the Director of projects admits,

> "The main difficulty I think we had with that was while governance concerned the businesses, **they had to keep reinforcing the message with the OCs**. It eventually worked but it certainly did not work to 100% the first attempt. Thus, it was a message that needed continual replenishment."

After costly delays, the companies accepted GID because they were already under pressure from their Excoms to cut costs and knew the committee was determined to see it succeed. This was a major success for ITI because by conscripting the large OCs with the strongest power bases, the division deprived any lingering opposition of the resources to question the legitimacy of the OPP. Therefore, the support of the committee and Excoms helped corner the entities ITI hoped to enrol and created a favourable balance of power for the division.

Enrolment and mobilisation

Callon (1986) reveals that moments may overlap. We believe enrolment and mobilisation overlapped at Oilcom. Enrolment is for the definition and attribution of interrelated roles to respective actors. GID enrolment relied on two basic statements. First, the agencies believed that GID would help profitability, despite the low oil price, by reducing costs. Second, in a departure from the consensual decision making approach, the agencies realised the CMD was determined to implement GI with or without their assent. Thus, they listened favourably to ITI's claim that it was much better to participate and shape GI than use a completely alien system. Due to the ambitious GI schedule, ITI concurrently consolidated the alliances through bargaining and concessions and translated other actor's wishes into a single will for which they (ITI) spoke. The platform for mobilisation was the GIPT. The GI proposal states,

> "A common GI is only possible if the Businesses speak to the supplier (ITI) with a single voice. Consequently, a small group has been established to represent Businesses and Group interests. ...The GIPT will set the specifications of the common GI and service levels, and will agree tariffs with ITI against best practice benchmarks."

[25] 'Business' units here refer to the five silos under which Oilcom is organised such as Exploration and Production that sit above the individual operating companies (OCs) under an Executive Committee (Excom).

ITI shrewdly allowed the more powerful operating companies (OCs) to dominate GIPT. In effect, a handful of OCs from developed countries became spokespersons for silent operating units in over a hundred and forty countries. The weaker OCs never contradicted their 'spokespersons' because they were neither invited to 'speak' nor had the expertise to present an effective counter case. ITI perpetuated the belief that what is true for a few is true for other OCs by stating that, "The GIPT will make proposals for a small number of archetype companies, which will serve as a template to judge OU[26] requests." Although ITI never gave the large OCs a veto, they greatly influenced GI features and largely got what they wanted. The concession gave ITI legitimacy as the official spokesperson for the whole project because the large OCs believed the division represented their interests too.

Then next question then is, did the silent majority OCs follow their representatives? Yes, but for a short while. The GIPT alliance caused a lot of resentment. We saw that ITI claimed that the GID project could only deliver benefits if the platform followed a standardised approach "with only limited flexibility to accommodate OU specific requirements." Interestingly, because of their huge financial resources, the large OCs were not badly affected by the locked down GID client because they could afford the unlocked but more expensive "Developer" machines. Apart from the reduced flexibility, the silent majority rebelled because GID clients were very expensive. The spiralling cost specifically enraged OCs in the Far East because local IT sourcing is cheaper in the region. ITI conceded as much by locating its server administration and GID scripting centre in Malaysia. The ITI take over of desktops was also troublesome because Oilcom does not have 100% control of most of the OCs in the region. The cost of the GID computer enraged many joint venture partners. In sum, the 'silent' OCs resisted GI because it eroded their capacity to control IT resources.

The GID architecture also suited OCs in countries with fast network connections because all data and applications reside on network drives. Users with slower connections faced problems with file synchronisation leading to frequent data loss. Searching for stored network files was also slow. At this stage, GI institutionalisation was incomplete because agencies saw it as a threat to their liberty and an impediment to work practices.

[26] Organisation Unit (OU) is synonymous with Operating Company (OC).

In response, ITI abandoned the core GI specifications in some locations and deployed GI-Lite, a variant of the platform with limited remote and central management capability. However, this was not a compromise because the GI proposal issued in 1999 discussed incorporating "lower service solutions" without central ITI management. The real GI objective was to 'take on' large sites that were still under local control. Since, enrolment involves trials of strengths and tricks accompanying interessement (Callon 1986), ITI organised a conference in May 2002 where it presented GI-Lite as a concession to the disgruntled OCs. They accepted the idea. In truth, ITI tricked OCs into accepting GI without modifying its architecture because GI-Lite was part of the original design.

We believe the translation of actors in the Oilcom internal PKI seems a success now. The positive outcome emanated from a combination of the CMD facilitative and dispositional power and the successful translation of various actors by ITI. Translation enabled ITI and a few powerful operating companies to represent many silent actors of the Oilcom social and natural worlds that they mobilised. PKI, smart cards and Active Directory are central to the stability of the network because they structure the power relationships.

Social integration circuit

Social integration or dispositional power focuses on the relation between rules governing meaning and membership. It is essentially the capacity of agencies to produce intended effects on others even though they may not manifest this potential in action. However, since the circuit also deals with legitimate and illegitimate power, rule change is contentious because it disturbs episodic power. Introna (1997) warns that information systems often fail when there is a lack of fit between the meanings the systems create and the existing organisational rules and norms. Yet sweeping change is what is required to create enduring episodic power effects that enable IS institutionalisation.

Before GI, Oilcom had failed to deploy global IT systems because of the resilience of its autonomous institutional order. The team responsible, ITSG[27], faced resistance because Oilcom has traditionally been a loose federation of OCs. The half-hearted standardisation efforts also soured social relationships, hardening the resolve of OCs to defy the service companies. If Oilcom is so disjointed, how then has it thrived in the turbulent oil sector? We saw that the Group attributes its longevity to scenario planning under which Oilcom suspends corporate rules to survive challenges. In a way, the ease with which Oilcom disregards corporate rules highlights the disintegrative nature of its culture. A security consultant also attributed the longevity to the brand, which he claims is sacrosanct. In Chapter 5, we saw that brands are powerful tools for enforcing discipline in distributed organisations. The social integration circuit includes norms, rules and meanings that identity organisational groupings. Likewise, under "brand culture" the Interbrand model identifies elements such as beliefs, values, norms and symbols that are vital for group formation and cohesion (Interbrand 2001). This is a useful insight because brands define rules of meaning and membership.

However, Oilcom never became cohesive because its structure and management actions enshrined decentralisation. The distributed structure encouraged the creation of professional fraternities and sub-cultures that competed with the official agenda (Angell and Smithson 1991). Therefore, deploying a global IT system was perilous because it was bound to contravene a sub-culture somewhere. For instance, while Oilcom officially runs PC platforms, a group quietly operated a full Apple Macintosh network for years. Thus, it was

[27] IT Steering Group (ITSG) recommended IT infrastructure standards for OCs

clear GID would fail unless there was a concomitant modification of the rules fixing relations of meaning and membership. With CMD and Excom support, ITI set out to either modify or contradict organisational meanings. First, ITI contradicted the legendary belief that autonomy was inviolable by rationalising IT support and funding arrangements. Thereafter, ITI controlled the user desktop and made it a launch pad for the new order.

How did the fixing of rules occur? ITI inscribed the rules and techniques of discipline into smart cards and Active Directory, the two most vital obligatory passage points for PKI. While the Group has over 100,000 employees in hundreds of professions, in one fell swoop, GID used technical artefacts to 'design' and only permit two groups of employees: 'developers' and 'users'. This move cut across social and professional groups to create uniform user groups. In other words, GID produced a lasting field of force for the articulation of episodic agency conceptions that support PKI. Having 'designed' and 'implemented' the new users, Oilcom relies on PKI to keep them faithful to their roles.

The smart card or 'corporate badge' is central feature of the new social order because it enforces the new rules and norms and thus stabilises associations at Oilcom. The card represents PKI because it stores user certificates. The internal authentication certificates have power effects because they moderate user activities directly depending on their Active Directory profile. The card stores the authentication certificate, private key, physical access features and a restaurant pass. The card uses a proximity and smart chip to identify employees to the physical access control systems and a magnetic stripe for the 'stored value' used in the restaurants. All the card functions are vital indicators of membership.

If we believe the cost argument, then network access control is the real objective of the card solution. However, to avoid resistance to network access control, ITI deliberately added physical access and restaurant access to the card. The food element is the most ingenious way of using smart cards to enforce PKI use and define membership. Getting food at work is an important feature of professional life at Oilcom because of severe time restrictions. We faced the pressure first hand when our contact revealed managers had complained that our research was taking too long and affecting people's pay! Consultants receive hourly pay.

Lunch serves specific professional functions. First, most of the elite Oilcom employees at the services company in London are often away on assignments to OCs across the globe.

Therefore, lunch is an opportunity to network and catch up on office gossip and/or politics. Even without leaving the country, the company of over 100,000 people is too big for people to see each other regularly during office hours. The London SC alone has over 3,000 employees. Second, consultants use lunchtime to present work on ongoing projects and seek advice. Since SC consultants compete among themselves and with internal OC consultants for work, the lunch presentations offer a chance to market one's expertise in a given area. Thus, the integration of functions ensures that users bring the cards along.

Introna (1997) reveals that the acceptance of new material conditions depends on their integration with the institutionalised order as encapsulated by norms, beliefs and values. Apart from being a useful device, employees readily adopted the card because they traditionally carried badges. The smart card did not disrupt social practices because even building structures assume their use. However, because ITI inscribed new rules that reconfigured the social groupings and political arrangements, the effect of the card was more revolutionary than people realised. A senior Security Consultant gleefully reveals,

> "All our Windows 2000 desktops/laptops are using Microsoft PKI for logon/authentication internally. **The users are not aware of this. This is how it should be!"**

In contrast to the orphaned Bankrecht PKI, the prime reason for the success of Oilcom PKI is its stealth association with the desktop standard. GID itself benefited from sweeping changes in IT provision structures. To complete a remarkable canopy of legitimations, Excoms linked GID to corporate governance. Officially, ITI insisted GID enhanced profitability through cost controls. In private, ITI officials readily admitted the real agenda of GID, and its support technologies like PKI, Active Directory and smart cards, was to break down fiefdoms within the Group and increase information sharing.

Therefore, the smart cards are the most visible physical manifestation of CMD attempts to transform Oilcom into a flexible and unified organisation. From our research, it appears that the smart card has not only successfully translated the actors and stabilised their associations, the agencies are also remaining faithful to their inscriptions. Using one card, employees can log onto any networked device such as desktop computer, thin client, laptop and PDA, at any Group location and access their data and settings from the network drives. As we explain in the system integration circuit, the ability to 'roam' and obtain the proper level of authentication depends on Group Policy, an Active Directory feature. The main beneficiaries of 'roaming' are service company (SC) consultants whose jobs require frequent global travel to advise OCs. With prior approval and a little ceremony of identification, ITI easily enables the card to access Oilcom offices globally. Inevitably, the operating companies see roaming as an intrusion on their space. The amalgamation of physical and logical access features on one smart card allows ITI, with little consultation, to open the 'gates' of an OC to a consultant because they centrally control all permissions within Active Directory.

The card also translates the interest of the committee and employees to exchange documents without worrying about version issues. In sum, the integrated card has greatly helped PKI institutionalisation at Oilcom. Since, Active Directory stores the entitlements details on the card, only authorised users access buildings and network resources. The smart card was able to enhance security, flexibility and information sharing by challenging key meaning and membership characteristics, notably the autonomous formal structure and culture.

System integration circuit

The circuit focuses on the material conditions of production and discipline. These are technological methods of control over the physical and social environment and associated skills. The circuit is synonymous with facilitative power that explains the coordination of work practices and hence extends power beyond the exclusive concern with conflict. Clegg (1989) sees the circuit as the prime source of change in the CoP because innovations in material conditions either empower or disempower agencies. The changes create new agencies and OPPs that may question existing rules, norms and episodic power.

We focus on Active Directory (AD) because it offers the technological means of control over the Oilcom physical and social environment. System integration deals with domination because facilitative power regards episodic power exercise as always beginning from conditions. Webber (1964) defines domination as the likelihood that a given group will obey a command with specific content. To Latour (1991) non-human actors woven into the social fabric can account for stability and domination. Active Directory fits the description because it stores user credentials that enable PKI to keep GID a centrally controlled and rigorously enforced technology platform. In turn, GID structures moderate relationships at Oilcom.

Active Directory (AD) is a potent tool of domination because it offers administrators a hierarchical view of the network and a single point of control for all objects therein. As a senior Security Consultant reveals, AD is such a critical infrastructure at Oilcom that "if we can't find people or certificates in it, we can't operate this business." Microsoft claims the AD logical hierarchy supports simplified management because it represents organisational business structures. However, the top-down organisation of network resources is problematic in distributed global organisations. For instance, a security consultant concedes,

> "It is clear Active Directory is a complicated animal to live with. It apparently has some restrictions and you have to be very thoughtful about how you lay out your directory schema, right from the very beginning because changing it is not easy at this moment."

Let us assess how ITI uses PKI and AD security features for domination, surveillance and discipline. Under the social integration circuit, we saw that a multipurpose 'corporate badge' allows agencies to 'roam' Oilcom and access their files and settings irrespective of location and device. Roaming relies on *IntelliMirror* a Windows 2000 feature that only works with Active Directory. *IntelliMirror* uses policy-based configuration management to enable data, software and settings to follow users in distributed computing environments. *IntelliMirror* benefited from the sweeping reconfiguration of Oilcom social groupings under GID. The fixing of the redefined rules governing meaning and membership into social relations relies on yet another Active Directory feature: Group Policy (GP).

Group Policy provides the primary techniques and means of controlling the Oilcom social environment because its settings manage the behaviours of objects in Active Directory. Group Policy defines and controls how programs, networks resources and operating systems function for users. Even if an administrator modifies properties of a file, access to the resources still depends on group membership. In terms of PKI, Group Policy controls auto-enrolment, a process by which a Microsoft CA uses certificate templates to automatically issue, renew and install certificates. Therefore, the association of PKI with AD has political implications because, if agencies have control over the directory, they decide who may request a certificate, fetch them from the directory and determine their validity.

The possibility of delegation is the common riposte to accusations that AD is authoritarian. The feature allows the assignment of responsibility for managing portions of the network to other users. However, GP allows administrators to decide how much authority to delegate. The AD deployment faced similar delays like the wider GI project. Local IT divisions were concerned that an enterprise AD would certainly confirm ITI as the overlord of IT. However, unlike Bankrecht, the AD deployment went ahead for two reasons. First, ITI relied on the formal power of the CMD and Excoms to install the directory. Second, the local IT team believed AD would largely manage Address books like the X.500 enterprise directory it replaced. Indeed, early uses of AD focused on the Address book. However, Active Directory (AD) is central to the reconfiguration of rules and norms. Oilcom ensured that OCs would not know much about AD by recruiting a special team for its deployment and later moving most members of the Europe-based team to Malaysia to offer IT backroom support. Since, even ITI is not conversant with AD, the manoeuvres deprived opponents of the means of opposing the directory. This approach also extends to the wider ITI efforts to deny the existence of PKI. For example, a security consultant claims,

> "There haven't been key stages in the rollout of the PKI because the certificates were part of the delivered service solution which is the GID solution ... People **don't know** they have the certificates."

Active Directory (AD) is a disciplinary system too. To Clegg (1989) disciplinary practices rely on the surveillance of agencies through the collection, recording and comparison of data about their activities. A senior Security Consultant reveals the Oilcom recruitment process starts with the creation of a minimal user profile in AD that includes a surname, given name and initials. Once the profile has sufficient rights, the employee receives a smart card. The link of card with the AD profile and its privileges automatically regulates its use. In addition, since the 'corporate badge' includes the picture of the user plus a chip that sends details to the physical access system about entry and exit times, it is a surveillance tool.

The directory incorporates micro-techniques of power since it inscribes and normalises actions of individuals and groups. Oilcom also requires employees and visitors to display their cards prominently on its premises. Unlike passwords that are only proofs of what you know, the card combines the knowing aspect (PIN) and possession factor (the card itself). This is a more robust tool of control. Since through smart cards, AD ensures that each agency sticks to their role, it is a tool of domination. Thus, ITI translated the agencies and kept their associations stable using technical artefacts. The empowerment of ITI and disempowerment of local IT divisions relied on the fixing of rules of practice coupled with systemic integration using AD and smart cards as sources and centres of control. ITI redefined social relations and causal power because it established strong networks of control that supported the use of PKI to underpin new standing conditions.

Outcomes

The Committee of Managing Directors (CMD) has obviously achieved its objective of better information exchange within the Group through GID. The desktop also enables Oilcom to gather more information about people connected to its network resources. For instance, the Director of Global IT projects revealed that ITI can within fifteen minutes, identify all users with licensed software on the network. However, influential agencies admit Oilcom has so far failed to achieve its poster objectives of cost reduction and increased flexibility. As the Director of projects concedes, "I think the value of what we have done is much more in terms of a business enabler rather than a cost reduction." Likewise, a vendor from the corporate badge provider warns GID will hamper the flexibility of the Group because it is too rigid. An Oilcom security consultant agrees. He admits,

> "The reality is that you create a huge solution that when you want to make one small change it has an effect on the wider structure. You cannot engineer for one circumstance because this is very expensive. **However, it takes a while to make the changes that benefit everybody.**"

We saw elsewhere that it takes weeks to script software not pre-installed with the desktop to operate on GID clients. Likewise, despite the main the logic of GID being the speed of replacing faulty PCs, rectifying problems takes longer than predicted. For instance, when the card is faulty users cannot logon at all. The Helpdesk cannot help either because, being remotely based, they can only take over a user's computer when they are logged on. In the situation, the user either gets a new card, or as often advised by the Helpdesk, they turn their computer off and try the next day. This is short of the dynamic support promised.

PKI as part of Oilcom life

An alliance of Oilcom agencies that includes the CMD, Excoms, ITI and big OCs along with external players notably Microsoft, Schlumberger and Gartner has wrestled power from hitherto autonomous operating companies. The outcomes are more durable than episodic power effects because PKI, smart cards and AD can reproduce the conditions for their institutionalisation in the general stock of knowledge. Conversely, PKI and its support technologies would not have achieved wide acceptance without the structural changes introduced as part of GI.

However, even with PKI holding it together, GID failed to achieve systemic integration at the start because it interrupted work through its lengthy logon procedures. Mobile workers and employees in companies with low bandwidth felt the pain the most. The system also frequently crashed during major software releases because all machines at sites concurrently attempted to download updates of over 150MB. This killed the connection. ITI deployed GI-Lite to placate OCs and mobile workers in low bandwidth areas who resented the interruption of their work practices. ITI also introduced a CD distribution service that every six months delivers software updates, patches and McAfee to a vocal group of about 1,000 employees who work from home. The changes collectively enabled GID to achieve systemic integration.

Oilcom agencies take the system for granted now because they no longer openly accuse it of threatening their freedom of action. Furthermore, because the system crashes less frequently, ITI tactical manoeuvres have mollified irate workers over its impact on work practices. The incorporation of self-help features in the design of GI also helped systemic integration. The Director of projects teasingly observes this was an attempt by ITI to "outsource some of this support back to our customers." This move initially caused uproar with employees fervently opposed to doing IT support. However, good documentation and the "follow the sun" Help Desk network made the changes an acceptable part of organisational life at Oilcom.

From infrastructure to institution

In Chapter 2, we saw that infrastructures are regulating skeletons that provide security and stability rather than liberty of action. Certainly, PKI has created more secure and stable IT structures compared with user ID and password authentication. The outcome has reduced fragmentation and improved information sharing at Oilcom. However, agencies only reaped the benefits at the expense of their freedom of action. PKI lies at the heart of GID and ensures it stays a centrally controlled technology platform with limited flexibility. The changes proved politically explosive because they demanded a reconstitution of norms, rules and meanings as well as techniques of production and discipline of a pluralistic and distributed organisation. However, GID succeeded because ITI enrolled interests of various agencies into stable representations creating alliances that enabled the standardisation.

A key reason for the success is that ITI astutely embedded PKI into other structures such as GID and smart cards to an extent that the infrastructure became transparent to users. Thus, unlike Bankrecht, *Oilcom introduced PKI by stealth* (Townsend 2001). ITI claims this is how it should be. One consultant even insists Oilcom has no PKI at all. By storing the certificate and private key on the card, PKI built on the long tradition of using cards and badges at Oilcom. Users also found the card helpful for mobile work because it enables access to files around the Group without the inconvenience of passwords. The card is also evidence of membership, because without it a person can neither enter buildings nor use computers. Thus, as personified by the smart cards, PKI effortlessly supports work at Oilcom and is part of it.

Well then, has the PKI been institutionalised? We can say yes to a certain extent. To Berger and Luckmann (1967) institutionalisation starts with habitualised actions routinised in the general stock of knowledge. Before 2000, the predecessor of ITI, Services International attempted to arrest IT fragmentation with the provision of pre-configured Windows 95 and NT server images. However, because of the "Not Invented Here" syndrome the OCs customised the images to suit their local needs. Therefore, ITI failed to routinise the meanings into the stocks of knowledge making it impossible to use the experience in future projects. However, the incorporation of PKI ensured that the GI desktop remained stable. Thus, PKI has created the background of stable practices that precede institutionalisation because, with the locked down GID, agencies know their network privileges. However, like other institutions, the PKI simultaneously empowers and controls agencies. Using the card, PKI allows employees to 'roam' the organisation and access their files and settings regardless of location and device. However, the privileges are constrained by roles.

Stinchcombe (1968) argues that the key to institutionalising a value is the concentration of power in hands of those who believe in it. The destiny of Oilcom PKI lies in the powerful hands of the CMD, ITI, Excoms and Microsoft. Each of the agencies has a stake in seeing the PKI succeed. After Jepperson (1991), we argue that the PKI is an institution because it represents and reinforces the rules that bind Oilcom together. PKI is the foundation of reciprocal typification of actions between ITI, users and OCs. For instance, PKI ensures that only employees with 'developer' machines can install software on their PCs. Others either use pre-installed software or send the applications for GID scripting.

After Berger and Luckmann (1967), we argue that like other institutions, Oilcom uses its PKI to predefine and channel patterns of conduct of its human and organisational agencies. Since PKI is part of other structures and agendas like GID, smart cards and organisational restructuring, its existence is independent of the agencies. The agencies could not avoid it even if they tried because ITI astutely attached the PKI to facilities that are central to Oilcom membership. Therefore, PKI has power of employees because of the physical access, lunch and network access facilities attached to it. More tellingly, employees cannot escape the reality of the PKI even when, as we have showed that they are neither aware of its existence nor understand its mode of operation.

In conclusion, Oilcom stealthily folded PKI into a larger infrastructure that includes a locked down GID client, Active Directory, smart cards and Exchange 2000. Along with network rationalisation, PKI benefited from a radical change of the politics, IT support structures and culture. Oilcom either used existing power structures or created new ones to support PKI. Conversely, PKI holds together the identified components and keeps various agencies faithful to their inscriptions. Therefore, PKI is an undeniable fact that Oilcom agencies cannot wish away. However, this is not a definitive outcome because by definition, the circuits of power are unstable since outcomes circulating in rules and techniques of production often challenge obligatory passage points. The biggest potential source of instability appears exogenous. Since, ITI does not control external PKI, the risk of organisational outflanking looms large.

CASE STUDY ANALYSIS: Bankrecht

At Oilcom, ITI consolidated PKI by embedding it into social relationships and practices. The practices include values, beliefs and norms that determine whether a technical artefact fits into an actual breathing organisation or not. As we emphasise in the next chapter, this finding alone is a significant contribution of our dissertation because it dispels the common belief in the literature that public key infrastructures can operate outside organisational practices. On the contrary, the Bankrecht project follows the trends promoted by vendors in which PKI is an obligatory passage point for secure e-commerce regardless of context. The argument goes that if global e-commerce is to thrive, organisations desperately (Ellison and Schneier 2000) need an infrastructure for large-scale permission and identity management. Put bluntly, "at present PKI interoperation best (and sometimes exclusively) satisfies the security requirements seen as critical to internet-based e-commerce (Baum 1999)."

As such, PKI at Bankrecht exactly fits the bill of what Clarke (2001) call, "the hammer that came to hand when the nail was discovered." What do we mean? We denote that since Bankrecht originally adopted PKI as a technological solution outside organisational practices, its objectives have kept mutating according to what supporters believed could keep the infrastructure alive. Therefore, while the underlying PKI technology (hammer) has remained stable, the uses (nails) have constantly evolved. The only times Bankrecht PKI has attained a semblance of stability is when its supporters aligned it with a broader agenda. However, since these are largely opportunistic localised agendas, PKI supporters have struggled to institutionalise it across the Group despite over ten years of trying.

Episodic circuit

Because PKI objectives at Bankrecht were highly malleable, the agencies involved changed regularly at various stages in its lifecycle. However, unlike Oilcom, power plays at Bankrecht largely remained in the episodic circuit because the sustenance of the infrastructure relied on ephemeral objectives. The failure to engender innovation in the techniques of production and discipline prevented the possibility of *power storage,* a key requirement for maintaining power effects. Thus, PKI supporters at Bankrecht often resort to a 'fire fighting' approach that involves active efforts to make other agencies use the infrastructure against their will. Let us assess the episodic circuit in detail.

In line with the traditional definition of power as the ability of individual A to make B do something they would otherwise not have done, let us identify the agencies involved in Bankrecht PKI and their standing conditions. We saw elsewhere that Bankrecht X initiated the PKI back in 1992. The original *As* were a small team that included a senior manager, two middle managers (one of whom is now a Vice President) and a technician. The *Bs* were employees of the centralised Bankrecht X. The objective of the PKI team was to increase security, because the move from mainframes to client-server systems had led to the proliferation of user passwords. The team believed that a combination of X.509v3 certificates and smart cards would stop employees from writing down passwords and hence risking the security of the entire bank. Maintaining security was critical because carelessness may have landed Bankrecht in trouble with the stringent Swiss secrecy laws.

In pushing the PKI solution, the Bankrecht X team relied on solid standing conditions. The team belonged to a powerful IT division with sizeable financial resources and equal standing with other business divisions. The division had control over IT and operated a standardised desktop architecture with a single domain across Switzerland. Therefore, the division had the capacity to change security behaviour. The server platforms division later joined the original team and strengthened the support network for the PKI solution. The team derived its standing conditions from its official responsibility for managing mainframes, all servers and developing middleware that controlled user applications. The enrolled agencies selected a Siemens smart card solution and started deploying the PKI across the bank.

However, the PKI bandwagon came to a shuddering halt because the 1998 merger unravelled the field of force that had supported the solution since 1992. The Bankrecht X team originally mobilised support for the PKI by aligning their security goals with the readiness of the top bank management to obey the Swiss laws. Therefore, the championing role for PKI strengthened the capacities of the IT division. However, the merger caused a drastic change in the balance of power between the IT division and the previous power targets, the employees. First, while the PKI originated in a centralised bank, a clash of cultures forced the merged Group to organise itself divisionally. Under the new structure, the IT division saw its standing conditions eroded because it no longer controlled a budget and became a subsidiary of business divisions. The IT team lost the capacity to exercise power because the divisions became autonomous and spent their budget as they saw fit. This caused a paradoxical role reversal where the divisions actually became the *As* and the IT security team the *B*.

Apparently, all divisions of Bankrecht X lost power after the merger. Bankrecht Y, the smaller of the two merger partners actually secured all the top management positions in the new entity. Financial industry analysts claim that this was because Bankrecht X had a huge financial hole and was struggling badly. This weakened its hand in negotiations. Therefore, unlike at Bankrecht X, the business divisions now have a veto over IT projects. This was a big reversal for the IT division because as we discuss elsewhere in this dissertation, power derives from the central control of resources and ability to effect decision making. Therefore, since the business divisions usurped the control of financial resources and the authority to make decisions about technology, the IT division lost power.

Since, the merger had eroded the pre-configured standing conditions of the IT division, the Switzerland-based team understood that the only way to embed PKI into the new institutional order was to justify it through a service that helps employees in their work. In other words, the IT division had to re-emphasise the legitimacy of the PKI. To Berger and Luckmann (1967) legitimation is vital for sustaining an idea because it explains and justifies its existence. Similarly, Stinchcombe (1968) argues that legitimacy creates readiness in other centres of power to support actions of other people. The need to legitimate the solution arose because IT Switzerland hoped to transmit it to employees of Bankrecht Y and later other global divisions that did not have individual recollection of the institutional order under which the PKI was developed. Thus, IT Switzerland created what Berger and Luckmann (1967) classify as a "corresponding canopy of legitimations" to associate the PKI with concrete social processes. Since the best way of legitimating an institution is making it useful (Stinchcombe 1968), the IT team made user convenience the key PKI objective. Why did they abandon security? According to a Vice President,

> "**We knew that we could not sell security to the bank, we could only sell convenience**. So, end users would not want a smart card that could only provide security, they could simply ask for ease of use. ...The users were clearly asking for convenience. Nothing else. ... The consequence of selecting Single Sign On as the dominant objective of the whole exercise was to bring convenience to the end user and increase security. But **security was only a by-product. You are not selling that to anybody. You do not sell security to end users. They don't care**."

User convenience was an excellent selling point because, since the two banks had separate applications for the similar functions, the merger worsened the already bad password proliferation problem. The situation left senior users with over twenty passwords leading to even worse security practices. The users complained in strong terms about what they termed a "silly strategy" of the IT division that created an ID and password for any new application. User groups even claimed that forgotten and blocked passwords were hampering their work. Top management asked the IT team to solve the password problem. Hence, despite its lost political influence, user convenience gave the IT team the excuse to deploy its PKI solution. The team also redesigned the solution to emphasise convenience because they were aware that users would abandon the smart cryptocards if it required excessive intervention. The Vice President reveals his team aimed to make cryptocard use more convenient than alternatives. Consequently, convenience was a good nail for the PKI hammer.

In Chapter 6, we saw that the clash of cultures between the two banks has its roots in the different institutional order their business focus created. Despite mergers and acquisitions abroad, Bankrecht X retained strong Swiss roots because it largely focused on the local market. In contrast, Bankrecht Y focused on the international market. However, since Bankrecht X was the bigger of the merger partners, its IT team tried to impose the centralised PKI solution after the merger. The drive failed because the IT team and the wider Bankrecht X had lost their power over business units due to divisionalisation.

However, despite losing discretion over user routines, the security team retained facilitative and dispositional power in Switzerland. This is because over 95% of the Swiss users have a highly standardised end-user platform called End User Platform Domestic (EUPD). Having showed the usefulness of the card, the IT team shifted focus to security. The IT team engaged in an extensive user education program that emphasised the importance of the cryptocard solution to security. By first showing the convenience of the PKI and later its security goals, the IT team got a sympathetic audience because Swiss employees are acutely aware of the role of secrecy in their profession and country. Failure to respect customer privacy has direct personal consequences in terms of a potential six months jail term, heavy fines and dismissal. After the campaign, card usage increased from 25% to 87%. From this evidence, we conclude that Bankrecht Switzerland (BS) has generally used its PKI to export secrecy to the digital world. Therefore, in terms of the CIA model, BS has focused on the confidentiality element.

Not Invented Here: Exporting the PKI solution

We previously saw that the resistance of different agencies has restricted the power effects of the PKI at Bankrecht to the episodic circuit, even in Switzerland, for three reasons. First, the solution was 'invented' in a centralised Bankrecht X but had to be used in a totally divionalised Bankrecht AG after the merger. Therefore, to ensure that the system remained alive, the security team adapted it to the new circumstances. The team opportunistically shifted the focus of the PKI from a security solution to a tool that solved the problem of proliferating passwords. Second, the original solution was problematic, because it assumed a well funded IT department with a strong power base to force its use. We have seen that after the merger, the IT division became an impoverished subsidiary of business divisions.

Third, the PKI solution suffered from a clash of cultures within the new Group because of regional differences. To overcome the problems, the Zurich security team appointed 'local champions' to spearhead the PKI project in other regions of Switzerland. The standing conditions of the champions derived from their limited authority delegated from Zurich. The association with the head office enabled the 'champions' to mobilise support for the PKI. Since even within Switzerland cultural differences weakened the shared meanings centred on banking secrecy laws, what were the prospects of institutionalising the PKI in foreign divisions? We explore this process through the efforts of the Swiss security team to fix the PKI as an obligatory passage point for the transformation of Bankrecht AG into a secure and pre-eminent integrated global investment services firm.

Obligatory Passage Points

To recapitulate, the concept of obligatory passage points is central to the circuits of power analysis. The concept is crucial for understanding institutionalisation because it defines strategies, resources and artefacts that agencies attempting to control organisational agenda claim are requisite for solving specific problems. Having learnt that the absence of a broad agenda delayed PKI institutionalisation in Switzerland, the security team saw the integration of foreign divisions after the 1998 merger as an opportune moment for exporting their solution. This was what the original PKI designers planned in 1992. Since, the PKI had helped enrol interests of different agencies in Switzerland they hoped to repeat the outcome abroad. To achieve their objective the team sought to make the PKI solution an OPP linking and translating actors such as management, business divisions, employees, Swiss security expertise, regulators, business partners and customers.

The security team claimed the PKI solution was critical for achieving the management goal of making Bankrecht X "pre-eminent global integrated investment services firm and the leading bank in Switzerland" after the merger. The team did not expect stiff resistance because it believed its association with the head offices and the appreciation of the resolve of top management to transform Bankrecht into an integrated global group gave it authority to implement the PKI abroad. Our analysis focuses on attempts by Bankrecht Switzerland (BS) to enrol and control the London-based Bankrecht Investment (BI) with the PKI solution. After Callon (1986), we assess the 'moments' of translation that BS used in attempts to impose its definition of the situation on Bankrecht Investment.

Problematisation

To reclaim control over IT systems lost after the merger, Bankrecht Switzerland (BS) identified the inconvenience and insecurity of passwords as a key problem facing the Group. The Swiss IT security team not only notified BI and the Group's top management about the problem, it also presented its 'home grown' PKI as the answer. For evidence, BS referred to the loss of productivity and escalating helpdesk costs. The team also highlighted a belief by Swiss users that the creation of a separate ID and password for all new applications was a "silly strategy." BS warned that the situation was worse across the Group after the merger since 120 applications were in heavy use. Besides, the increased use of client-server systems had eradicated the benefit of Single Sign On (SSO) offered by mainframe architectures.

Since the merger had deprived the IT team of its control of financial resources and forced the move from a centralised to a divisionalised structure, BS knew the only way to make BI and other foreign divisions adopt the PKI was through building alliances with other agencies. Hence, BS claimed that since BI and the Group top management wanted to reduce password problems and create an integrated global financial services firm respectively, they should support the deployment of the PKI solution. In the process, the Swiss team established the PKI as the OPP in the network of relationships it constructed.

Interessement

In this 'moment', we discuss the efforts of BS to impose and stabilise the identity of the agencies it defined through problematisation. The agencies include BI, top management, regulators, customers, shareholders, business divisions and employees. BS promised different benefits to the various agencies. For top management it was the creation of an integrated firm and improved compliance. Despite having a history of taking little interest in technology, BS informed the managers that PKI deployment across the Group would support the integration of various divisions. This would satisfy a key goal of the 1998 merger. BS also notified management that the global PKI roll out would ensure that the Group complied with the Swiss banking secrecy laws despite pursuing a model of banking "at any time, in any place, by any device." This was a compelling argument because poor risk management and absence of tools to enforce compliance in foreign divisions troubled Bankrecht X. Therefore, the PKI appeared an efficacious tool for showing regulators and business partners that the bank took risk control seriously. Since the PKI supported business integration, management believed it could also convince shareholders that the merger was, after all, a wise decision.

To Bankrecht Investment, BS promised convenience of use and deployment, and better security. The BS team claimed the adoption of their solution would be painless to BI because they had experience of deploying a PKI solution for 40,000 users in Switzerland. The Vice President summed it up as, "Because we know how to use it, we have deployed it." The experience argument was a double movement attempting to render the Swiss PKI solution an automatic choice and discount competitor solutions, notably Microsoft PKI. BS stuck to convenience as a key objective for pushing PKI to foreign divisions and informed BI that the Swiss experience would be beneficial. BS believed the OPP was a success. They were wrong.

The experience argument did not convince BI because they too had previously deployed an Entrust-based PKI, although it turned out nobody used it. BI expressed concern that since Switzerland had 'invented' the solution, it did not meet the specific needs of the London-based investment division. BI objected to the centralising features of the Swiss PKI solution and demanded their removal if they were to adopt the solution. BI believed the PKI managed from Switzerland would only increase their dependence on the headquarters and reduce their desired 24*7 availability of information. Timely access to information is more vital to investment banking operations than to the Switzerland-based private banking and wealth management business. The London-based merchant bankers also privately derided the risk-averse culture of the Swiss and their number of holidays and feared this could paralyse their work. Therefore, BI asked the Swiss team to modify the solution, which they saw as a threat to their time-pressured work practices.

BS could not discount the views of BI for several reasons. First, the Swiss security team needed the good will and financial help of London to deploy the PKI abroad, since it did not control funding for IT projects. Second and probably most important, BI was originally part of Bankrecht Y, the more internationalist and highly distributed merger partner. We have seen that since Bankrecht Y dominated top management positions, BI probably had more friends in high places than BS after the merger. Despite operating from the Zurich head office, BS did not control enough resources to compel BI to adopt the PKI against their will. On the contrary, being a profitable operation BI had more capacity to mobilise resources and form alliances to limit, resist and escape BS's exercise of 'power over' them. To the frustration of the Swiss team, top management was unwilling to force PKI onto BI fearing it may disrupt operations such as when a re-organisation exercise led to a drastic reduction in private banking profits from the first quarter of 1999. Claiming that "Many things are not seen totally at the top", the Director of IT Security argues that Bankrecht management instructed BS to deploy PKI only if it was not disrupting banking services.

Third, BI initiated its own bout of 'interessement' by offering the Swiss team free access to the Entrust licenses that cost the investment bank $0.5 million but were never used. BI promised to adopt the Swiss solution on condition that the BS team integrated the Entrust CA into their SCI-PKI solution. This was an attractive proposition because BS was itself in a process of replacing its own 'home grown' CA and proprietary network protocols with open standards. At the time, many people in Switzerland favoured a Baltimore PKI solution because they believed it was less prone to bugs from US intelligence than Entrust. Although they could not prove the existence of Trojan horses, since World War II Switzerland and United States have often clashed over banking secrecy (Guex 2000, Schneider 2002). For instance, VeriSign policies oblige subscribers to revoke certificates at the issuer's (VeriSign) request and surrender the private key to US authorities. The fear that US products could be bugged probably explains why the Swiss are major developers of cryptographic systems.

Despite these concerns, after close to a decade of research and pilot projects, Bankrecht seemed ready for a Group-wide PKI solution. However, it never happened. When BS integrated the Entrust CA into their solution, BI adopted Microsoft PKI instead. Thus, BS failed to ensure that its assumed ally BI stuck to their part of the deal. We explore this outcome under enrolment because interessement does not necessarily lead to alliances. The purpose of this 'moment' is to corner the entities for enrolment. We assess the measures BS adopted to keep the PKI alive under the mobilisation moment.

Enrolment

To Callon (1986) enrolment constitutes multilateral negotiations, trials of strength and tricks that accompany interessement and enable it to succeed. The purpose of the 'moment' is to define and attribute interrelated roles to respective actors. To enrol BI, Bankrecht Switzerland had to ensure they were willing to adopt the PKI solution. When BI granted BS access to their Entrust licenses, this seemed a possibility. The question then is why was BS unable to hold Bankrecht Investment (BI) to their promise to adopt the integrated solution? Enrolment failed because of the seemingly rational BI arguments, the weakened standing conditions of BS and their failure to see the big picture. BI attributed their rejection of the Swiss PKI on cost and support concerns. On cost, BI credibly argued that the solution was too expensive compared to Microsoft PKI. From rough BI estimates, Microsoft certificates cost about £4 a year per user because the division had a worldwide software license. The Director IT Security at BS admits their solution was more expensive and states,

> "The costs are high. I do not have a very good impression about what they are because in BS we do not even know how much we have invested in the project or the different projects surrounding cards ... However, as an estimate we pay per certificate – including tokens, cost and support – **around £200 annually per user**. .... We hope it is lower."

The costs cover secure servers, key management, and personnel. The costs were not only high but also unpredictable. However, this seemingly rational BI argument failed to add that like other infrastructures, the costs of running a PKI come down with scale. Thus, despite dressing their objections in judicious arguments, both parties admit the rejection of the PKI was political. While BI expressed concern about the lack of 24-hour support in Switzerland, privately the division dismissed BS promises that the solution would have delegation capacity. They discounted the use of delegation and argued that the support model would increase the control of BS over their activities. Therefore, Bankrecht Investment insisted the PKI should be "deployed for the right technical reasons and not for political reasons."

The engineer responsible for charting the PKI direction at BI also argues, "The service that BS is providing has been designed by Switzerland alone." He claims the solution does not address the specific needs of the investment banking and securities division. The Zurich-based Vice President who formed part of the original PKI team classified this fear as the Not Invented Here (NIH) syndrome. He agrees that BI rejected the Swiss solution because they would have had to live with an application they did not invent. As we saw in the Oilcom study, the NIH syndrome is a common feature of global organisations because they run diversified businesses in numerous jurisdictions under localised organisational structures. The Vice President claimed the Microsoft CA is a mere toolkit but not a working solution. BI counters that the product would get better and has lower support and development costs.

Since enrolment is a trial of strength and tricks, we believe BS committed elementary tactical blunders in their dealings with BI leading to a failure to translate interessement into enrolment. First, the Swiss division naively allowed BI to make cost a deciding factor in PKI adoption. Since infrastructures are heterogeneous, embedded into other structures and are socio-technical in nature due to their links with practice (Ciborra 2000, Star and Ruhleder 1996), it is impossible to ascertain the real cost of running one. As such, since the Swiss team did not control any budget but BI did and Microsoft was obviously cheaper than Entrust, the cost argument should not have arisen in the first place. However, even if BI had forced the cost issue upon BS, we believe they could have got a better outcome by focusing not on the costs of connecting but the opportunity cost of the absence of a PKI. A little spin on the argument would have won favour with top management because they were looking to create an integrated global firm and the PKI is a tool for such an agenda. Tellingly, BI understood that the failure to deploy a global PKI and Active Directory would cost the organisation dear in terms of future integration costs. Revealingly, a Bankrecht Investment PKI engineer did not blame cost for this failure but technical and political issues.

Incidentally, the engineer is an employee of US IT contractor, Perot Systems. He claims that outsourcing has enabled BI to agree divisional IT solutions and deploy them without thinking about organisational political implications. However, this is unconvincing. We believe BI brought in Perot not to reduce politics within the Group but to reinforce it. We saw that the ability to produce and achieve collective goals depends on material conditions, which are technological methods of control and associated skills and means. Despite its loss of power, Bankrecht Switzerland still controls the IT infrastructure that supports wealth management, the bank's core business. Therefore, the only way London could avoid the claws of Zurich is by proving that it has the capacity to provide a credible and cheaper alternative to the Swiss PKI solution. Perot Systems is thus a vital ally in BI's quest to reproduce existing configurations of rules and domination that support its independent IT.

After comparing proposals from Switzerland and London, each justifying their own PKI solution, the divisions decided to go separate ways. BI elected to install and run its own hierarchy of Microsoft Certification Authorities (CAs). Although cost was the main reason, the Swiss Director IT Security added, "They are probably not unhappy about the fact that this enables (BI) to remain independent of Switzerland as regards PKI." Thus, BS failed to establish its PKI solution as an OPP for a secure and integrated Bankrecht AG.

Mobilisation

Having failed to enrol BI with the experience angle, BS continued to explore ways of keeping the dream of deploying their PKI solution across the Group alive. Fortuitously for the Swiss team, the wrangle with BI alerted top management to the potential conflicts and confusion that a failure to coordinate PKI activities at Group level could cause. Emboldened by this opening, BS tactfully abandoned the push for their PKI solution from a technical experience angle and instead emphasised the costs of disintegration arising from separate PKIs. As we observe elsewhere, the Swiss team should have used the same argument to anchor its earlier interessement drive because top management had a similar agenda. Management quickly grasped the dangers at hand.

We should mention that in fulfilment of our research access obligations we submitted a report to Bankrecht on 12th December 2002, which highlighted the lack of coordination of PKI and the inherent risks to future interoperability. The report covered the views of both BS and BI regarding PKI activities in Group. The report seems to have pleased BS more than BI. For instance, on 17th December 2002 Director IT Security wrote that,

> “Thank you for the report - it gives us good feedback on how our solutions and views are perceived by "unbiased" people. On top of that, there are also a number of very interesting hints about how (BI) judges our approaches to PKI and tokens - this is not always very transparent to us.”

The BS team shifted from the experience angle and highlighted conflicts and paralysis created by divisional PKI arrangements. They claimed that the lack of PKI coordination was not only impeding current business, defeating the objectives of the merger, pursuing the same course of action could totally paralyse operations and lead to unbearable future integration costs. This was a fundamental statement in the BS quest to mobilise support for the PKI solution because nobody could contradict it. The lead PKI engineer at BI had admitted as much. Crucially, top management was sensitive to any statements that implied that the merger was not working properly. The attitude is understandable because commentators had dismissed the merger as an effort to save Bankrecht X from collapse without business logic. Therefore, Bankrecht was unwilling to vindicate its critics.

Callon (1986) regards mobilisation as the ‘moment’ for determining the legitimacy of the spokesperson. An actor who becomes a spokesperson translates the wishes of other actors into a single will for which they speak. Thus, since Bankrecht Switzerland (BS) articulated the wishes of top management for an integrated group and was unopposed by BI, it became a macro-actor. BS became a single voice that spoke for silent actors like customers, business partners, employees and regulators who had a stake in a successful Bankrecht. However, what BS lacked was a powerful agenda upon which to anchor the unison voice it had created. The re-branding drive that started in late 2002 offered the required platform.

Mobilising PKI support through branding

In Chapter 6, we saw that the re-branding initiative implemented in June 2003 abolished all subsidiary brands and replaced them with a single corporate brand. The drive added credence to BS claims that divisionalised PKI arrangements would create anarchy within the Group. BI normally retorted that these were manageable risks over-emphasised by BS to achieve political objectives. However, branding convinced top management of the significance of the BS apocalyptic claims. Why then was branding able to galvanise support for a centralised PKI? First, top management believed the branding initiative was a great opportunity to achieve its cherished but elusive ‘integrated business model’ or ‘one firm’ approach. Second, Bankrecht could not risk the failure of the drive because it was an extremely costly venture.

For instance, the bank wrote down about CHF 1 billion for abolishing a subsidiary brand that was capitalised on its balance sheet.

Ironically, the actions of BI triggered the confirmation of Switzerland as the legitimate spokesperson for an integrated firm agenda. BI brought management wrath down upon itself by contravening branding regulations in their naming of the root CA and certificates for their divisional PKI. The powerful branding team called 'Project Orlando' promptly reprimanded BI over their actions. A Swiss IT team based in the Wealth Management & Business Banking (WM&BB) division took the opportunity to stress the vitality of PKI coordination across the Group. Its new member, the Director IT Security, wrote,

> "On Group level there is an urgent need for governance for PKI activities as there is already a number of CAs in operation and others planned by the different members of the Group. The primary goals of the governing body (should be) setting the framework for (...) internal PKIs by issuing guidelines ...; **supervising PKI activities in (...) to force conformance** with above regulations and coordination among different applications and user communities..."

The WM&BB IT team suggested the creation of a Centralised Certificate Management (CCM) scheme. They issued a 'request for proposal' document to solicit opinions of different Bankrecht divisions about a centralised PKI. In his response to the document, the Director IT Security appealed to project Orlando to evaluate PKIs already deployed to identify the ones acceptable to Bankrecht AG and define their purposes. In his view, this would minimise the number of separate PKIs. Because of the potentially huge financial and market implications of failed branding, management asked the WM&BB team to lead the CCM initiative and instructed BI to participate. WM&BB invited BI, divisions in Switzerland and the US, and a private law firm to form a CCM interest group under Orlando.

Starting March 2003 Orlando set out to establish a centralised PKI as spelt out in 1992 by the Bankrecht X security team. In the first action against independent PKIs, the CCM team decided to move all divisional websites to Bankrecht main domain. This was a significant decision because it effectively installed Switzerland-based WM&BB as PKI coordinator across the Group. Second, the WM&BB IT team barred divisions from either ordering certificates or assigning this task to a third party. WM&BB claimed this was because from a legal perspective only the owner of the domain is entitled to make such arrangements. WM&BB argued this favours centralised certificate management. BI was the obvious target of the directives. As we saw, BI not only triggered the branding crisis that led to the formation of the cross Group PKI coordination team, it relied on third parties for its needs. Therefore, the CCM scheme reduced the number of intermediaries and confirmed WM&BB as the undisputed spokesperson for PKI at Bankrecht AG.

WM&BB organised a workshop that rubber-stamped its position as a macro-actor that spoke for top management, the brand, the PKI solution and surprisingly, BI. WM&BB manoeuvred BI into endorsing its network of alliances by appointing one of its senior managers as coordinator of the CCM scheme. While in the past BI easily dismissed the PKI as 'made in Switzerland', they could not make similar claims with their own manager coordinating CCM. Therefore, branding coerced hitherto warring divisions into an accommodation that brought the dream of a centralised PKI closer. The magnitude of the feat only gets clearer when we remember that in three months the brand-inspired CCM drive achieved more than what the team achieved in 11 years of research, pilot projects and re-invention of PKI objectives.

Since an OPP enrols interests of different agencies into stable representations to create alliances for achieving outcomes of power, should Bankrecht expect the branding forced PKI compromise to endure? We are doubtful for these reasons. First, although the Orlando project re-distributed power for PKI management, it was unable to erode the standing conditions of business divisions because they still control IT funds. For instance, WM&BB warned that without extra funding for CCM responsibilities, "we'll have to keep managing certificates in a decentralised manner."

Second, despite setbacks that led to the creation of the Centralised Certificate Management (CCM) scheme, our sources indicate that BI, recently renamed Bankrecht Investment Bank, continues to lobby management and the branding team that CA and certificate names are strictly technical issues best left to the independent divisional IT teams. This is no surprise because as Callon (1986) reveals, translation involves dissidence where agencies question, discuss, negotiate and potentially reject the authenticity of the spokesperson. We believe the arrangements are precarious because branding only achieved the CCM outcome through the episodic circuit without affecting rules and techniques of production. The latter are critical for reproducing episodic power because they constitute the field of force that enable strategies espoused in the circuit to make sense in an organisational context.

Social integration

Under this circuit, we analyse the relationship between the PKI solution and rules of meaning and membership. Despite efforts to control policy from the 'Corporate Centre' with an emphasis on shared values, culture and the brand, Bankrecht is anything but a cohesive social arrangement. Let us explain why. The first reason for social disintegration is the Swiss origin of the bank. Switzerland is a small but diverse country. While Swiss bankers have a shared understanding of the importance of the stringent Banking Secrecy laws, there are sharp regional differences. Bankrecht AG has two head offices because Bankrecht X (BX) and Bankrecht Y (BY) had offices in Zurich and Basel respectively. Although both cities are in the German speaking area, Basel is more cosmopolitan because it is located on the Rhine where the borders of Switzerland, Germany and France meet. To a French-speaking Swiss respondent, the two cities speak different dialects of Swiss-German. Basel residents also speak limited French and English. However, he adds,

> "Zurich does not really 'speak' French and they are actually trying to get rid of French as the primary foreign language and replace it by English... Culture is difficult to define... I usually place the Basel-people in a separate category from the other Swiss-Germans (i.e. they happen to vote on the same side as the French-speaking people on various issues). I must point out that **Zurich is in a category of its own and many Swiss-Germans resent the people there as being too snobbish...**"

Regional cultural differences forced the PKI team to create documentation, learning programs and structure helpdesk support in German (North), French (West) and Italian (South) and English. The sharp cultural differences between the two merger partners only aggravated the regional differences. BY, the smaller bank, organised itself on the lines of a dynamic American-style financial institution. This bank had a young board of directors composed of former management consultants, academics and veterans of international expansion. BY never actively tried to change the cultures of the numerous investment banks, derivative houses and asset managers it purchased in the late 1980s in the United States and the UK. On the contrary, old guard Swiss bankers managed BX. In a sharp difference to BY, this bank actively sought to re-model acquisitions on its own image. Observers claim BX 'attempted to conquer the world with Swiss culture.' Unlike BY, that opened branches abroad soon after its creation, BX only ventured abroad after it became Switzerland's largest bank in the 1960s. The banks also had different business structures. BY had autonomous global divisions while BX operated a rigidly controlled hierarchical structure with all decisions emanating from its

Zurich corporate centre. Earlier efforts to merge the two banks reportedly failed because BX refused to abandon its structure in favour of more dynamic arrangements at BY. Observers claim that with problems mounting, BX jumped at the merger to stave off collapse.

The cultural differences hampered PKI institutionalisation because the different meanings assigned to the solution forced the security team to re-emphasise its legitimacy constantly in other business divisions. This is why attempts by the former BX team to force the PKI solution on the new entity failed. We argue that this was because the original PKI and its objective of security conceived at BX, resulted in a conflict of understanding between the two sets of employees. Put differently, the PKI designed to reflect the bureaucratic requirements of BX failed to make sense in the new environment with new meanings. This is why user convenience became a central tenet of the PKI drive. The spin on the PKI objective made good sense to most employees because the merger had doubled user applications and passwords. Since, Bankrecht was not ready to eradicate duplicate applications owing to the politics of the process, users found the cryptocard a helpful support for work. Redefining the PKI objective was the only feasible alternative because the Swiss team lacked the capacity to either modify or contradict the meanings held by employees.

To consolidate the new interest, the security team launched a big educational campaign to fix the rules of meaning and membership attached to the PKI. This was vital for the social integration of the PKI in Switzerland because it cemented its new role as a useful tool. However, the cryptocard is not a critical tool for membership since employees use different cards for physical and network access. Users could leave their cards at home and/or lose them but still access resources because management stopped the security team from enforcing card use. Management intervened because the PKI demanded more sweeping changes to the rules of meaning and membership than what was politically feasible. With its weak control of resources, the security team accepted the outcome to keep the PKI alive. Thus, the PKI failed to achieve wide social integration because of the absence of direct alignment with rules of membership. However, despite the poor fixing in rules of membership, cryptocard usage jumped from 25% to 82% when it became obligatory for internet surfing.

Let us conclude this circuit with a brief comment about the Bankrecht brand. Under the OPP section we saw that progress on a Group-wide PKI came after the rationalisation of brands and enforcement of the 'one firm' approach in 2002. Why then did the security team not use the brand to drive PKI deployment earlier? The answer is that since all power and money went to the divisions after the merger, corporate management lacked the resources to enforce rationalisation. In admitting defeat, management claimed that diversity is strength. Of course, this contradicted the official goal of having an 'integrated business model' or 'one firm' approach that implied a consistent corporate culture across the globe.

System integration

To reiterate, this circuit deals with the material conditions of production and discipline. It also explains the coordination of work practices through a link with facilitative power. We have argued that PKI institutionalisation has been problematic at Bankrecht because the solution has both remained outside work practices and contradicted rules of meaning and membership. The PKI solution failed to attain systemic integration with its original focus on security because employees and management saw it as an impediment to work practices. However, 87% of employees later adopted the PKI when it helped their work by arresting the password nightmare. The security team did not modify the technical features of the PKI, but simply aligned it with the prevailing institutional order.

However, developers refused to use the card because they did not perceive its usefulness. For example, they did not share concerns about proliferating user passwords because their job barred them from using banking applications. In general, the group had different norms, rules and meanings from the rest of the employees and saw the cryptocard as a nuisance. Without shared meanings over the role of the cryptocard, the security team attached the PKI to techniques of production and discipline. The security team used its standing conditions, notably control over IT in Switzerland and shared meanings about secrecy laws, to make cryptocard logon mandatory for internet browsing in February 2002. The developers 'voluntarily' adopted the cryptocard because mandatory certificate-based logon transformed it from a nuisance to an essential gateway to the internet, a vital tool for their work. Although the enrolment of developers only added 5% new users, it was significant because they have the skills to evade most technical controls.

A major reason developers resisted the cryptocard is because they knew it was a tool for surveillance and discipline. According to the Director IT Security, "The bank wants to monitor who is communicating and what they are downloading from the Internet. People intervene if you download things you are not expected to download." An IT support specialist agrees. He reveals Bankrecht Switzerland employees are aware of the internet monitoring but they still use it. The bank does not monitor the information downloaded but keeps a log of website URLs and compiles a monthly tally for each individual. From the information, the IT division selects frequently visited inappropriate websites and blocks them. As spelt out in the internet access policy, the culprits may also face disciplinary action. If employees have many websites blocked in quick succession, senior administrators reprimand them. For example, managers questioned an employee who visited a website of a rival bank about three times a day because they thought he had a stock account with them. Bankrecht forbids stock dealing with rivals. However, he argued the website had clearer charts. Therefore, the conversion of the cryptocard into a disciplinary tool enabled the PKI to achieve systemic integration in Switzerland. The PKI disciplinary features relied on the surveillance of employees through the collection, recording and comparison of data about their internet activities.

Enterprise Directory

If the PKI achieved systemic integration in Switzerland, why was it so difficult to deploy it at Bankrecht Investment and other divisions? The explanation largely lies with the failed attempt to deploy an enterprise directory. At Oilcom, we saw that Active Directory (AD) provides the technological means of control over its physical and social environment. Likewise, in Chapter 6 we saw that a key component of the Bankrecht Switzerland PKI under the "Security Base Services" layer is an LDAP directory. The directory provides the material conditions for controlling the Bankrecht Switzerland environment because it stores PKI credentials and access control data that authenticates the cryptocard. The PKI credentials include the encryption and authentication certificates and private keys. In the event of card loss or an employee leaving the bank, the directory also supports key recovery because it stores a copy of the encryption certificate private key for cloning the certificate. Therefore, the directory helped PKI achieve systemic integration in Switzerland because it upholds the bureaucratic and formalised procedures embedded in the infrastructure. Like AD at Oilcom, this directory offers the Swiss IT team a hierarchical view of the network and a single point for controlling the behaviour of network objects and actions of agencies.

However, the biggest problem with this hierarchical directory structure was that it still assumed the powerful IT division at Bankrecht X that controlled all computer resources in the bank. We saw that the merger disempowered the IT division. Bankrecht Investment rejected the Swiss efforts to create an enterprise wide Active Directory citing technical and political reasons. We believe the technical reasons are political too. For instance, BI complained that since Switzerland designed the directory structure and its support model alone, it would raise administrative strains. This is true because while Active Directory (AD) relies on a logical hierarchy to manage information this conflicted with the divisional Bankrecht structure.

The acceptance of a common AD would have given Bankrecht Switzerland control over the whole infrastructure for the following reasons. In Switzerland, the directory affected organisational power distribution because it gave the security team a better capacity to monitor and control activities of other agencies. BS argued that the goal of the directory was to improve information flows within the bank in support of the 'one firm' philosophy. However, BI rejected the argument insisting that a central directory implied a single body of administration that would increase the dominance of the network by Switzerland.

Bankrecht Switzerland also promised to delegate administrative duties to BI. This idea was a non-starter as well because it still envisaged the discarded institutional logic of Bankrecht X. In this structure, the IT division was a benevolent 'dictator' that rigidly enforced standards and occasionally shared its powers with grateful business divisions. We believe BS attempted to reconstitute this order stealthily using Active Directory, because the Group Policy feature gives administrators power to decide how much authority to delegate. In practice, Bankrecht Switzerland asked BI to surrender control over IT to boost the wider 'corporate interest' of an integrated group. Incidentally, this 'corporate' interest was itself politically constructed because to BS it meant the extension of Swiss caution to a foreign division that they believed was wilfully aping the mistakes of American banks. Conversely, BI saw itself as a bulwark against reactionary tendencies espoused by its Swiss bosses.

BI believed that a Swiss-controlled enterprise directory would disempower it by limiting its influence over the IT infrastructure it funded from its own resources. BI pointed out that its businesses such as equity trading demand a 24*7 IT services yet Switzerland did not have this provision in its support arrangements. Therefore, London would have had to work on Swiss time. BI also claimed that the Swiss could not manage the directory for the entire bank because they had more holidays than the UK.

Under these circumstance the success of the directory relied on either BS inducing or forcing BI to adopt the directory. Compulsion would not work because Switzerland's weakened resource control translated into little causal power. The Swiss IT team lacked inducements because the divisions controlled IT funds. Lastly, BS could not rely on top management because of concerns AD could disrupt work. Therefore, the enterprise directory idea failed owing to BS' limited control of resources, a failure to reshape rules of practice and its interruption of techniques of production. The failure presented a colossal obstacle to PKI institutionalisation because the directory is critical for maintaining user discipline. Even attempts to force a global PKI under the guise of branding are precarious because the CCM scheme does not cater for a common directory. In addition, BI is attempting organisational outflanking with a concerted effort to convince management that the Swiss PKI is both disruptive to work and is more costly than Microsoft PKI. Therefore, without a directory to 'store power' won through branding, the centralised Swiss PKI looks vulnerable.

Outcomes

The PKI solution has tremendously improved security and user convenience in its native Switzerland. The success is owed to the willingness of the security team to redefine its objectives to fit changing organisational meanings. Throughout its life in Switzerland, the PKI has relied on changing legitimations to keep track with concrete social processes. However, whatever the changes, the PKI benefits from the backdrop of shared meanings emanating from the strict Swiss banking secrecy laws. Thus, the PKI not only reflects the Bankrecht AG institutional order but also responds to wider pressures within Switzerland.

Despite over a decade of research and pilot projects, the Swiss PKI has failed to become a Group-wide solution. We show that power and politics explain this failure. The PKI was problematic even in Switzerland until February 2002 because it reflected the institutional order of Bankrecht X that disappeared with the merger. Put differently, the PKI was a packaged solution whose survival relied on being unbundled for the different conditions. Williams (1997) argues that implementation problems for packaged solutions often reflect lack of fit between the social relations in the developer firm, which become embedded in the software, and the actual circumstances of the user (Avgerou 2000, Silverstone and Haddon 1996). Ciborra (2000) also warns that hospitality for systems with panoptic abilities (Zuboff 1988) may turn into hostility because users require circumspection to embed the incongruous systems into work routines.

The conflict with work routines in the new Bankrecht AG has been a critical hurdle to PKI institutionalisation because this stopped top management from actively supporting it. The security team proved ingenious in constantly aligning the PKI solution to changing meanings and membership rules in Switzerland. However, these legitimations emphasised secrecy and offered nothing to foreign divisions that prized availability. Bankrecht Investment, the most vocal division, claimed Switzerland had rigged the PKI and its support model to increase its control over the activities of foreign divisions. Although BI officially rejected the solution with rational total cost of ownership and disruption of work arguments, privately they insist the Swiss PKI is technically inefficient and politically motivated.

PKI as part of Bankrecht life

In early 2002, PKI attained systemic integration at Bankrecht Switzerland when the smart cryptocard became mandatory for internet access. After Berger and Luckmann (1967), we argue that the link of the cryptocard with internet access enabled institutionalisation because it controlled the actions of recalcitrant developers and users by setting predefined patterns of conduct. Consequently, while before certificate-based internet logon became mandatory the PKI was optional, the removal of the password option made the cryptocard an undeniable fact of Bankrecht Switzerland life. The PKI became external to employees and persisted whether they liked it or not because the criticality of the internet to work enabled the security features on the cryptocard to resist attempts to evade them. In brief, the cryptocard graduated from a nuisance to an essential support for work practices that agencies took for granted.

However, the PKI remains highly visible because of frequent problems with cryptocard lockouts that require intervention from the IT support division. In early 2003, BS issued new certificate pairs on the cryptocard for all employees in Switzerland using an Entrust CA to phase out the old proprietary or 'home grown' CA. Originally, the certificates supported certificate-based login to a hundred banking applications. Bankrecht Switzerland also enabled the use of the certificates for encrypting internal e-mail from June 2003. This was after a secure e-mail pilot project involving one hundred users that tested Microsoft Outlook and Entrust plug-ins in July 2002. It uses an authenticating certificate for signing e-mails and an encrypting certificate to decipher. However, PKI institutionalisation is incomplete because about 2.5% of all employees refused to use their cryptocards and hence have remained outside the scope of the system. However, to Bankrecht AG this is a negligible number.

From infrastructure to institution

Certificate-based logon certainly offers Switzerland more security and stability of action than the user passwords and scripts that it replaced. Despite problems with developers, the majority of employees adopted the PKI after an extensive educational exercise. The solution succeeded in Switzerland because BS shrewdly linked it to work processes and structures such as the LDAP directory and smart cryptocards. However, unlike Oilcom, the Bankrecht cryptocard is not ultimate evidence of membership because the use of separate physical and logic access cards has allowed some users to ignore the certificate scheme.

The clash of cultures between Bankrecht X and Y slowed down PKI institutionalisation in Switzerland. However, the problems are even worse abroad. The PKI became divisive after it required a uniform modification of rules, meanings and techniques of production in a distributed organisation. Institutionalisation failed because of dissidence in the ranks of powerful actors that BS had enrolled to support the PKI. BI led the voices questioning the authenticity of BS as spokesperson for an integrated and secure Bankrecht AG. The London division officially baulked at the PKI cost but covertly questioned its political motivation. This organisational outflanking sowed doubt in the minds of top managers and reduced their determination to push the radical social and political change envisaged by the Swiss PKI.

Consequently, the merger caused a fundamental change in the politics, IT support structures and culture of Bankrecht AG. There was an open clash between the meanings embedded in the PKI and the new organisational rules and norms. We argue that the institutionalisation problems are not because the PKI is technically inefficient but because the system lacked support from existing institutional structures. Unlike Oilcom, this became critical because BS lacks the standing conditions to create new support structures for the PKI solution.

CHAPTER 8:
CONCLUSIONS

Introduction

This is our closing chapter and it proceeds as follows. The first section gives an overview of the research. Next, we present our theoretical, methodological and practical contributions. Thereafter we discuss the import of the research approach focusing on design limitations and adequacy of the framework. We conclude with ideas for further research.

Overview of the research

This study began with a general interest in large information infrastructures and their impacts on managerial and decision-making structures of global organisations. Infrastructures reach beyond single events and incorporate other structures, social arrangements and technologies. Thus, their institutionalisation may have political implications in pluralistic organisations. We outline our arguments, motivation and scope of the research in Chapter 1. The chapter takes readers to the subject matter with a 'sneak preview' of the storyline we develop later in the dissertation. We also set the tone for the rest of the dissertation and present debates surrounding PKI and power. We focused on PKI for two reasons. First, PKIs are vital for e-commerce, e-business and e-government security because they support authentication and authorisation in stranger-to-stranger transactions. Second, the real objective of PKIs is to restrict the actions of users and eventually create a stable and secure operational environment. Since "we all hate the constraints of security controls on our freedom of moving about and reading, talking and writing (Parker 1997)," a PKI can potentially cause user disaffection.

Chapter 2 reviews literature on cryptography and its effects on organisational power and responsibility structures. To our chagrin, both cryptography and general IS infrastructure literature is mainly technical in focus. For instance, a focus on interoperation issues dominates PKI literature. The belief is that the main hindrance to PKI interoperation is the lack of technical capacity to connect infrastructures owing to incompatible implementations. However, recent literature on PKI has exposed flaws in this purely technical approach. First, authors warn that cryptography may not live up to the hyped vendor claims because it was originally a communication security tool not a web security solution. Second, encryption algorithms routinely fail because security is a process not a product. Third, critics counsel that since it is difficult mathematically to ensure that individuals properly use their keys, it is vital to focus on procedures. Despite this new realism, the literature still largely attributes the low uptake of PKI to technical factors not organisational problems.

Since a public key infrastructure shapes its context and vice versa, we assess how insights from political and organisational theory can enrich technical security approaches. We start with a review of the literature discussing the role of power and politics in IS adoption. Thereafter, we explore the technical security literature focusing on cryptography. To show how a public key infrastructure becomes a catalyst for organisational power and politics, we use the concepts of infrastructure and institution to link technical security and power.

Chapter 3 presents the theoretical framework. We review the elusive concept of power, how to gain and manage with it. Accepting that there is no single all-embracing concept of power, we explore the relational notions advanced by Law (1991b). These are ‘power to’, ‘power over’, ‘power storage’ and ‘power discretion’. Law observes that power networks are never purely social because they are a product of a fabric that integrates social relations and technical, architectural, textual and natural non-human actors. He believes that the Circuits of Power (CoP) can explain the relationships in this socio-technical network. The CoP offers a central tradition of power that includes different debates and explains well-grounded alternative conceptions. The chapter also briefly considers insights from Structuration Theory on power and legitimation of institutions.

Chapter 4 examines the philosophical aspects of this dissertation and its relationship with the broader IS research traditions. The first part focuses on epistemological assumptions and their impact on how researchers understand the world and communicate this knowledge. Next, we assess the three major IS research epistemologies namely positivist, interpretive and critical. We give reasons for our selection of the interpretive tradition. Thereafter, we briefly discuss the philosophical roots of computer security. The chapter then examines research strategies with a focus on case studies. We give our rationale for selecting this strategy and explore different case study types, designs and controversies. Next, we describe the selection of the study organisations and our research decisions. An examination of data collection techniques follows. We assess the contributions and limitations of the native CoP in data collection. After this review, we introduce three data collection themes. Lastly, we describe our data analysis procedure. Starting from the broad CoP lenses, we apply the iterative data analysis approach entitled *telling-showing-telling.*

Chapters 5 and 6 present the findings from the two case studies. We use our own themes to present the findings. Starting with the business environment theme, Chapter 5 discusses the history and current governance structures of Oilcom. The governance structures link to the social aspects theme. The technology adoption theme starts with a discussion of GID, a mandatory desktop infrastructure. GID is a vital system because it gives the context for the use of PKI and explains its success. Chapter 6 begins with a summary of the two phases of the pioneering PKI efforts at Bankrecht AG. Under business environment, we explore the import of banking secrecy to the profitability and survival of this archetypal Swiss bank. Under social aspects, we explain the cohesive power of the Bankrecht brand. Technology adoption also reflects the omnipotence of banking secrecy laws. The theme traces the two phases of PKI evolution starting 1992. PKI efforts end in disarray in the first phase with the creation of numerous independent divisional Certification Authorities. However, branding intervenes in the second phase to bolster the tottering efforts to create a group-wide PKI.

In Chapter 7, we bring the findings from the two studies together and analyse them with the CoP framework lenses. Using the *telling-showing-telling* characterisation, this chapter *tells* readers what the data in the previous two chapters *showed.* We use the framework to explore the political undercurrents of the two PKI projects based on the theoretical ideas presented in Chapter 3. We discuss each case study separately but, where appropriate, we compare the findings as we go along. Overall, the findings support the arguments outlined at the beginning of the study. We show that since PKIs restrict freedom of action, they affect power and responsibility structures and hence the infrastructure may face institutionalisation hurdles.

The two cases demonstrated that shifting power balances is not only the desired outcome of PKI deployment, the institutionalisation of the infrastructure itself relies on power. As we emphasise later, we believe this socio-technical study offers a useful explanation of the political ramifications of PKIs that should enrich the dominant technical approaches.

Contributions

This section discusses the contributions of our research. There is a close link between the three types of contributions because the Circuits of Power provides both the theoretical foundation for the research and informs our methodological approach. We group the contributions into theoretical, methodological and practical subdivisions.

Theoretical contributions

As stated in Chapter 3, we build on the works of other IS researchers who have used the Circuits of Power (CoP) framework notably (Introna 1997, Silva 1997, Silva and Backhouse 1997). Silva (1997) adapted the framework for IS research from Clegg (1989). However, there are differences between our contributions and previous research. First, we evaluate a pervasive technology that changes work habits and opens up the organisation to the outside world. Second, apart from their scope, PKIs focus on security - a "moving target." Hence, our contribution is two fold. First, we assess the efficacy of the framework in informing and guiding information security studies. We use the two empirical studies to provide a more detailed appraisal of the framework's utility in explaining the relationship between power and institutionalisation. Second, since the CoP links context and process, it helps us challenge the philosophical foundations of security literature.

Starting from the episodic circuit, the study underlined the vitality of mobilising resources and alliances to achieve PKI institutionalisation. While the focus of current PKI research is on creating interoperable infrastructures, we show that the decisive factors are organisational. Findings from both Oilcom and Bankrecht showed that Microsoft PKI was inferior to solutions from vendors like Entrust and Baltimore. For example, security consultants at Oilcom described Microsoft PKI as unsuitable for large e-business applications. However, despite its debatable technical efficacy, Oilcom and Bankrecht Investment (BI) selected Microsoft PKI because its supporters mobilised a strong field of force. BI used a seemingly rational and correct observation that Microsoft PKI was cheaper than Entrust. However, they revealed that they chose the solution because it kept their IT independent of Switzerland. We conclude that as long as powerful interests wish a system to succeed, they will mobilise resources to achieve the outcome irrespective of whether it is technically efficient or not.

We found substantial PKI institutionalisation at Oilcom and partial success at Bankrecht Switzerland. Power and politics influenced both outcomes. At Bankrecht, there was a failure to create a socio-technical network durable enough to support PKI and generate conditions and effects of power. Management vetoed the forced use of the early PKI version because of a fear that onerous security requirements would harm time-sensitive businesses. However, when the security team presented the PKI as a support for user convenience, both managers and employees accepted the solution. Unfortunately, this alliance collapsed after the merger. However, the chances of a centralised PKI recently improved not because of technical reasons but owing to the constitution of a network of alliances to support a re-branding initiative. Overall, success will depend on whether the Zurich-based Wealth Management & Business Banking division can hold the alliances together. At Oilcom, system integration was problematic too at the start. Group Infrastructure (GI) disrupted work practices by increasing network logon times. GI also assigned employees more IT support responsibilities. Hence, system integration was vital for both PKIs because of its link with work practices.

However, the social integration circuit was the most decisive at both organisations. In making the changes, Oilcom built on the existing institutional order notably the use of smart cards and badges. Unlike Bankrecht where employees viewed the cryptocard as an inconvenience, the Oilcom card is proof of membership because it incorporates physical and logical access functions. Of course, the ability of the card to control membership relied on PKI and Active Directory features that belong to the system integration circuit. This was at the individual level. At the organisational level, Oilcom changed norms, challenged the autonomy of operating companies, restructured user groups and made the changes durable using the system integration circuit. The changes in the institutional order ensured that the PKI-supported systemic integration remained stable long enough to achieve episodic outcomes of power. Since the CoP framework considers power to be circulating through the episodic, social integration and system integration circuits, it gives a fuller picture of the impact of power in PKI institutionalisation.

Bankrecht had PKI too but failed to change the social rules and norms for two reasons. First, the merger dismantled the alliance that supported PKI. Second, a bewildering spate of restructuring exercises led to the situation where the business divisions, the power targets, eventually became more powerful than the IT team. Thus, systemic integration enabled by the PKI did not generate conditions for power because without social integration in the new Bankrecht entity, the security infrastructure never made contextual sense.

We saw that the structures of both organisations had features that hampered the exercise of power. Let us focus on Oilcom. The Group is a distributed organisation by tradition with operating companies (OCs) largely autonomous. This structure made it difficult to drive projects from the top. Oilcom also operated on a consensus basis. Under these circumstances, despite the dispositional and facilitative power of the Board and its representatives such as service companies and Excoms, no project proceeded without the consent of the OCs. The PKI drive under GID totally went against these arrangements. Therefore, the redefinition of rules decisively helped PKI institutionalisation.

While the social integration circuit was decisive at both organisations, our findings show the symbiotic nature of the circuits. At Oilcom, systemic integration succeeded because of changes in the institutional order. However, the stability of the new order rests on systemic integration elements notably Active Directory and smart cards. In turn, the social integration circuit ensures that the artefacts make sense in the new context. Bankrecht had problems with its PKI because the solution lacked the support of organisational processes after the merger and hence did not make sense in the new order.

Methodological contributions

There is a close link between our methodological and theoretical contributions because we used the Circuits of Power framework as both theory and methodology. We use the two case studies to assess the efficacy of the framework in guiding research design, data collection and analysis in information security. While we build on the work of Silva (1997), we abandoned his "interviews and data collection guide" to overcome repetitions and tone down ominous language. Instead, we created three themes to cover the business environment, technology adoption and social aspects. The decision was useful because we not only studied a difficult topic of power and politics, we focused on the sensitive area of security with one study based in secrecy-crazed Switzerland. To facilitate replication we include a sample set of questions developed with our themes in the Appendix. The rest of this subsection discusses our methodological contributions.

Hard systems thinking still dominates security approaches despite its declining appeal in information systems design. As the obsessive focus on PKI interoperability issues shows, the approach assumes that IS institutionalisation problems are technical not social or political. As such, security professionals believe that once the technology functions properly, the value-consensus employees will accept it. Shunning this orthodoxy, we use an interpretive approach to examine the role of power and politics in security practice. Our methodology relies on the ideographic view. To reiterate, this approach emphasises letting the subject unfold its nature and characteristics during the study. With this background, we adopted a case study research strategy because of its ability to explain the link between PKI, power and work practices. An explanation of this problematic interaction is vital because PKI only become useful to organisations if embedded in everyday work practices.

We saw that defining work is complex and politically sensitive (Star and Bowker 1995). Therefore, we make a useful methodological contribution to security research by introducing an approach that captures the essentially contested nature of organisational life. Unlike the objective school that seeks general laws, the case study strategy enabled us to evaluate a full variety of evidence and opinions in real life organisational settings. A major flaw of the technical literature is its inability to elicit the different organisational views regarding technology. The few opinions expressed tend to come from interested parties such as senior management, IT security and the external consultants. We show that since one person's infrastructure may be another's barrier it is important to understand the political landscape that supports PKI use. Moreover, due to the rapid change in work practices, decision processes, roles and responsibilities, interviews give a more realistic picture of security problems than static techniques such as checklists.

As such, we show that an emphasis on interoperability has hampered PKI institutionalisation because it focuses on symptoms (interoperation) instead of politics, the real cause of the problems. Social scientists define power as the ability of an individual to make another do something they would otherwise not have done. Security authors have also defined security in power terms. Schneier (1999c) argues that security products are useful "precisely because of what they don't allow to be done." Likewise, Anderson (2001) warns that organisational issues are not just a contributory factor in security failure, they can often be a primary cause.

This dissertation shows that the risk of political conflict is highest in distributed global organisations due to different cultures, objectives and the limits of hierarchical control. For instance, respondents at Oilcom claimed colleagues stole their work. We also found mutual mistrust at Bankrecht with the Zurich head office describing its London-based investment division as reckless. London in turn accused Zurich of relying on reactionary practices that suit defence organisations not banks trying to make money. The problem is that while Switzerland office specialises in wealth management and hence respects the stringent banking secrecy laws, BI prizes availability due to the time-sensitive nature of their securities and exchange businesses.

The rich repertoire of sources we used in the case study strategy enabled us to unravel the conflicts in PKI institutionalisation. The detailed description unearthed the aptly named "Not Invented Here" syndrome from which we get our title. The syndrome combines the mixed interest nature of organisations with the zero-sum character of technical artefacts. Kling (1980) believes organisations rarely accept large solutions because the zero-sum nature of technical artefacts ensures that the inclusion of given features precludes preferences of other stakeholders. Bankrecht Switzerland had trouble exporting its complete PKI solution to other divisions because it was a packaged solution. Oilcom and Bankrecht AG changed the PKI technical features and objectives with varying degrees of success. These insights would have been difficult to unearth if we had restricted ourselves to research tools such as questionnaires and checklists under a sociological positivism school.

Our methodology also showed that the interaction between the underlying PKI standard and power and responsibility structures fans political conflict. The ITU-T X.509 standard, seen as the conventional public key infrastructure (PKIX), is particularly susceptible to politics. First, PKIX superimposes hierarchical and authoritarian structures such as Active Directory onto decentralised organisations. The model is problematic because, as we saw elsewhere, the rapid change in work practices, decision processes, roles and responsibility discourages inflexible technologies. These findings show that unless the security team assembles a powerful alliance of interests, PKIX solutions will be problematic in distributed organisations. Second, PKIX certificate extensions encourage politics. The extensions started with the X.509v3 certificate to counter accusations that PKIX was authoritarian and hierarchical. The goal was to encourage the tailoring of PKIX to organisational processes. However, because of mixed interest and because PKI controls freedom of action, interested parties use the X.509v3 extensions to enshrine their political goals. Powerful actors may use the extensions to determine who uses the keys and for what purpose. For instance, they can also denote their fields of interest critical and totally ignore competing voices. Therefore, politically minded groups can use PKIX extensions to change work and its representation.

Since PKIX offers many options in dynamic business environments, it is difficult to define a framework that enables separate PKI entities to communicate with each other. Indeed, vendor interpretations of the X.509v3 format have accentuated the interoperability problems. A politicised context hurts interoperability because for a PKI to support specific organisational needs it has to embed administrative routines. This is the purpose of the X.509v3 extensions. However, once an organisation customises a PKI to fit its business processes, it differentiates it from other infrastructures. Therefore, interoperability can never be automatic as expected under the ITU-T X.509 standard. Hence, if these large organisations cannot consolidate their internal PKI islands because of politics, it does not matter how many Request for Comment (RFC) documents created, interoperability will remain difficult to achieve.

Data collection insights

As part of the methodological contribution, we provide insights into data collection and research access procedures that would specifically benefit researchers focusing on the role power and politics in information security management. Previous applications of the Circuits of Power framework have largely relied on secondary data. Silva (1997) claimed his use of secondary data is justifiable "when access to original source is difficult to obtain." A more recent study that uses a socio-technical approach (Willison 2002) also uses secondary data. The author insists his approach is appropriate because it overcomes the trouble involved in gaining access for IS research especially "those who focus on security."

However, we decided against secondary literature because it does not fully depict the richness of conducting an empirical study of power. Hence, we navigated the research access minefield by using a "pragmatic, almost opportunistic approach" to getting access (Buchanan *et al.* 1988). We summarise our observations as follows.

Our approach appreciates that realities and constraints of conducting social research always test well-constructed academic views. We took the advice of Buchanan *et al.* (1988). First, we used friends at both organisations to gain access. At Oilcom this was two former LSE students and at Bankrecht AG a columnist of a security publication. Second, we toned down threatening language and removed the repetitions in the questions suggested by Silva (1997), after problems with the first interview. Thereafter we coined a generic title "Organisational and management implications of introducing a PKI." To overcome potential bias, we used both interviews and documentary analysis to triangulate our findings. We also presented views from interviews for the comment of respondents at various levels of the hierarchy. This procedure greatly helped clarify and eradicate biased views.

As the researchers who opted for secondary literature testified, studying power and politics is difficult in any event. The difficulty drastically increased because we focused on the role of power in PKI institutionalisation with one of the studies at a Swiss bank. The approach allowed us to study this novel technology in the few organisations that use it on a large scale.

Practical contributions

Our practical contributions derive from the adoption of the CoP framework to provide theoretical coherence to security work. In Chapter 1, we saw that the “year of …” syndrome dominates security practice. Briefly put, it is a voracious quest for the best technical fix to eradicate security threats. However, since both the products and problems targeted frequently run of fashion, investment in a plethora of gadgets has not increased security. In a seminal insight into security practice, the SANS Institute identified seven management errors that lead to computer security vulnerabilities. Briefly, practitioners reveal a prevalence of reactive, short-term fixes and a failure to understand the relationship between security and business problems (SANS 1999). Likewise, Ross Anderson believes fashion has led companies into spending too much money on the wrong security threats (Heiser 2002).

Through the literature review and empirical data, we showed that security practice lacked the tools to account for the capricious interaction between the at once restrictive and flexible PKIX features, organisational structures and user resistance. Practitioners comfortably discuss aspects of PKIX such as Certification Authorities and directory services. However, there is limited knowledge on how PKI interacts with organisational processes, policies and procedures. In line with the prevalent fire-fighting approach, many practitioners regard security either as an event that happens when an intruder breaks into a computer system or when another worm exploits a known flaw in a common operating system. Security also traditionally enforced a fortress mentality to foil external attackers. As we saw elsewhere, even ‘modern’ tools such as firewalls enforce similar principles. However, the practices are deficient because they focus on specific technologies not the entire security domain. They also ignore the insider threat in pursuit of hackers. However, since “the information security problem is basically a problem of politics and regulation, rather than technology (Heiser 2002),” let us summarise the practical contributions of the CoP framework.

The framework shows security as a process that affects the entire organisational fabric. We saw elsewhere that, like systems rationalism, the PKIX model treats organisations as machines that reliably relay orders to enhance top management control. Conversely, the CoP framework treats organisations as mixed interest social arrangements with technical support. Dhillon and Backhouse (2001) reveal that information security research chiefly explores the formal automated part of an information system. Indeed, computer security traditionally relied on tools such as checklists and risk analysis. However, the tools are static and wrongly assume security is measurable. In contrast, the CoP is dynamic because it intimately follows the interaction of the PKI with concrete social processes throughout its lifecycle. We believe the CoP analysis is more useful in explaining the unpredictable field of information security. The framework directly shows how the effects and conditions of power that a PKI generates circulate through the episodic, social integration and system integration circuits.

Our findings show that despite officially talking about reducing the Total Cost of Ownership (TCO) and increasing information sharing and security, political considerations drove PKI deployment and use. The IT divisions at both organisations saw PKI as a chance to reclaim the powers lost to end users at the advent of the personal computer. This became an all-consuming ambition because the demise of the mainframe computers meant that the IT division at the head office had little control over applications on the end user PC. The low cost of PCs also convinced top management to delegate procurement decisions to the businesses removing the IT division's last vestige of power. From the perspective of Barnes (1986, 1988), the IT departments became mere authorities that lacked discretion since the business divisions controlled the money. The divisions selected the services to use and wilfully customised the IT infrastructure to suit their local needs.

Therefore, despite claiming that the top management call for "free flowing information" at Oilcom and the creation of an integrated bank at Bankrecht was the reason for PKI, reclaiming power topped the agenda of both IT divisions. Hence, PKI reflected the meanings that the IT teams subjectively assigned to events and actions. To convert perceptions into real needs the divisions used a "corresponding canopy of legitimations" to associate the PKIs with concrete social processes. Oilcom was more successful because management made PKI a support for corporate governance. The perceptions became real when the IT team convinced the management committee to link GID with cost control and profitability.

We reviewed the prevalent belief in the value-consensus literature that resistance to the progress of technology is pathological and must be purged (Knights and Murray 1994). However, some of these concerns may be genuine because PKIs affect work practices. Our findings show that the political conflict over PKI benefited both firms. At Bankrecht, the fight slowed the deployment of a PKI whose features, cost and support arrangements could have hampered work at Bankrecht Investment. The Swiss division created the solution under a centralised IT division with assumptions informed by a fear of the stringent banking secrecy laws. However, the PKI became a misfit after the merger because political mayhem wrecked the centralised structure, subsequently empowering foreign divisions that prized availability over confidentiality of information. The conflict forced the Swiss team to focus on password proliferation, which was a real problem. Oilcom also experienced dissidence leading to small operating companies rejecting their representatives on the project team. The discord forced the deployment of a less centralising GI version entitled GI-Lite. If both organisations had simply quashed the resistance, work could have suffered.

While politics hampered PKI at Bankrecht, its masterly was the reason for the success of the infrastructure at Oilcom. If understanding politics improves the success of IT projects, why do researchers on PKI and practitioners ignore it? We believe this is because most people involved with PKI are mathematicians, engineers and computer scientists. Therefore, they routinely produce papers that describe “a mathematical utopia” and often produce “provably secure cryptosystems” that may never work in real life organisations.

Let us now assess the specific contributions of the various elements of the CoP to security practice. From the episodic circuit, the CoP can help practitioners evaluate the power required to accept a security infrastructure. Pfeffer (1992) classifies this as diagnosing the political landscape that involves the following. First, the security team should identify the dominant political subdivisions and their social relationships. Second, establish their views about the new system. Third, establish their standing conditions. Fourth, evaluate how they acquire and exercise power. We saw that Oilcom usually conducted ‘stakeholder analyses’ prior to deploying large IT systems. This assesses the impact of the systems on different groups and evaluates whether they will support or oppose it. Oilcom skipped this analysis for GID because the project had restricted time and financial resources. They also assumed that since the system had the support of the Board, the companies would accept it unconditionally. The failure to assess episodic power led to numerous delays and unanticipated cost overruns. The delays undermined the official line that GID was a cost reduction since the budget increased three fold. Similarly, the Bankrecht Switzerland security team failed to appreciate the changing episodic power configurations and paid with the rejection of the PKI solution.

The system integration circuit is synonymous with facilitative power and deals with the coordination of work practices. However, the link between PKI and work practices causes the following problems. First, PKI automatically becomes a subject of power struggles because as we saw in Chapter 2, representing work is messy and politically sensitive. If a security team captures what it feels are work practices and configures the PKI accordingly some users may feel the technology was not 'invented' for them. Second, since the system integration circuit also deals with disciplinary techniques, new technologies are always contentious. This is especially true with products such as PKI whose cardinal role is to limit freedom of action.

Sociology of translation and security practice

Few social science frameworks link information security and business problems because computer security has roots in objective science. However, since organisations are mixed interest, it is problematic to view security as purely technical. Therefore, we enlisted the CoP framework to provide broad insights into why security tools and techniques are essentially political. While the framework offers a plausible narrative of power in security practice, it is complex and may baffle practitioners. Hence, as efforts continue to simplify the entire framework for practice, we suggest that professionals use the Sociology of Translation ideas incorporated in the Obligatory Passage Points to mobilise support for security projects. Let us assess how the 'moments' of translation can support security practice.

Problematisation is a crucial step in winning support for security projects. First, like air-conditioning the benefits of security are not immediately obvious to the Returns on Investment (ROI) obsessed chief financial officers. Second, the profession has a tarnished reputation because despite years of investment in hyped products, organisations remain insecure. Our findings show that despite the wishful claims of the trade press, security teams have limited dispositional and facilitative power. Hence, security practitioners need political skills to win funding and convince users that security is not a nuisance.

Successful problematisation and *interessement* require the appreciation of what Markus and Pfeffer (1983) term as the organisation's paradigm. The paradigm covers values such as language and symbolic content that shape attitudes and beliefs about the legitimacy and rationality of decisions and actions. Security systems that openly contradict the dominant organisational paradigm face more resistance and risk failure unless supported by power and responsibility structures. The problems are rife because agencies use language and symbols to mobilise political support and quieten opposition. Early GID versions violated Oilcom's paradigm by attacking the autonomy of operating companies. However, PKI succeeded because it relied on the dispositional and facilitative powers of the CMD and Excoms. Hence, symbolic skills are as vital as technical efficiency in institutionalisation.

Practitioners can also derive direct lessons from the *enrolment* 'moment'. This is a vital step for consolidating alliances because it attributes interrelated roles to respective actors. Enrolment is critical for institutionalisation because it involves multilateral negotiations, trials of strength and tricks that ensure the success of interessement. The Zurich team failed to enrol BI because of tactical blunders that gave credence to the latter's misgivings. At Oilcom enrolment succeeded, partly, because the IT division cunningly presented GI-Lite as a compromise to disgruntled local companies. However, this was a trick, because the original GI proposal incorporates GI-Lite features. Therefore, while expertise in security is useful, it is obviously not enough in mixed interest organisations without political skills to accompany.

Lastly, *mobilisation* gives practitioners the skills to establish themselves as the legitimate spokespersons for information security and control its agenda. It has been widely claimed that security is of strategic importance to modern organisations (Parker 1997). However, security remains a maligned bad cousin of the IT department that rarely controls its own destiny. For example, there is no agreement on a common name for security teams. An outcome of the lack of a precise purpose and name is that security can belong to the IT department, infrastructure team, corporate security, risk management, physical security and sometimes even the finance division. In brief, many organisations lack proper responsibility structures for security. This anarchy in security management spurred the development of ISO 17799. The standard shuns the reactive approach and attempts to establish proper security management responsibility. However, ISO 17799 cannot help the security teams if they lack the political skills to portray themselves as the macro-actor that translates the wishes of other actors on security. The Oilcom team succeeded in its mobilisation drive because it translated the wishes of other actors for a profitable and secure firm into a single agenda: Group Infrastructure. However, the Bankrecht team failed to become a legitimate spokesperson because it relied on opportunistic localised agendas that had no organisation-wide resonance.

Research Design Limitations

Our research design anticipated the difficulty of gaining permission to conduct studies on PKI that assessed the role power and politics in its institutionalisation. Hence, we adopted non-threatening language, pre-emptively answered concerns about time and confidentiality and offered a report of our findings. However, this design may pose problems for scholars attempting to produce a similar investigation for the following reasons. Gaining permission would be the first challenge. Obviously, it is difficult to recreate the serendipity that aided our research. Second, researchers would also face the hurdle of convincing respondents to talk about power and politics candidly. This is always problematic because agencies speak from positions of comparative power and vulnerability that researchers may compromise. To conduct a similar study, researchers would require strong rapport and trust with interviewees. Buchanan *et al,* (1988) describe this as "Getting on" and argue it leads to highly personal relationships with the respondents. It involves constant renegotiation of access to the lives and experiences of the individual respondents such that you can get personal and potentially sensitive and embarrassing information (Buchanan *et al.* 1988).

Establishing an understanding with respondents is central to this sort of study because it determines the quantity and quality of data collected. We built this trust by explaining our research agenda and listening carefully to the respondents. Our background in newspaper and magazine journalism probably helped us elicit sensitive views. Clearly, the demands of the approach may handicap researchers with different skills.

The reliance on the trust of respondents poses specific problems. First, while earning trust takes time, it was difficult to spend much time with respondents at both organisations. At Oilcom, we visited the London head office for several hours at a time. We were ushered into a meeting room for the interviews by our gatekeepers and escorted out of the building as soon as they were over. Bankrecht was even worse because the bank allowed us a working day to conduct the bulk of the interviewees in Zurich. Part of the reason for the time pressure was that many respondents were senior managers including a Vice President, Director of IT Security and project leaders. Fortunately, both firms allowed us to record the interviews. We also continued the study off-site via e-mail and documentary analysis.

Furthermore, Buchanan *et al,* (1988) warn that because you have to get on personally with respondents, they may demand censorship rights over the information that you gather. Bankrecht originally offered to participate in our research on condition that we sent the questions to the Director IT Security to consolidate the answers to each. At Oilcom, one vendor threatened us with legal action if we reproduced graphics of their solution that we had obtained during the research.

Respondents may also use the research as an opportunity to spy on other employees and departments. Bryman (1998) warns that researchers may be, "asked about the information they glean from a different 'side' of the organisation." Hence, research in organisations is something of a political minefield. For instance, at Oilcom when we asked a security consultant about the eArchitecture project, his answer was a question, what do you know about eArchitecture? It may not be fair to infer a sinister motive because he may not have known the project details. Alternatively, he may have wanted to know what other people thought about it before committing himself. Hence, researchers should not automatically assume that following our research design would yield similar results.

Adequacy of the Theoretical framework

The presence of multiple paradigms to understand the interrelationships between power, politics and information technology pose problems for researchers (Keen 1981). The paradigms are grounded in political science, management, sociology and marketing (Keen 1981, Saunders *et al.* 2000). The different paradigms have thwarted efforts to create a consistent research body on organisational power and politics. As such, we selected the CoP framework because it includes different views of power. However, like other CoP informed studies, we encountered some problems using the framework. After Silva (1997), we group them into ethical, censorship and time categories.

First, the pre-occupation with achieving specific outcomes (Pfeffer 1992) could lead to managers to ignore ethical concerns such as user satisfaction. This is because such concerns often contradict the management desire to control the IS and extend their power. Our findings show that the PKI affected the work practices at both organisations. However, despite problems of increased workload, reduced flexibility and slow data access speeds, Oilcom managed to institutionalise Microsoft PKI because the IT team constituted an effective field of force. In their desire to extend control over all IT systems across the Group, the Bankrecht Switzerland team was ready to disregard user concerns. However, this effort faltered because of weak social integration.

Still, the sensitive nature of the information that CoP studies requires may put researchers in a position where they may support conduct that disregards ethical issues to retain research access. As part of our pragmatic approach, we promised Bankrecht AG a report of our findings. We believe Bankrecht Switzerland may have used our report for fan internal PKI wrangles. For instance, we witnessed a shift in the thrust of the argument for a central PKI, controlled by BS, from technical expertise to the cost of integrating disparate infrastructures and failure to work as a Group. These were the main observations of our report. This turn of events may have disappointed our sources at BI because they cancelled follow-up interviews.

Furthermore, we believe that in an effort to offer a framework that encompasses different but complementary approaches to power, Clegg may have included too many ideas. The circuit has roots in organisational and political theories. For example, Silva (1997) reveals that the social, system integration and exogenous contingencies link process with context. The ideas from the sociology of translation explain the role of science and technology in structuring power relationships. In our experience, the multifarious views of power make the use of the framework a potentially explosive intellectual effort.

This problem also crops into the methodological application of the framework. In an effort to keep the 'circulating' concept, Clegg ended up repeating and throwing themes across the whole circuit. This causes problems in research that may actually undermine the strength of the circuit, which is an ability to inform studies that generate information of a personal nature. We argued elsewhere that getting useful information depends on 'getting on' with respondents. One way of discouraging respondents is by using an interview schedule with repetitive questions and threatening terms such as power and resource control. Thus, while the 'circulating' idea is nice when the CoP merely gives a metaphysical underpinning for power concepts, the thinking does not translate well into methodological terms.

Suggestions for further research

The Circuits of Power framework ably illuminated the role of power and politics in PKI institutionalisation. Its major contribution lies in giving theoretical coherence to security practice. We saw that the quest for reactive, short-term fixes and a failure to understand the impact of technologies on organisations characterise security practice and research. The result is a huge gulf between technical security research and practice. The CoP framework enabled us to bridge this gap because it explains the relationship between PKI features, organisational structures and work practices. This dissertation is unique because it focuses on the internal impact of PKI as opposed to the external technical interoperation agenda.

From our experience undertaking this research, we would like to outline ideas for further research. First, researchers should explore the development of appropriate vocabulary from the CoP to aid empirical data gathering. Since it is difficult to gain access to conduct research especially when the study involves power and security, researchers currently have two options. Ideally, we should use the CoP elements such as domination and control prominently in research proposals and interview schedules. The obvious danger is that few organisations would grant access to such studies because power is contentious. Alternatively, we could use a less direct approach that relies on generic themes that still add up to the main thesis of the CoP framework. This is the reason why we coined the three themes to guide our data collection. The downside is that this approach may encourage unorthodox applications of the framework. Hence, we encourage research that would systematically assess elements of the CoP to develop 'standardised' language and notational features that would make the framework easier to use in empirical research.

As for practical contributions, we explored the usefulness of the 'moments' of translation in analysing the political landscape of an organisation. Practitioners can directly use the 'moments' to create alliances to support security projects. However, like the mainstream CoP, the sociology of translation ideas, as presented in the daunting obligatory passage points, need unpacking at two levels. Researchers may create easier alternative titles for the terminology of the 'moments'. Second, further research may extract the 'moments' from the broader CoP framework and present it as a mini-framework for analysing and mobilising support for security projects. We may extend this idea to other elements of the framework such that security practitioners select the relevant circuit depending on organisational need. This process may imitate the 'need to know' approach to security.

In conclusion, rather than being a final word, we regard our thesis as an opening remark in what we hope will become a long discussion of the role of power in security practice. Our evaluation of the technical features of PKI should dispel fears that we believe that security is all about power and politics. However, we provide a novel insight by showing PKI as a power tool that expressly restricts organisational action. Obviously, it will be foolhardy to abandon research into technical aspects of cryptography to channel all resources into power and politics because many issues are unresolved. For instance, Blanchette (2000) wonders whether certificates should bind public keys to identities or roles. Even the certification models are still in infancy. Besides, quantum computing may in the intervening decades render today's ciphers such as RSA useless. All that said we believe that the technical side of PKI is reasonably well developed. In brief, what security practice needs is research with an appreciation of how ciphers operate in real life organisations. Our dissertation highlighted the limitations of purely technical approaches to PKI that dominate security research. We show that far from being pathological, power and politics are central to PKI institutionalisation.

Bibliography

Abrahamson, E. (1991) "Managerial fads and fashions: The diffusion and rejection of innovations", *Academy of Management Review,* **16 (3),** pp. 586-612.

Ackoff, R. L. (1967) "Management Misinformation Systems", *Management Science,* **14 (4),** pp. 147-156.

Adams, C. and S. Lloyd (1999) *Understanding Public Key Infrastructure: Concepts, Standards and Deployment considerations,* Macmillan Technical Publishing, Indianapolis, USA.

Adams, D. (2000) "A flexible model for PKI" *Trustis Limited,* London.

AICPA and CICA (2000) "WebTrust program for Certification Authorities" *American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA),* New York.

Alchian, A. A. and H. Demsetz (1972) "Production, Information Costs, and Economic Organization", *American Economic Review,* **62 (5),** pp. 777-795.

Anderson, R. J. (1994) "Why Cryptosystems fail", *Communications of the ACM,* **37 (11),** pp. 32-40.

Anderson, R. J. (2001) *Security Engineering: A guide to building dependable Distributed Systems,* John Wiley & Sons, Inc., New York.

Anderson, R. J. and R. Needham (1995) "Programming Satan's Computer" in *Computer Science Today: Recent Trends and Developments, volume 1000 of Lectures Notes in Computer Science*, (van Leeuwen, J. ed.) Springer, pp. 426-440.

Angell, I. O. (2000) *The new Barbarian Manifesto: How to survive the Information Age,* Kogan Page, London.

Angell, I. O. and S. Smithson (1991) *Information Systems Management: Opportunities and Risks,* Macmillan, London.

Armstrong, C. P. and V. Sambamurthy (1999) "Information Technology Assimilation in firms: The influence of senior leadership and IT infrastructures", *Information Systems Research,* **10 (4),** pp. 304-327.

Austin, T. (2001) *PKI: A Wiley Tech Brief,* Wiley Computer Publishing, New York.

Avgerou, C. (2000) "IT and organisational change: An institutionalist perspective", *Information Technology & People,* **13 (4),** pp. 234-262.

Avgerou, C. (2001) "The significance of context in Information Systems and organizational change", *Information Systems Journal,* **11 (1),** pp. 43-63.

Ba, S. (2001) "Establishing online trust through a community responsibility system", *Decision Support Systems,* **31 (3),** p. 323–336.

Bachrach, P. and M. S. Baratz (1962) "Two Faces of Power", *American Political Science Review,* **56 (3),** pp. 947-952.

Bachrach, P. and M. S. Baratz (1975) "Power and its Two Faces Revisited: A reply to Geoffrey Debnam", *American Political Science Review,* **69 (3),** pp. 900-904.

Backhouse, J. (1997) "Information @ Risk", *Information Strategy,* **3 (1),** pp. 33-35.

Backhouse, J. (1999) "Keynote Speech: The logic of Security and the insecurity of logic. A Social Science agenda for Information Systems Security research". in *Verlässliche Informationssysteme: IT-Sicherheit an der Schelle des neuen Jahrtausends,* Essen, Germany,September 22-24 1999,

Backhouse, J. (2002) "Assessing Certification Authorities: Guarding the Guardians of Secure E-Commerce?" *Journal of Financial Crime,* **9 (3),** pp. 217-226.

Backhouse, J. and G. Dhillon (1996) "Structures of responsibility and security of information systems", *European Journal of Information Systems,* **5 (1),** pp. 2-9.

Baltimore (2000) "An introduction to PKI-based e-security" *Baltimore Technologies Plc,* Basingstoke.

Bannon, L. J. (1995) "The politics of design: Representing work", *Communications of the ACM,* **38 (9),** pp. 66-68.

Barber, R. (2000) "Implementing Public Key Infrastructures in a dynamic business environment", *Computers & Security,* **19 (3),** pp. 230-233.

Barley, S. R. and P. S. Tolbert (1997) "Institutionalization and Structuration: Studying the links between Action and Institution", *Organization Studies,* **18 (1),** pp. 93-117.

Barnes, B. (1986) "On Authority and its relationship to Power" in *Power, Action and Belief: A New Sociology of Knowledge?,* (Law, J. ed.) Routledge & Kegan Paul, London, Boston and Henley, pp. 180-195.

Barnes, B. (1988) *The Nature of Power,* Polity Press, Cambridge.

Baum, M. S. (1994) "Federal Certification Authority liability and policy" *US Department of Commerce, NIST* Gaithersburg, Maryland.

Baum, M. S. (1999) "Technology neutrality and secure Electronic Commerce: Rule making in the Age of "Equivalence"; Exposure Draft Version 1.1" *VeriSign, Inc.,* Mountain View, CA.

Baum, M. S. and W. Ford (1998) "Public Key Infrastructure Interoperation", *Jurimetrics,* **38 (3),** pp. 359-384.

BBC (2002) *Security checks promised for tax site,* BBC News Online Last accessed: 19 August, 2002; Last updated: 12 June, 2002; Address: http://news.bbc.co.uk/1/hi/uk_politics/2041390.stm.

BBC (2002a) *Taxman halts online filing,* BBC News Online Last accessed: 19 August, 2002; Last updated: 30 May, 2002; Address: http://news.bbc.co.uk/1/hi/business/2016945.stm.

Bellovin, S. M. and M. Merritt (1991) "Limitations of the Kerberos Authentication System". in *USENIX Winter '91,* Dallas, Texas, AT & T Bell Laboratories.

Benbasat, I., D. K. Goldstein and M. Mead (1987) "The Case Research Strategy in Studies of Information Systems", *MIS Quarterly,* **11 (3),** pp. 369-386.

Berger, P. L. and T. Luckmann (1967) *The Social Construction of Reality: A Treatise in the Sociology of Knowledge,* Penguin, Harmondsworth.

Bhimani, A. (1996) "Securing the commercial Internet", *Communications of the ACM,* **39 (6),** pp. 29-35.

BIS (2001) "Basel Committee on Banking Supervision: Risk Management Principles for Electronic Banking" *Bank for International Settlements (BIS)* Basel, Switzerland.

Bjørn-Andersen, N. and J. Turner (1998) "The metamorphosis of Oticon" in *Information Technology and Organizational Transformation,* (Galliers, R. D. and W. R. J. Baets eds) Wiley, Chichester.

Blanchette, J.-F. (2000) "Dematerializing French Bureaucracy: (Ethno)graphic tales of cryptology in the field". in *Virtual Society? Get Real! Conference, Virtual Society? 4-5th May 2000,* Ashridge House, Hertfordshire, UK,

Blaze, M., *et al.* (1996) "Minimal key lengths for symmetric ciphers to provide adequate commercial security" *Adhoc Group of Cryptographers and Computer Scientists* Chicago.

Bryman, A. (1988) "Introduction: 'Inside' accounts and Social Research in Organizations" in *Doing Research in Organizations,* (Bryman, A. ed.) Routledge, London.

BSI (1999) *Code of Practice for Information Security Management - BS 7799-1:1999,* British Standards Institute, London.

Buchanan, D., D. Boddy and J. McCalman (1988) "Getting in, Getting on, Getting out and Getting back" in *Doing Research in Organizations*, (Bryman, A. ed.) Routledge, London.

Buchanan, D. A. and D. Boddy (1983) *Organizations in the Computer Age: Technological Imperatives and Strategic Choice,* Gower, Aldershot.

Bulmer, M. (1988) "Some reflections upon research in organizations" in *Doing Research in Organizations*, (Bryman, A. ed.) Routledge, London.

Bumgarner, J. N. (2001) "Hashing out Encryption solutions", *Security Management,* **45 (6),** pp 67-71.

Burrell, G. and G. Morgan (1979) *Sociological Paradigms and Organizational Analysis: Elements of the Sociology of Corporate Life,* Heinemann, London.

Byrd, T. A. and D. E. Turner (2000) "Measuring the flexibility of Information Technology Infrastructure: Exploratory analysis of a concept", *Journal of Management Information Systems,* **17 (1),** pp. 167-208.

Callon, M. (1986) "Some elements of a Sociology of Translation: Domestication of the Scallops and the fishermen of St Brieuc Bay" in *Power, Action and Belief: A New Sociology of Knowledge?*, (Law, J. ed.) Routledge & Kegan Paul, London, Boston and Henley, pp. 196-233.

Callon, M. and B. Latour (1981) "Unscrewing the big Leviathan: How actors macro-structure reality and how Sociologists help them to do so" in *Advances in Social Theory and Methodology: Toward an integration of Micro- and Macro-sociologies,* (Knorr-Cetina, K. and A. V. Cicourel eds) Routledge & Kegan Paul, Boston, pp. 277-303.

Camp, L. J. (1999) "Web Security and Privacy: An American Perspective", *The Information Society,* **15 (4),** pp. 249-256.

Carroll, J. M. and P. A. Swatman (2000) "Structured-case: A methodological framework for building theory in Information Systems research", *European Journal of Information Systems,* **9 (4),** pp. 235-242.

Cavaye, A. L. M. (1996) "Case study research: a multi-faceted research approach for IS", *Information Systems Journal,* **6 (3),** pp. 227-242.

Chadwick, D. W. (2002) "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv3" *PKIX WG, Internet Draft, Issued: 5 January 2002; Expires: 5 July 2002.*

Checkland, P. (1981) *Systems thinking, Systems Practice,* Wiley, Chichester.

Checkland, P. (1989) "Soft Systems Methodology" in *Rational Analysis for a Problematic World: Problem Structuring Methods for Complexity, Uncertainty and Conflict,* (Rosenhead, J. ed.) Wiley, Chichester.

Checkland, P. and J. Scholes (1990) *Soft Systems Methodology in action,* Wiley, Chichester.

Chen, D., A. Perez, S. Sasanus and S. S. Verma (1999) "Encryption: Technical and Policy issues" *University of Colorado* Boulder.

Chokhani, S. and W. Ford (1999) "Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework - RFC 2527" *The Internet Society, Networking Group, Request for Comments (RFC).*

Chua, W. F. (1986) "Radical Developments in Accounting Thought", *The Accounting Review,* **61 (4),** pp. 601-632.

Ciborra, C. (1993) *Teams, Markets, and Systems : Business innovation and Information Technology,* Cambridge University Press, Cambridge [England] ; New York.

Ciborra, C. (2000) "A critical review of the literature on the Management of Corporate Information Infrastructure" in *From Control to Drift: the dynamics of corporate Information Infrastructures,*Oxford University Press, New York, pp. 16-40.

Ciborra, C. and O. Hanseth (2000) "Introduction: From Control to Drift" in *From Control to Drift: the dynamics of corporate Information Infrastructures,* Oxford University Press, New York, pp. 2-11.

Clark, D. (2000) "Encryption Advances to Meet Internet Challenges", *IEEE Computer,* **33 (8),** pp. 20-24.

Clarke, R. (2001) "The fundamental inadequacies of conventional Public Key Infrastructure". in *Proceedings of European Conference on Information Systems (ECIS 2001), 27-29 June 2001,* Slovenia, ECIS.

Clegg, S. and F. Wilson (1991) "Power, technology and flexibility in organizations" in *A Sociology of Monsters: Essays on Power, Technology and Domination,* (Law, J. ed.) Routledge, London and New York, pp. 223-273.

Clegg, S. R. (1989) *Frameworks of Power,* Sage Publications, London.

Clemons, E. K. and L. M. Hitt (2000) "The future of financial services: Transparency, differential pricing and disintermediation" *University of Pennsylvania,, Wharton School,* Philadelphia.

Cohen, F. (1995) "A short history of Cryptography" in *Introductory information protection,* Fred Cohen & Associates, Livermore, California.

Comrie, M. N. (1998) "The role of the financial industry and law enforcement in combating money laundering: A cooperative approach" *Police of Victoria,* Melbourne, Australia.

Coppersmith, D. (2000) "Cryptography", *IBM Journal of Research and Development,* **44 (1/2),** pp. 246-250.

Creswell, J. (1994) *Research design: Qualitative and Quantitative Approaches,* Sage Publications, Thousand Oaks, California.

Crossley, J. (2002) "Schlumberger DeXa.Badge: The Solution for Logical & Physical Security". in *Critical Role of IT in National Defence, 19 September 2002,* The Oberoi, New Delhi, Sun Microsystems Asia South.

CygnaCom (1995) "Federal Public Key Infrastructure (PKI) Technical Specification: Part D - Interoperability profiles" *Federal PKI Technical Working Group (edited by CygnaCom Solutions, Inc.)* McLean, Virginia.

Dahlbom, B. (1997) "The New Informatics", *Scandinavian Journal of Information Systems,* **8 (2),** pp. 29-48.

Dahlbom, B. (2000) "Postface: From Infrastructure to Networking" in *From Control to Drift: the dynamics of corporate Information Infrastructures,* Oxford University Press, New York, pp. 212-226.

Datamonitor (2000) "Datamonitor IMPACT 2000 - A Financial Services report series" *Datamonitor Corporation,* London.

Davis, D. (1996) "Compliance defects in Public Key Cryptography". in *Proceedings of the 6th USENIX Security Symposium,* San Jose, CA, pp. 171-178,

Day, R., J. Daly and C. A. Christiansen (Eds.) (1999) *eSecurity: The essential eBusiness enabler,* International Data Corporation (IDC), Framingham, MA.

Debnam, G. (1975) "Non-decisions and Power: The two Faces of Bachrach and Baratz", *American Political Science Review,* **69 (3),** pp. 889-899.

Debnam, G. (1975a) "Rejoinder to "Comment" by Peter Bachrach and Morton S. Baratz", *American Political Science Review,* **69 (3),** pp. 905-907.

DeSanctis, G. (1993) "Theory and Research: Goals, Priorities, and Approaches", *MIS Quarterly,* **17 (1),** pp. vi-viii.

Dhillon, G. and J. Backhouse (2000) "Information system security management in the New Millennium", *Communications of the ACM,* **43 (7),** pp. 125-128.

Dhillon, G. and J. Backhouse (2001) "Current directions in IS security research: Toward socio-organizational perspectives", *Information Systems Journal,* **11 (2),** p. 30 pages.

Diffie, W. and M. Hellman (1976) "New Directions in Cryptography", *IEEE Transactions on Information Theory,* **IT-22 (6),** pp. 644-654.

DiMaggio, P. J. and W. W. Powell (1991) "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields" in *The New Institutionalism in Organisational Analysis,* (Powell, W. W. and P. J. DiMaggio eds) The University of Chicago Press, Chicago, pp. 63-82.

Dorey, P. (1991) "Security management and Policy" in *Information Security Handbook,* (Caelli, W., D. Longley and M. Shain eds) New York, Stockton Press, pp. 27-73.

Dutton, W. H. and J. N. Danziger (1982) "Computers and politics" in *Computers and politics: High technology in American Local Governments*Columbia University Press, New York, pp. 1-21.

Earl, M. J. and D. F. Feeny (1994) "Is your CIO adding value?" *Sloan Management Review,* **35 (3),** pp. 11-20.

Eisenhardt, K. M. (1989) "Building theories from case study research", *Academy of Management Review,* **14 (4),** pp. 532-550.

El-Ata, A. A., *et al.* (2002) *"Our PKI-Experience": Towards an Enterprise-Wide PKI: Concepts, Architecture and Decision drivers for the CSG-PKI,* Syslogic Press, Birmensdorf, Switzerland.

Ellison, C. and B. Schneier (2000) "Ten risks of PKI: What you're not being told about Public Key Infrastructure", *Computer Security Journal,* **XVI (1),** pp. 1-7.

Ellison, C. M. (1997) "What do you need to know about the person with whom you are doing business?" in *House of Science and Technology Subcommittee: Hearing of 28 October 1997: Signatures in a Digital Age,* Washington, US Congress.

Etzioni, A. (1964) *Complex Organizations : A Sociological Reader,* Holt, Rinehart & Winston, New York ; London.

Fernandes, A. B. (2001) "Risking "trust" in a Public Key Infrastructure: Old techniques of managing risk applied to new technology", *Decision Support Systems,* **31 (3),** pp. 303-322.

Finne, T. (1996) "The information security chain in a company", *Computers & Security,* **15 (4),** pp. 297-316.

Forné, J. and J. C. Castro (1999) "A model to evaluate Certificate Revocation" *Department of Applied Mathematics and Telematics, Universidad Politecnica de Cataluna* Barcelona, Spain.

Forrester (2000) "The UK Internet Survey 2000" *Fletcher Research, a Forrester Research Company* London.

Foucault, M. (1979) *Discipline and Punish: The Birth of the Prison /Michel Foucault; Translated from the French by Alan Sheridan,* Penguin, Harmondsworth.

Foucault, M. (1980) *Power/Knowledge: Selected Interviews and Other Writings 1972-1977/Michel Foucault; edited by Colin Gordon; translated by Colin Gordon, Leo Marshall, John Mepham, Kate Soper,* Prentice Hall, London.

Foucault, M. (1982) "The Subject and Power" in *Michel Foucault: Beyond Structuralism and Hermeneutics / Hubert L. Dreyfus and Paul Rabinow; with an Afterword by Michel Foucault,*Harvester Wheatsheaf, Hemel Hempstead, pp. 208-226.

Foucault, M. (1986) *Foucault: A Critical Reader/David Couzens Hoy, Editor,* Basil Blackwell, Oxford.

Franz, C. R. and D. Robey (1984) "An investigation of user-led System Design: Rational and Political perspectives", *Communications of the ACM,* **27 (12),** pp. 1202 - 1209.

Fratto, M. (2000) *PKI: Struggling for Interoperability,* Network Computing, Last accessed: 12 October 2000, Last updated: 29 May 2000, Address: http://www.networkcomputing.com/1115/1115f2.html.

Galliers, R. D. (1991) "Choosing appropriate Information Systems research approaches: A revised Taxonomy" in *Information Systems Research: Contemporary Approaches and Emergent Traditions*, (Nissen, H. E., H. Klein and R. Hirschheim eds) Elsevier Science Publishers, North-Holland, pp. 327-345.

Galliers, R. D. and F. F. Land (1987) "Choosing appropriate Information Systems research methodologies", *Communications of the ACM,* **30 (11),** pp. 900-902.

Ganesan, R. (1996) "How to use Key Escrow", *Communications of the ACM,* **39 (3),** pp. 32-33.

Gardner, M. (1977) "Mathematical Games: A New Kind of Cipher that Would Take Millions of Years to Break." *Scientific American,* **237 (8),** pp. 120-124.

Garfinkel, S. and G. Spafford (1997) *Web security & Commerce,* O'Reilly UK, Cambridge.

Giddens, A. (1984) *The Constitution of Society: Outline of the Theory of Structuration,* Polity Press, Cambridge.

Gilmore, W. C. (1993) "Money Laundering: The International Aspect", *Money Laundering-Hume Papers on Public Policy,* **1 (2),** p. 1.

Gilmore, W. C. (1999) *The evolution of money laundering countermeasures,* Council of Europe Publishing, Brussels.

Golden-Biddle, K. and K. D. Locke (1997) *Composing Qualitative Research: Crafting Theoretical Points from Qualitative Research,* Sage Publications, Thousand Oaks, California.

Gollmann, D. (2000a) "New paradigms - old paradigms?" *Future Generation Computer Systems,* **16 (4),** pp. 343-349.

Gottschalk, P. (1999) "Strategic information systems planning: The IT strategy implementation matrix", *European Journal of Information Systems,* **8 (2),** pp. 107-118.

Guex, S. (2000) "The origins of the Swiss Banking Secrecy Law and its repercussions for Swiss Federal Policy", *Business History Review,* **74 (2),** pp. 237-266.

Gutmann, P. (1999a) "X.509 Style Guide" *Department of Computer Science, University of Auckland* Auckland.

Gutmann, P. (2002) "PKI: It's not dead, just resting", *IEEE Computer,* **35 (8),** pp. 41-49.

Hammer, M. (1990) "Reengineering work: Don't automate, obliterate", *Harvard Business Review,* **68 (4),** pp. 104-112.

Hammer, M. and J. Champy (1993) *Reengineering the corporation: A manifesto for business revolution,* Nicholas Brealey Publishing Ltd., London.

Hance, O. and S. D. Balz (1996) "Payments via the Internet" in *Business and Law on the Internet,*McGraw Hill, London, pp. 165-176.

Handy, C. (1990) *The Age of Unreason,* Harvard Business School Press, Boston, Massachusetts.

Hanseth, O. (2000) "The Economics of Standards" in *From Control to Drift: the dynamics of corporate Information Infrastructures,*Oxford University Press, New York, pp. 56-70.

Hanseth, O. (2000a) "Infrastructures: From systems to infrastructures" in *Planet Internet,* (Braa, K., C. Sorensen and B. Dahlbom eds) Studentliteratur, Lund, Sweden.

Hanseth, O. and K. Braa (1998) "Technology as Traitor: Emergent SAP Infrastructure in a Global Organization". in *Proceedings of the Nineteenth International Conference on Information Systems,* Helsinki, Finland, pp. 188-196.,

Hanseth, O. and E. Monteiro (1998) "Inscribing behaviour in information infrastructure standards", *Accounting, Management & Information Technologies,* **7 (4),** pp. 183-211.

Hanseth, O., E. Monteiro and M. Hatling (1996) "Developing information infrastructure: The tension between standardisation and flexibility", *Science, Technology and Human Values,* **21 (4),** pp. 407-426.

Heiser, J. (2002) "Is your company spending too much on the wrong threats? Author and crypto maven Ross Anderson takes aim at infosec assumptions". in *Information Security,* 5 (2), pp. 55-56, 58, 60.

Hinds, P. and S. Kiesler (1999) "Communication Across boundaries: Work, Structure, and use of Communication Technologies in a large organization" in *Shaping Organization Form: Communication, Connection, and Community*, (DeSanctis, G. and J. Fulk eds) Sage Publications, Thousand Oaks, California.

Hirschheim, R. and H. K. Klein (1989) "Four Paradigms of Information Systems Development", *Communications of the ACM,* **32 (10),** pp. 1199 - 1216.

Hirschheim, R. and H. K. Klein (1994) "Realizing emancipatory principles in Information Systems Development: The case for ETHICS;" *MIS Quarterly,* **18 (1),** pp. 83-109.

Hitchings, J. (1995) "Deficiencies of the traditional approach to Information Security and the requirements for a new methodology", *Computers & Security,* **14 (5),** pp. 377-383.

Hobbes, T. (1968) *Leviathan; edited with an introduction by C. B. Macpherson,* Penguin Books, Harmondsworth.

Hoffman, T. (2002) "TCO: Flawed but useful", *Computerworld,* **36 (49),** p. 52.

Hofstede, G. (1993) "Cultural constraints in management theories", *Academy of Management Executive,* **7 (1),** pp. 81-94.

Hoy, D. C. (1986) "Power, Repression, Progress: Foucault, Lukes, and the Frankfurt School" in *Foucault: A Critical Reader,*Basil Blackwell, Oxford, pp. 123-147.

Huang, C. S. J. (1997) "Context, content and the process of participation in Information Systems development: A Structuration perspective" *Unpublished PhD Thesis, London School of Economics and Political Science,* London.

Hughes, J. (1998a) "Notary and PKI" *Entegrity Solutions,* London.

Hughes, J. (1998b) "PKIX overview" *Entegrity Solutions,* London.

Hunt, R. (2001) "PKI and Digital Certification Infrastructure". in *Ninth IEEE International Conference on Networks (ICON'01), October 10 - 12, 2001,* Bangkok, Thailand, pp. 234-239, IEEE Computer Society.

Interbrand (2001) "Interbrand Insights: Aligning your Organisation and your Brand for Performance" *Interbrand,* New York.

Introna, L. D. (1997) "Power: The Network of Force Relations" in *Management, information and power: A narrative of the involved manager*, (Angell, I. O. ed.) MacMillan Press Ltd, London.

iT_SEC (2002) "iT-SEC_signon Whitepaper," *iT_SEC iT_Security Ltd,* Zurich, Switzerland.

Ives, B. and G. P. Learmonth (1984) "The information system as a competitive weapon", *Communications of the ACM,* **27 (12),** pp. 1193 - 1201.

Jepperson, R. L. (1991) "Institutions, Institutional Effects, and Institutionalism" in *The New Institutionalism in Organisational Analysis*, (Powell, W. W. and P. J. DiMaggio eds) The University of Chicago Press, Chicago, pp. 143-163.

Jones, M. (1999) "Structuration Theory" in *Rethinking Management Information Systems : An Interdisciplinary Perspective*, (Currie, W. and R. D. Galliers eds) Oxford University Press, Oxford; New York, pp. 103-135.

Jøsang, A., P. M. Møllerud and E. Cheung (2001) "Web Security: The Emperor's new armour". in *Proceedings of European Conference on Information Systems (ECIS 2001), 27-29 June 2001,* Slovenia, ECIS.

Jupiter (2000a) "Electronic Bill Payment and Presentment adoption finally takes hold: 40 million households in 2005" *Jupiter Research, a Jupiter Media Metrix company* New York.

Jupiter (2000e) "WAP, not Web: 95 million browser handsets in 2004, marketers must resist imposing web models on mobile access" *Jupiter Communications Inc.* New York.

Kahn, D. (1996) *The Codebreakers: The comprehensive History of Secret Communication from Ancient Times to the Internet; Revised and Updated,* Scribner, New York.

Karahanna, E., D. W. Straub and N. L. Chervany (1999) "Information Technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs", *MIS Quarterly,* **23 (2),** pp. 183-213.

Keen, P. G. W. (1981) "Information Systems and Organisational Change", *Communications of the ACM,* **24 (1),** pp. 24-33.

Keil, M. (1995) "Pulling the Plug: Software Project Management and the Problem of Project Escalation", *MIS Quarterly,* **19 (4),** pp. 421-447.

Kettinger, W. J. and C. C. Lee (2002) "Understanding the IS-User divide in IT innovation", *Communications of the ACM,* **45 (2),** pp. 79-84.

King, S. (1996) "CASE tools and organizational action", *Information Systems Journal,* **6** pp. 173-194.

Klang, M. (2001) "Who do you trust? Beyond encryption, secure e-business", *Decision Support Systems,* **31 (3),** pp. 293-301.

Klein, H. K. and M. D. Myers (1999) "A set of principles for conducting and evaluating Interpretive field studies in Information Systems", *MIS Quarterly,* **23 (1),** pp. 67-94.

Kling, R. (1980) "Social Analyses of Computing: Theoretical Perspectives in Recent Empirical Research", *ACM Computing Surveys,* **12 (1),** pp. 61-110.

Kling, R. (1990) "Information systems, social transformations, and quality of life". in *Proceedings of the conference on Computers and the quality of life, September 13 - 16, 1990,* Washington, ACM.

Kling, R. and W. H. Dutton (1982) "The computer package, dynamic complexity" in *Computers and politics: High technology in American Local Governments*Columbia University Press, New York.

Kling, R. and S. Iacono (1984) "The control of information systems developments after implementation", *Communications of the ACM,* **27 (12),** pp. 1218 -1226.

Kling, R. and T. Jewett (1994) "The Social Design of Worklife With Computers and Networks: An Open Natural Systems Perspective" in *Advances in Computers,* (Yovits, M. C. ed.) Academic Press, Orlando, Fl., pp. 239-293.

Knights, D. and F. Murray (1994) *Managers Divided: Organisational Politics and Information Technology Management,* John Wiley, Chichester.

Kohl, J. and C. Neuman (1993) "The Kerberos Network Authentication Service (v5) - RFC 1510" *Networking Group, Request for Comments (RFC).*

Kraemer, K. L. and W. H. Dutton (1982) "The automation of bias" in *Computers and politics: High technology in American Local Governments,*Columbia University Press, New York, pp. 170-193.

Landau, S. (2000) "Designing Cryptography for the New Century", *Communications of the ACM,* **43 (5),** pp. 115-120.

Latour, B. (1991) "Technology is society made durable" in *A Sociology of Monsters: Essays on Power, Technology and Domination,* (Law, J. ed.) Routledge, London and New York, pp. 103-131.

Law, J. (1991b) "Power, discretion and strategy" in *A Sociology of Monsters: Essays on Power, Technology and Domination,* (Law, J. ed.) Routledge, London and New York, pp. 165-191.

Layder, D. (1996) "Power, Structure and Agency" in *Anthony Giddens: Critical Assessments,* (Bryant, C. G. A. and D. Jary eds) Routledge, London and New York.

Lee, A. S. (1989) " A Scientific Methodology for MIS Case Studies", *MIS Quarterly,* **13 (1),** pp. 33-50.

Lee, A. S. (1991) "Integrating Positivist and Interpretive Approaches to Organizational Research", *Organization Science,* **2 (4),** pp. 342-365.

Levitt, J. (1999) "In Keys we trust". in *InformationWeek,* 14 June 1999 (pp. 75-76, 80, 82,86.

Lindup, K. (1996) "The role of information security in corporate governance", *Computers & Security,* **15 (6),** pp. 477-485.

Linn, J. (1997) "Generic Security Service Application Program Interface (GSSAPI), Version 2 - RFC 2078" *The Internet Society, Networking Group, Request for Comments (RFC).*

Lowe-Norris, A. G. (2000) *Windows 2000 Active Directory,* O'Reilly & Associates, Inc, Sebastopol, CA.

Lukes, S. (1974) *Power: A Radical View,* Macmillan, London.

Luthans, F. and T. R. V. Davis (1982) "An Idiographic Approach to Organizational Behavior Research: The use of single case Experimental designs and direct measures", *Academy of Management Review,* **7 (3),** pp. 380-391.

Machiavelli, N. (1997) *The Prince,* (trans. Detmold, C. E.) Wordsworth, Hertfordshire, England.

Malone, T. W., J. Yates and R. I. Benjamin (1987) "Electronic Markets and Electronic Hierarchies", *Communications of the ACM,* **30 (6),** pp. 484-497.

Markus, M. L. (1983) "Power, politics and MIS implementation", *Communications of the ACM,* **26 (6),** pp. 430-444.

Markus, M. L. and N. Bjørn-Andersen (1987) "Power over users: Its exercise by system professionals", *Communications of the ACM,* **30 (6),** pp. 498-504.

Markus, M. L. and M. Keil (1994) "If we build it, They will come: Designing Information Systems that people want to use", *Sloan Management Review,* **35 (4),** pp. 11-25.

Markus, M. L. and A. S. Lee (1999) "Special issue on Intensive research in Information Systems: Using Qualitative, Interpretive and Case Methods to study Information Technology - Foreward", *MIS Quarterly,* **23 (1),** pp. 35-38.

Markus, M. L. and J. Pfeffer (1983) "Power and the design and implementation of Accounting and Control systems", *Accounting, Organizations and Society,* **8 (2/3),** pp. 205-218.

Mathiassen, L. and J. Stage (1992) "The Principle of Limited Reduction in Software Design", *Information Technology & People,* **6 (2-3),** pp. 171-185.

McCabe, D., D. Knights and A. Wilkinson (1998) "The politics of IT-enabled restructuring and the restructuring of politics through Total Quality Management", *Accounting Management and Information Technologies,* **8 (2-3),** pp. 107-126.

McLoughlin, I. and M. Harris (1997) "Introduction: Understanding innovation, organizational change and technology" in *Innovation, organizational change and technology,* (McLoughlin, I. and M. Harris eds) International Thomson Business Press, London, pp. 186-206.

Menezes, A., P. van Oorschot and S. Vanstone (1996) *Handbook of Applied Cryptography,* CRC Press, Boca Raton, FL.

Meyer, J. W. and B. Rowan (1991) "Institutionalized Organisations: Formal Structure as Myth and Ceremony" in *The New Institutionalism in Organisational Analysis,* (Powell, W. W. and P. J. DiMaggio eds) The University of Chicago Press, Chicago, pp. 41-62.

Microsoft (1999a) *Microsoft Windows NT Server Smart Card Logon White Paper,* Microsoft Corporation, Last accessed: May 26, 2002; Last updated: June 22, 1999; Address: http://www.microsoft.com/windows2000/docs/sclogonwp.doc.

Microsoft (2000a) *Windows 2000 Security Technical Overview,* Microsoft Corporation, Last accessed: May 26, 2002; Last updated: August 11, 2000; Address: http://www.microsoft.com/windows2000/docs/SecTech.doc.

Microsoft (2001) *PKI enhancements in Windows® XP Professional and Windows® Server 2003,* Microsoft Corporation, Last accessed: May 22, 2003; Last updated: August 24, 2001; Address: http://www.microsoft.com/windowsxp/pro/techinfo/planning/pkiwinxp/PKIEnhancements.doc.

Microsoft (2001a) *Benefits of Active Directory in a Windows 2000 Environment,* Microsoft Corporation, Last accessed: May 22, 2002; Last updated: September 20, 2001; Address: http://www.microsoft.com/windows2000/server/evaluation/business/adwin2k.asp.

Microsoft (2002) *An introduction to the Windows 2000 Public Key Infrastructure,* Microsoft Corporation, Last accessed: April 21, 2002; Last updated: July 15, 1999; Address: http://www.microsoft.com/windows2000/techinfo/howitworks/security/pkiintro.asp.

Microsoft (2002a) *Technical Overview of Security for Microsoft® Windows® Server 2003,* Microsoft Corporation, Last accessed: May 21, 2003; Last updated: July 2002; Address: http://www.microsoft.com/windowsserver2003/docs/SecurityOverview.doc.

Microsoft (2002b) *MS Windows 2000 Public Key Infrastructure,* Microsoft Corporation, Last accessed: April 21, 2002; Last updated: April 21, 2002; Address: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/evaluate/2000pk.asp.

Mingers, J. (2001) "Combining IS Research Methods: Towards a Pluralist Methodology", *Information Systems Research,* **12 (3),** pp. 240-259.

Monteiro, E. and V. Hepsø (1998) "Diffusion of infrastructure: mobilisation and improvisation". in *Proc. IFIP WG 8.2 & 8.6 - Information systems: current issues and future challenges,* Helsinki, IFIP.

Morgan, G. (1997) *Images of Organization,* Sage Publications, Thousand Oaks, California.

Morgan, S. M. (1998) *Money laundering: The United States law and its global influence,* International Finance and Tax Law Unit, London.

Mumford, E. (1985) "Researching People Problems: Some Advice to a Student" in *Research Methods in Information Systems: Proceedings of the IFIP WG 8.2 Colloquim, Manchester Business School,1-3 September 1984,* (Mumford, E., R. Hirschheim, G. Fitzgerald and A. T. Wood-Harper eds) Elsevier Science Publishers, Amsterdam, pp. 315-320.

Myers, M., *et al.* (1999) "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP) - RFC 2560" *The Internet Society, Networking Group, Request for Comments (RFC).*

Nash, A., W. Duane, C. Joseph and D. Brink (2001) *PKI: Implementing and Managing E-security,* Osborne/McGraw-Hill, New York.

Nelson, K. and M. Ghods (1998) "Measuring technology flexibility", *European Journal of Information Systems,* **7 (4),** pp. 232-240.

Neuman, B. C. and T. Ts'o (1994) "Kerberos: An Authentication Service for Computer Networks", *IEEE Communications Magazine,* **32 (9),** pp. 33-38.

Newell, S., J. A. Swan and R. D. Galliers (2000) "A knowledge-focused perspective on the diffusion and adoption of complex information technologies: The BPR example", *Information Systems Journal,* **10 (3),** pp. 239-259.

Newman, D. (2001) "PKI: Build, buy or bust?" *Network World,* **18 (10),** pp. 50, 54.

Nietzsche, F. (1968) "The Will to Power", (Kaufmann, W. ed.) (trans. Kaufmann, W. and R. J. Hollingdale) Vintage Books, New York.

NIST (1997) "Public Key Infrastructure technology" *US Department of Commerce - National Institute of Standards and Technology Administration,* Washington.

Nosworthy, J. D. (2000) "Implementing information security in the 21st Century - Do you have the balancing factors?" *Computers & Security,* **19 (4),** pp. 337-347.

Nutt, P. C., R. W. Backoff and M. F. Hogan (2000) "Managing the paradoxes of strategic change", *Journal of Applied Management Studies,* **9 (1),** pp. 5-31.

Oilcom (1997) "Commercial Use of Cryptography: An Introduction to the use of Encryption to provide confidence in global commerce" *Oilcom Information Services,* London.

Orlikowski, W. J. (1996) "Improvising Organisational Transformation over Time: a Situated Change Perspective", *Information Systems Research,* **7 (1),** pp. 63-92.

Orlikowski, W. J. and J. J. Baroudi (1991) "Studying Information Technology in Organizations: Research Approaches and Assumptions", *Information Systems Research,* **2 (1),** pp. 1-28.

Orlikowski, W. J. and S. Iacono (2001) "Research Commentary: Desperately seeking the "IT" in IT research - A call to Theorizing the IT artifact", *Information Systems Research,* **12 (2),** pp. 121-134.

Ortiz, S. (2000) "Will PKI Become a Key to Online Security?" *IEEE Computer,* **33 (12),** pp. 13-15.

Parker, D. B. (1997) "The strategic value of information security in business", *Computers & Security,* **16 (7),** pp. 572-582.

Pettigrew, A. M. (1990) "Longitudinal Field Research on Change: Theory and Practice", *Organization Science,* **1 (3),** pp. 267-292.

Pfeffer, J. (1992) "Managing with Power" in *Managing with Power: Politics and influence in organizations,*Harvard Business School Press, Boston, Mass.

Piper, F. and S. Murphy (2002) *Cryptography: A very short introduction,* Oxford University Press, New York.

Porter, M. E. and V. E. Millar (1985) "How Information Gives You Competitive Advantage", *Harvard Business Review,* **63 (4),** pp. 149-160.

Pounder, C. (2002) "The emergence of a comprehensive obligation towards computer security", *Computers and Security,* **21 (4),** pp. 328-332.

Pratt, M. K. (2002) "Finding the T in TCO", *Computerworld,* **36 (46),** pp. 48-49.

Price, S. A. (1999) "Understanding contemporary Cryptography and its wider impact upon the general law", *International Review of Law Computers & Technology,* **13 (2),** pp. 95-126.

Puhakainen, P. (2000) "Certification Authority in a X.509 Public Key Infrastructure," *Helsinki University of Technology,* Helsinki.

Radicati, S. (1998) "Public Key Infrastructure security: Products and services," *The Radicati Group Inc.,* Palo Alto, CA.

Ransom, J. S. (1997) *Foucault's Discipline: The Politics of Subjectivity,* Duke University Press, Durham and London.

Ritter, T. (1999) "Cryptography: Is Staying with the Herd Really Best?" *IEEE Computer,* **32 (8),** pp. 94-95.

Rivest, R. L., A. Shamir and L. Adleman (1978) "A method for obtaining Digital Signatures and Public Key Cryptosystems", *Communications of the ACM,* **21 (2),** pp. 120-126.

Rod, T. (2000) "On the relationships of Structuration Theory to interpretive information systems research". in *UKAIS conference 2000,* Cardiff, Wales,

Rogers, E. M. (1983) *Diffusion of Innovations,* Free Press, New York.

Rolland, K. H. and E. Monteiro (2002) "Balancing the Local and the Global in Infrastructural Information Systems", *The Information Society,* **18 (2),** pp. 87-100.

Romm, C. T. and N. Pliskin (1997) "Playing politics with E-mail: A Longitudinal Conflict-based Analysis" in *Information Systems and Qualitative Research: Proceedings of the IFIP TC8 WG 8.2 International Conference on Information Systems and Qualitative Research.*, (Lee, A. S., J. Liebenau and J. I. DeGross eds) Chapman and Hall, London, pp. 365-388.

Romm, C. T., N. Pliskin and W. D. Rifkin (1996) "Diffusion of e-mail: An organisational learning perspective", *Information & Management,* **31 (1),** pp. 37-46.

RSA (Ed.) (1999) *A guide to security technologies: A primer for IT professionals,* RSA Security, Berkshire, United Kingdom.

Russell, D. and G. T. Gangemi Sr (1991) *Computer Security Basics,* O'Reilly & Associates, Sebastopol, CA.

Said, E. W. (1986) "Foucault and the Imagination of Power" in *Foucault: A Critical Reader,*Basil Blackwell, Oxford, pp. 149-155.

Salmela, H. (1993) "Designing Information Systems for Changing Organizations". in *Proceedings of the 1993 Conference on Computer Personnel Research,* St. Louis, Missouri, United States, pp. 243-254, ACM Press.

Salmela, H., A. Lederer and T. Reponen (2000) "Information Systems planning in a turbulent environment", *European Journal of Information Systems,* **9 (1),** pp. 3-15.

SANS (1999) "The 7 Top Management Errors that lead to computer security vulnerabilities". in *SANS99 and Federal Computer Security Conference May 7-14, 1999,* Baltimore, SANS Institute Resources.

Saunders, C. S., *et al.* (2000) "Power and Information Technology: A review using metatriangulation". in *Proceedings of the Twenty First International Conference on Information Systems, December 10 - 13, 2000,* Brisbane, Australia, ICIS.

Sawyer, S. (2000) "Studying Organizational computing Infrastructures: Multi-Method approaches" in *Organizational and Social Perspectives on Information Technology,* (Baskerville, R., J. Stage and J. I. DeGross eds) Kluwer Academic Publishers, Boston, pp. 213-231.

Schneider, I. (2002) "Swiss banks guard privacy - or is it secrecy?" *Bank Systems & Technology,* **39 (5),** p. 10.

Schneier, B. (1996) "Cryptography, security and the future", *Communications of the ACM,* **40 (1),** p. 138.

Schneier, B. (1996a) *Applied Cryptography: Protocols, Algorithms and Source Code in C,* John Wiley & Sons, Inc., New York.

Schneier, B. (1997) "Why cryptography is harder than it looks", *Information Security Bulletin,* **2 (2),** pp. 31-36.

Schneier, B. (1999a) "Cryptography: The importance of not being different", *IEEE Computer,* **32 (3),** pp. 108-109, 112.

Schneier, B. (1999b) "Satan's computer: Why security products fail us". in *ComputerWorld,* 2000 (November 15, 2000), p. 2.

Schneier, B. (2000) *Secrets and lies: Digital security in a networked world,* John Wiley and Sons, London.

Schultz, E. E. (2002) "The gap between cryptography and information security", *Computers and Security,* **21 (8),** pp. 674-676.

Schultze, U. (2000) "A confessional account of an Ethnography about knowledge work", *MIS Quarterly,* **24 (1),** pp. 3-41.

Schwartau, W. (1998) "Time-Based Security explained: Provable security models and formulas for the practitioner and vendor", *Computers & Security,* **17 (8),** pp. 693-714.

Scott, S. V. (2000) "Lived Methodology: A situated discussion of 'Truth and Method' in Interpretive Information Systems research", *LSE Working Paper Series,* **#91.**

Shain, M. (1991) "An overview of security" in *Information Security Handbook*, (Caelli, W., D. Longley and M. Shain eds) Stockton Press, New York.

Shelfer, K. M. and J. D. Procaccino (2002) "Smart Card evolution", *Communications of the ACM,* **45 (7),** pp. 83-88.

Sherif, M. H. (2000) *Protocols for secure Electronic Commerce,* CRC Press, Washington, D.C.

Silva, L. (1997) "Power and politics in the adoption of information systems by organisations: The case of a research centre in Latin America," *Unpublished PhD Thesis, London School of Economics and Political Science,* London.

Silva, L. and J. Backhouse (1997) "Becoming part of the furniture: The Institutionalization of Information Systems" in *Information Systems and Qualitative Research: Proceedings of the IFIP TC8 WG 8.2 International Conference on Information Systems and Qualitative Research*, (Lee, A. S., J. Liebenau and J. I. DeGross eds) Kluwer Academic Publishers, Boston, pp. 389-414.

Silva, L. and J. Backhouse (2003) "The Circuits-of-Power Framework for Studying Power in Institutionalization of Information Systems", *Journal of the Association for Information Systems,* **4 (6),** pp. 294-336.

Silverman, D. (1998) "Qualitative research: meanings or practices?" *Information Systems Journal,* **8 (1),** pp. 3-20.

Silverstone, R. and L. Haddon (1996) "Design and domestication of information and communication technologies: Technical change and everyday life." in *Communication by Design: The politics of information and communication technologies*, (Mansell, R. and R. Silverstone eds) Oxford University Press, Oxford, pp. 44-74.

Singh, S. (1999) *The Code Book: The Secret History of Codes and Code-breaking,* Fourth Estate, London.

Smith, J. H. G. (1996) *Internet Law and Regulation,* FT Law and Tax, London.

Smith, M. (1993) *Commonsense computer security: Your practical guide to information protection,* McGraw-Hill, London.

Smithson, S. (1994) "New Organizational Forms for an Information Rich Society". in *International Conference on Information Technology (ICIT94),* Kuala Lumpur, Malaysia, 9th-12th August.,

Standage, T. (1999) *The Victorian Internet: The remarkable story of the Telegraph and the Nineteenth Century's Online pioneers,* Phoenix, London.

Star, S. L. (1991) "Power, technologies and the phenomenology of conventions: on being allergic to onions" in *A Sociology of Monsters: Essays on Power, Technology and Domination*, (Law, J. ed.) Routledge, London and New York, pp. 26-56.

Star, S. L. and G. C. Bowker (1995) "Work and Infrastructure", *Communications of the ACM,* **38 (9),** p. 41.

Star, S. L. and K. Ruhleder (1994) "Steps towards an ecology of infrastructure: Complex problems in design and access for large-scale collaborative systems". in *Proceedings of the conference on Computer Supported Cooperative Work,* Chapel Hill, United States, pp. 253-264, ACM.

Star, S. L. and K. Ruhleder (1996) "Steps toward an ecology of infrastructure: Design and access for large information spaces", *Information Systems Research,* **7 (1),** pp. 111-134.

Stinchcombe, A. L. (1968) *Constructing Social Theories,* Harcout, Brace & World, Inc., New York.

Studer, M. (1997) "Banking on Secrecy", *Management Today,* **February 1997,** pp. 71-72.

Suchman, L. (1995) "Making Work Visible", *Communications of the ACM,* **38 (9),** pp. 56-64.

Sun (1998) *What's Inside an X.509 Certificate?* Java Software Division - Sun Microsystems Last accessed: 29 September, 2001 Last updated: 20 May, 1998 Address: http://java.sun.com/products/jdk/1.2/docs/guide/security/cert3.html#inside.

Swanson, E. B. and N. C. Ramiller (1997) "The organizing vision in Information Systems Innovation", *Organization Science,* **8 (5),** pp. 458-474.

Tan, Y. H. and W. Thoen (2000) "Formal aspects of a generic Model of Trust in electronic commerce". in *Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS'00),* Maui, Hawaii, IEEE Computer Society Press.

Taylor, F. W. (1911) *The Principles of Scientific Management,* Harper Bros, New York.

Torvinen, V. and K. Jalonen (2000) "Stimulating power games as a part of systems development", *European Journal of Information Systems,* **9 (1),** pp. 16-24.

Townsend, K. (2001) "Should you trust it?" in *ComputerWeekly,* 15 February 2001, p. 3.

Trauth, E. M. and B. O'Connor (1991) "A study of the interaction between Information Technology and Society: An illustration of combined Qualitative research methods", (Nissen, H. E., H. Klein and R. Hirschheim eds) Elsevier Science Publishers, North-Holland, pp. 131-143.

Truex, D. P., R. Baskerville and H. Klein (1999) "Growing systems in emergent organisations", *Communications of the ACM,* **42 (8),** pp. 117-123.

van Krugten, P. and M. Hoogenboom (2000) "B2C security - Be just secure enough", *Computers & Security,* **19 (4),** pp. 348-356.

Venkatraman, N. (1991) "IT-induced Business Reconfiguration" in *The Corporation of the 1990s,* (Scott-Morton, M. S. ed.) Oxford University Press, New York, pp. 122-158.

Wahl, M. (1997) "A summary of the X.500 (96) User Schema for use with LDAPv3 - RFC 2256" *The Internet Society, Networking Group, Request for Comments (RFC).*

Walsham, G. (1993) *Interpreting Information Systems in organisations,* Wiley, Chichester.

Walsham, G. (1995) "Interpretive case studies in IS research: nature and method", *European Journal of Information Systems,* **4 (2),** pp. 74-81.

Walsham, G. (1995a) "The emergence of Interpretivism in IS research", *Information Systems Research,* **6 (4),** pp. 376-394.

Walsham, G. (1997) "Actor-Network Theory and IS Research: Current status and future prospects" in *Information Systems and Qualitative Research: Proceedings of the IFIP TC8 WG 8.2 International Conference on Information Systems and Qualitative Research,* (Lee, A. S., J. Liebenau and J. I. DeGross eds) Chapman and Hall, London.

Weber, M. (1964) "The Three Types of Legitimate Rule" in *Complex Organizations : A Sociological Reader,* (Etzioni, A. ed.) (trans. Gerth, H.) Holt, Rinehart & Winston, New York ; London, pp. 4-14.

Weizenbaum, J. (1984) *Computer power and human reason: From judgement to calculation,* Penguin, Harmondsworth.

Wheatman, V. and J. Pescatore (2001) "The Information Security Hype Cycle: PKI Users Should Give It Time" *Gartner Group,* New York.

Whitley, E. A. and I. Hosein (2001) "Doing Politics around Electronic Commerce: Opposing the Regulation of Investigatory Powers Bill" in *Realigning Research and Practice in Information Systems Development: The Social and Organizational Perspective,* (Russo, N. L., B. Fitzgerald and J. I. DeGross eds) Kluwer Academic Publishers, Boston, pp. 415-438.

Williams, C. and N. Zunic (2000) "Global interoperability for Key Recovery", *Computers & Security,* **19 (1),** pp. 48-55.

Williams, R. (1997) "Universal solutions or local contingencies? Tensions and contradictions in the mutual Shaping of Technology and work organization" in *Innovation,* *organizational change and technology*, (McLoughlin, I. and M. Harris eds) International Thomson Business Press, London, pp. 170-185.

Willison, R. A. (2002) "Opportunities for computer abuse: Assessing a Crime Specific approach in the case of Barings Bank," *Unpublished PhD Thesis, London School of Economics and Political Science,* London.

Wood, C. C. (1996) "Cryptography Plays Central Role in Future Electronic Commerce", *Computer Fraud & Security,* **March 1996 (3),** pp. 9-10.

Wood, C. C. (1997) "Policies alone do not constitute a sufficient awareness effort", *Computer Fraud & Security,* **December 1997 (12),** pp. 14-19.

Wood, C. C. (2000) "Integrated approach includes security", *Security,* **February 2000,** pp. 43-44.

Wrong, D. H. (1995) *Power: Its Forms, Bases, and Uses /with a new introduction by the author,* Transaction Publishers, New Brunswick, N.J.

Xenitellis, S. (2000) *The Open–source PKI Book: A guide to PKIs and Open–source Implementations,* OpenCA Team, Athens, Greece and Boston, MA.

Yates, J. (1989) *Control through communication: The rise of system in American management,* Johns Hopkins University Press, Baltimore, MD.

Yin, R. K. (1993) *Applications of Case Study Research,* Sage Publications, London.

Yin, R. K. (1994) *Case Study Research: Design and methods,* Sage Publications, London.

Zimits, E. C. and C. Montano (1998) "Public Key Infrastructure: Unlocking the Internet's economic potential". in *iStory,* 3 (2), April 1998, p. 27.

Zimmermann, P. R. (1998) "Cryptography for the Internet", *Scientific American,* **279 (4),** pp. 82-87.

Zuboff, S. (1988) *In the Age of the Smart Machine: The future of work and power,* Basic Books, New York.

Zucker, L. G. (1991) "The Role of Institutionalization in Culture Persistence" in *The New Institutionalism in Organisational Analysis,* (Powell, W. W. and P. J. DiMaggio eds) The University of Chicago Press, Chicago, pp. 83-107.

End Matter

Sample questions

THE LSE COMPUTER
SECURITY RESEARCH
CENTRE ■

Research on the use of PKI-enabled security services at Oilcom

Draft Research Questions:

MANAGERIAL

Frederick Wamaia

Computer Security Research Centre,
London School of Economics and Political Science,
Houghton Street, London WC2A 2AE,
E-mail: f.wamala@lse.ac.uk

Issues to discuss

Business environment

- *History of the organisation and its mission*
- *Position in the market*
- *Strategies and tactics used to maintain or improve this market position*
- *Role of technology adoption in the firm's market position*
- *Organisations that influence the adoption of new technology*
- *Procedure for adopting information systems and/or innovations*
- *Technology adoption drivers: legislation; market uncertainty; partners*
- *General expectations from technology adoption e.g. efficiency*

Technology adoption process

- *Rationale for the emergence of the Cryptography [PKI] project*
- *Why was this infrastructure but not another security solution selected?*
- *Which people/groups were behind the introduction of PKI*[28] *services?*
- *What were the main objectives?*
- *Have these objectives been realised?*
- *How did different stakeholders view the introduction of this PKI?*
- *In what terms do they characterise the PKI?*

- *Architecture of the PKI/technical platform*
- *Scope of the PKI: - departmental; organisation-wide; external*
- *What is the PKI mainly used for?*
- *Why were these applications selected?*
- *Do you think the infrastructure offers adequate: Security; evidence; options*

- *How was the PKI introduced? -: Explanations, negotiations or instruction*

- *What were the key stages in the adoption of the PKI?*
- *Were other stakeholders won over by the explanations or coerced into accepting it?*
- *How were the arguments for the adoption of the PKI presented?*
- *Who is directly affected by the PKI?*
- *What are their interests in organisational activity – roles/responsibilities?*
- *Does the PKI enhance these interests?*
- *Who benefits most from the functionality of this system?*

- *Does the PKI impact on work practices?*
- *What about the division of work/responsibilities?*
- *Has it affected the organisational structure?*

[28] In PKI services we include: Single Sign On; secure E-mail; encrypted data streaming; communication between servers and browsers; Virtual Private Networks; secure Credit card transactions

- *What procedural changes in user departments have occurred due to the system?*
- *Have departments adopted their design to suit the new system?*
- *Are the work practices the system pre-supposes acceptable to you?*
- *Any other points of strain between the PKI and the institutional order?*

- *Is PKI usage attached to tenure of office (you either ... or ...?)*
- *How have the strategies and tactics to boost PKI acceptance evolved?*
- *Can you say the PKI is now an accepted component of organisational life?*
- *Any examples of how this is manifested?*

Social aspects of the organisation

- *Departments/divisions of the Oilcom company*
- *Who shapes organisational objectives/mission/strategy?*
- *Different types of people/professionals employed by your company*
- *Material resources, techniques and skills required to perform tasks*
- *How are employees achieving these goals?*
- *Groupings that allow influence over organisational activities*

- *What are the different professional/social groupings in this organisation?*
- *How does one become and remain a member of the groupings you know?*
- *What is the relationship between the PKI and these groups?*
- *How was the adoption of the PKI interpreted?*
- *Whose idea was it to see PKI in that way?*
- *Has the PKI affected the standing of these groups?*
- *How have different groups reacted to it?*

- *Has this security infrastructure been resisted/resented?*
- *Any manifestations of this resistance/resentment?*
- *What are/were the causes of this resistance?*
- *What resources/tactics were employed to resist it?*
- *What has management done about this resistance/resentment?*

- *What are the general mechanisms of control and discipline in your department?*
- *Are there any control and discipline mechanisms embedded in the PKI?*
- *Do you think these mechanisms (if any) affect PKI acceptance?*
- *What other resources are deployed along with the PKI to achieve control?*
- *Are all employees subject to the same regime of control enabled by the PKI?*

Many thanks for your time!

Selected definitions

Certification Authority (CA)
This is an organisation or technical system trusted by one or more users to manage public key certificates throughout their lifecycle. The CA issues, manages and revokes certificates, when necessary. It also creates and manages Certificate Revocation Lists (CRL) for discontinued certificates.

Cipher
Ciphers are also known as algorithms. Ciphers are either a mathematical function or any general system for hiding the meaning of information. Modern cryptography uses keys to eradicate the need for security to rely totally on the secrecy of the algorithm.

Ciphertext
This is a message (*plaintext*) transformed into gibberish using either a symmetric or an asymmetric cryptographic algorithm.

Client-Server architecture
Under this versatile network architecture, user computers (clients) rely on the more powerful computers (servers) for resources such as files, devices and sometimes, processing power. The architecture provides more usability, flexibility and scalability than centralised mainframe computing systems.

Cryptanalysis
Cryptanalysis is widely understood as the ability to practically 'break' a cipher and recover *plaintext* from the c*iphertext* alone. Broadly, it also occurs when a cryptanalyst finds a weakness that proves that a cipher does perform as well as claimed by its manufacturers.

Cryptography
Cryptography is the art and science of keeping messages secure. Cryptography has traditionally been synonymous with secrecy or the science of concealing the meaning of messages.

Cryptology
Cryptology is a branch of Mathematics that covers both cryptography and cryptanalysis. It is generally the science of information secrecy.

Data Encryption Standard (DES)
IBM developed DES in 1976. DES later became the most popular block symmetric cipher. In 2001, the US chose the Rijndael algorithm as the Advanced Encryption Standard (AES) to replace DES.

Encrypt/ encipher
Encryption is the transformation of data into a format that is practically impossible to understand (*ciphertext*) without the recipient having additional information. *Decryption* is the reverse process.

GSS-API
Generic Security Services Application Program Interface (GSS-API) is a standard for implementing cryptographic authentication services. GSS-API allows applications to share user credentials without re-authentication. It supports secret key and public key cryptography.

IETF
The Internet Engineering Task Force is a community concerned with the evolution of the Internet architecture and the smooth operation of the Internet. IETF specifies protocols and related standards.

LDAP

Lightweight Directory Access Protocol (LDAP) is an offshoot of the standard X.500 directory. LDAP is a set of protocols that define access procedures for directory information. The protocol is much simpler and easier to program than the complex X.500 access standard. LDAP also demands fewer network resources than X.500. Microsoft' Active Directory implements LDAP.

Public Key Infrastructure (PKI)

PKI is a *pervasive security substrate* that supports the use of public key cryptography applications. A PKI is combination of hardware, software, roles, policies and procedures that jointly help create, manage, store, distribute and revoke public key certificates.

Registration Authority (RA)

This function provides an interface between subscribers and the CA. The RA uses offline means to perform administrative duties such as confirming the subject's identity, validating their eligibility for a certificate and ensuring that they possess the corresponding private key for the public key requested. The CA issues the certificates.

Relying Party

The term refers to a person, machine or any other end entity that depends on a certificate issued by a CA to a specific organisation and digital signatures verified with the certificate to conduct transactions.

RSA

The most widely used asymmetric algorithm. Ron Rivest, Adi Shamir and Leonard Adleman developed the algorithm in 1977. RSA gets its name from their initials.

Secure Sockets Layer (SSL)

This is an open standard developed by Netscape Corporation. SSL provides data encryption, server authentication, message integrity, and optional client authentication for TCP/IP connections. All major browsers and web servers incorporate SSL meaning that the installation of a certificate instantly turns on their SSL capabilities.

X.500

The standard defines the structuring of global directories. X.500 directories are hierarchical in design with different levels for each category of information for example country, region and city.