Two worlds, one smart card*

An integrated solution for physical access and logical security using PKI on a single smart card

Jaap-Henk Hoepman[1 2], Geert Kleinhuis[1]

[1] TNO Information and Communication Technology
P.O. Box 1416, 9701 BK Groningen, The Netherlands
jaap-henk.hoepman@tno.nl, geert.kleinhuis@tno.nl
[2] Institute for Computing and Information Sciences
Radboud University Nijmegen
P.O. Box 9010, 6500 GL Nijmegen, the Netherlands
jhh@cs.ru.nl

Abstract. We present a use case of the introduction of a large scale Public Key Infrastructure (PKI) environment in an incumbent telecommunications company in The Netherlands. The main characteristics of the case are the integration of an existing physical access facility with a PKI environment for logical security of the company ICT infrastructure. In fact, both are accessed using a single (smart) company card. The purpose was to implement a high level of security, within the practical constraints at hand, and to reach a level of *reduced sign-on* for company employees. This integration poses numerous challenges. In this article we describe how PKI is actually introduced to support authentication, signing and encryption services for its employees.
18.000 personalised smart cards with PKI were issued, controlling access to over 1500 buildings, fitted with in total more than 6000 smart card readers. The smart cards also controlled access to 14.000 personal workstations both desktops and laptops (each fitted with a contact smart card reader), with access to over a 1000 different applications.
Keywords: PKI, Access control, smart card, reduced sign-on.

1 Introduction

To grant their employees access to office buildings and plants, companies these days issue their employees a (smart) card that is both an identity card as well as an electronic key. Usually, this key can be used without any further authentication to enter the premises. Few companies would require their employees to enter a PIN code as well as presenting their card to open a door, for instance. Such a system for access control to physical objects has been known and in use for quite some time. It grants or denies access to office buildings and sectors within such buildings in a convenient and uniform manner.

* Id: pki-geert.tex,v 1.7 2007/04/16 11:56:59 jhh Exp

However, access control to objects in the digital domain (like computing systems, company applications and information) is usually not handled in the same uniform manner. They often have their own access control mechanism. This is a burden on employees. Consider, for example, the multitude of user names and passwords an office worker may have to enter during the course of a single working week.

This difference can be explained partially by the fact that implementing access control for digital objects is considered more difficult than implementing access control for physical objects. It is also caused by the fact that no single system for uniformly handling authentication and access control is in widespread use today. This is true because Kerberos[NT94], and other methods of single sign-on, largely remain academic exercises, even though (a variant of) Kerberos is part of the Microsoft code base.

This paper describes a use case where all employees of a large telecommunications company in the Netherlands were issued with a *single* smart card to obtain access to both physical and digital objects. Security, authentication and access control in the digital domain is based on a Public Key Infrastructure (PKI) (cf. [AL99, RFC 3280, ES00]).

There were three reasons to use a single smart card for access control in the digital as well as the physical domain.

1. There were high security requirements concerning the general handling of digital information, as well as the authentication of the actor in a workflow.
2. The aim was to arrive at a more user-friendly system of *reduced sign-on*.
3. It was desirable to reduce cost through a simpler and unified access control management organisation.

The latter point could only be achieved through a scalable solution that was usable for a large population of workers with varying skills and technical background. This solution is documented in this paper.

The remainder of this paper is structured as follows. We first discuss the issue of how many keys are needed for physical and logical access control. Section 3 describes the functional architecture. Details on the use case are presented in Section 4. The concrete architecture is given after that. We finish with an example of how an employee is entered into the system (section 6) and conclude with user experience, security issues and conclusions.

2 How many keys do we need?

A number of international information security organisations have studied the trend that security increasingly crosses the confines of individual objects, towards a more holistic, integrated, approach. They concluded that the convergence of security within (large) enterprises is rapidly emerging and enterprises need to adapt accordingly [Ham05]. In fact, this convergence may cover all the objects within a value chain, and extends through physical as well as informational goods.

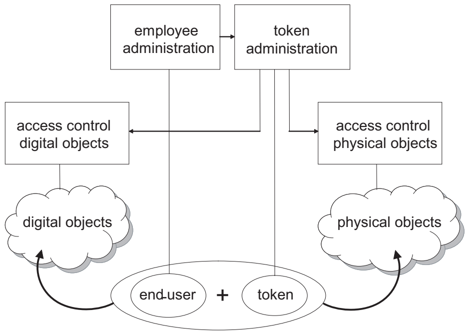

Fig. 1. Our vision on keys

In practise, access control in the physical world is achieved by companies throughout the world using one electronic key. Access to individual doors and entrances is managed by an access control management system, that maintains an access control list (ACL) of all allowed keys for each individual door. Of course, this concept can in principle also be used to manage access to objects in the digital domain. As figure 1 shows, one single token[3] could even suffice to control access to both physical and digital objects. However, there are practical issues that lead us to the conclusion that we need two separate tokens, one for the digital and one for the physical domain (that can, of course, be stored on a single carrier like a smart card).

2.1 Access to physical objects

First of all, there already exists, within the company, a huge nationwide up-to-date installed based for physical access to the company premises. A lot of physical readers are installed nationwide, that would need to be replaced in case of technology change. So for costs reasons a change to this installed base should be avoided.

For physical objects, companies may pose, as an extra requirement, that the handling of an access request is handled very quickly. This way, the number of entry doors in a company can be kept low even when many employees enter at the start of the working day. For this reason, entering a PIN code when entering the building is not an option, as it would be prohibitively expensive in terms of time.

Moreover, access to different sectors within a building are usually protected using locked doors that need to be unlocked separately.

[3] Note that a token refers to a ticket, or access right, not a hardware token. In other words, a token is not the same as a smart card.

2.2 Access to digital objects

For digital objects, usually the access rights for all available objects are determined the moment the user is authenticated by the system. That means, however, that a more thorough access procedure is in order. If the key grants access to a large collection of objects (which is typically the case) then the applications with the most stringent security requirements determine the minimal requirements for this access procedure. A PKI based solution then appears to be an appropriate choice compared with other forms of authentication (like username/password approaches). Once the decision to base the solution on PKI is made, the smart card containing the key can also be used to store other keys for other applications one wishes to distribute to the employee [GK03].

3 Functional architecture

At a high level of abstraction we have distinguished four building blocks in our architecture for access management:

- identity management,
- requesting and managing of assets and access rights,
- provisioning (actually delivering) the assets and the access rights, and
- the actual use of the assets and the access rights by the user.

These four building blocks and their interdependence are depicted in figure 2. In the use case, each of the four building blocks is implemented using one or more specific components, as described in section 5.

The four building blocks in figure 2 have been drawn in their logical process order. Each building block provides information to the audit and control layer. Because business more and more need to prove that rules and regulations were followed within their business processes (think, for example, about the Sarbanes-Oxley legislation), a separate layer addressing policy and auditing issues has been added to the picture. This layer can also support special forms of assigning access rights to business processes (for instance classical function separation, or geographically determined access rights).

Using a common architecture can reduce costs. Becker & Drew [BD05] report on practical experiences with investing in solutions for the building blocks ’requesting and managing assets and access rights’ and ’provisioning’. They conclude that in order to obtain an acceptable return-on-investment (ROI), the number of employees using the building blocks for which the investment was made should be larger than 10.000. Applying the same architecture to 5-10 systems simultaneously will considerably increase the ROI.

4 The use case

The use case concerns a large incumbent telecommunications company in The Netherlands. In this case, more than 18.000 personalised smart cards with PKI

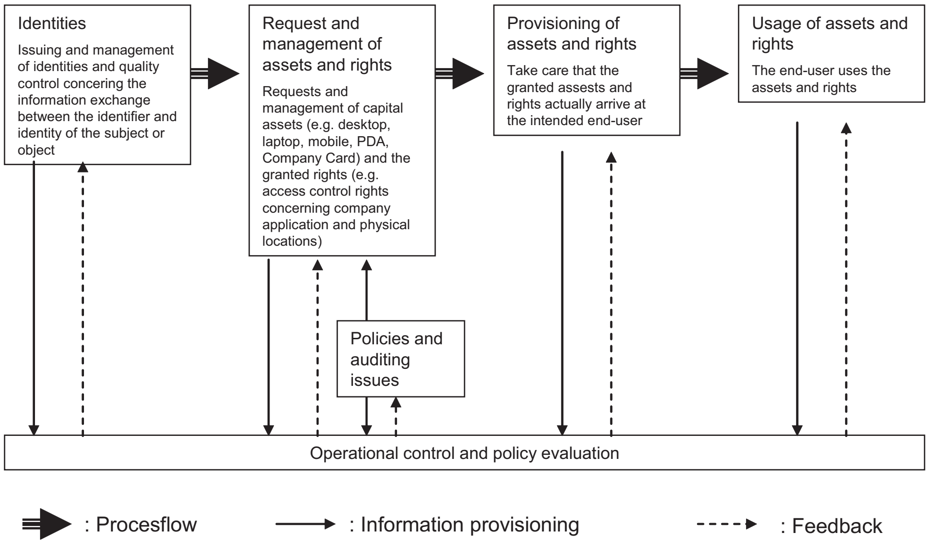

Fig. 2. The four building blocks of the architecture

were issued, controlling access to over 1500 buildings, fitted with in total more than 6000 card readers. The smart cards also controlled access to 14.000 personal workstations both desktops and laptops (each fitted with a contact smart card reader), with access to over a 1000 different applications. These numbers made the case a challenging one.

The smart card used actually contains two chips: a contactless Mifare chip[4] to access physical objects (containing the physical access key), and a contact Philips microcontroller with 32K EEPROM, Triple-DES coprocessor and FameX RSA coprocessor for access to digital objects (containing the PKI keys). The latter chip uses the GlobalPlatform[5] Card Specification v2.1.1. Mifare is an industry standard for contactless communication developed by Philips. It is also subsumed by the newer NFC standards[6]. For the sake of completeness, actually the contact microcontroller contains two PKI key pairs. One key pair is used for authentication (which is also used for digital signatures) and one key pair is used for encryption.

The name of the holder and a passport photo are printed on the smart card. For the sake of completeness the smart card was also fitted with a magnetic stripe to remain fully backwards compatible with the installed base of magstripe readers. The smart card is used to authenticate its holder, to grant access to physical buildings and digital applications and information.

[4] www.mifare.net
[5] www.globalplatform.org
[6] www.nfc-forum.org

Depending on the security level required by the application, authentication is performed through one of the following 3 functions:

1. the smart card with a passport photo that resembles the holder, or
2. the smart card itself (mainly to open physical doors), or
3. the smart card together with the pin code unlocking the embedded PKI controller.

The smart card is personalised in a single phase, in which also the PKI key pairs and certificates are being generated. In the use case it was decided that two separate token mechanisms were needed to meet the different requirements regarding authentication, speed and robustness. By integrating these separate mechanisms on a single smart card the total constellation of access control procedures and mechanisms remain manageable both for employees as well as the managers. Once combined, future applications can choose whichever authentication token they wish to use. In the future a PKI based authentication (involving a PIN) could be used to grant access to highly sensitive areas of a building.

Function 1 is used to bind the card to a physical person.

Function 2 is primarily used to grant access to company buildings. Another application that uses function 2 lies on the boundary of the physical and the digital world. It concerns the selection of printers to which documents in a print queue should be printed. Printers only actually print a job in the queue when the owner of the job presents the smart card to the printer. The owner does not select the printer when issuing the print command, but physically when reaching the actual printer and presenting the card.

Function 3 is primarily used to grant access to the personal account in the digital world. The employee presents the smart card to the desktop computer (or the laptop), and is asked for the PIN code.

Moreover, the smart card can also be used to read encrypted mail and digitally sign mails or e-forms (in a legally binding way [1999/93/EC]).

At the end of 2008, most of the company applications can only be accessed through function 3, meaning that employees are less confronted with a plethora of username and password combinations than before, to achieve a form of *reduced sign-on*.

5 Technical Architecture

We will now discuss the building blocks used in the technical architecture, and and how these building blocks relate to the procedures surrounding identity management. In the use case, the building blocks together implement a full-service 'token management' system: all phases in the life cycle of a smart card are supported (such that the end user does not have to worry about smart card production and data processing), such that they can rely on the quality of the authentication offered by the card. Some of these building blocks are offered commercially as a service component (e.g. the token management application)

The existing ICT infrastructure of the use case was taken as point of departure. This guarantees optimal reuse of existing infrastructure, which results in faster implementation and less cost. The most important element to be integrated is PKI. In the global architecture we distinguish the following building blocks (for ease of presentation not all elements that exist in reality are mentioned). See Figure 5 for details.

- Personnel administration (functional block: 'identities')
  - status employee: processes for job-entry (A-0) and exit.
  - core data for smart card and access control (personnel number, name on card, e-identifier (i.e. email address), state, function, manager, organisation code, etc.)
  - self-service interface for employees and managers (function interface X-1)
- Token Management Application (functional block 'request and management')
  - status smart card: processes for issuing and management
  - core smart card date (card id, state, corresponding employee number)
  - flow control for life-cycle smart card
  - self service and signalling functions for employees and managers
  - back office functions and help desk
  - control and audit functions
- Order application for end-user accounts (function-interface X-3; functional block 'request and management')
  - status end-user accounts and processes for delivery and management
- Management application for authorisations on digital objects (function-interface X-4; functional block 'request and management')
- Management application for authorisations on physical objects (functional interface X-2; functional block: 'request and management')
- Passport photo function for passport photo and identity control (functional block 'issuing')
- Production line for smart cards and mailings (functional block 'issuing')
  - processes for production and control
  - scalable issuing (100-10.000 smart cards a week)
  - core data smart cards and mailings
  - direct mail
  - PKI Certificate Authority (functional block 'issuing')
  - PKI local Registration Authority (functional block 'issuing')

As an example of the type of adjustments needed to the existing situation, and as a prime example of the general design philosophy, consider the process of entering identifying information for a new employee. The new employee first needs to be entered into the personnel administration. All items that need to be put at the disposal of the new employee (smart card, end-user account) can only be issued to the end-user after this registration. The order in which these items are issued cannot be guaranteed by a certain order. The smart card needs to contain the end-user account details of the employee. The logical consequence

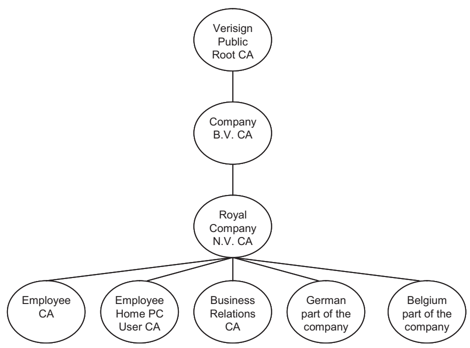

Fig. 3. PKI Hierarchy

of this fact is that the issuing of email address and account details is shifted from the party normally issuing the end-user accounts to the personnel department. This way the smart card (that contains the PKI certificates and email address) can be produced even before the user owns an end-user account and has a working email address. Only after the employee gets access to his account, his reserved email address is activated. A notice is sent to the personnel administration. As a consequence, the email addresses are no longer under the control of the ICT environment (those are now controlled by the personnel administration), but the status of the email addresses (whether they are activated or not) still is under the control of the ICT environment.

5.1 End-user certificates, Certificate Authorities, and PKI Hierarchy

Five different Certificate Authorities (CA's) are available to create end-user certificates. These CA's each cover a different domain and have different policies to issue certificates. The five domains are:

1. Employee CA
2. Employee Home PC User CA
3. Business Relations CA
4. German part of the company
5. Belgium part of the company

At the moment the Employee CA and Business Relation CA are operational. The five CA's are part of a hierarchy. In figure 3 the hierarchy is depicted. The hierarchy is setup this way to possibly create a commercial proposition as well. It is possible to create another 'Company subCA' at the same level as the 'Royal Company N.V. CA'. This can than possibly create its own different subCA's depending on the requirements of that company. Still leaving the 'Company B.V. CA' responsible.

End-user certificates (issued by the Employee CA) and accompanying private keys all reside on a smart card. End-user certificates (issued by the Business

Relations CA) and accompanying private keys all reside on a USB stick. No final decision is made concerning the other three CA's concerning the way end-user certificates and accompanying private keys are issued.

5.2 End-user PKI key generation and certificate creation process

The process of PKI key generation and certificate creation starts with an input file generated by the Token Management Application (TMA), see figure 4. TMA is responsible for the employee information in the certificate. This information is retrieved from the Company employee information database combined with the information that is provided by the photographers. The smart card prepersonalistion and personalisation is outsourced to a dedicated company with a dedicated smart card production line. This company is responsible for the generation of the signing PKI key pair. The public key of the signing key pair and the employee information with regard to the signing related certificate is than sent to a System Integrator in a secure way. The Key Manager process that resides at the System Integrator generates the encryption PKI key pair and stores the encryption key pair in a secure way. Both the public signing key and the public encryption key together with the employee information ending up in the certificate are used by Verisign[7] (the Employee CA, see also figure 3) to create the final end-user certificates. The certificates together with the private encryption key are sent in a highly secure way to the smart card personalisation system. This information is put on the smart card.

6 How a new employee is entered into the system

The flow 'new employee' can globally be determined from the scheme in Figure 5. The flow starts at A-0, were the new employee 'is born' in the system. As soon as the personnel file contains enough data, the applications in the function block 'request and management' (see Figure 2) can be fed with the relevant data. After that, management actions X-1 up to X-4 can be executed independently from smart card production. These management actions comprise requesting an end-user account and setting access rights to buildings, for example. Smart card production is controlled by step B. The smart card production flow is controlled by the token management application (TMA). In step C-1, the new employee receives a letter instructing him to obtain a passport photo from a passport photographer. The employee is free to choose the photographer from a list of photographers offering the service. In step E the token management application receives the passport photo digitally from the photographer, together with control information regarding the identity paper presented by the employee at the photographer. The control information is necessary for securing this part of the smart card issuing process, to prevent issuing smart cards to the wrong people.

[7] www.verisign.com

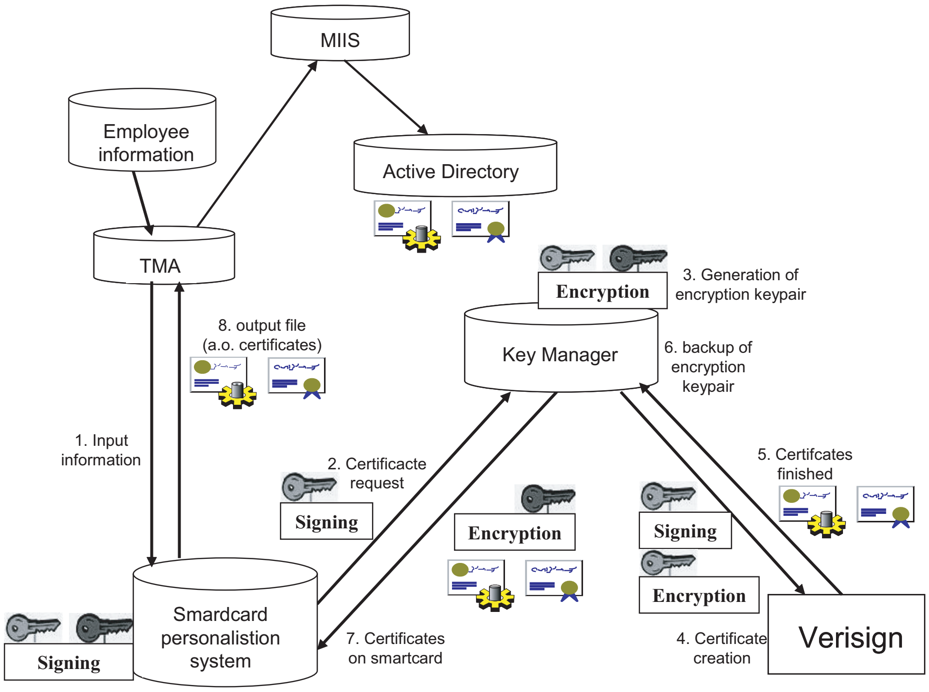

Fig. 4. Card production and key generation

After a quality check the smart card can be produced (step F-1). The card is produced by an external, third, party, see also figure 4. The production process facilitates key recovery for the private decryption key.

The private authentication key (also signing key) never leaves the smart card (and is also not recoverable). This offers a very high level of trust in the authentication provided through messages signed by this key. Public certificates are generated, signed by the PKI Certification Authority and stored on the smart card (steps G-1 through G-4). From that point onwards both PKI key pairs can be used. The card (and independently the PIN and the PUK (recovery PIN)) are sent to the employee. The token management application receives, through H-2, a signal regarding the state of the smart card request. When the card is produced, applications are notified (J-1, J-2). The employee is also sent a separate activation code. Only after activation (I) the functions for (physical) access are available.

The PKI key recovery function for the private decryption key is triggered whenever an encryption certificate is revoked through the token management application. When that happens, the lost key is provided automatically to the end-user environment of the corresponding user, or his/her manager in case the person is no longer employed by the company.

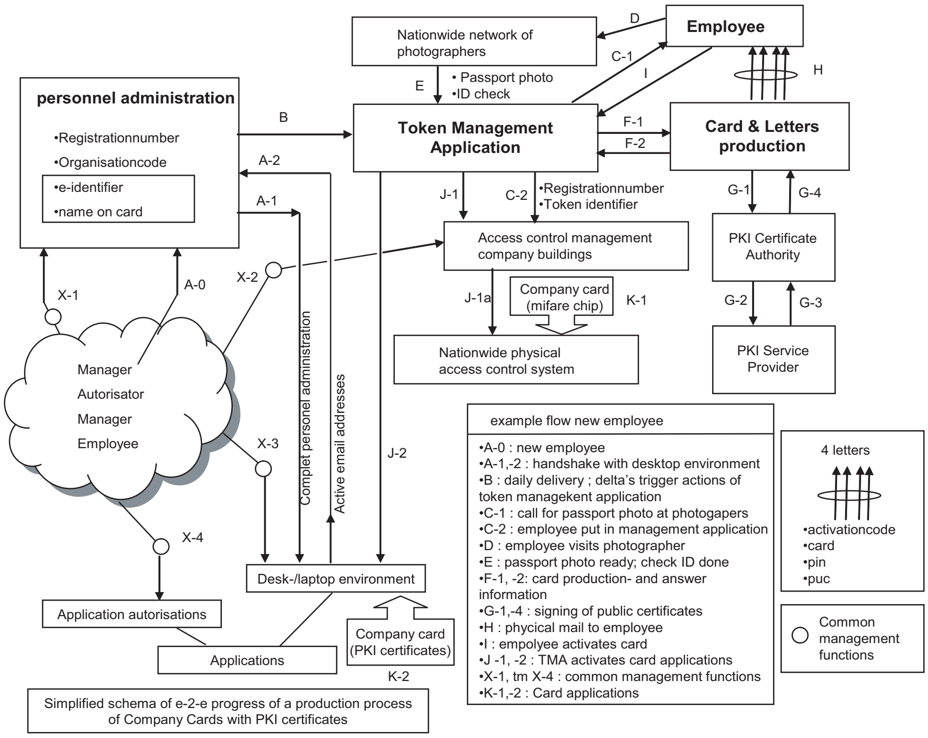

Fig. 5. How a new employee is entered into the system.

The large scale roll out of the smart card took place without any significant problems. Because of the close cooperation between all parties involved, startup problems could be resolved immediately.

7 Conclusions

7.1 Security level

The whole process of issuing smart cards and providing authentication runs at a high security level. Smart card production is performed in a secured facility and data is exchanged through virtual private networks (VPNs). The whole process satisfies the requirements for a Verisign class 3 environment. Because of existing contractual obligations between the telecommunication company and Verisign in the use case Verisign class 2 was chosen.

7.2 User experiences

User satisfaction concerning the operation of access control to the buildings remained positive after introduction of the new smart card. Regarding access control to the digital objects, results are only known for the test environments. They are also positive. A first point of particular interest is the handling of the smart card by end-users. After the complete changeover, there is no longer a need to change passwords every 6 months. We expect a considerable reduction in calls to the help desk because of this. People that (have to) use the secure email functionality will notice a change and a slight increase in the complexity of their tasks (related to the management aspects of secure email). We do not have concrete user experience data for this yet.

7.3 Summary

Using available building blocks and by following the process oriented functional architecture, a production line for a smart card supporting several security mechanisms was implemented in a period of 10 months. The combination of physical and digital access on the same smart card offers increased user convenience. With the large scale introduction of PKI an important component to secure digital objects has become available within the company. The smart card was issued to a total of 18.000 people in a matter of four weeks.

References

[1999/93/EC] Community framework for electronic signatures, 1999. Directive 1999/93/EC.

[AL99] Adams, C., and Lloyd, S. *Understanding Public-Key Infrastructures.* SAMS, 1999.

[BD05] Becker, M., and Drew, M. Overcoming the challenges in deploying user provisioning/identity access management backbone. *BT Technical Journal* **23**, 4 (2005).

[ES00] Ellison, C., and Schneier, B. Ten risks of pki: What you're not being told about public key infrastructure. *Computer Security Journal* **16**, 1 (2000).

[GK03] Gelbord, B., and Kleinhuis, G. On the use of pki in a residential gateway environment. In *ICWI 2003* (2003), pp. 1125–1128.

[Ham05] Hamilton, B. A. Convergence of enterprise security organisations, 2005.

[RFC 3280] IETF. RFC 3280, Internet X.509 public key infrasturcture. Tech. rep., 2002.

[NT94] Neuman, B., and Ts'o, T. Kerberos: an authentication service for computer networks. *IEEE Communications Magazine* **32**, 9 (1994), 33–38.