Real-world Application of Public Key Infrastructures Deployment Methodology

Noel Nazario and Martijn van Oosten

With the rise of transaction-based e-Business, especially in the business-to-business segment, Public Key Infrastructures (PKI) have become one of the fastest growing security solutions. PKIs are complex systems with multiple components, that require policies, and practices which need to be coordinated and integrated into an organisation's business models. The level of effort required for the successful implementation, integration and maintenance of a PKI should not be underestimated. This article discusses a structured PKI implementation methodology and provides a practical example of its application in two case studies.

Introduction

The Internet has become the new frontier for global commerce. Its attractions, easy access and anonymity, are however the very obstacles that stand in the way of its further expansion with e-Business and e-Government applications and services. Internet security is increasingly a critical factor in an organisation's e-Business strategies.

Now that passwords and hardware tokens prove to be insufficient means by which to realise security requirements, PKIs emerge as a suitable security solution for Internet and internal network environments.

In this article, we provide an introduction into PKI and KPMG's international PKI Life Cycle Methodology. This methodology is specially designed to support organisations in their implementation of a PKI. It has been successfully applied by several KPMG clients around the world. In order to provide an example of possible PKI practices and KPMG's approach to PKI implementations, this article describes two successful cases.

The road to PKI

It is relatively easy to find tools with which to eavesdrop on e-mail traffic, impersonate users, intercept passwords or otherwise invade computers that are connected to the Internet. Unsophisticated users thereby pose a significant threat to legitimate users and service providers. Security countermeasures such as the use of PINs/passwords and the Secure Sockets Layer (SSL) have rapidly become the rule rather than the exception, among many Internet operations. Still these measures provide limited protection. Passwords are regularly exposed by their owners for reasons of convenience (e.g. written down on paper where anyone can see them) or intercepted by eavesdroppers (e.g. by looking over a user's shoulder or using a program to intercept passwords when the user logs in). Even though SSL relies on public key (digital) certificates to establish the identity of communicating parties (usually only the web servers) and to protect the confidentiality of data exchanged (e.g. protection of credit card information), the protection provided by SSL exists while the data are transmitted. Once data are delivered to their destination, there is no verifiable record of the place of origination or of any modifications on receipt.

These security threats understandably undermine trust in the Internet as a safe medium for the transfer of services, trade, and payments. Surveys by research organisations such as Gartner and Forrester show that businesses consider the lack of security (and privacy) to be the main obstacle to trade on the Internet. A 1999 e-Business survey that supports this view is provided in figure 1.

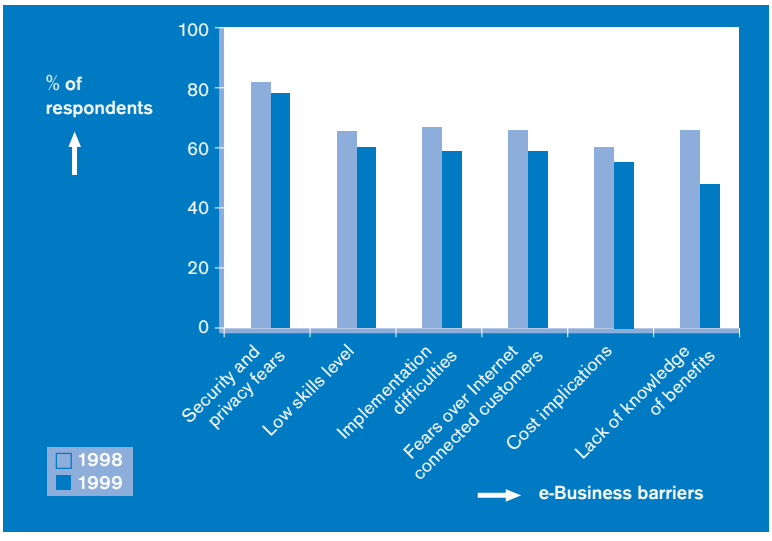

Figure 1. e-Business survey results ([KPMG99]).

Companies that fail to implement proper security measures face risks such as unauthorised disclosure of strategic and private data, theft, a damaged reputation or the loss of the customer's trust. Although the complex implementation of technical and procedural controls for the benefit of risk management create added expenses, these should be considered as regular business costs. Better controls need to be implemented in order to establish the required level of trust for the development of e-Business and e-Government services and applications. Furthermore, these new and improved controls must be integrated into the design and operational policies of the systems supporting such applications and services.

To create this trust, organisations need to address the following issues:

* *Identification and authentication of the communicating parties:* The now famous joke published in the New Yorker Magazine reads 'On the Internet, no one knows you're a dog'. The mechanisms used by Internet communications protocols can be violated using readily available tools and are therefore not reliable with respect to the release of personal and other valuable information. Nor is it possible to show a third party that a certain action can be attributed to a specific party.
* *Confidentiality of data:* The exchange of messages and other data through the Internet takes place primarily through the 'broadcast channel' and is exposed to interception at various points. Applications involving personal information and data of financial or other strategic value require that the privacy of transactions and data be preserved. They must therefore rely on the use of cryptography to avoid accidental interception or leakage, theft, and intentional electronic eavesdropping.
* *Integrity of data:* Although Internet communications protocols include various forms of error recovery, they do not guarantee delivery of data nor can they detect accidental or intentional modification of data. This goes particularly for the application level. Methods such as encryption and the application of digital signatures can help protect information against unauthorised modification by making it impossible to modify the data without being detected.
* *Non-repudiation of messages:* Without a proper tool with which to demonstrably link data to its source, any of the parties involved is able to deny having participated in the process or having the intent to enter into a transaction. The Internet is inherently anonymous and unreliable, its communications protocols cannot by themselves support a form of non-repudiation. There is no simple way to include such a guarantee, though it would clearly contribute to the success of electronic payment services, the electronic despatch of legally binding documents and other business and government transactions.

PKI is an enabling technology that can provide the trust basis for enhanced e-Business services and applications. Specifically, PKI facilitates encrypted communications for confidentiality, data integrity and non-repudiation through digital signatures, as well as

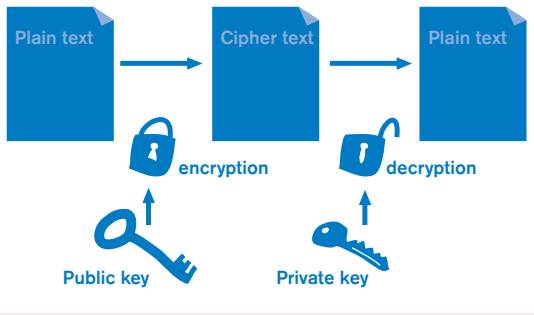

Figure 2. Encryption.

authentication by providing a method with which to verify the link between parties and their public keys. However, PKIs are complex systems with multiple components, that require policies, and practices which need to be coordinated and integrated into the organisation's business models. The level of effort required for the successful implementation, integration and maintenance of a PKI should not be underestimated.

Public Key Infrastructures

A PKI system uses a key pair that consists of one secret key (private key) and one public key. To ensure the confidentiality or access control of a transaction, the sender should encrypt the message and only the receiver should be able to read (decrypt) the message. In other words, to send an addressee a message, the message is encrypted with the addressee's public key and then sent to the addressee. The addressee can use the secret private key to decrypt the message (see figure 2). Because messages can only be decrypted with the private key and the addressee is the only party in possession of it (e.g. on a smart card or stored in the browser), confidentiality and access control can be ensured.

A Public Key Infrastructure is an enabling technology that can provide the trust basis for enhanced e-Business services and applications.

Digital signatures can be used to establish the origin of a message. To 'sign' a message, a hash function is used to produce a unique summary of that message. This summary is then encrypted using the sender's private key. The result, referred to as a digital signature, is then appended to the message. The addressee can confirm both the origin of the message and the integrity of the information therein, by decrypting the digital signature using the originator's public key, and comparing the result with a summary produced by passing the received message through the same mathematical function. This process is visualised in figure 3.

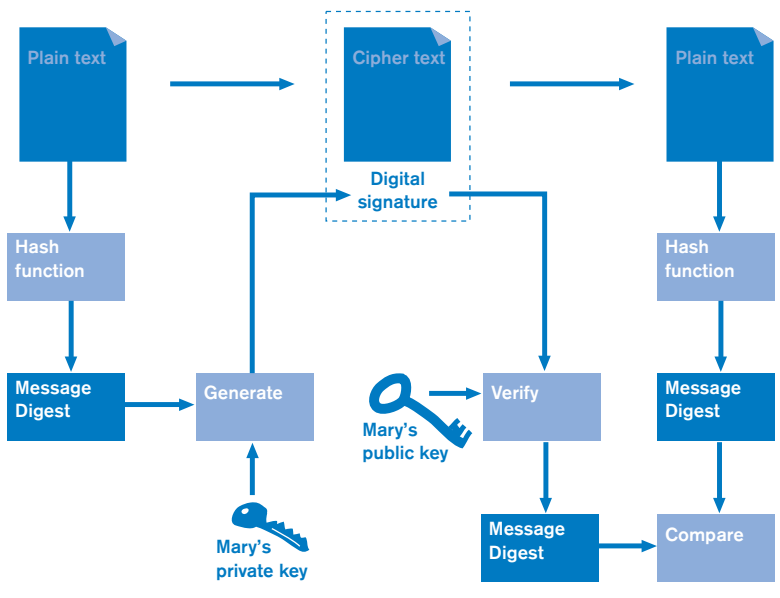

Figure 3. Digital signature.

The use of asymmetric encryption requires that the public key of the asymmetric key pair is linked with the holder of the private key of that key pair. In a PKI, the establishment of such a link is typically assigned to a Registration Authority function.

As figure 4 shows, a PKI consists of at least one Certification Authority (CA), one or more Registration Authorities (RA) and the users of the certificates that are issued. The CA is responsible for the issue and revocation of certificates and for the maintenance of the directory, or repository, that contains the issued certificates and a list identifying the revoked certificates, known as Certificate Revocation List (CRL). The CA guarantees that the public key contained in the certificate belongs to the party named in the certificate. The digital signature placed on the public key certificate by the CA binds the public key, and name of the key pair owner with other information, such as a validity period. To determine whether the certificate was issued by a legitimate CA, the party in question must verify the issuing CA's signature on the certificate. The RA is responsible for the identification, authentication and registration of users, but does not sign or issue certificates. In a geographically distributed environment RAs can be useful in creating scalable implementations that allow organisations to distribute functionality across the network.

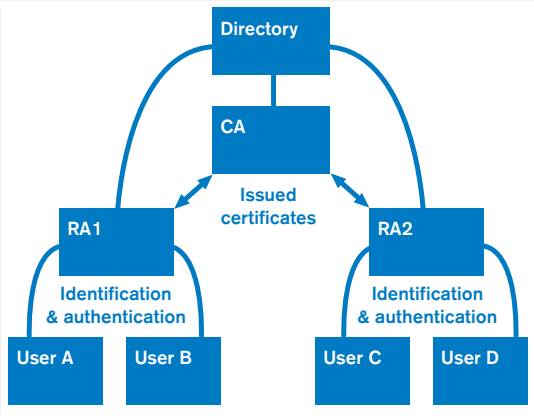

Figure 4. PKI components.

PKI implementation

As noted in the introduction of this article, it is often a complex task to design and maintain a PKI that fits the organisation's needs. Organisations tend to think of PKI implementation as a technical issue, while our experience shows that approximately 60% of implementation time is spent on business, legal and procedural issues. When an organisation intends to use a PKI, it has to decide whether to insource or outsource the PKI and which PKI solution to adopt. The design of the PKI raises the following issues:

- *Technical issues*. The technology often brings with it a host of unresolved uncertainties. Companies encounter problems when trying to implement PKI with regard to applications that were once password-protected. Additionally, difficulties regularly arise when an attempt is made to utilise digital signatures in existing and in new applications. Furthermore, scaling a PKI can be a challenging task.
- *Organisational issues*. The implementation of a PKI requires the design of new business processes (e.g. key management process and certificate life cycle management) and the establishment of an organisation that manages the PKI (e.g. the RA function). Change management and problem management procedures for the PKI environment must be adequately defined. Furthermore, the continuity of the PKI services must be guaranteed in order to meet availability requirements.
- *Legal issues*. The use of a PKI involves a number of legal issues, for example the legal status of digital signatures, laws concerning the use of encryption, privacy legislation and liabilities of the parties involved.
- *Policy issues*. The certificates that are issued within a PKI can be used for different purposes. An organisation that deploys a PKI must define in a document called a Certificate Policy (CP) for which purposes different types of certificates can be used. Another important document is the Certificate Practice Statement (CPS) which describes the policies and procedures for the management of certificates and provides a blueprint of the CA's reliability. The drafting of these documents often takes considerable time. Furthermore, these policies must me managed adequately. Generally, if the PKI domain includes multiple CAs, a separate unit called the Policy Approval Authority is responsible for setting standards for policies and the approval and assessment of the policies of the CAs involved.
- *Security issues*. The protection of the PKI domain requires special attention. Adequate physical and access controls, the allocation of duties, sufficient security monitoring and protection are crucial. Security is an aspect that cannot be underestimated. According to Gartner [Pesc99], by 2002, 80 percent of businesses using a PKI to support e-Business applications will

experience attacks from hackers against the PKI components (0.7 probability). Recovery after each successful attack will cost USD 200,000 or more (0.8 probability).

The considerable number of issues that an organisation has to deal with when planning to implement a PKI, requires a structured and well-considered approach. To meet the needs of clients faced with these issues, KPMG has developed an international methodology to help clients in the end-to-end implementation of a PKI: the PKI Life Cycle Methodology.

PKI Life Cycle Methodology

The KPMG PKI Life Cycle Methodology provides a standard framework for the provision of the PKI services. As illustrated by figure 5, the methodology consists of four phases: Focus/Analysis, Design, Implementation, and Management & Operations. These phases focus on the activities that underlie PKI implementation/integration.

The phases and activities are defined in such a way that a subset of phases and activities can be implemented as part of a particular project or a larger effort (e.g. an Enterprise Security Architecture or e-Business programme where a PKI is just one component of the overall electronic commerce strategy). Furthermore, a subset of phases and activities can be completed using an incremental provision approach. Various activities in each of these phases can overlap or can be performed simultaneously. For example, a Certificate Policy (CP) may be drafted in an earlier stage than the Methodology allows for, in order to serve as a vehicle for the analysis of requirements and the registration of workshop results. Consequently, there may be some overlap between the phases.

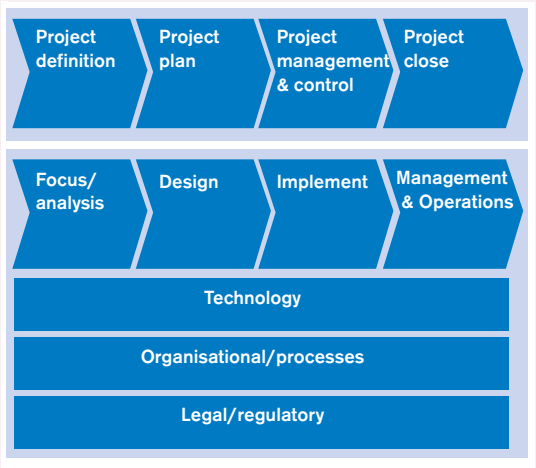

Figure 5. KPMG's PKI Life Cycle Methodology.

As demonstrated in figure 5, the PKI Life Cycle Methodology consists of the three aspects of PKI: Technology, Organisational/Processes, and Legal/Regulatory (including policy). These 'work streams' can be considered as underlying themes to which the various activities in each phase relate. Table 1 (page 44) provides an overview of the objective of each phase and the major deliverables concerned.

The Life Cycle Methodology consists of a sequence of activities yielding specific deliverables. This sequence follows a logical progression that begins with an assessment of the existing business environment, moves on to the design of their infrastructure and then proceeds with the implementation, documentation and maintenance of the infrastructure. The latter concerns a continuous process that allows the PKI to provide adequate service without interruption and makes sure it is operated in the correct way. In practice, this sequence is frequently adapted to the specific needs, capacities and limits of the organisation.

Case study #1: my-ePayments.com

my-ePayments.com has implemented a PKI to support its Internet payment service. KPMG's PKI Team applied a customised approach to the Life Cycle Methodology to help my-ePayments implement its PKI. Prior to the application of the Methodology, my-ePayments.com had selected a service provider to set up and operate their PKI, provide customer support and registration services, and integrate other (non-PKI-related) processing. my-ePayments had also selected the desired CA product and the support platform.

The PKI team's role was first to make an assessment of the technology at hand and of the intended design as well as the limits to the design as imposed by the selection of technology and contractual agreements. Then to examine risks, develop a control framework and draft policies and practices for the implementation and operation of the client's PKI. During the process, the PKI team developed a strong relationship with the client, offered advice, warned of pitfalls and became a trusted advisor. my-ePayments' initial strategy failed to satisfactorily address many issues that are crucial to the effective implementation and management of a critical PKI. Furthermore, lack of understanding of some of these issues resulted in poorly crafted agreements with service providers and subcontractors.

On the basis of these conditions, the following approach was developed:

1. to assess the existing environment and develop a PKI Conceptual Model;
2. to develop Certificate Policies;
3. to develop a Certification Practices Statement;
4. to develop a PKI Business Security Controls Framework.

The Life Cycle Methodology calls for the development of the PKI Business Security Controls Framework (BSCF) after the Conceptual Model has been completed and accepted by the client organisation. Typically, most of the main decisions and difficult

Phase	Objective	Major deliverables		
Focus/analysis	The objective is to gain an understanding of the business strategy, define the business goals and/or requirements for a PKI, assess the current infra-structure to identify issues, determine the level of readiness for PKI implementation, and develop a business rationale. A formal trust model needs to be established.	* **Business Justification Document** – Defines the justification for a PKI in business terms, and where appropriate in financial terms. This may include development of a business case and financial model(s) for the PKI. * **Quick Scan Report** – The objective is to gain an understanding of the current technical infrastructure, organisational structure, policies, procedures and legal framework in a relatively short time frame. The information collected during this activity should identify business, organisational, legal and technical issues and give an indication of the degree of 'readiness' for implementation/ integration of a PKI solution, documented in a Quick Scan Report. * **Project Plan** – A 'roadmap' for the execution of the project.		
		Technical	**Organisational/ processes**	**Legal/regulatory**
Design	The objective of the Design phase is to develop/agree on the business, organisational, legal, and technical framework for the PKI.	* **PKI Architecture Specifications** – The architecture specifications can be expressed in terms of network topology, distribution of PKI components, trust model, certificate requirements, hardware/software specifications, and/or API requirements.	* **Security Plan** – PKI system classification, risk analyses and the measures taken to reduce these risks. * **Business Security Controls Framework (BSCF)** – A model that defines the processes and controls framework needed to manage the key and certificate life cycle and consequently the core business practices of the CA.	* **Certificate Policy (CP)** – Defines the use and applicability of digital certificates within a business community, including the implied liabilities and other legal implications in the context of the business applications. * **Legal Issues Paper** – Research of the legal issues that might be of relevance with respect to the CA.
Implementation	The objective is to acquire, install, initialise, and test the elements of the PKI, develop the CPS and other supporting documentation, and ensure that relevant personnel are trained	* **PKI Solution Selection** – Research on PKI insourcing or outsourcing, Request for information, CA Service Provider/PKI Package selection. * **Installation Plan** – Plan to ensure that the selected elements (i.e. hardware and software) are installed and configured in accordance with the specifications. * **Test Plan and Acceptance Criteria** – Plan for testing the PKI elements. * **Operation guides** – Operation guides for the CA and RA system. * **PKI Initialisation Procedure** – To ensure that the CA certificates are generated in accordance with the CP and CPS.	* **Training** – Training programme to ensure that personnel performing key operational/ management roles have the under-standing and skills to operate the PKI. * **PKI Continuity Plan** – Describes the required organisation of dealing with critical incidents in relation to the PKI.	* **Certificate Practice Statement (CPS)** – A document that describes the activities of the CA when issuing certificates and which processes, and procedures he has to follow.
Management & Operations	The objective of this phase is to ensure that the PKI service provision is run and managed effectively and efficiently in accordance with the business strategy, require-ments, and stated practices and procedures.	* **Service Level Agreement** – A written agreement between an ICT service provider and the customer that documents agreed service levels for an ICT-service. * **CA/PKI Audit Report** – An assessment of the adequacy and effectiveness of the controls defined in the CPS; whether these controls meet the objectives and criteria defined in the CP, and whether the CA and RA operations are consistent with the CP and CPS.		

Table 1. Main PKI implementation phases, objectives and deliverables.

questions are addressed during the development of the BSCF. It therefore constitutes a major input to the development of the CP and CPS.

For this particular project, the BSCF was completed after the CP and CPS. The main reason for this was to provide my-ePayments with an appropriate set of requirements that referred to, or could be incorporated into, the PKI service contract. The drafted contractual agreements needed to be completed within a rather short timeframe in order to avoid certain costs and penalties for my-ePayments. The contract clauses concerning the level of service provided to my-ePayments in the operation of the CA, failed to address many important requirements. To avoid exposing my-ePayments to a situation in which they would have no alternative if the CA services failed to provide the necessary level of service, priority was given to the development of CP that would include most requirements as soon as possible.

The race to complete the implementation of the PKI constituted another reason for postponing the development of the PKI BSCF. Since the critical decisions and issues were already being addressed during the development of the CP and CPS, the completion of the BSCF was given a lower priority. The BSCF was nevertheless completed eventually and stands as a record of the rationale that underlies the various decisions that were made. The information in the BSCF will prove useful when the existing controls are re-evaluated to determine if they continue to offer adequate protection. It will provide a historical perspective and a guiding principle for any future modifications to the CP and the CPS.

Other services provided to my-ePayments during this project included:
* feedback on the implementation and integration of the PKI into my-ePayments business model;
* consultation on security issues not directly related to PKI, but to the overall security architecture;
* input for negotiations with the service provider regarding the implementation of controls;
* attesting to the CA Key Generation Ceremony.

PKI Conceptual Model
The my-ePayments PKI Conceptual Model describes the distribution of PKI-related functions among different infrastructure components, the types of transactions involved, and the flow of information. It also shows where the PKI and its components fit within the overall operation.

Development of the PKI Conceptual Model requires a good understanding of the types of applications that the PKI will support, the types of transactions, and the parties involved in those transactions. This conceptual model has been developed on the basis of design documents, interviews, and inspection of the system components already in place.

Given the high level of abstraction of the Conceptual Model, most of the modifications and adjustments that might be made to the PKI during the implementation and integration phases of the project should prevent it becoming obsolete.

Development of the PKI Conceptual Model requires a good understanding of the types of applications that the PKI will support, the types of transactions, and the parties involved in those transactions.

Certificate Policies (CP)
Three separate certificate policies were developed to support my-ePayments PKI. One for consumers making the purchases, one for the dealer accepting the payments, and one for the Root CA. A CP sets out the rules and conditions for the management and the use of certificates. The CP can be used to decide whether or not to rely on a certificate. The information provided by a CP includes requirements for the identification and authentication of the parties requesting the certificates, the choice of cryptographic algorithms and requirements for their implementation and use, the life span of keys, CA operational requirements etc.

A CP can serve the following purposes:
* to provide a vehicle for dependent parties to specify assurance and reliability requirements on certificates that they will use to validate electronic transactions;
* to constitute the basis on which a CA is audited;
* to enable interoperation between the subscribers of multiple CAs supporting the same CP;
* to define the scope of acceptable use for the certificate and acceptable behaviour by certificate holders;
* to define or limit the risks involved in my-ePayments' transactions by imposing guidelines for the enrolment, separation and training of users, and by defining guidelines, best practices and duty assignments for operators.

Certification Practices Statements (CPS)
A related concept, the 'Certification Practices Statement' (CPS), is defined in the American Bar Association *Digital Signature Guidelines* as 'a statement of the practices which a Certification Authority employs in issuing the certificates'. Even though the CP and CPS follow a common format, they should not be confused as they differ in terms of:
* *authorship:* while dependent parties express their own requirements through a CP, the CPS is a statement of the procedures and practices the CA follows to meet the requirements of the CP;
* *purpose:* the purpose of the CPS is to describe the service or services provided by CAs;
* *level of specification:* a CP is a high-level document, while a CPS can be very specific and as detailed as an operations manual;
* *approach:* a CP is defined independently of the specific details of the operating environment of any particular CA, while a CPS is particular for each CA

and its organisational structure, operating procedures, facilities, and computing environment.

A CPS was developed for my-ePayments even though an independent organisation operates its branded CA. This external organisation may be viewed as a 'certificate manufacturing operation' for the my-ePayments CA, but in fact it carries out almost all CA-related tasks (issuance, revocation, repository hosting, archiving and enrolment of consumers). Only customer enrolment, integration, and revocation directly involve my-ePayments personnel.

Figures 6 and 7 show simplified forms of enrolment and transactional processes.

PKI Business Security Controls Framework (BSCF)
The PKI BSCF describes the relevant ICT controls of the my-ePayments PKI as well as the organisation of its management structure. The BSCF is directed at the design and maintenance of a secure, controllable PKI for my-ePayments. The BSCF covers the requirements for the set-up of a PKI security architecture and provides guidelines for the documentation of specific policies and procedures. The controls described, apply to my-ePayments, outsourced management and staff involved in the development, implementation and maintenance of the PKI.

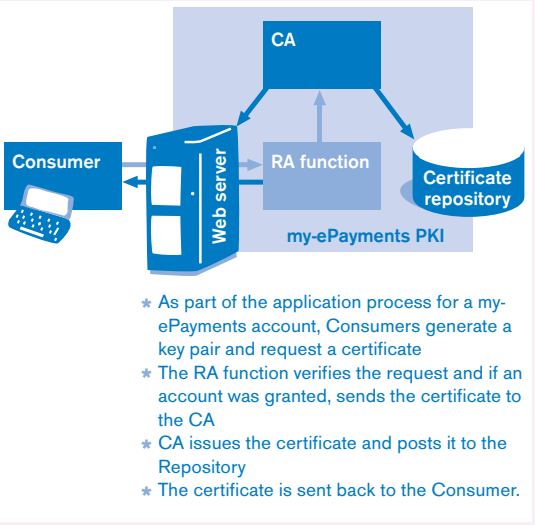

Figure 6. Registration Authority enrolment process.

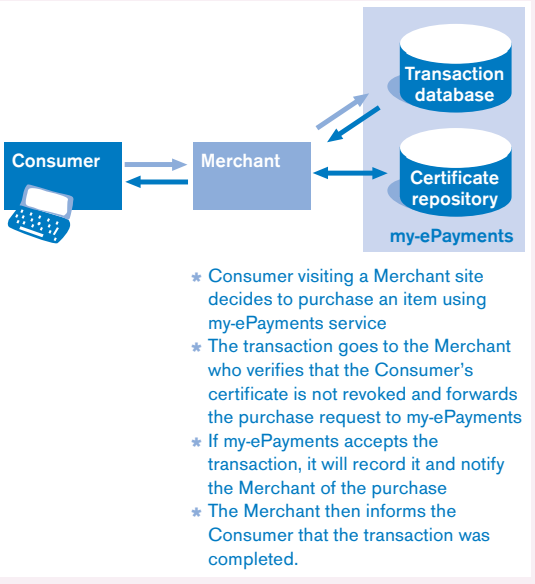

Figure 7. Transaction processing.

The development of the BSCF was driven primarily by the risks to the business processes. It specifies control directives aimed at minimising or limiting business risks and improving system security. The BSCF also addresses key management controls, ICT environmental controls and core decisions regarding certificate life cycle management and key operational roles. The activities and deliverables described here, provided my-ePayments with the support they required to establish their PKI. By customising the application of the Life Cycle Methodology, the PKI team was able to respond to my-ePayments' needs and priorities. Although the sequence of events was altered, this case study shows how effective the Methodology can be in complex real-world situations. Given the nature of my-ePayments' business activities, not only do they require a PKI, but they require a PKI that is clearly structured, well designed, and well documented. The application of the PKI Life Cycle Methodology gave my-ePayments the tools with which to achieve their goal: implementation of a reliable PKI.

Case study #2: Financial Services Company, First European Bank

In 1996, KPMG IRM the Netherlands established a centre of excellence for the provision of PKI services ranging from full or partial PKI implementations to the review and audit of existing PKI implementations. This centre of excellence has been involved in a joint PKI project at First European Bank with technology provider Baltimore Technologies.
The PKI project consisted of three constituent projects:
1 the creation of the First European Bank Root CA;
2 the creation of a CA for Branch Office network user authentication;
3 the creation of a CA to facilitate both internal use and business-to-bank transactions.

The First European Bank Root CA is a global CA with which to certify the primary level of CAs used by the First European Bank. From this primary level of CAs other, subordinate CAs (Sub CA) may be certified to create a CA hierarchy.

The second CA provides certification services for client authentication on the Windows 2000 network. Employees at the branch offices receive a smart card, which contains the private key. The public key is stored in the Directory Service (Active Directory). For authentication of the client, the public key is used to create a 'challenge'. The challenged party needs the private part of the certificate to answer with the correct 'response'. Once the identity of the client is verified, the server establishes a security context with a matching authorisation which determines what resources the client is allowed to use on the server.

The latter PKI is part of the Corporate Cryptographic Infrastructure (CCI) project that supplies standards-based cryptographic services to First European staff, customers and applications anywhere in the world. The CCI CA will e.g. issue certificates to clients for digitally signing electronic financial transactions.

For each of these three constituent projects KPMG was asked to assist in the development and implementation of the security infrastructure, the governance structure and the legal framework, as well as develop the main policies and procedures.

In addition to these CAs, based on the bank's root CA, an Identrus CA was implemented. Identrus is a consortium of approximately 40 leading banks that has developed a global, standardised and interoperable PKI in which financial institutions operate as certificate authorities (CAs). Identrus issues certificates to financial institutions that are responsible for issuing certificates to corporate clients and their employees. Identrus will operate the root CA at the top of the enterprise's certificate hierarchy. Identrus also enables corporate trading partners to reduce time, costs and effort involved in building up trust relationships with counterparts around the world. By doing so, the system will encourage the adoption of trusted B2B e-Business. KPMG was involved in the development of additional e-Business trust services for other financial institutions, as well as the creation of an online marketplace by leveraging the Identrus PKI.

The approach

During the realisation of the projects, KPMG used the relevant constituents of KPMG's PKI Life Cycle Methodology. This methodology provided tools and templates for addressing the organisational and legal aspects. The technical part of the project was realised by various specialists of the First European Bank, Baltimore Technologies and IBM. They designed and developed the PKI architecture and relevant technical documentation.

The result

KPMG has helped the First European to develop and implement a PKI that consists of a Root CA, and a Windows 2000 CA for user authentication, and a PKI for the issue of digital certificates that support a wide range of secure-commerce applications, such as secure e-mail and internet banking.

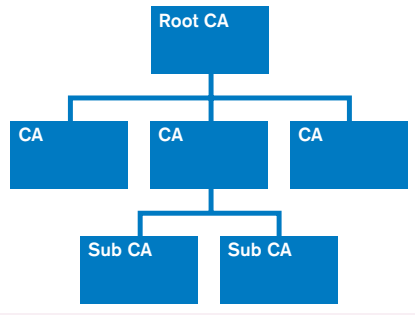

Figure 8. Bank's CA hierarchy.

Conclusion

PKI is often characterised by research bureaus as one of the fastest growing security infrastructures. According to Datamonitor's PKI study [Data99], PKI will continue to grow over the next four years. By 2003, revenues will reach USD 1.4 billion worldwide. This article argues that a large-scale PKI implementation requires a structured design and implementation approach. This view is endorsed by the Gartner Group who claims that 40 percent of PKI implementations will fail within two years because they do not provide assessable benefits. Implementation problems can have several causes. Though standards have been defined for the PKI industry, the technology to support it is still lacking. Standards for PKI implementation vary to a certain degree, which results in interoperability problems. Additionally, the use of digital signatures in existing and new applications that support business operations, as well as the scaling of the PKI to incorporate it in the infrastructure, can both be very challenging. Furthermore, there are still some unresolved problems with respect to revocation and directory use, certificate portability and cross-certification.

Though standards have been defined for the PKI industry, the technology to support them is still lacking.

PKI comprises a very complex technical concept, which requires a well-considered multidisciplinary approach. A complicating factor is that people with experience in real-life implementations of PKIs are hard to find. PKI implementation models designed in the past, often no longer apply. Nevertheless, they are still used. For example, many projects start out by defining a CPS, which is regarded as the guideline for the PKI implementation. Later on it becomes clear that the CPS is set on too high a level to be useful as a guideline. It consequently needs to be adapted as the organisation develops more insight into PKI issues.

We have found that the CPS comprises a variety of issues formulated in different documents (e.g. key and certificate management guidelines, legal issues inquiry, technical documentation). These issues should be worked out in set stages. By way of exception, for instance if an organisation needs to define the requirements for a PKI service contract, one could start out with the definition of the CPS. KPMG's Life Cycle Methodology follows a logical progression: from initial assessment to planning implementation and maintenance. Frameworks for the different deliverables are available and can easily be tailored to the client's

Noel Nazario
(nnazario@kpmg.com)
is a senior consultant in KPMG's Information Risk Management practice in Washington D.C. with eleven years of technical experience in computer and communications security at NIST and KPMG. For over five years he has been a key figure in the development of PKI technology in support of e-Business and e-Government services.

Martijn van Oosten
(vanoosten.martijn@kpmg.nl)
is a senior consultant in KPMG's Information Risk Management practice in Amsterdam, the Netherlands. For over five years he has been a key figure in the development of products and services for the implementation and audit of PKIs and is responsible for the development of the PKI Business Security Controls Framework.

specific needs. The complex legal, organisational and technical aspects of PKI implementation however require multidisciplinary expertise and an experienced project team. KPMG's PKI Centres of Excellence are established in 1997 to combine the skills of PKI professionals. They are able to offer substantial support to organisations in the implementation of a PKI.

Literature

[Data99]
Datamonitor, *Global PKI Markets, 1999-2003*, November 1999.

[KPMG99]
KPMG, *Electronic Commerce Research Report*, 1999.

[Pesc99]
J. Pescatore, *Network Security for Public Key Infrastructures*, Gartner, August 1999.