PKI and Digital Certification Infrastructure

Ray Hunt, Associate Professor, Department of Computer Science, University of Canterbury, New Zealand

Abstract

Secure VPN technology is only possible with the use of appropriate security systems such as encryption, digital signatures, digital certificates, public/private key pairs, non-repudiation, and time-stamping. A PKI comprises a system of certificates, certificate authorities, subjects, relying partners, registration authorities, and key repositories that provide for safe and reliable communications. This paper discusses these key technologies focusing particularly on recent standardisation as well as looking at some of the challenges pending its widespread operation in the industry.

1. Introduction

Public key cryptography can play an important role in providing security services including confidentiality, authentication, digital signatures and integrity. This paper provides a brief outline of the basic concepts and principals involved in its operation including issues such as how a PKI operates, its characteristics and what problems need to be addressed before the use of PKI becomes more widespread. PKI can be used to solve many problems, however there are still several problems and risks involved in its use as well as organisational and management issues for which solutions are still evolving.

2. PKI background and standards developments

Public key cryptography was conceived in 1976 by Diffie and Hellman [1] and in 1977, Rivest, Shamir and Adleman designed the RSA Cryptosystem [2], the first public key system. Each public key cryptosystem has its own technical features, however they all share the property that given an encryption key it is computationally infeasible to determine the decryption key and vice versa. Theoretically, no confidential information needs to be exchanged before secure communication is possible. Everyone has access to the recipient's public key and even though the communication is private, the message cannot be authenticated. This shows that public key cryptography on its own, is not enough. If traditional paper based commerce are to be reproduced in the electronic environment, the following are required:

- Security policies to define the rules under which cryptographic systems should operate
- Products to generate, store and manage certificates and their associated keys
- Procedures to dictate how keys and certificates are generated and distributed

A trusted and authenticated key distribution infrastructure is necessary to support the use of public keys in a public network such as the Internet. Recent efforts in standardisation have seen developments on a number of fronts.

2.1 Evolution of PKI standards

The X.509 Recommendation provides a useful basis for defining data formats and procedures for the distribution of public keys via certificates that are digitally signed by CAs. X.509 does not however include a profile to specify the supporting requirements for many of the certificate's sub-fields, extensions or for some data values.

The standards effort produced an outline for PKI of X.509 Version 3 certificates as well as Version 2 Certificate Revocation Lists (see Section 3.2.3). The Internet PKI profile went through eleven draft versions before becoming RFC 2459 [3]. Other profiles have been developed for particular algorithms to make use of RFC 2459.

The development of the PKI management protocols has gone though a number of iterations. RFC 2510 [4] was developed to specify a message protocol to be used between entities in a PKI. The need for an enrolment protocol and the preference to use PKCS#10 message format as the certificate request syntax lead to two parallel developments.

The Certificate Request Syntax was developed in the S/MIME WG which used PKCS#10 [5] as the certification request message format. Certificate Request Message Format RFC 2511 [6] draft was also developed but in the PKIX WG. It was to define a simple enrolment protocol that would work for the RFC 2510 [4] enrolment protocols, but it did not use PKCS#10 as the certificate

Proceedings of the 9th IEEE International Conference on Networks (ICON'01)
1531-2216/02 $17.00 © 2002 IEEE

request message format. Then, RFC 2510 [4] and [7] were developed to define an extended set of management messages that flow between the components of the Internet PKI. These, combined with CMS [7] allowed the use of an existing protocol (S/MIME) as a PKI management protocol, without requiring the development of an entirely new protocol such as CMP [4]. It also included PKCS#10 as the certificate request syntax.

Development of the operational protocols has been more straightforward. Two documents for LDAP have been developed — one for defining LDAPv3 as an access protocol to repositories [8] and one for storing PKI information in an LDAP directory [9]. Using FTP and HTTP to retrieve certificates and CRLs from PKI repositories is specified in RFC 2585 [10].

3. Public Key Infrastructure

PKI provides the core framework for a wide variety of components, applications, policies and practices to combine and achieve the three principal security functions (integrity, authentication and non-repudiation). A PKI is a combination of hardware and software products, policies and procedures. It provides the basic security required for secure communications so that users who do not know each other or are widely distributed, can communicate securely through a chain of trust. Digital certificates are a vital component in the PKI infrastructure as they act as 'digital passports' by binding the user's digital signature to their public key

3.1 Components of a PKI

A PKI consists of:

- Security policy
- Certificate Authority (CA)
- Registration Authority (RA)
- Certificate repository and distribution system
- PKI-enabled applications

3.1.1 Security policy

A security policy defines an organisation's top-level direction on information security as well as the processes and principles for the use of cryptography. Typically it will include statements on how the organisation will handle keys and valuable information and will set the level of control required to match the levels of risk.

Some PKI systems are operated by Commercial Certificate Authorities (CCAs) or Trusted Third Parties (TTPs) and therefore require a Certificate Practice Statement (CPS) [11]. This is a detailed document containing the operational procedures on how the security policy will be enforced and supported. It includes specifications on how the CAs are constructed and operated, how certificates are issued, accepted and revoked, how keys will be generated, registered and certified, where they will be stored and made available to users.

3.1.2 Certification Authority (CA)

The CA is an entity which issues and revokes certificates. An in-house server or a TTP such as Entrust, Baltimore or VeriSign, can provide a CA function. A CA provides the trust basis for a PKI as it manages public key certificates for their whole life cycle. The CA will:

- Issue certificates by binding the identity of a user or system to a public key with a digital signature
- Schedule expiry dates for certificates
- Ensure certificates are revoked by publishing Certificate Revocation Lists (CRLs)

When implementing a PKI, an organisation can either operate its own CA or use the services of a Commercial CA or TTP. While the principles of PKI are the same there are currently *two* major commercial implementation models which depend upon who the CA is. (On each of the respective web sites are a number of white papers claiming the advantages of each of these models [12]):

1. Private CA — vendors sell a complete PKI system to an organisation which then becomes its own CA and is responsible for the issuing and management of certificates. Examples include RSA's Keon 5.0, IBM's Secureway Trust Authority 3.1, Baltimore's Unicert 3.0.5 and Entrust's PKI 4.0.
2. Public CA — certificates are purchased from a public CA organisation as required. The most common example of this approach is VeriSign.

3.1.3 Registration Authority (RA)

An RA provides the interface between the user and the CA. It authenticates the identity of the users and submits the certificate request to the CA. The quality of this authentication process determines the level of trust that can be placed in the certificates. For example, if all an RA requires is an e-mail address and a name, the level of trust that should be placed in that certificate would be considerably lower than if more stringent registration procedures were required.

3.1.4 Certificate repository and distribution system

The Certificate Repository provides a mechanism for storing keys, certificates and Certificate Revocation Lists (CRLs) which is usually based on an LDAP-enabled directory service. Key recovery is an advanced function required to recover data or messages when a key is lost and a PKI may provide such an automated key recovery service.

3.1.5 PKI-enabled applications

A PKI is a means to an end — providing the security framework by which PKI-enabled applications can be confidently deployed to achieve the end benefits. Figure 1 shows the relationship between some applications and infrastructure, and their related standards

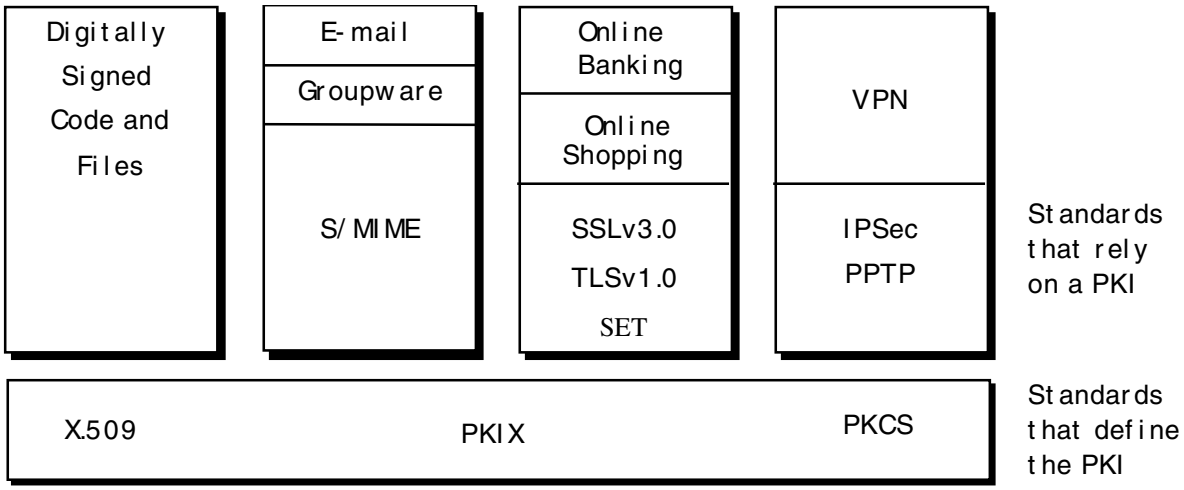

Figure 1 PKI security architecture [13]

3.2 Operations of PKI

The main PKI functions are shown in Table 1. These include — registration, issuing and revoking certificates, creating and publishing CRLs, storing and retrieving certificates and CRLs, as well as key lifecycle management. Some of the enhanced functions include time-stamping and policy-based certificate validation.

Function	Description	Implementation
Registering users	Collect user information, verify identity	Function of CA, or separate RA
Issuing certificates	Create certificates in response to user or administrator request	Function of the CA
Revoking certificates	Create and publish Certificate Revocation Lists (CRLs)	Administrative software associated with the CA
Storing and retrieving certificates and CRLs	Make certificates and CRLs available to authourised users	Repository for certificates and CRLs in secu replicated directory service accessible via LDAP
Policy-based certificate path validation	Impose policy-based constraints on certificate chain, and validate if all constraints are met	Function of the CA
Time-stamping	Time-stamp each certificate	Function of the CA or a dedicated Time Server (TS)
Key lifecycle management	Update, archive and restore keys	Automated in software or performed manuall

Table 1 Public Key Infrastructure (PKI) Functions

These functions can be described in terms of three basic PKI infrastructures:

- Certification is the process of binding a public key value to an entity

- Validation is the process of verifying that a certificate is valid and revoking where necessary
- Key management - updating, backing up and archiving

3.2.1 Certification

Certification is the fundamental function of all PKIs and it is the means by which the public keys and information pertaining to those keys are published. A CA might have different classes of certificates with each class providing a designated level of trust. For example to overcome these inherent limitations VeriSign has introduced four different levels of certificate [14] (each with different cost structures) corresponding to the degree of authentication required and shown in Table 2.

VeriSign Class 1 Individual Certificates enhances the security of some applications by assuring that a certificate's subject and e-mail address are included within VeriSign's repository but do not provide proof of identity.
VeriSign Class 2 Individual Certificates provide a reasonable level of assurance of a subscriber's identity. Identities ar checked against local records or Trusted Third Parties (TTP).
VeriSign Class 3 Individual Certificates provides a higher level of assurance by validating the identity via in-person presentation of identification credentials or other enhanced procedures. Used in banking and contracting applications.
VeriSign Class 3 Organisational (Server) Certificates provide assurances for web site authentication. Validation includes comparison of certificates to information held by TTPs or official records.

Table 2 Classes of Digital Certificates available from VeriSign

In addition to the content and authenticity of a transaction, the exact time of the transaction can be important. For example, it may have to be submitted within a specified time to be valid. The solution therefore is to combine signatures with a time-stamping service. (Section 5.5)

3.2.2 CA hierarchy

It is impractical to have a single universal CA and most PKIs permit CAs to certify other CAs. Different PKIs arrange their CAs in different hierarchies or they may even have arbitrary or bilateral structural agreements.

The scalability of a PKI depends on the relationship between its CAs. A problem here is that CAs may allocate trusts differently and this problem increases as the certification path grows. The certification path also runs the risks of becoming too long. Path discovery and trust delegation is difficult to achieve across company and/or geographical boundaries. The dominant hierarchy is top down, but it has the problem that all users must trust the root CA and since so many paths pass through the root CA, it is vulnerable to attack.

3.2.3 Validation and revocation

The information in a certificate can change over time and a certificate user needs to validate that the certificate's data is current. Users can either:

- Ask the CA about a certificate's validity every time it is used (online validation)
- Request the CA to include a validity period in the certificate (offline validation)

Closely related to the issue of validation of certificates is certification revocation. A certificate should be revoked when it is suspected that it has been compromised. If a certificate is validated online with the CA, the CA can simply state that the certificate is no longer valid. With offline validation, the most common method is to use Certificate Revocation Lists (CRLs). A CRL is a list of certificates that have been revoked before their scheduled expiration date. For example, the key specified in the certificate might have been compromised or the user specified in the certificate may no longer have authority to use the key.

The PKIX recommendation does not require CAs to issue CRLs [15]. On-line methods of revocation notification may be applicable in some situations as an alternative to CRLs. PKIX defines an Online Certificate Status Protocol that facilitates on-line checking of the status of certificates [16] [17].

3.2.4 Key management

Each user is likely to have a number of keys that require lifecycle management. For example, users typically have at least one key pair for each secure application (e.g. e-mail, desktop file encryption, VPN). Some applications use several key pairs for different purposes, such as digital signatures, bulk encryption, and authentication.

Updating keys - new keys are usually issued at regular intervals so as to reduce the exposure from keys that have been unknowingly compromised.

Backing up keys - Users frequently forget passwords that protect their private keys — or they may lose the keys, for example, through a disk crash or virus attack.

Archiving keys - When employees leave the company, their keys must be invalidated, while retaining the keys in order to access previously encrypted files and messages. Keys used for digital signatures may be retained for as long as the signed documents exist so that signatures can be verified.

Key expiry - To guard against a long-term cryptanalytic attack, every key must have an expiration date. The key length should be long enough to make the chances of cryptanalysis before key expiration extremely small. The validity period for a key pair may also depend on the circumstances in which the key is used. The appropriate key size is determined by the validity period, together with the value of the information protected and the estimated strength of an expected attacker.

5. PKI Working Group activities

There are two main IETF working groups focused on PKI standards and implementations.

The SPKI (Simple Public Key Infrastructure) working group (www.ietf.org/html.charters/spki-charter.html) is developing Internet drafts for public key certificate formats, signature formats and key acquisition protocols. SPKI is intended to provide mechanisms to support security over a range of protocols (e.g. IPSec) and applications which may require public key certificates such as encrypted e-mail, web documents and electronic payment systems. Two important RFCs developed under SPKI include RFC 2692 [18] and RFC 2693 [19].

The PKIX working group has developed recommended standards covering five significantly different sections (www.ietf.org/html.charters/pkix-charter.html) [15]:

- Profiles of the X.509v3 certificate standards and the X.509v2 CRL standards for the Internet
- Operational protocols — relying parties can obtain information such as certificates or certificate status
- Management protocols, in which different entities in the system exchange information needed for proper management of the PKI
- Certificate policies and certificate practice statements, covering the areas of PKI security not directly addressed in the rest of PKIX
- Time-stamping and data certification services, which can be used to build services such as non-repudiation

5.1 X.509v3 profiles

X.509v3 certificates are complex data structures as they 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 with many applications. Unfortunately, this same flexibility makes it extremely difficult to produce independent implementations that will actually inter-operate. To build an Internet PKI based on X.509v3 certificates, the PKIX working group developed a profile of the X.509v3 specification — RFC 2459 [3] together with additional ongoing work [20].

In addition to profiling the certificate and CRL formats, it is necessary to specify particular Object Identifiers (OIDs) for certain encryption algorithms, since there are a variety of OIDs registered for certain algorithm suites. PKIX has produced two documents [21] and [22], which provide assistance on the implementation of specific algorithms.

5.2 Operational protocols

Certificates and CRLs can be delivered by protocols such as LDAP, HTTP, FTP and X.500. Operational protocols that facilitate certificate delivery are defined in [10], [17], [16] and [23].

5.3 Management protocols

Management protocols are needed to support online interactions between PKI user and management entities. For example, a management protocol might be used between a CA and a client with whom a key pair is associated, or between CAs which cross-certify one another. A management protocol can be used to carry user or client system registration information, or requests for certificate revocation. Management protocols that facilitate message format and transmission are defined in [4] and [7]. Certificate Policies and practice statements are defined by [24].

5.4 Time-stamp and data certification

Time-stamping is a service in which a Time-stamp Authority (TSA) signs a message to provide evidence that it existed prior to a specific time. A Time-stamping protocol [25] provides some support for non-repudiation so that a user cannot claim that a transaction was later forged after compromise of a private key.

A Data Certification Server protocol [26] is a TTP that verifies the correctness of specific data

submitted to it, thus going beyond a simple time-stamping service. The DCS certifies possession of data or validity of another entity's signature. As part of this, the DCS verifies the mathematical correctness of the actual signature value contained in a request and also checks the full certification path from the signing entity to a trusted point (e.g., the DCS's CA, or the root CA in a hierarchy).

6. Summary

This paper has reviewed a range of technical, infrastructural, operational and management issues associated with the use of PKI. There is no weakness in the cryptographic strength of the encryption and digital signature processes, however the management of these processes, storage of cryptographically strong keys, identification of entities, storage of certificates etc, all need be subject to good business practices.

PKI is still in its infancy and yet many organisations have already begun deploying certificate-enabled applications and infrastructures. Looking ahead, businesses and organisations who intend to use PKI will have to examine issues such the legal aspects of liability, interoperability between multiple PKIs, certification validation paths, protection of private keys and user acceptance. Given the complexity of the infrastructure required to implement and support a public PKI system, in the short term continued deployment of PKI-enabled applications for specific industry groups seems to be the most likely scenario.

8. References

[1] Diffie, W. and Hellman, M. E., New Directions in Cryptography. IEEE Transactions on Information Theory, 22 (1976), pp. 644-654.

[2] Rivest, R., Shamir, A. and Adleman, L., A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Communications of the ACM, 21(1978), pp. 120-126.

[3] RFC 2459, Housley, R., Ford, W., Polk, W., and Solo, D., "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", January 1999

[4] RFC 2510, Adams, C., Farrell, S., "Internet X.509 Public Key Infrastructure Certificate Management Protocols", March 1999

[5] PKCS#10, RSA, "The Public-Key Cryptography Standards ", RSA Data Security Inc., November 1993

[6] RFC 2511, Myers, M., Adams, C., Solo, D., and Kemp, D., "Internet X.509 Certificate Request Message Format", March 1999

[7] Myers, M., Liu, X., Fox, B., and Weinstein, J., "Certificate Management Messages over CMS", <draft-ieft-pkix-cmc.txt>, July 1999

[8] RFC 2251, Wahl, M., Howes, T., Kille, S. "Lightweight Directory Access Protocol (v3)" 1997

[[9] RFC 2587, Boeyen, S., Howes, T., Richard, P., "Internet X.509 Public Key Infrastructure LDAPv2 Schema", June 1999

[10] RFC 2585, Housley, R., and Hoffman, P., "Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP", July1998

[11] Arsenault, A & Turner, S., Certification Practice Statement, Internet Draft PKIX Roadmap, October 1999

[12] Public- Key Infrastructure – The VerisSign Difference; VeriSign whitpaper, 1999 (www.verisign.com/whitepaper/enterprise/difference)

[13] RSA Data Security, "Understanding PKI". (www.rsa.com) 1999

[14] VeriSign., VeriSign Certification Infrastructure, www.verisign.com/repository/CPS1.2/CPSCH2.HTM#toc361806948, 1997

[15] Arsenauly, A and Turner, S., "Internet X.509 Public Key Infrastructure PKIX Roadmap". <draft-ietf-pkix-roadmap.txt>, November 2000

[16] RFC 2560, Arsenauly, A and Turner, S., X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, 2000

[17] Myers, M., Ankney, R., Malpani, A., Galperin, S., and Adams, C., "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP Extensions", September 1999

[18] RFC 2692, Ellison, C., "SPKI Requirements", September 1999

[19] RFC 2693 Ellison, C. et al, SPKI Certificate Theory, September 1999

[20] Santesson, S., Polk, W., Barzin, P., and Nystrom, M., "Internet X.509 Public Key Infrastructure Qualified Certificates", <draft-ietf-pkix-qc.txt>, February 2000

[21] Bassham, L., Johnson, D., and Polk, W., "Internet x.509 Public Key Infrastructure: Representation of Elliptic Curve Digital Signature Algorithm (ECDSA)", <draft-ietf-pkix-ipki-ecdsa.txt>, October 1999

[22] Housley, R., and Polk, W., "Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates", March 1999

[23] RFC 2559, Boeyen, S., Howes, T., and Richard, P., "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2", April 1999

[24] RFC 2527, Chokhani, S., and Ford, W., "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", March 1999

[25] Adams, C., Cain, P., Pinkas, D., and Zuccherato, R., "Internet X.509 Public Key Infrastructure Time Stamp Protocols", <draft-ietf-pkix-time-stamp.txt>, 2000

[26] Adams, C., Sylvester, P., Zolotarev, M., Zuccherato, R., "Internet X.509 Public Key Infrastructure Data Certification Server Protocols", <draft-ietf-pkix-dcs-.txt>, March 2000