Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Interoperability in PKI

With increasing emphasis and reliance upon everything from VPNs and ecommerce to remote access and authentication, PKI is rapidly becoming an essential piece of the information age. However, there are several factors that have kept PKI from widespread deployment including confusion about what makes up a PKI, the complex and costly implementations, and immature industry standards and incompatibility among those standards. In the environment of electronic communication, the establishment of trust depends on electronic or...

Copyright SANS Institute
Author Retains Full Rights

AD

INTEROPERABILITY IN PKI

1 Why do we need interoperability?

With increasing emphasis and reliance upon everything from VPNs and e-commerce to remote access and authentication, PKI is rapidly becoming an essential piece of the information age. However, there are several factors that have kept PKI from widespread deployment including confusion about what makes up a PKI, the complex and costly implementations, and immature industry standards and incompatibility among those standards. In the environment of electronic communication, the establishment of trust depends on electronic or digital objects and processes and procedures that manage them. This paper will introduce some of the interoperability issues in PKI which applies to processing and managing the establishment of those trust and the challenges it faces.

PKI standards come in a variety of forms and there are numerous standards bodies that engage in the development of those standards. In particular, standards are necessary for enrollment procedures, certificate formats, CRL formats, formats for certificate enrollment messages (client requests, certificate, server issues certificate), digital signature formats, and challenge/response protocols.

There are basically three reasons why we need PKI interoperability. First is the need of the users to rely upon different trusted services, second is by the providers of trusted services to interoperate between themselves and their customers as well as with other trusted service providers, and third is by solution vendors' need to meet the user and service provider requirements.

For a user, there are three factors essential in using the solutions and services provided by trusted services. They are interoperability, portability, and mobility. Interoperability means being able to work with a number of trusted services without the need for special procedures such as data format conversion. Portability means being able to move application solutions from one software and hardware environment to another and so one can combine an application with a choice of trusted services. Mobility means being able to access the same trusted services, with the same functionality, when away from the usual place of work, particularly when in other countries. Users will also need to have confidence in the solutions and services that they use. This confidence may be based on already existing bases, such as the market presence of a service provider or vendor or it may be based on the trust already placed in an organization for other reasons such as the trust relationship between a bank and its customers.

For service providers, there are several functional reasons why they would need interoperability in PKI:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- They want to provide services to as wide a market as possible and this can only be achieved if there is interoperability with their current and potential clients since their clients will not all have the same application, software, and hardware systems.

- They need to establish relationships with other service providers, both in their own country and globally in order to support global transactions. The ability to support their customers when their customers are away from their usual place of business which dictates interoperability among service providers.

- Portable solutions means the ability to move their application systems from one software and hardware environment to another, and the ability to combine an application with a choice of trusted services, thus protecting their investment in that application.

- There may also be a need for management standards which the service providers will need to establish bases on which they can trust other service providers; standards against which the operation of providers can be measured may assist the establishment of mutual co-operation agreements.

For solution vendors, they need to produce solutions to meet the needs of users and service providers. Their solutions need to interoperate with solutions from other vendors. An incentive to develop portable solutions is the availability of a larger market for their products.

With the need for interoperability in PKI laid out, we will review major standards and specifications which exist or are being developed which may enable the wide implementation and acceptance of PKI, and discuss some of the challenges and problems facing the PKI standardization. Among the organizations and groups actively pursuing or studying different PKI standards today, there are three most prominent groups leading the effort on PKI standards. They are Public Key Cryptography Standards (PKCS), International Standards Organization/International Telecommunication Union (ISO)/(ITU), and International Engineering Task Force (IETF). This paper will cover the standardization efforts of these three groups as they relate to PKI. It should be noted here that the development of standards and specifications is an on-going process and that it may be revised as further standards and specifications are produced.

2 PKI Standards

2.1 ISO/ITU-T X.509

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The X.509 comes from the X series of the International Telecommunications Union – Telecommunications (ITU-T), formerly known as the CCITT. The purpose of the X series is the standardization of data networks and open system communications. X.509 is the authentication framework designed to support X.500 directory services and both X.509 and X.500 are part of the X series of international standards proposed by the ISO and ITU.

The first version of X.509 version appeared in 1988, making it the oldest proposal for a worldwide PKI. Coupled with its ISO/ITU origin it has made X.509 the most widely adapted PKI. There are at least a dozen companies worldwide that produce X.509-based products, and that number is growing. Along with PGP, X.509 is the only PKI system that has yet to be put into practical use.

The X.509 standard is important for two reasons:

- Defines a framework for the provision of authentication services
- Defines a certificate format for public keys

The standard proposes a process where one user is authenticated to another using a certificate containing a public key and is signed by a Certification Authority the user trusts. This process is based on a certification path which logically forms an unbroken chain of trusted points in the Directory Information Tree between two users wishing to achieve authentication. As part of the standardization process, the management of keys and certificates is included as well as the revocation of certificates.

However, the important feature of the X.509 comes from the powerful extension mechanism it has proposed in its Version 3 Certificates and CRL extensions. This feature enables the X.509 implementers to define certificate contents as they fit.

2.2 Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) is the body primarily responsible for creating, standardizing, and promoting the protocols/functions that make the Internet useful and valuable. Within the IETF, a number of working groups have published and are preparing specifications of major relevance to different aspects of implementing Trusted Services. There are nine sectors considering those specifications which are important both as users of trusted services and as enabling components. We will focus on two main sectors which deals with infrastructure component of PKI.

2.2.1 Internet Public Key Infrastructure (IPKI)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

IPKI was created to address the realization that more detailed application of X.509 standard was warranted than simply profiling the X.509 certificate and CRL work. This led to the formation of IPKI and its four part standards:

Part 1: X.509 Certificate and Certificate Revocation List Profile
Part 2: Operational Protocols
Part 3: Certificate Management Protocols
Part 4: Certificate Policy and Certification Practices Framework

X.509 Certificate and Certificate Revocation List Profile

The goal of the specification is to develop a profile and associated management structure to facilitate the adoption and use of X.509 certificates within Internet applications for those communities wishing to make use of X.509 technology. Such applications may include WWW, electronic mail, user authentication, and IPSEC, as well as others. In order to relieve some of the obstacles to using X.509 certificates, this document defines a profile to promote the development of certificate management systems, development of application tools, and interoperability determined by policy, as opposed to syntax.

Operational Protocols

The “Operational Protocols" defines two protocol profiles for retrieving certificates and certificate revocation lists from an information repository. The document also describes a protocol for ascertaining the status of a certificate from a CA. The protocols profiled for retrieval are:

- Lightweight Directory Access Protocol (LDAP) and
- File Transfer Protocol (FTP)

The protocol specified for communicating directly with a CA about the status of a certificate is called the On-line Certificate Status Protocol (OCSP). The OCSP is specified to use HTTP as its access method.

Certificate Management Protocols

Management protocols are specified to support on-line interactions between Public Key Infrastructure (PKI) components.

The management protocols include the following functions:

- Between the end entity and the certification authority
  - initial registration and certification
  - key pair recovery
  - key pair update

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

  - certificate update
  - revocation request
- Between two certification authorities:
  - cross-certification
  - cross-certificate update
- Between the end user and the repository
  - certificate publication
- Between the certification authority and the repository
  - publication of certificates and certificate revocation lists

Certificate Policy and Certification Practices Framework

The purpose of this part is to present a framework that identifies the elements that may need to be considered in formulating a certificate policy or a Certification Practice Statement (CPS). It is to assist the writers of certificate policies or CPSs with their task, but not to define particular certificate policies or CPSs.

The framework addresses and will contain these nine top-level elements:

- Community definition and applicability
- Identification and authentication policy for subjects, Registration Authorities and Certification Authorities
- Key management policy
- Non-technical security policy
- Technical security policy
- Operational requirements
- Legal & business provisions
- Certificate and CRL profiles
- Policy administration

2.2.2 Simple Public Key Infrastructure (SPKI)

This approach proposes a simpler PKI standard compared to the PKIX effort. Originally two separate developments, the Simple Distributed Security Infrastructure and Simple Public Key Certificate have merged to form the Simple Public Key Infrastructure. A defining characteristic of an SPKI certificate is that it is a text-based structure which does not use ASN.1 to define its data structures. The main purpose of an SPKI certificate is to authorize some action, give permission, grant a capability, etc. The first requirement for an SPKI certificate is then to bind a meaningful or useful attribute to a public key (and therefore to the keyholder of the corresponding private key). In many cases, the attribute would not involve any recognizable name.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The definition of attributes or authorizations in a certificate is up to the author of the application code who uses the certificate. The creation of new authorizations should not require interaction with any other person or organization but rather be under the total control of the author of the code using the certificate. The main driving forces behind the proposal are the desire to keep down overheads arising from use of an ASN.1 based certificate and an infrastructure supporting a global directory, the search for an efficient implementation, and freedom and flexibility to develop structures for a growing number of applications.

2.3 Public Key Cryptography Standards (PKCS)

PKCS is a numbered set of standards defined by RSA since 1991. Because standards are normally defined and agreed by a number of organizations working together, PKCS is considered informal standards because it is controlled by RSA. However, they are widely accepted in the industry based on the dominant RSA public key algorithm. There is a proposal that the PKCS be published as IETF documents although not under the control of the IETF. Whatever happens in the future, the PKCS currently occupy an important place in the development of trusted services. The particular standards most relevant to trusted services are:

1) PKCS #1: RSA Encryption Standard
2) PKCS #3: Diffie-Hellman Key Agreement Standard
3) PKCS #7: Cryptographic Message Syntax Standard
4) PKCS #10: Certification Request Syntax Standard

PKCS #1 describes how data is encrypted using the RSA public-key cryptosystem. Its intended use is in the construction of digital signatures and digital envelopes, as will be described in PKCS #7. For digital signatures, before signing the content, it is first reduced to a message digest with a message-digest algorithm (such as MD5); signing is done by encrypting with the signer's RSA private key the message digests. For digital envelopes, the content to be enveloped is first encrypted under a content-encryption key with a content-encryption algorithm (such as DES), and then the content-encryption key is encrypted with the RSA public key(s) of the recipient(s) of the content. PKCS #1 also describes syntax for RSA public keys, which is identical to that in both X.509 and PEM and for RSA private keys. The public-key syntax would be used in certificates.

PKCS #3 describes a method for implementing Diffie-Hellman key agreement, whereby two parties, without any prior arrangements, can establish a secret key which can then be used.

PKCS #7 describes a general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes. The syntax supports recursion, so that for example, one envelope can be nested inside another, or one party can sign some previously enveloped digital data. Other

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

attributes, such as signing time, can be authenticated along with the content of a message, and countersignatures can be associated with a signature.

PKCS #10 describes a syntax for certification requests, which are sent to a certification authority, which using the information received produces an X.509 public-key certificate. The certification request contains a distinguished name, a public key, and optionally a set of attributes, collectively signed by the entity requesting certification. The set of attributes can be information such as the postal address to which the signed certificate should be returned if electronic mail is not available or a "challenge password" by which the entity may later request certificate revocation.

3 Interoperability Issues

As we present some of the major PKI standards activities, it is becoming increasingly clear that interoperability in PKI may have a difficult road ahead due to lack of clear standards. Although standards are instrumental in promoting interoperability, many standards do not guarantee it in a multi-vendor environment. Each group's standardization efforts differ in terms of their approach, focus, and scope and there are a number of other issues that can have influence on the success or failure of a given standard. Some of the issues include the following:

- Participation in the standardization groups are voluntary and may lack the broad cross section representation of relevant organization
- Lack of implementation practice or conflicting implementation experience which may be incorrectly reflected in the standards
- Quality of various standards can vary among the committees and subcommittees depending on the participants and on the rules governing the participation

Standards are essential in promoting interoperability; yet many standards do not guarantee interoperability in a multi-vendor environment. In addition, there are numerous difficulties encountered when attempting to reach agreement on numerous technical and many times political issues that arise during the standards process. Currently, even the experts have difficulty in determining what may happen with PKI standards and the issue of interoperability. However, the lack of a clear leader in PKI standards have not kept the PKI from being implemented into practical use today as the industry itself tries to find its footing on the issue.

4 Summary

There are a couple of things that can be accomplished beyond the development of a standard to help attain the desired level of multi-vendor interoperability. First, there is a need to profile the standards that apply to a particular

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

environment. The purpose of a profile is to clearly identify which features of the more generic standards are mandatory, optional or prohibited for a given environment. In other words, it is necessary to profile the protocols used, the schema and protocols associated with ancillary repository components, the certificates and the CRLs. Specifically, both certificates and CRLs include extensions that must be profiled to eliminate ambiguities and meaningfully specify particular uses for those extensions within a given target community or environment. The second thing that is required to help realize the goal of multi-vendor interoperability is to establish interoperability test scenarios and to conduct interoperability testing.

There are signs that market vendors, users, and solutions providers are cooperating to address interoperability in PKI and they are pooling their resources together to make their PKI products and systems operate with others. For example, Verisign, Microsoft, IBM, WebMthods, Entrust Technologies, Baltimore Technolongies and HP have announced plans to support a new XML-based key-management specifications dubbed XKMS. RSA and Baltimore Technologies have announced interoperability between their PKI products as well. It will take more time and some strong leaders in the area to emerge to finally put the interoperability issue to rest. And it is these types of efforts that will pave the way for widespread implementation of PKI.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

REFERENCES

Carlisle Adams & Steve Lloyd, *Understanding Public-Key Infrastructure, MacMillan Technical Publishing*, USA

National Institute of Standards and Technology (NIST) Project Team. "*Minimum Interoperability Standards for PKI Components, Version 2. Second Draft*. November 1998

NIST PKI Program, 23 February 2000. http://csrc.nist.gov/pki

PKCS. *Deploying a Public Key Infrastructure*, October 1999. IBM Corp.

PKI vendors push for interoperability; http://www.internetwk.com/story/INW20000825S0003

Public Key Infrastructure; see http://www.ietf.org/

Simple Public Key Infrastructure Charter; see http://www.ietf.org/rfc/rfc2692.txt

Vendors adding to PKI Interoperability; http://www.internetwk.com/news0199/news012299-8.htm

Wanted: PKI interoperability; http://www.nwfusion.com/archive/2001/119647_04-16-2001.html

© SANS Institute 2001, Author retains full rights

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**