WP8 D8.3
PKI Challenge (pkiC) - Recommendations for Vendors

Authors: David Tillemans, Chris Gilbert, Kevin Blackman

A two-year project

fully-funded by the European Commission and the Swiss Government

run by EEMA as part of a 13-strong management consortium

to solve the current interoperability problems associated with the deployment of Public Key Infrastructure (PKI) technology

www.eema.org/pki-challenge

The pkiC Management Consortium: -

Baltimore + Belgacom + Royal Mail + EEMA + GlobalSign + KPMG + Makra Security & Standards + SmartTrust + University of Leuven + University of Salford + Utimaco + WISeKey

An EEMA Project

The European Forum for Electronic Business

Funded by

European Commission

Swiss Government

Bundesamt für Bildung und Wissenschaft
Office fédéral de l'éducation et de la science
Ufficio federale dell'educazione e della scienza
Uffizi federal da scolaziun e scienza
Federal Office for Education and Science

Contents

1. Introduction

This paper is one of three papers that have emerged from the analysis of the results of the EU and Swiss government sponsored pkiC project. The purpose of the papers is to offer advice and guidance that will foster the deployment of interoperable PKIs and thus encourage the widespread adoption of PKI-supported trust. The other two papers make recommendations to PKI End Users and list the challenges that the PKI industry (Standards bodies, European Commission, users groups with an interest in this area, PKI Forum and other participants) must overcome. This paper is aimed at the manufacturers and vendors of PKI products.

2. Background

PKI Vendors have one of the toughest jobs in the PKI business. If the invention of the RSA algorithm can be taken as the true starting point of PKI then the Public Key Algorithms which form the foundations of the technology have existed for more than 25 years, while RFC 2459, a key standard which describes the structure and content of digital certificates and Certificate Revocation Lists (CRLs), was finalised only as recently as January 1999. PKI vendors have thus been required to develop and market their products during times of rapid and continual standards change.

Comprehensive PKI products need to implement all the relevant standards without sacrificing flexibility by selectively implementing only a subset of the standards. This makes a PKI product one of the most flexible but most complex pieces of software. The number of configuration options in PKI Systems can also lead to inconsistencies between implementations.

If properly implemented and configured, the standards should allow products from different vendors to interoperate.

This document considers the implications for the vendor community in the light of the conclusions of the pkiC and makes recommendations about the features and levels of support for standards that PKI products should exhibit to encourage interoperability between users of different vendors products. Section 3 deals with the issues that concern the PKI infrastructure components. Section 4 looks at the issues relating to Public Key Applications. Section 5 looks briefly at the list of standards involved.

3. Public Key infrastructure components

From a PKI Vendor point of view products are divided into two categories; the products that deliver the infrastructure and the products that use the infrastructure.

A Public Key infrastructure is needed for certificate management. Certificate management implies the creation, modification, revocation of certificates and their publication in some form of publicly accessible repository. When a certificate is revoked the Certificate Revocation List (CRL) is also published in a repository and, optionally, to an OCSP server.

The diagrams below show the main components of a PKI.

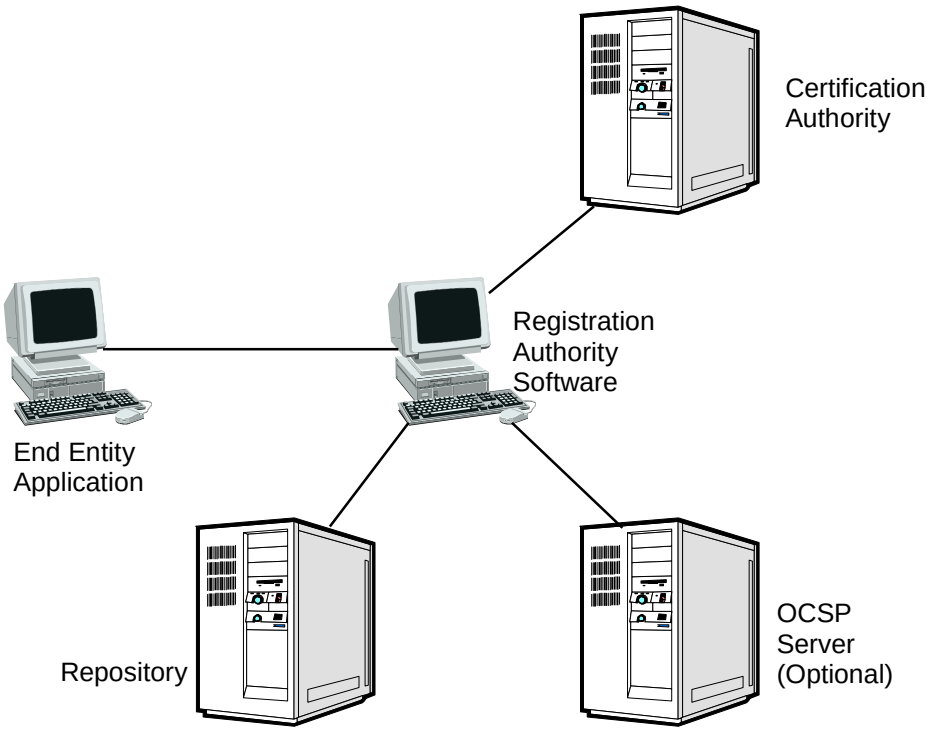

Figure 1 – PKI components for certificate management

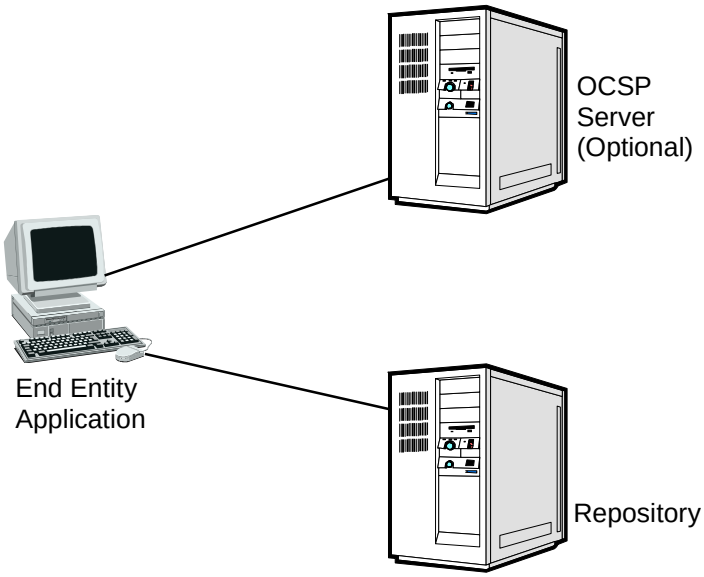

Figure 2 – PKI components for certificate validation

3.1. The Certification Authority

The Certification Authority (CA) is the central point of trust for all of the programs that rely on and trust this PKI (cfr RFC2510/RFC2511). It should create certificates that comply with X.509 v3 and with all of the extensions specified in RFC3280. Further requirements for certificates are specified by RFC3039, which defines the structure of Qualified Certificates as specified under the European Digital Signature Directive. Additionally, some customers will also need to define their own, custom extensions for special applications.

The CA should publish CRLs that conform to the X.509 v2 standard. This means that the vendor should support at least consolidated CRLs but also have the option to generate delta CRLs. It should also support the definition of additional CRL Distribution Points (CDPs) and the inclusion of these additional CDPs in certificates.

CAs play an important role in an organisation's security infrastructure and interaction with the system should only be done through a suitably certified system such as a Registration Authority (RA). CAs should only accept incoming messages from RAs. Outgoing messages to support, for example, the publication of certificates and CRLs should be possible but should be sent through an RA. This enables tighter control over access to the CA, which after all is the root of trust for the organisation's PKI.

Additionally, to create a trustworthy system, all actions carried out by a CA (e.g. certificate revocation or the addition of administrators) should be logged to allow auditing to take place. These audit logs must also be protected from tampering.

Recommendation

CA software should support the inclusion of additional CRL Distribution Points in certificates.

The pkiC reference implementation provided support for automatic cross certification and end entity (EE) enrolment by supporting both CMP and Simple CMC certificate management protocols. During testing, however, most of the Participants chose to implement cross certification through the manual exchange of PKCS#10 enrolment requests and PKCS#7 certificates and the project concluded that many products do not yet fully support automated cross certification.

Lack of support for automated cross-certification is not likely to be an issue for CAs. The actual process of producing a cross-certificate pair between organisations is just a small part of a lengthy legal process and would not necessarily benefit from automation anyway.

The lack of support for automated end entity enrolment is a bigger problem, particularly for CAs that plan to issue millions of certificates. Any process that requires manual intervention creates unacceptably high support costs. Some vendors have addressed this by providing proprietary client software but this locks the customer into a proprietary PKI architecture.

Anything that makes enrolment easy, particularly between different PKI products, would be a welcome step forward and should help to remove the barriers to adoption of digital certificates.

Recommendation

PKI vendors should support at least Simple CMC to allow automatic end entity enrolment.

3.2. The Registration Authority

The RA software is used to manage the CA and acts as an interface between it and the end user community. The RA officers, according to their roles, manage or verify the certification requests, revocation requests and certificate update requests, verify the contents of the issued certificates and check that CRLs are published properly.

Depending on the procedures defined by the CA operator, the RA can be a multifunctional system, which provides an interface between an organisation's identity management processes and its CA. The following examples of RA functionality are commonly found among PKI users in the business community:

- The RA can be a gateway that translates different incoming, possibly incompatible, PKI communications protocols to a commonly supported standard as defined by IETF (namely RFC2510bis and RFC2511bis).

- The RA interfaces with the repository system to publicise CRLs and CA certificates. If required the RA is also able to publish End Entity certificates.

- The RA System can write to Smart Cards when centralised key generation is required.

The pkiC did not observe any decoupling of CA and RA operations. There was no demand for support for stand-alone RA functionality.

3.3. The Repository

Ideally a PKI should support different kinds of standard repositories although without question the currently preferred repository is an X.500 directory service, accessed using the LDAP protocol. This position is by no means ideal and the pkiC document 'pkiC - Challenges for the PKI Industry' elaborates on the position of LDAP as a publication mechanism for the industry.

Some vendors have not yet implemented support for LDAPv3, despite the known issues with LDAPv2, for example:

- The mandatory-to-implement authentication mechanism between a client and the repository is based on Userid and password transmitted in the clear.
- A standard access control scheme does not exist.
- No standard mechanism for data replication between LDAP repositories exists.
- Search filters are considered to be inadequate.
- The X.500 attributes used to store PKI items such as Certificates and CRLs have more than one accepted method of naming them (i.e. either with or without the *;binary* description).

There is also a large number of interoperability problems caused by the structure and flexibility allowed in the Directory components, particularly in the Distinguished Name. This issue causes problems in the real world for both certificate and CRL retrieval.

There can be significant problems in locating the certificate repository, for both certificate and CRL retrieval. The base criteria for the pkiC were largely based on RFC2459, which was superseded by RFC3280 in April 2002. RFC3280 introduced extensions that allow the basic structure for X.509 certificates to provide information that allows relying software to locate the CA Issuers and the CA Repository. Interoperability testing using these extensions, the Authority Information Access – CA Issuer method, and the Subject Information Access – CA Repository method, should be pursued, and once successful widespread adoption should be encouraged.

Recommendations

Vendors should implement support for LDAPv3 as soon as possible.

All PKI systems should support the following minimum set of components in the Distinguished Name (DN):

- C (country)
- L (locality)
- O (organisation)
- OU (organisational unit)
- CN (common name)
- DC (domain component)

Any other components found in the DN should not cause a system failure.

Vendors should implement and test (with other vendors) the extensions introduced in RFC3280 that provide information for relying software to locate its CA Issuers and CA Repository.

3.4. Online Certificate Status Protocol

Online Certificate Status Protocol (OCSP) is a certificate validation service that is designed to overcome some of the issues associated with full CRL retrieval (e.g. where bandwidth is restricted).

RFC2560 describes three valid response models for OCSP. The OCSP response must be signed using a key that is one of the following:

1) The key that signed the certificate being checked i.e. the response is signed by the CA that issued the certificate being validated.
2) A key issued to an OCSP responder with an associated public certificate that has "OCSP-Signing" in the ExtendedKeyUsage extension. That certificate must be issued by the same CA that issued the certificate being validated.
3) A key that is valid within a local configuration of OCSP signing authority for the certificate being validated.

Model 3 is the one used by the pkiC Reference System, whereas model 2 is probably the most widely deployed / supported.

Recommendation

Those vendors that do not already support it should implement model 2.

4. Public Key Applications

The pkiC used S/MIME-enabled email clients to prove the trust established by the enrolment, cross certification and subordination exercises. The test process revealed a considerable number of interoperability issues between clients that are beyond the scope of the project to address but the issues encountered will be common to all PKI exploiting applications and are worthy of inclusion here.

To maximize the chances of interoperability an End Entity (EE) application should be capable of generating key pairs for enrolment purposes, it should also be able to manage a local repository into which it can publish local copies of trusted Root CA certificates, CRLs and correspondent's certificates.

4.1. Key Management

An EE application should at least be able to manage the user's credentials locally and may also offer the facility to manage them remotely, at the CA.

In the local context, key pairs generated for enrolment are most commonly encapsulated in the PKCS#10 format and signed. The resulting certificates are most commonly returned in PKCS#7 format. EE applications should thus understand and use both of these formats. EE applications that use smartcards should also understand PKCS#11 format.

In the remote context some applications allow the EE to revoke their own certificates with the CA that published them. Remote management of this kind requires the EE application to understand either PKIX-CMP or Certificate Management over CMS (CMC).

Recommendation

PKI-exploiting applications should understand and use PKCS#7, PKCS#10 and PKCS#11 file formats as well as supporting either PKIX-CMP or CMC.

4.2. Certificate Validation

A Public Key Application (PKA) should be able to:

- Retrieve CRLs from the repository using the appropriate protocol.
- Determine the status of a certificate using an OCSP service.
- Perform search queries on the directory to retrieve EE certificates for confidentiality.
- Perform search queries to retrieve CA certificates when validating the chain of trust.

Extensions in the certificates such as CRL Distribution Point (CDP), Authority Information Access (AIA) and Subject Information Access are the EE application's links and connections to the rest of the PKI. The EE application therefore should recognise and process these extensions.

Recommendation

PKI exploiting applications should be capable of performing LDAP searches on any LDAP-enabled directory.

PKI exploiting applications should understand the extensions in certificates that link the certificate to the infrastructure that supports it (i.e. crlDistributionPoint, authorityInformationAccess and subjectInformationAccess)

4.3. Local Repository Management

When an EE application uses the local repository (e.g. Microsoft Key and Certificate stores, Netscape Certificate Store) it should be able to perform limited management on its contents. Local management functions include storing, updating, and deleting personal, trusted Root CA and correspondent certificates and CRLs (unless restricted by policy).

Recommendation

An EE application should be able to perform basic content management on the local certificate store.

5. Applicable Standards

Vendors are faced with the daunting prospect of having to support a very large number of different standards due to the very wide and complex range of software products involved in PKI, all of which must work in an open market if interoperability is to be realised. Furthermore, given the lag in technology deployment that the PKI market exhibits vendors must also provide backward compatibility with some standards that have been superseded or otherwise rendered 'officially' redundant.

Recommendation

As a minimum, vendors should comply with the following list of standards

- RFC 2459 / RFC3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 2510: Internet X.509 Public Key Infrastructure Certificate Management Protocols
- Draft: RFC 2510bis: Internet X.509 Public Key Infrastructure Certificate Management Protocols
- RFC 2511: Internet X.509 Certificate Request Message Format
- RFC 2511bis: Internet X.509 Certificate Request Message Format
- RFC 2797: Certificate Management Messages over CMS
- RFC 1777: Lightweight Directory Access Protocol
- RFC 1823: The LDAP Application Program Interface
- RFC 2251: Lightweight Directory Access Protocol (v3)
- RFC 2252: Lightweight Directory Access Protocol (v3) : Attribute definition
- RFC 2253: Lightweight Directory Access Protocol (v3) : UTF-8 String Representation of Distinguished Names
- RFC 2254: Lightweight Directory Access Protocol (v3) : The String Representation of LDAP Search Filters
- RFC 2255: Lightweight Directory Access Protocol (v3) :The LDAP URL Format

- RFC 2559: Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2
- RFC 2587: Internet X.509 Public Key Infrastructure LDAPv2 Schema
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- Draft: Internet X.509 Public Key Infrastructure LDAP Schema for X.509 CRLs
- Draft: Internet X.509 Public Key Infrastructure LDAP Schema for X.509 Attribute Certificates
- Draft: LDAPv3 DN strings for use with PKIs
- RFC 3369: S/MIME
- PKCS#1: RSA Cryptography Standard
- PKCS#7: Cryptographic Message Syntax Standard
- PKCS#10: Certification Request Syntax Standard
- PKCS#11: Cryptographic Token Interface Standard
- PKCS#12: Personal Information Exchange Syntax Standard
- PKCS#15: Cryptographic Token Information Format Standard