PKI: Public Key Infrastructure Library
brief overview
-

Paolo Ottolino
(OPST CISSP-ISSAP CISA CISM ITIL)

12 gennaio 2012

Addressing
Thse simple notes were collected during my work experience in the PKI field. The following aspect are shortly treated:

1. General concepts: Functionalities
2. Architecture: Components
3. Certificates: Usages

Indice

Capitolo 1

Introduzione

1.1 Crittografia

Tempo medio necessario per un ■choosen cypher-text attack■:

- 1024: un anno
- 2048: 5-10 anni

PKCS#7: standard per la creazione della ■busta■:

- documento
- hash criptato del documento (con chiave privata)
- chiave pubblica

1.2 Trust Model

Diretto: si invia la chiave face-to-face. Il punto iniziale dovrebbe essere sempre questo. ATTENZIONE all'Auto-Enrollment (MS). Ci deve sempre essere:

- 1 persona fisica cui consegnare il certificato
- 1 persona fisica responsabile della emissione del certificato (referente, garante)

Third Party: ente terzo che attesta l'identità, analogamente e quanto si fa con il passaporto → Certification Authority. Eliminare tutte le CA che non vengono riconosciute (trusted). Occorrerebbe eliminare anche tutti i certificati che non vengono usati.

Da un punto di vista legale, chi accetta l'ingresso nella struttura di una un-trusted CA è responsabile delle relative conseguenze negative. Nel CP e CPS → Responsabile.

Extended Third Party: entità esterna che garantisce i trust reciproci di 2 entità in dominio di trust.

Network: CA - CA

Gerachica: CA - CA Root - CA

1.3 Il Certificato

E' il mezzo per effettuare il binding tra:

- chiavi pubblica e privata
- la persona cui si associa (controllo che sia vera)

Corrisponde ad un passaporto, contiene:

- Nome e Cognome (dati personali e NON riservati)
- Indirizzo
- Chiave Pubblica
- Serial Number
- Utilizzo possibile (e.g. chiave per firma, per autenticazione, cifratura, etc)
- Key Usage
- Extended Key Usage (un certificato non deve essere usato per uno scopo diverso da quello prefisso)
- Issuing Date (Data Inizio Validità)
- Expiring Date (Data Fine Validità)
- CA emittente

Tutto il Trust Model si basa sulla sicurezza della chiave privata della CA. Per questo la chiave privata viene messa in un HSM (Hardware Security Module), scatolotto bianco con led blu, compatibile FIPS3.

PKCS#7 (CA): in caso di CA, lo standard diviene:

- documento
- hash documento cifrato
- certificato mittente (Distinguished Name)
- certificato CA che garantisce il mittente

1.3.1 Estensioni

Devono essere controllate molto bene. Se l'applicazione legge un'estensione critica che non conosce, dovrebbe rigettare il certificato

1.4 PKI Core Services

1.4.1 Third Party Trusted Model (CA)

1.4.2 Emissione e Revoca (CRL) dei certificati

Di solito il tutto viene messo su un LDAP. Le CRL divengono grosse → Elevato Traffico di Rete. Per limitare il traffico, la CRL vale 24 ore o 12 ore. La responsabilità di non andare a rileggere la CRL è della macchina server.

Online Certification Status Protocol: fa una query unicamente per un singolo utente. Tiene storia dell'utilizzo dei certificati nei vari anni.

Trust Domain: tutti i certitificati emessi da una CA e gli utenti cui si riferiscono

1.4.3 Key Backup History & Recovery

Quando si cifra per un utente → perdita Private Key = impossibilità di decription

Key History: sulla chiave di cifra

Key Recovery: consente all'utente di eseguire il restore delle chiavi di cifra da utilizzare

Ovviamente occorre fare una gestione accurata degli accessi ai programmi: NON tutti gli utenti devono poter eseguire il restore

1.4.4 Update Automatico Chiavi e Certificati

Il client chiede alla CA con il PKXCMP l'update del certificato. Le sessioni CMP possono essere autenticate a fronte di certificati.

1.4.5 Trust Model Complessi

Cross-Certification (PKCS#10, PKXCMP, manuale)

- unilaterale
- bilaterale

Per effettuare il trust di CA di produttore diverso → PKCS#10.

1.4.6 Gestione Trasparente del Certificato

L'aggiornamento e la gestione del certificato è trasparente all'utente.

1.5 Policy

Documenti che attestano, descrivono e regolano l'utilizzo che si intende fare dei certificati in azienda. Essi sono identificati tramite un meccanismo analogo ai MIB dell'SNMP. Per avere il numero:

- IANA (gratis ma numero molto lungo)
- ...

1.5.1 Certificate Policy

Limiti di utilizzo del certificato → Documento Tecnico-Legale (e.g. limitata a firmare, connessione SSL, con transazioni non superiori a ..., etc).

1.5.2 Certification Practice Statement

Modo di Operazione → Documento Tecnico

1.6 Catalogazione Certificati

I certificati possono essere catalogati, sul S.O., secondo i seguenti criteri:

- Account
- Service
- Computer

ovvero:

- Account
- Revocation List
- CA

1.7 Acronimi

CA: Registration Authority

CDP: CRL Distribution Point

CMS: Card Management System

CRL: Certificate Revocation List

CPS: Certificate Provider Server

CSP: Certification Service Provider

LDAP: Lightweight Directory Access Protocol

LDIF: LDAP Data Interchange Format

PKI: Public Key Infrastructure

PKIX-CMP: PKI Exchange Certificate Management Protocol

RA: Registration Authority

SEP: Secure Exhange Protocol

Capitolo 2

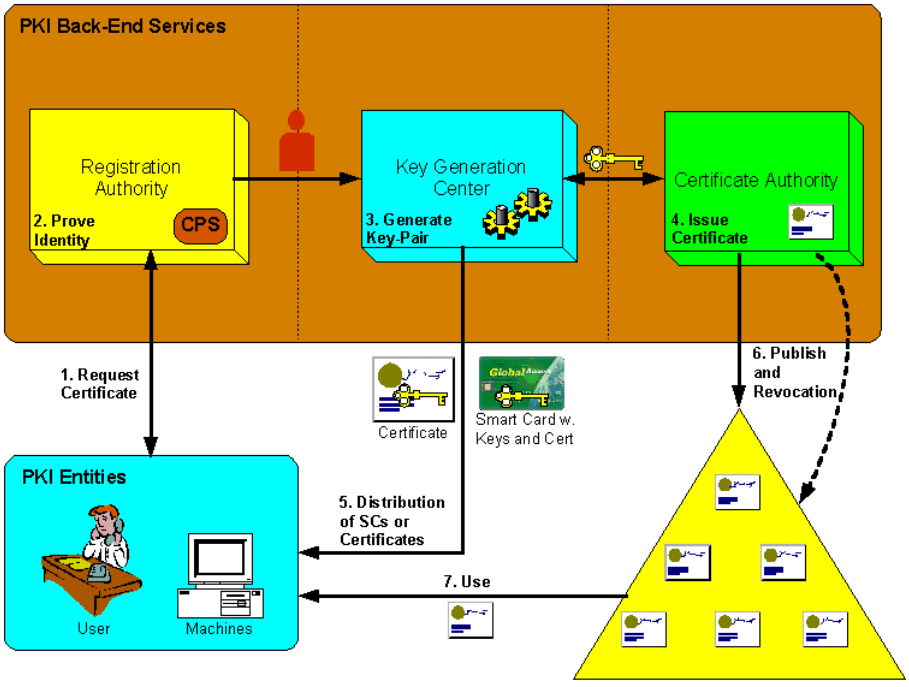
Componenti

2.1 Core Architecture

A PKI should be composed at least by the following components:

- CA: Certification Authority
- RA: Registration Authority
- LDAP: Directory Server
- Client: whatever application used by the final user

The communications happen via the proper PKI protocols. In the following picture a simple arcthitecture:



2.1.1 CA

In the PKI it is the core component that issues digital certificates. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that

is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate.
It encompasses also the Key Generation Center.

2.1.2 RA

In the PKI it is an authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it. That is, the RA acts like the user interface to the CA.

2.1.3 Directory Service

Each user has an entry. Each entry contains a list of:

- attribute - value

as defined in the template. The Direcotry server is used by many applications. The CA harvest only PKI-useful entries.
The certificate could be written in the LDAP.
Users perform "Anonymous Bind" to read attributes.
The standard X.500 was published in 1993.

2.1.3.1 Scalability

For a multi LDAP, the following mechanisms should be allowed:

Shadowing: information replication on other directory server

Chaining: referral to a external domain directory server

Referral: referral to another directory server

Binding: ?

Base Search: identification of the point to be used as the root of the sub-tree to perform the reach on.

2.1.3.2 Security Policy

The policies are created during installation phase. In the LDAP the policy templates are stored. Common templates are:

- End User
- Security Officer

The policies are signed with CA ceritifcate. The users download the policies, in order to understand which task they could perform.
The policies define:

Constraints: general permissions

Roles: permissions granted to the users

2.1.3.3 LDAP & CA

CA accesses LDAP server in read-write, in order to store information. CA could not work without LDAP, so proper High Availability should be configured. Usually this is obtained through "Directory Master - Directory Shadow" configuration.

2.1.4 Protocols

In order to perform cross-component communications, the following protocols are used:

Protocol	Port	Description
SEP	**709**	**old PKIXCMP version**
ASH	**710**	**Authentication**
PKIXCMP	**829**	
XAP	**443**	**XML Application Protocol**

2.2 Applicativi a Corredo

Non sono indispensabili ma aiutano a facilitare le operazioni di amministrazione.

2.2.1 Web Administration

GUI di amministrazione della CA, sviluppata su Web. (Parla con ASH). Presenta i seguenti componenti:

Admin Center: interfaccia utente

Authorization Service: implementazione degli Access Control secondo quelle che sono le policy di CA

Mapping Service: associa al nome il DN del certificato

Vengono eseguite le seguenti operazioni

Client Side Operation: operazioni che vengono compiute lato utente

Zero Footprint Side Operation: operazioni di firma, senza avere applicazioni della PKI installate

Time Stamping: marca temporale di qualche evento

2.2.2 Web RA

GUI di amministrazione della RA sviluppata su web

2.2.2.1 Auto-RA

COme la RA ma SM e AC vengono gestite automaticamente dalla CA e valgono per un tempo minore dei consueti 3 gg.

2.2.3 Verification Server

XML Key Management Specification (XKMS) uses the web services framework to make it easier for developers to secure inter-application communication using public key infrastructure (PKI). XML Key Management Specification is a protocol developed by W3C which describes the distribution and registration of public keys. Services can access an XKMS compliant server in order to receive updated key information for encryption and authentication.

2.2.4 Proxy Server

Proxy tra user e CA per poter fare le operazioni correnti (Key Update, etc) e non far fare agli utenti sessioni sulla CA. Generalmente viene usato il CMP imbustato nell'HTTP.

Capitolo 3

Certificati

I certificati costituiscono l'entità atomica (il file, per intenderci) nel quale è effettuata la mappatura di congiunzione tra:

- identità: Common Name della persona, dell'ente o della applicazione
- chiave assegnata: nel certificato è contenuta la sola chiave pubblica, distribuibile
- utilizzi consentiti: attributi che illustrano gli usi che è possibile fare della chiave (es. cifratura, non ripudio, firma, etc)

Vediamo nel dettaglio la forma che assumono i certificati ed il contenuto presente in essi.

3.1 Forma

The certificate takes the shape issued by:

- Standard ITU 509. Published by ISO.
- RFC 3280
- Internet X.509: Internet Public Key Infrastructure Certificate (and CRL)

3.1.1 Certificate Types

There are a lot of certificate types, new types could be defined. The most common are:

End User: CA signed, binding between Entity and Certificate

CA: self signed, it contains the key for integrity verification of the certificate in itself

Link: it allows for verification after a CA certificate update. Usually, two types:

- old-with-new
- new-with-old

Cross: it is for trust cross-relation among between different CAs

3.2 Contenuto

Contiene dati, organizzati in diversi campi (attributo:valore), i cui valori sono espresso come ObjectID.

3.2.1 Basic Fields

Issuer Name: univoco nel mondo

DC: Domain Component (guaranted by IANA)
CN: Common Name

Serial Number: univoco per l'Issuer

Validity: perchè l'algoritmo criptografico non dura per sempre

Not Before
Not After

Subject: certified entity

DC= ...
CN= ...

Version: versione del certificato (binaria o esadecimale)

Signature Algorithm: algoritmo di firma (e.g. SHA1 with RSA)

Subject Public Key Info:

Public Key Algorithm: used algorithm
RSA Public Key: esponente (es. 1024 bit)
Modulus: modulo (1024 bit)

Distinguish Name: for directory authentication, used also for certificates (Relative DN)

C: Country (it)
O: Organization (tim)
OU: Organization Unit (root)
OU: Organization Unit 2
CN: Common Name

ASN.1: the certificate

3.2.2 Extension Fields

Additional Information, useful for security management. The extension could be:

- normal: informative (it is analogous to status bit in Computer Technology set off: normal usage, not critical one)
- critical: the application should be able to search it, identify and treat. If a wrong value is contained the application should discard the certificate acting as "no authenticated"

CRL Distribution Point: it provides indication where to download CRL for each user. It is mandatory. The CDP could not be changed → Critical Extension. It uses the same syntax of Alternative Name:

- https: uniformResourceIdentifier
- ldap: directoryName

Partioned CRL: CRL is splitted among users

Combined CRL: MS compatibility (no list increase)

Delta CRL: workaround. It contains differs

Key Usage: multiple value could be instructed (only non-Repudians needs to be alone, by law).

DigitalSignature: signature without legal force

nonRepudians: strong signature

KeyEncipherment: cyphering (simmetric key)

DataEncypherment: cyphering (asimmetric key)

KeyCertSign: certificate signature (for CA)

CRLSign: CRL signature (for CA)

Key Usage Period: limitation to the usage period of the certificate, before the expiration.

Extended Key Usage: Key Purpose

id-kp-timestamping: for make stronger KeyCertSign

id-kp-serverAuth: for https authentication server

id-kp-clientAuth: https client authentication

id-kp-codeSigning: code signing

Basic Contraints: specification on user or CA certificate.

Issuer(Subject) Alternative Name: additional identification mode

otherName: user principal name

rfc822Name: email

dNSName:

x400Address:

directoryName:

ediPartyName:

uniformResourceIdentifier:

iPAddress:

registeredID:

Authority Key Identifier: Hash of CA public key (for mutual trust)

Subject Key Identifier: Hash of the subject public key (for speeding up calculation)

Certificate Policies: CA Policy Identifier

Policy Mappings: for cross-certificates rule mapping among the 2 different policies

Policy Contraints: rules for policy validation

Subject Directory Attribute: corresponding to GCOS fields. Possible to add special pointers to user specific policy

3.3 CRL

The CRL contains the following info:

Header:

Version:

Signature Algorithm:

Issuer: (C, O, OU, OU, CN)

Last Update

Next Update

CRL Extension:

x509v3AuthorityKeyID:

x509CRLNumber: for Delta CRL

Revoked Certificates:

SerialNumber:

RevocationDate:

CRLReasonCode: one of the following reasons are allowed:

- Key Compromise
- Cessation of Operation
- Certificate Hold (temporary suspension)
- Superseded

3.4 Other Certificates

Qualified Certificate: a special certificate in which a only usage is allowed

Attribute Certificate: special certificate to provide additional info (e.g. company roles) to be used in the authorization phase (that is, after authentication)