

PKI

Milan Sova, CESNET

EuroCAMP, Porto, 2005-11-07

Public Key Infrastructure

- Public key cryptography
 - pair of keys
 - public key (encryption, signature verification)
 - private key (decryption, signing)
- Infrastructure
 - binding public keys to identities
 - public keys management
 - revocation, key usage...

PKI Architectures

- PGP
 - everybody can provide identity assertions
 - "Web of trust"
- X.509
 - defines roles for entities
 - separated identity providers (Certificate Authorities)
 - hierarchical management of trust

X.509 PKI

X.509 PKI Roles

- Certificate Authority
 - certificate issuer
- Registration Authority
 - identity vetting
- End Entity
 - private key holder
- Relying Party (“user”)
 - relies on the certificate

X.509

Certificate

X.509 Certificate - Content

- public key
- validity
- subject names
- issuer names
- key usage restrictions
- operational information
 - serial number, standard version, policies, CDP, AIA
- issuer signature

X.509 Certificate - Structure

```
Certificate ::= SEQUENCE {
    tbsCertificate      TBSCertificate,
    signatureAlgorithm  AlgorithmIdentifier,
    signatureValue      BIT STRING }
```

```
TBSCertificate ::= SEQUENCE {
    version             [0] EXPLICIT Version DEFAULT v1,
    serialNumber        CertificateSerialNumber,
    signature           AlgorithmIdentifier,
    issuer              Name,
    validity            Validity,
    subject             Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
    issuerUniqueID      [1] IMPLICIT UniqueIdentifier OPTIONAL,
    subjectUniqueID    [2] IMPLICIT UniqueIdentifier OPTIONAL,
    extensions          [3] EXPLICIT Extensions OPTIONAL
}
```

X.509 Certificate - Structure

Version ::= INTEGER { v1(0), v2(1), v3(2) }

CertificateSerialNumber ::= INTEGER

Validity ::= SEQUENCE {
 notBefore Time,
 notAfter Time }

Time ::= CHOICE {
 utcTime UTCTime,
 generalTime GeneralizedTime }

UniqueIdentifier ::= BIT STRING

SubjectPublicKeyInfo ::= SEQUENCE {
 algorithm AlgorithmIdentifier,
 subjectPublicKey BIT STRING }

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Validity

- notBefore
- notAfter
 - dates

Naming

- Distinguished Name (Subject, Issuer)
 - sequence of sets of attribute-value pairs
 - highly structured, hierarchical
 - **looks** like a globally unique ID
 - in fact just an "opaque string"

Naming 2

- using existing managed name systems
 - DNS
 - RFC822
 - IP Addresses
- **subjectAltName**
 - { DNS: host1.domain.tld,
 - DNS: host2.domain.tld,
 - email: admin@domain.tld,
 - IPAddress: 1.2.3.4 }

X.509 Certificate - Names

...

subject:

cn=myserver, o=myOrg, dc=myDomain, dc=org

...

subjectAltName: {

DNS: host1.domain.tld,

DNS: host2.domain.tld,

IPAddress: 1.2.3.4

}

...

Key Usage Restrictions

- keyUsage (BIT STRING)
 - 0 digitalSignature
 - 1 nonRepudiation
 - 2 keyEncipherment
 - 3 dataEncipherment
 - 4 keyAgreement
 - 5 keyCertSign
 - 6 cRLSign
 - ...

Key Usage Restrictions 2

- extendedKeyUsage (OID)
 - 1.3.6.1.5.5.7.3.1 TLS server authentication
 - 1.3.6.1.5.5.7.3.2 TLS client authentication
 - 1.3.6.1.5.5.7.3.3 code signing
 - 1.3.6.1.5.5.7.3.4 email protection
 - ...
 - 1.3.6.1.5.5.7.3.0 Any usage

Key Usage Restrictions 3

- basicConstraints
 - CA (boolean)
 - true in CA certs
 - false in EE certs (or no basicConstraints at all)
 - path length (if CA == true)
 - maximum of non-self-issued intermediate certificates in path

X509. Certificate - Key Usage

...

```
[basicConstraints: {critical,  
  CA: false},]
```

...

```
keyUsage: {critical,  
  101 (digitalSignature,  
    keyEncipherment)},
```

...

```
extendedKeyUsage: {non-critical,  
  1.3.6.1.5.5.7.3.1 (tLSServerAuth)}
```

...

Operational Information

- version (v3)
- serial number
- Certificate Policies
 - OID, qualifiers
- CRL Distribution Points
 - access to CRL (URL)
- Authority Information Access
 - OCSP URL

X.509 CRL

&

Revocation

Certificate Revocation List

- version (v2)
- issuer
- this update
 - time of issuance
- next update
 - expected next issuance
- revoked certificates
- signature

CRL Extensions

- CRL Extensions
 - Authority Key Identifier
 - CRL Number
- CRL Entry Extensions
 - Reason Code
 - Invalidity Date

On-line Certificate Status Protocol

- request
 - certificate ID
- response
 - status
 - good, revoked, unknown
 - signature

X.509 CA

as

Identity Provider

Role of CA/RA

- identity vetting [CA/RA]
 - **ALL** names (Subject, subjectAltName)
- Proof Of Possession (of the private key) [CA/RA]
 - access to the private key (sign/decrypt)
 - PK delivery
- revocation [CA/RA]
- publishing (CP, CPS, CRL, OCSP...)
- Certificate Policy & Certificate Practice Statement

Common Myths

Subject Content

“Subject must contain

C, ST, L, O, OU, CN, Email”

- no rules for Subject names
- keep as short as possible
- use DC naming
- use `subjectAltName` for email

Hostname in CN

“CN must contain FQDN for host verification”

- obsolete, never standardized
- use `subjectAltName` for FQDN
 - RFC 3280, 2818, 2595

One Valid Certificate per Subject

“There may be at most one valid certificate for any given subject”

- OpenSSL implementation flaw
- overlapping validity intervals when re-keying
- different key usages

nonRepudiation vs. authentication

“One can use (commercial = high quality) qualified digital signature certificates for authentication”

- authentication = signing server provided challenge
- user has no control over the challenge

PKI & IdM

Naming

- X.500 global namespace is not managed
 - problems using Subject for identities
- alternative names (subjectAltName)
 - using existing managed namespaces
- DC naming (Subject, Issuer)

Private Key Management

- software tokens
 - quality of encryption
 - copyable
- hardware tokens
 - expensive
- site storages
 - only authentication keys (no non-repudiation)
- short-lived certificates

X.509 Certificate as Identity Assertion

- all required content
- cryptographically strong
- compact, small
- ubiquitous tools to handle
- rich “historical experience”

References

RFC 3280. Certificate and Certificate Revocation List (CRL) Profile

RFC 2560. Online Certificate Status Protocol – OCSP

RFC 3647. Certificate Policy and Certification Practices Framework

RFC 2247. Using Domains in LDAP/X.500

References

X.501. Information Technology – Open Systems
Interconnection - The Directory: Models, 1993.

X.509. Information Technology - Open Systems
Interconnection – The Directory: Authentication
Framework

X.520. Information Technology – Open Systems
Interconnection - The Directory: Selected
Attribute Types