openHPI – Confidential Communication in the Internet

Certificate Standards

Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

Digital Certificates – Introduction

- In a **PKI** (Public Key Infrastructure), verifiable bindings between the PKI users and their public keys are established with the help of **digital certificates**
- To be able to work with digital certificates on the various systems, they must be standardized
- **Standards for certificates** are therefore an essential part of PKI standards
  - The **X.509** certificate format has become widely used because of its application in various PKI standards (X.509, PKIX, ISIS-MTT)
  - Other certificate formats are also in use, e.g. with **OpenPGP**

X.509 Certificates
X.509v1 Certificates

1988: First version of the X.509 certificates

- X.509v1 certificate has seven fields:
  - **Version number**
  - Certificate **serial number** - unique among all certificates of a CA
  - OID (e.g. RSA, DSA, ...) of the **signature procedure** with which the certificate is signed
  - **Name of the CA** that signed the certificate
  - **Name of the certificate holder** following the X.500 naming convention
  - **Public key** of the certificate holder
  - **Validity** period of the certificate (start and end date)

X.509 Certificates
X.509v2 Certificates

1993: Second version of the X.509 certificates

- **Innovation** in this version:
  - Additional fields:
    - **unique identification** of the certificate holder (important when names coincite)
    - unique identification of the CA
  - In practice without meaning:
    - Most X.509 implementations do not use these fields
    - PKIX and ISIS-MTT recommend to leave fields empty – coincidence of name is otherwise avoided

X.509 Certificates
X.509v3 Certificates (1/3)

Shortcomings with X.509v1 and X.509v2:

- X.500 **naming convention** is to restrictive, e.g. email addresses cannot be used as names
- No conclusions can be drawn to the **intended use** of a public key, e.g. no possibility of distinguishing between keys used for encryption and used for verification of signatures
- No statement about the **Certificate Policy** of the CA possible
- …

X.509 Certificates
X.509v3 Certificates (2/3)

1996: X.509v3

X509.v3 specifies a syntax for defining new fields, so-called "**Extensions**":

- An **Extension** contains a text field indicating whether the extension is critical or non-critical
  - software that cannot deal with a **critical** extension of a certificate considers it invalid
  - unknown **non-critical** extensions are simply skipped
- Extension mechanism is very flexible and future-proof, but makes it difficult to read
- …

X.509 Certificates
X.509v3 Certificates (3/3)

To support compatible implementations in 1997 a **standard extension** was defined with additional fields:

- Identification of the **key of the CA**
  - CA may use multiple keys
- Identification of the **certificate holder key**
  - possibly it is certified several times
- Intended use of the key, e.g. encryption or signature
- …

X.509 Certificates
X.509 Certificate Standard

- **X.509** is one of the most **important** crypto standards ever
- X.509 certificates have found **widespread use**
- Development of the standard at a very early stage explains the immature nature and the initial problems
- The loosely defined standard leaves scope for interpretation, which is the reason that X.509 implementations are often incompatible

Certificate Management

To manage the use of certificates at **Certificate Management Protocols** – **CMP** – are available in PKIX standard, using the usual Internet protocols: HTTP, FTP, TCP, or email

Certificate Management Tasks:

- CA initialization
  - generation and protection of the private key of the trust centers
- Generation of certificates, e.g.
  - for new PKI users
- Publication of certificates and revocation lists:
  - regulates information exchange between CA and certificate server

Certificate Management
Key Recovery

For several reason there it would be **desired to recovery encryption keys**

- Recovery of private keys, e.g. to decrypt messages
- Key recovery is useful/necessary, e.g. for the authorized subsequent decryption of company data

But key recovery is **very problematic** as misuse is possible

Requirement

- Storage of keys in a highly secure environment
- Precise definition necessary, who/when/how/under which circumstances a key may be restored

But: German signature law prohibits trust centers to store keys used for signing...

Certificate Management
Key Revocation

Revocation of keys is urgently necessary if keys are compromised. In hierarchical PKIs this can be easily implemented

Reasons for key revocation according to **X.509 standard**:

- Key Compromise
- CA Compromise
- Modification of the content of the certificate
- Exchange against new certificate
- Retirement of the PKI user
- Suspension (or: temporary suspension)