
Public Key Infrastructure

Cryptography Four

Ed CrowleyA

Fall '09

Topics

- Public Key Infrastructure
- Intro
- PKI Architecture
- Trust Models
- Components
- X.509 Certificates
- X.500
- LDAP

Public Key Infrastructure Defined

A public key infrastructure (PKI):

- Binds public keys to entities
- Enables other entities to verify public key bindings
- Provides the services needed for ongoing management of keys in a distributed system.

-- NIST 800-32

Provides confidence that:

- The person or process identified as sending the transaction is actually the originator.
- The person or process receiving the transaction is the intended recipient.
- Data integrity has not been compromised.

Public Key Infrastructure

- Public key infrastructure enables enterprises to protect the security of their communications and business transactions on networks.
 - An enterprise-wide network security architecture, PKI integrates:
 - Digital certificates
 - Public key cryptography
 - Certification authorities.
 - Facilitates specific security services including:
 - Public key exchange
 - User authentication
 - Nonrepudiation.



Public Key Infrastructure Issues

Specific Public Key Infrastructure (PKI) issues include:

- Key Authentication and Non-repudiation
 - Nothing about a key proves to whom it belongs
- Revoking keys
 - Nothing about a key indicates whether it has been revoked
- Policy enforcement
 - Any organization utilizing PKI needs to create and enforce a local policy.

PKI Architecture Overview

- PKI architecture consists of:
 - A Trust Model
 - Servers (Certificate, Revocation, Registration)
 - Certificates/Data format standards
 - Public key mechanism standards
 - Related infrastructure including
 - Programs
 - Protocols
 - Policies and Procedures
- All components work together to enable trusted and secure communications.

Three PKI Trust Models

1. Hierarchical Trust

- ❑ Sets up an independent certificate authority (CA) with authority to sign digital certificates.
- ❑ A CA can revoke a certificate
- ❑ Facilitates enforcement of a local policy
- ❑ Most complex, most efficient trust model

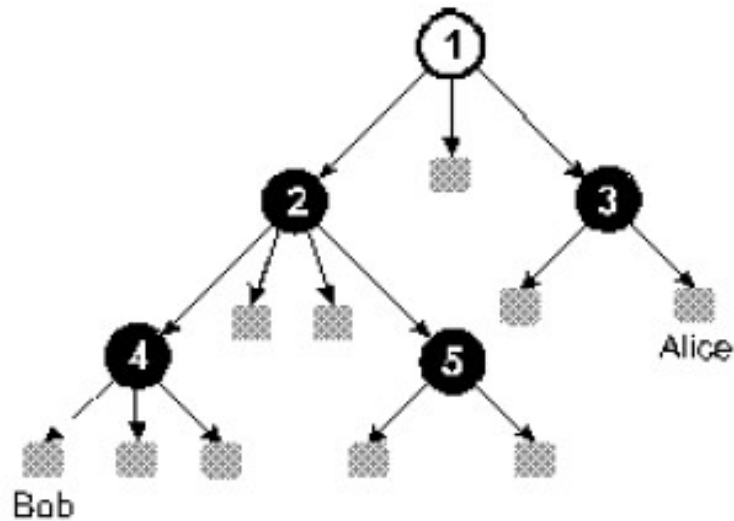
1. Web of Trust

- ❑ Random trust chains produce a network of signed keys.
- ❑ Invented by Phil Zimmerman -- Used by PGP

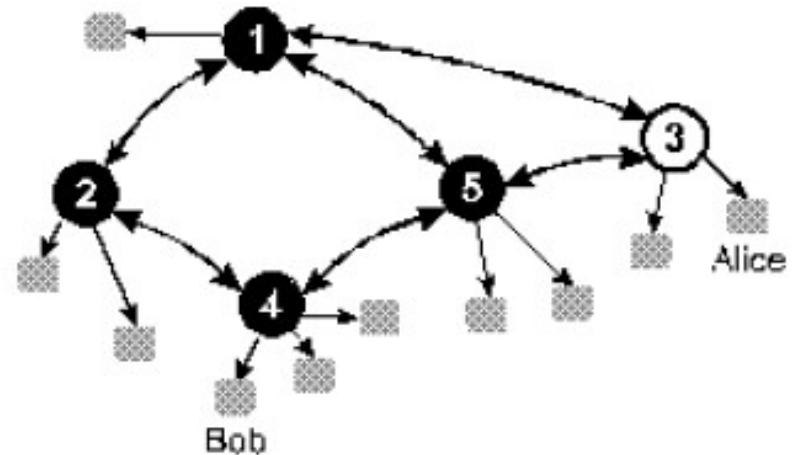
1. Direct Trust

- ❑ Each person confirms their authenticity by personally delivering their public keys

Traditional PKI Trust Architectures



a. hierarchical infrastructure



b. mesh infrastructure

Figure 1. Traditional PKI Architectures

PKI Web Model

- A form of hierarchical trust, in which there are many independent CAs.
- Cross Certification
 - Allows two CAs to exchange certificates with one another.
 - An alternative to cross certification is a CA hierarchy with a root authority at the top

PKI Support Infrastructure

- Includes
 - Certificates
 - X.509 Standard
 - Certificate Authority
 - Trusted entity that maintains and issues digital certificates.
 - Registration Authorities
 - Performs certificate registration duties
 - Acts as a broker between users and CA
 - Certificate revocation process
 - CA maintains a Certificate Revocation List (CRL)
 - Local Policies and Procedures
 - Non-repudiation service
 - Digital Signature

Certificate Servers

- Certificate servers validate, or certify, keys.
- A certificate server holds a large number of:
 - Certificates
 - Associated data sets
 - Revocation lists
- Three data structures
 1. Certificates
 2. Certificate revocation lists
 3. Attribute certificates.
- Include:
 - Certificate Authorities
 - Registration Authorities

Directory Services

- A directory server could hold and make available data such as email addresses, telephone numbers etc. ready for retrieval by company employees.
- X.500 is a directory services standard based on the ISO/OSI model developed by the ITU.
 - Many organizations choose the TCP/IP based LDAP

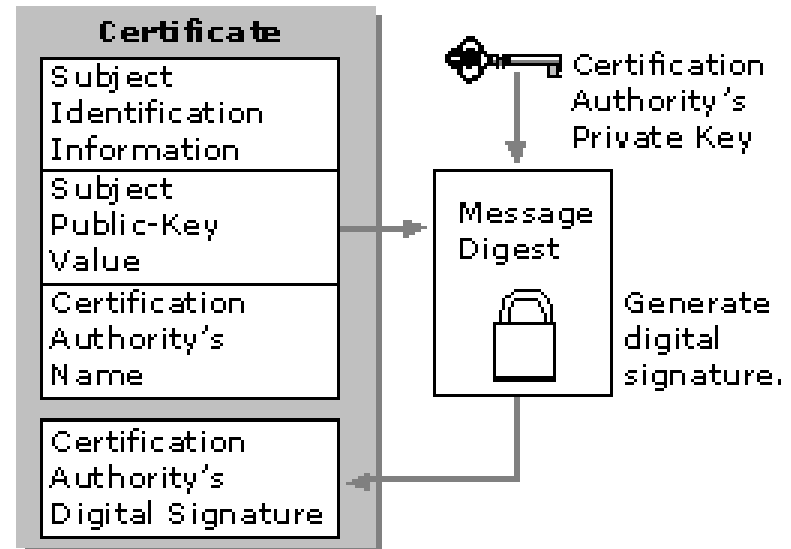
X.509 Certificate Standard

- ITU/CCITT X.509
 - X.500 component
 - Initially intended to provide X.500 authentication
 - Produced by a ISO and ITU collaboration
- Describes digital certificate format.
 - Several versions.
- PKIX – IETF working group
 - Specifies protocols for managing digital certificates as well as protocols for their use.
 - RFC 2459

Public Key Certificates

Sample digital certificate components

1. Public key
2. Certificate attributes
 - ◆ “Identity” information about user, including name, user ID...
1. One, or more, digital signatures from the Certificate Authority.



Certificate

The screenshot shows a web browser's 'Page Info' window with the 'Security' tab selected. The window is titled 'Certificate Viewer: "shop.pacsun.com"'. It displays the following information:

- Web Site Identity Verified:** The web site shop.pacsun.com supports authentication for the page you are viewing. The identity of this web site has been verified by VeriSign Trust network, a certificate authority you trust for this purpose.
- View:** A button to view the security certificate that verifies this web site's identity.
- Connection Encrypted: High-grade Encryption (RC4 128 bit):** The page you are viewing was encrypted before being transmitted over the Internet. Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

The right-hand pane of the Certificate Viewer shows the following details:

- Certificate Hierarchy:**
 - Bufltn Object Token/Verisign Class 3 Public Primary Certification Authority
 - OU=www.verisign.com/CPS Incorp. by Ref. LIABILITY LTD. (CN=VeriSign,OU=VeriSign,OU=www.verisign.com)
- Certificate Fields:**
 - Validity
 - Not Before
 - Not After
 - Subject
 - Subject Public Key Info
 - Subject Public Key Algorithm
 - Subject's Public Key** (highlighted)
 - Extensions
 - Certificate Basic Constraints
- Field Value:**

```
30 81 83 02 81 21 00 ba 19 23 06 b8 36 62 38 f4
c0 e7 83 a2 68 d7 bc 34 49 14 2f 99 2f 3c 72 84
f9 07 10 04 dc 07 89 1e 4b 88 88 3a 71 28 cf 0d
2b db 22 f8 0a 95 de 06 d1 4b cb 3c ea 24 1b ea
a3 0d 93 62 cb be c3 47 dc fc 63 4c 3a d0 1e 82
15 05 f1 6c 55 47 32 dd 11 1f 39 a9 7e bc 52 4e
12 af aa 1f 24 dc 78 fc 9e 41 e4 24 bd 05 0b d6
b0 38 34 40 42 0b 6e ef 8c a3 1a b9 41 c4 92 e5
f3 aa eb 70 d0 9d 58 02 03 01 00 01
```

PKI Attributes

Can also include:

- Timestamping
- Lightweight Directory Access Protocol (LDAP)
 - Security concerns include availability and integrity of LDAP servers
- Security enabled applications
- Cross certification.

LDAP

- An OSI protocol, designed to be lighter (faster) than Directory Access Protocol (DAP).
 - TCP/IP based
 - Uses Internet address
- Evolved from a protocol to a directory services standard.
- Most important certificate server standard
 - While NDS and Active Directory may be used as certificate servers, LDAP is used most often.

Certificate Revocation Process

- Utilizes Certificate Revocation Lists (CRLs)
 - A revocation list is a signed list (usually signed by CA) in which the serial numbers of revoked certificates are detailed.
- A revocation list is replaced by an updated version from the Trust Center at regular intervals, or as necessary.
 - Validity period determined by Trust Center
 - Usually one day

Attribute Certificate

- A data structure that resembles a PKI key certificate but does not contain a public key.
- Normally an adjunct to a key certificate.
- Rarely used.

PKI Applications

- SSL
- VPN
- E-mail encryption
- File encryption
- SAP R/3
- Single Sign On (SSO)
- SET
- Others

SET

- Secure Electronic Transaction
 - Because it uses certificates, considered a PKI application
 - Level 7 protocol
 - Developed by a consortium including Cybercash, MasterCard and Visa.
- Provides confidentiality for purchases by encrypting the payment information.
- Covers end to end transactions.

Questions?

References

NIST Special Publications

<http://csrc.nist.gov/publications/PubsSPs.html>