
Cryptography

PKI, *and* Digital Signatures

Topics

- Cryptography
 - Services
 - Digital Signature Process
 - Public Key Infrastructure
 - Certificates
-

Cryptographic Services Review

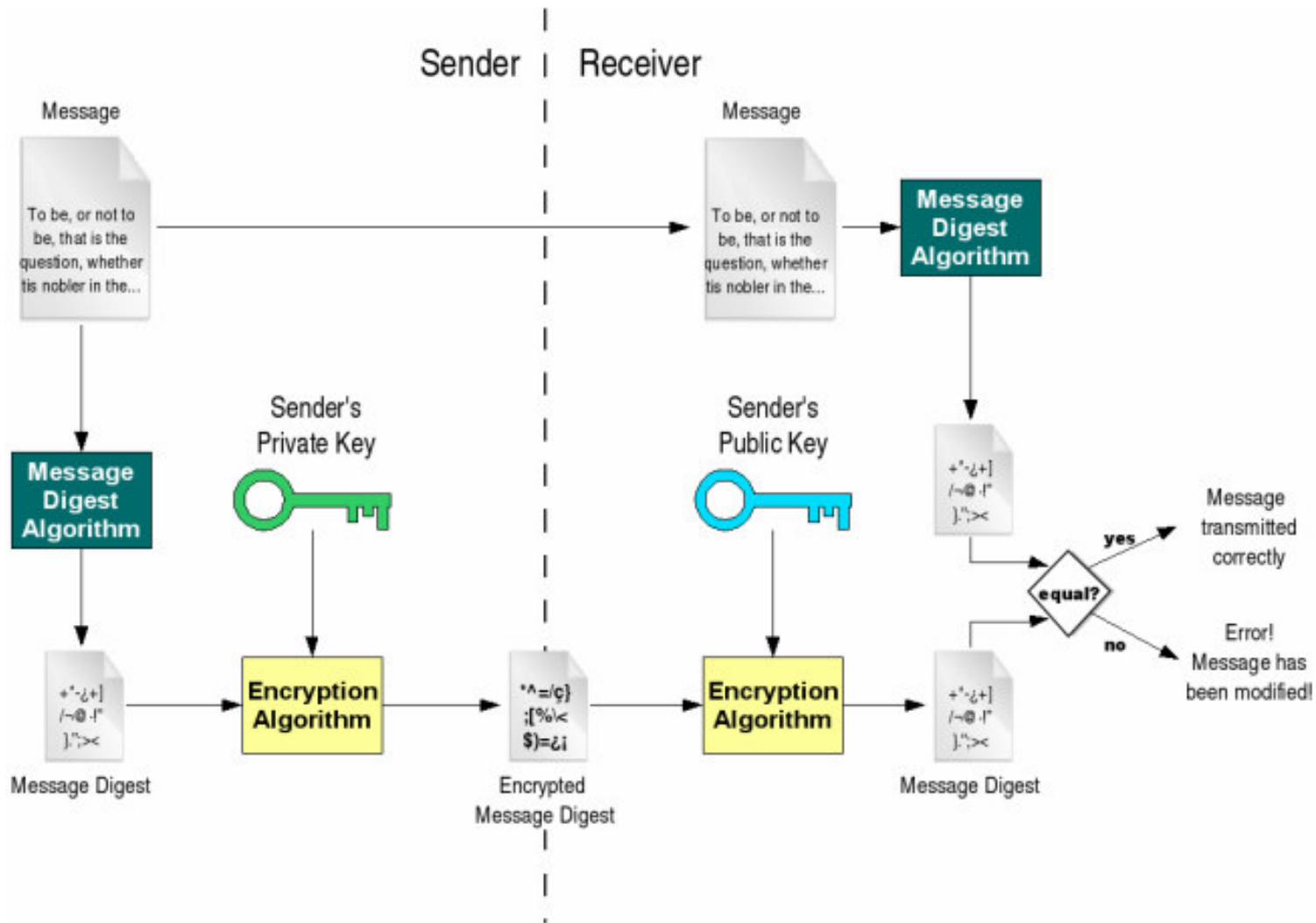
- Confidentiality -- Encryption
 - Only authorized people –e.g., the sender and recipient of a message, not eavesdroppers – can know the message.
 - Integrity – Message Digests (MAC or MIC), and Digital Signatures
 - When Bob receives a message, he can be sure that it was not modified en route after Alice sent it.
 - Authentication – PKI and Digital Signatures
 - When Bob receives a message that purports to be sent by Alice, Bob can be sure that the message was really sent by Alice.
 - Nonrepudiation – MAC and Digital Signatures
 - Alice cannot later deny that the message was sent.
 - Bob cannot later deny that the message was received.
-
- *Note: cryptography is not concerned with availability.*

Authentication and NonRepudiation

Goals and Process

- Authentication verifies that a message came from whom it is represented to come from.
 - Non repudiation provides evidence so that a message can not be disavowed at a later time.
 - Process utilizes a secret known to only one person (private key).
 - Methods include digital signatures.
-

Digital Signature Process



Public Key Infrastructure Defined

Digital Key Signatures are part of a Public Key Infrastructure (PKI) that:

- 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
 - All components work together to enable trusted and secure communications.
-

PKI Hierarchical Trust Model

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

Note

- ❑ *There are other trust models such as PGP's web of trust*
-

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
-

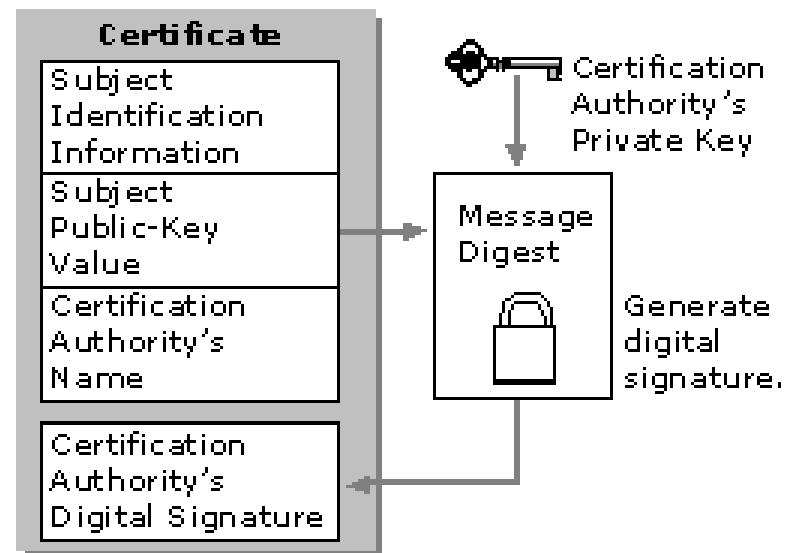
X.509 Certificate Standard

- 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...
3. One, or more, digital signatures from the Certificate Authority.



Example Certificate

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](#) 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.

Certificate Viewer: "shop.pacsun.com"

Certificate Hierarchy

- Bufltn Object Token/Verisign Class 3 Public Primary Certification Authority
 - OU=www.verisign.com/CPS Incorpor. by Ref. LIABILITY LTD. (CN=VeriSign,OU=VeriSign,shop.pacsun.com)

Certificate Fields

- Validity
 - Not Before
 - Not After
- Subject
- Subject Public Key Info
 - Subject Public Key Algorithm
 - Subject's Public Key**
- Extensions
 - Certificate Basic Constraints

Field Value

```
30 81 83 02 81 21 00 ba 19 23 26 b8 36 62 38 f4
c0 e7 33 a2 68 d7 bc 34 49 14 2f 39 2f 3c 72 84
e9 07 10 0d 4c 07 89 1e 4b 88 38 3a 71 28 cf 0d
2b d8 22 f8 0e 38 d8 06 d1 4b cb 3c ea 24 1b ea
a3 0d 33 62 cb be c3 47 dc fc 63 4c 3a d0 1e 8f
15 05 21 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 f5 0b d6
b0 38 34 40 42 0b 6a ef 8c a3 1a b8 41 c4 92 e5
f3 aa eb 70 d0 3d 58 02 03 01 00 01
```

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
-

Questions?

Selected References

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

http://en.wikipedia.org/wiki/Digital_signature

http://www.simonsingh.net/Crypto_Corner.html

<http://www.schneier.com/>
