

Week 15

INTERNET SECURITY PROTOCOLS AND STANDARDS
INTERNET AUTHENTICATION APPLICATIONS

Chapter 22

Internet security protocols and standards

MIME and S/MIME

MIME

Extension to the old RFC 822 specification of an Internet mail format

- RFC 822 defines a simple heading with To, From, Subject
- Assumes ASCII text format
- Provides a number of new header fields that define information about the body of the message

S/MIME

- Secure/Multipurpose Internet Mail Extension
- Security enhancement to the MIME Internet e-mail format
 - Based on technology from RSA Data Security
- Provides the ability to sign and/or encrypt e-mail messages

S/MIME Functions

Enveloped
data

Encrypted
content
and
associate
d keys

Signed data

Encoded
message
+ signed
digest

Clear-signed
data

Cleartext
message
+
encoded
signed
digest

Signed and
enveloped
data

Nesting of
signed
and
encrypted
entities

Enveloped Data

Default algorithms used for encrypting S/MIME messages are AES and RSA

- S/MIME generates a pseudorandom secret key that is used to encrypt the message using AES or some other conventional encryption scheme
- A new pseudorandom key is generated for each new message encryption
- This session key is bound to the message and transmitted with it
- The secret key is used as input to the public-key encryption algorithm, RSA, which encrypts the key with the recipient's public RSA key
- On the receiving end, S/MIME uses the receiver's private RSA key to recover the secret key, then uses the secret key and AES to recover the plaintext message
- If encryption is used alone, radix-64 is used to convert the ciphertext to ASCII format

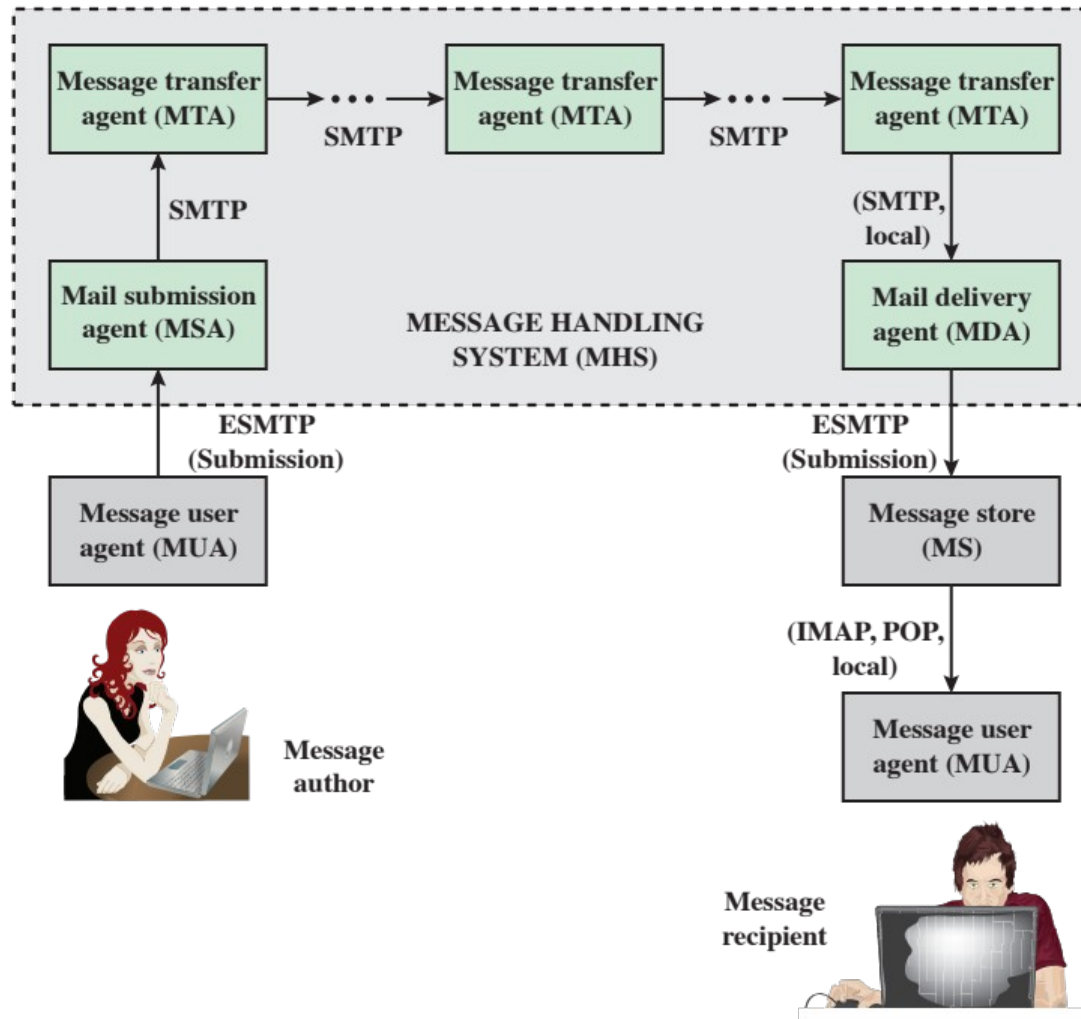
Signed/Clear-signed Data

The preferred algorithms used for signing S/MIME messages use either an RSA or a DSA signature of a SHA-256 message hash

The process works as follows:

- Take the message you want to send and map it into a fixed-length code of 256 bits using SHA-256
- The 256-bit message digest is unique for this message making it virtually impossible for someone to alter this message or substitute another message and still come up with the same digest
- S/MIME encrypts the digest using RSA and the sender's private RSA key
- The result is the digital signature, which is attached to the message
- Now, anyone who gets the message can recompute the message digest then decrypt the signature using RSA and the sender's public RSA key
- Since this operation only involves encrypting and decrypting a 256-bit block, it takes up little time

Internet Mail Architecture



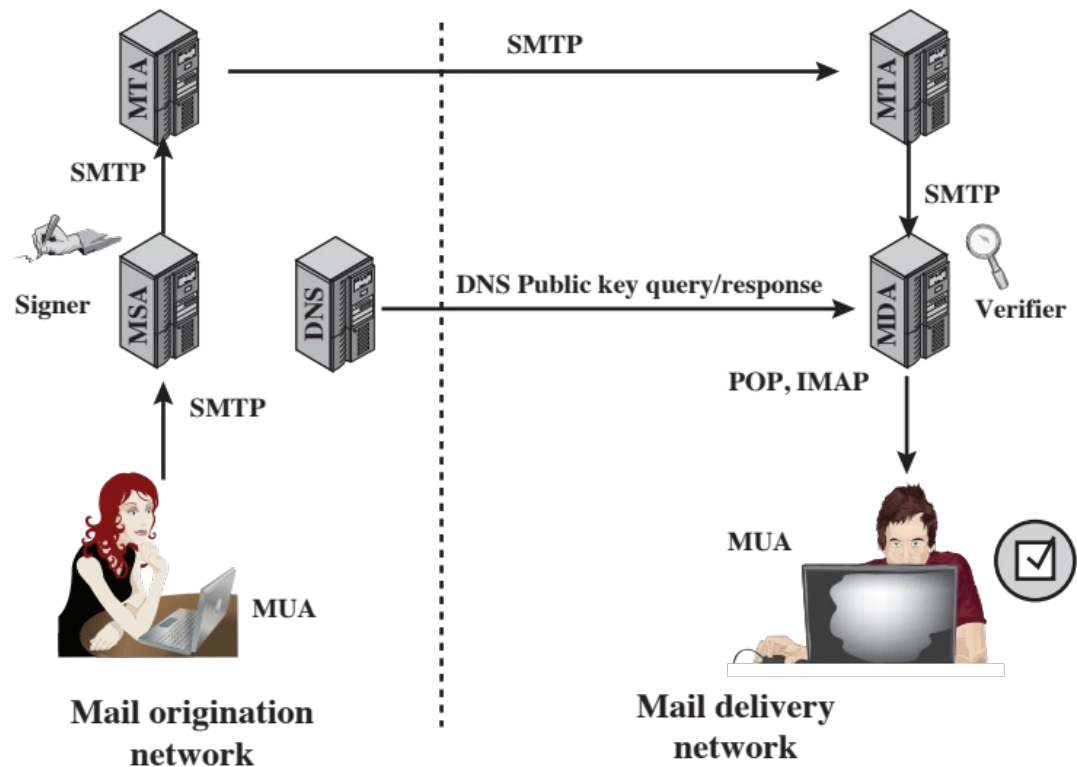
**Figure 22.2 Function Modules and Standardized Protocols
Used Between Them in the Internet Mail Architecture**

Domain Keys Identified Mail (DKIM)

Specification of cryptographically signing e-mail messages permitting a signing domain to claim responsibility for a message in the mail stream

Proposed Internet Standard (RFC 4871: DomainKeys Identified Mail (DKIM) Signatures)

Has been widely adopted by a range of e-mail providers



DNS = domain name system
MDA = mail delivery agent
MSA = mail submission agent
MTA = message transfer agent
MUA = message user agent

DKIM Deployment

Figure 22.3 Simple Example of DKIM Deployment

Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

- ▢ One of the most widely used security services
- ▢ General-purpose service implemented as a set of protocols that rely on TCP
- ▢ Subsequently became Internet standard RFC4346: Transport Layer Security (TLS)

Two implementation choices:

Provided as part of the underlying protocol suite

Embedded in specific packages

TLS Concepts

TLS SESSION

- ▢ An association between a client and a server
- ▢ Created by the Handshake Protocol
- ▢ Define a set of cryptographic security parameters
- ▢ Used to avoid the expensive negotiation of new security parameters for each connection

TLS CONNECTION

- ▢ A transport (in the OSI layering model definition) that provides a suitable type of service
- ▢ Peer-to-peer relationships
- ▢ Transient
- ▢ Every connection is associated with one session

Alert Protocol

Conveys TLS-related alerts to peer entity

Alert messages are compressed and encrypted

Each message consists of two bytes:

First byte takes the value warning (1) or fatal (2) to convey the severity of the message

Second byte contains a code that indicates the specific alert

If the level is fatal, TLS immediately terminates the connection

Other connections on the same session may continue, but no new connections on this session may be established

Handshake Protocol

Most complex part of TLS

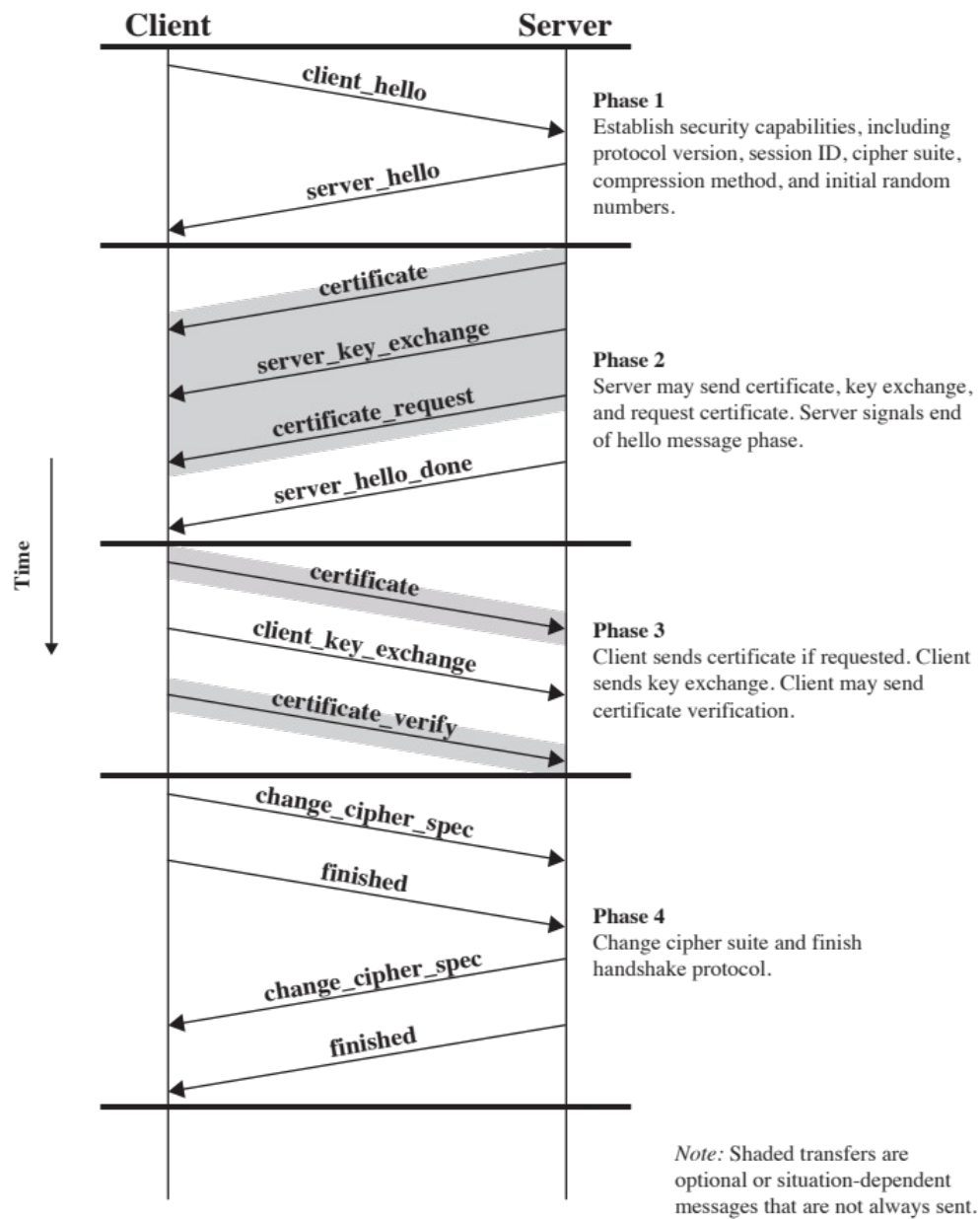
Is used before any application data are transmitted

Allows server and client to:



Comprises a series of messages exchanged by client and server

Exchange has four phases



Handshake

Figure 22.6 Handshake Protocol Action

Heartbeat Protocol

A periodic signal generated by hardware or software to indicate normal operation or to synchronize other parts of a system

Typically used to monitor the availability of a protocol entity

Defined in 2012 in RFC 6250

Runs on top of the TLS Record Protocol

Use is established during Phase 1 of the Handshake Protocol

Each peer indicates whether it supports heartbeats

Serves two purposes:

- Assures the sender that the recipient is still alive
- Generates activity across the connection during idle periods , which avoids closure by a firewall that does not tolerate idle connections.

SSL/TLS Attacks

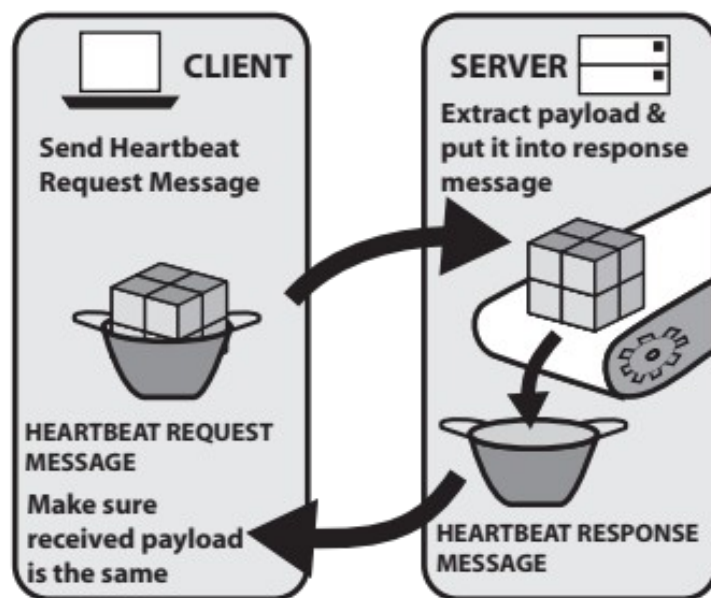
**Attacks on the
Handshake Protocol**

**Attacks on the record
and application data
protocols**

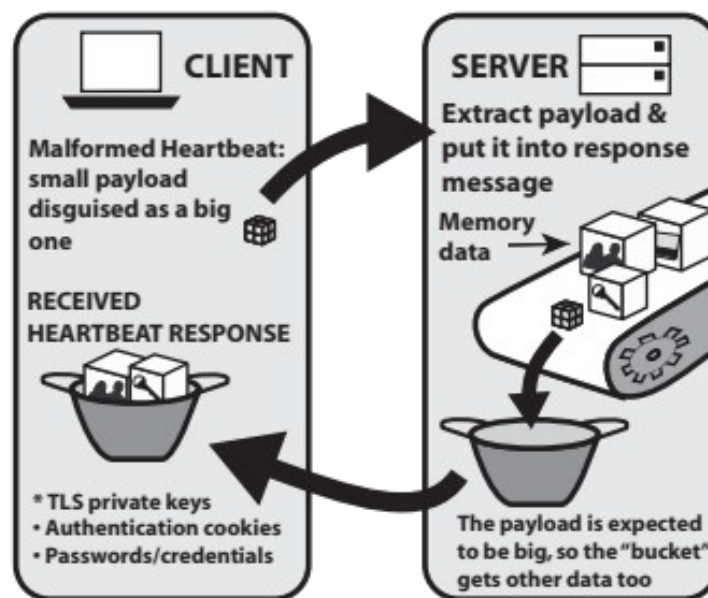
**Four general
categories:**

Attacks on the PKI

Other attacks



(a) How TLS Heartbeat Protocol works



(b) How TLS Heartbleed exploit works

Heartbleed

Figure 22.7 The Heartbleed Exploit
Source: BAE Systems

HTTPS (HTTP over SSL)

- ❑ Combination of HTTP and SSL to implement secure communication between a Web browser and a Web server
- ❑ Built into all modern Web browsers
- ❑ ~~Search engines do not support HTTPS~~
- ❑ URL addresses begin with https://
- ❑ Documented in RFC 2818, HTTP Over TLS
- ❑ Agent acting as the HTTP client also acts as the TLS client
- ❑ Closure of an HTTPS connection requires that TLS close the connection with the peer TLS entity on the remote side, which will involve closing the underlying TCP connection

IP Security (IPsec)

- ❑ Various application security mechanisms
 - ❑ S/MIME, Kerberos, SSL/HTTPS
- ❑ Security concerns cross protocol layers
- ❑ Would like security implemented by the network for all applications
- ❑ Authentication and encryption security features included in next-generation IPv6
- ❑ Also usable in existing IPv4

Benefits of IPsec

- ❑ When implemented in a firewall or router, it provides strong security to all traffic crossing the perimeter
- ❑ In a firewall it is resistant to bypass
- ❑ Below transport layer, hence transparent to applications
- ❑ Can be transparent to end users
- ❑ Can provide security for individual users
- ❑ Secures routing architecture
- ❑ <https://www.youtube.com/watch?v=doSW8d2iLFM>

Scope of IPsec

Provides two main functions:

- A combined authentication/encryption function called Encapsulating Security Payload (ESP)
- Key exchange function

VPNs want both authentication and encryption

Also an authentication-only function, implemented using an Authentication Header (AH)

- Because message authentication is provided by Encapsulating Security Payload (ESP), the use of AH is included in IPsecv3 for backward compatibility but should not be used in new applications

Specification is quite complex

- Numerous RFC's 2401/4302/4303/4306

Security Associations

A one-way relationship between sender and receiver that affords security for traffic flow

- If a peer relationship is needed for two-way secure exchange then two security associations are required

Is uniquely identified by the Destination Address in the IPv4 or IPv6 header and the SPI in the enclosed extension header (AH or ESP)

**Defined by 3
parameters:**

Security Parameter
Index (SPI)

IP Destination Address

Protocol Identifier

Transport and Tunnel Modes

TRANSPORT MODE

- ▢ Extends to the payload of an IP packet
- ▢ Typically used for end-to-end communication between two hosts
- ▢ ESP encrypts and optionally authenticates the IP payload but not the IP header

TUNNEL MODE

- ▢ Provides protection to the entire IP packet
- ▢ The entire original packet travels through a tunnel from one point of an IP network to another
- ▢ Used when one or both ends of a security association are a security gateway
- ▢ A number of hosts on networks behind firewalls may engage in secure communications without implementing IPsec

Chapter 23

Internet Authentication Application

Kerberos Overview

- ❑ Initially developed at MIT
- ❑ Software utility available in both the public domain and in commercially supported versions
- ❑ Issued as an Internet standard and is the defacto standard for remote authentication
- ❑ Overall scheme is that of a trusted third party authentication service
- ❑ Requires that a user prove his or her identity for each service invoked and requires servers to prove their identity to clients

Kerberos Protocol

Involves clients, application servers, and a Kerberos server

- Designed to counter a variety of threats to the security of a client/server dialogue
- Obvious security risk is impersonation
- Servers must be able to confirm the identities of clients who request service

Use an Authentication Server (AS)

- User initially negotiates with AS for identity verification
- AS verifies identity and then passes information on to an application server which will then accept service requests from the client

Need to find a way to do this in a secure way

- If client sends user's password to the AS over the network an opponent could observe the password
- An opponent could impersonate the AS and send a false validation

Kerberos Protocol

<https://www.youtube.com/watch?v=5N242XcKAsM>


Watch first 5 minutes

Kerberos Performance Issues

Larger client-server installations



Very little performance impact in a large-scale environment if the system is properly configured



Kerberos security is best assured by placing the Kerberos server on a separate, isolated machine



Motivation for multiple realms is administrative, not performance related

Certificate Authority (CA)

Certificate consists of:

- A public key with the identity of the key's owner
- Signed by a trusted third party
- Typically the third party is a CA that is trusted by the user community (such as a government agency, telecommunications company, financial institution, or other trusted peak organization)

User can present his or her public key to the authority in a secure manner and obtain a certificate

- User can then publish the certificate or send it to others
- Anyone needing this user's public key can obtain the certificate and verify that it is valid by way of the attached trusted signature

X.509

Specified in RFC 5280

The most widely accepted format for public-key certificates

Certificates are used in most network security applications, including:

- IP security (IPSEC)
- Secure sockets layer (SSL)
- Secure electronic transactions (SET)
- S/MIME
- eBusiness applications

Alternatives

Conventional (long-lived) certificates

- CA and “end user” certificates
- Typically issued for validity periods of months to years

Short-lived certificates

- Used to provide authentication for applications such as grid computing, while avoiding some of the overheads and limitations of conventional certificates
- They have validity periods of hours to days, which limits the period of misuse if compromised
- Because they are usually not issued by recognized CA's there are issues with verifying them outside their issuing organization

Proxy certificates

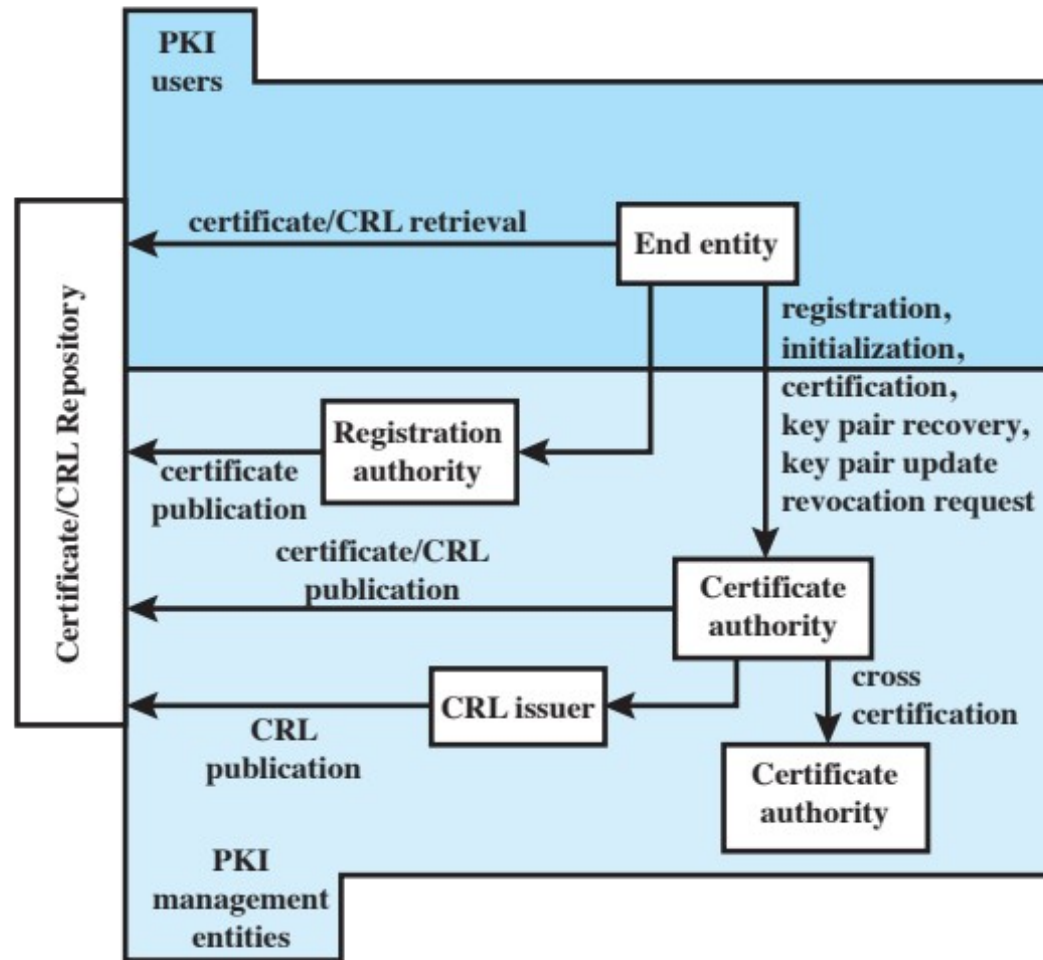
- Widely used to provide authentication for applications such as grid computing, while addressing some of the limitations of short-lived certificates
- Defined in RFC 3820
- Identified by the presence of the “proxy certificate” extension
- They allow an “end user” certificate to sign another certificate
- Allow a user to easily create a credential to access resources in some environment, without needing to provide their full certificate and right

Attribute certificates

- Defined in RFC 5755
- Use a different certificate format to link a user's identity to a set of attributes that are typically used for authorization and access control
- A user may have a number of different attribute certificates, with different set of attributes for different purposes
- Defined in an “Attributes” extension

Public-key Infrastructure

- The set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography
- Developed to enable secure, convenient, and efficient acquisition of public keys
- “Trust store”
 - A list of CA’s and their public keys



PKIX Architectur al Model

Figure 23.4 PKIX Architectural Model