Kerberos
Key Distribution Center (KDC) 

(1) $ID_A \parallel ID_B \parallel N_1$

Key distribution steps

(2) $E(K_a, [K_s \parallel ID_A \parallel ID_B \parallel N_1])$
   $\parallel E(K_b, [K_s \parallel ID_A])$

(3) $E(K_b, [K_s \parallel ID_A])$

Authentication steps

(4) $E(K_s, N_2)$

(5) $E(K_s, f(N_2))$ 

Figure 14.3 Key Distribution Scenario
1. User logs on to workstation and requests service on host.

2. AS verifies user's access right in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.

3. Workstation prompts user for password to decrypt incoming message, then send ticket and authenticator that contains user's name, network address and time to TGS.

4. TGS decrypts ticket and authenticator, verifies request then creates ticket for requested application server.

5. Workstation sends ticket and authenticator to host.

6. Host verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, server returns an authenticator.

Figure 15.1 Overview of Kerberos
Figure 15.3 Request for Service in Another Realm
Certificates and PKI
Certificates

Created by a trusted Certification Authority (CA) and have the following elements:

- Version
- Serial number
- Signature algorithm identifier
- Issuer name
- Period of validity
- Subject name
- Subject’s public-key information
- Issuer unique identifier
- Subject unique identifier
- Extensions
- Signature
Figure 14.16  X.509 CA Hierarchy: a Hypothetical Example
Figure 14.15 X.509 Formats
Federated Identity Management
Figure 15.4 Generic Identity Management Architecture
Figure 15.5 Federated Identity Operation

1. End user's browser or other application engages in an authentication dialogue with identity provider in the same domain. End user also provides attribute values associated with user's identity.

2. Some attributes associated with an identity, such as allowable roles, may be provided by an administrator in the same domain.

3. A service provider in a remote domain, which the user wishes to access, obtains identity information, authentication information, and associated attributes from the identity provider in the source domain.

4. Service provider opens session with remote user and enforces access control restrictions based on user's identity and attributes.
The Extensible Markup Language (XML)

A markup language that uses sets of embedded tags or labels to characterize text elements within a document so as to indicate their appearance, function, meaning, or context.

The Simple Object Access Protocol (SOAP)

Enables applications to request services from one another with XML-based requests and receive responses as data formatted with XML.

WS-Security

A set of SOAP extensions for implementing message integrity and confidentiality in Web services.

Security Assertion Markup Language (SAML)

An XML-based language for the exchange of security information between online business partners.
SSL / TLS
Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Phase 4
Change cipher suite and finish handshake protocol.

Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

Figure 17.6 Handshake Protocol Action
Figure 17.3 SSL Record Protocol Operation