UNIT V E-MAIL, IP & WEB SECURITY 9

E-mail Security: Security Services for E-mail-attacks possible through E-mail - establishing keys privacy-authentication of the source-Message Integrity-Non-repudiation-Pretty Good Privacy-S/MIME. IPSecurity: Overview of IPSec - IP and IPv6-Authentication Header-Encapsulation Security Payload (ESP)-Internet Key Exchange (Phases of IKE, ISAKMP/IKE Encoding). Web Security: SSL/TLS Basic Protocol-computing the keys- client authentication-PKI as deployed by SSLAttacks fixed in v3-Exportability-Encoding-Secure Electronic Transaction (SET).

PART-A

1. **What is tunnel mode in IPsecurity? Apr/May'15**

   Tunnel Mode

   1. It provide the protection for entire IP Packet
   2. ESP in this mode encrypt authenticate the entire IP packet.
   3. AH in this mode authenticate the e tire IP Packet plus selected portion of outer IP Header.

2. **List out the services provided by PGP. May/June'13**
   - Digital signature
   - Message encryption
   - Compression
   - E-mail comp tibility

3. **Expand and define SPI. May/June'13**

   Security Parameter Index (SPI)

   A 32-bit unsigned integer assigned to this SA and having local significance only. The SPI is carried in **Authentication Header (AH)** and **Encapsulating Security Payload(**ESP) headers to enable the receiving system to select the security association (SA) under which a received packet will be processed.

4. **Define: SET. Nov/Dec'2013.**

   Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transactions on the Internet.
   - ✓ Confidentiality of information
   - ✓ Integrity of data
   - ✓ Cardholder account authentication
   - ✓ Merchant authentication

5. **What are the different types of MIME? Nov/Dec'12**
   - Text
     - Plain and Enriched
   - Multipart
     - Mixed
     - Parallel

- Alternative
- Digest

- Message
  - rfc822.
  - Partial
  - External-body.
- Image (jpeg and gif)
- Video mpeg MPEG format.
- Audio (Basic)
- Application (PostScript Adobe Postscript format).

6. What protocol comprises SSL? Nov/Dec'12

SSL is a general-purpose service implemented as a set of protocols that rely on TCP.

7. Why does ESP include a padding field? May/June'2012

Padding- Variable length, 0 to 255bytes.Padding may be required, irrespective of encryption algorithm requirements, to ensure that the resulting cipher text terminates on a 4 byte boundary. Specifically, the Pad length and Next header fields must be right aligned within a 4 byte word to ensure that the Authentication data field, if present, is aligned on a 4 byte boundary. Pad length. 8 bits. Specifies the size of the Padding field in bytes.

8. Define TLS.(IT2352 / May/June'12)

TLS is an IETF standardization initiative whose goal s to produce an Internet standard version of SSL. TLS is defined as a Proposed Internet Standard in RFC 5246. RFC 5246 is very similar to SSLv3.The TLS Record Format is the same as that of the SSL Record Format, and the fields in the header have the same meanings. The one difference is in version number.

9. What do you mean by S/MIME? (IT2352 / May/June'12)

Secure/Multipurpose Internet Mail Extension is an Internet standard approach to e-mail security that corporates the same functionality as PGP.Secure/Multipurpose Internet Mail Extension (S/MIME) is a security enhancement to the MIME Inter et e-mail format standard based on technology from RSA Data Security. PGP a d S/MIME are on an IETF standards track.

10. Mention four SSL protocols. (Apr/May'11)

- SSL Handshake P otocol
- SSL Change Cipher Spec Protocol
- SSL Alert Protocol
- HTTP

- SSL Record Protocol
- TCP and IP

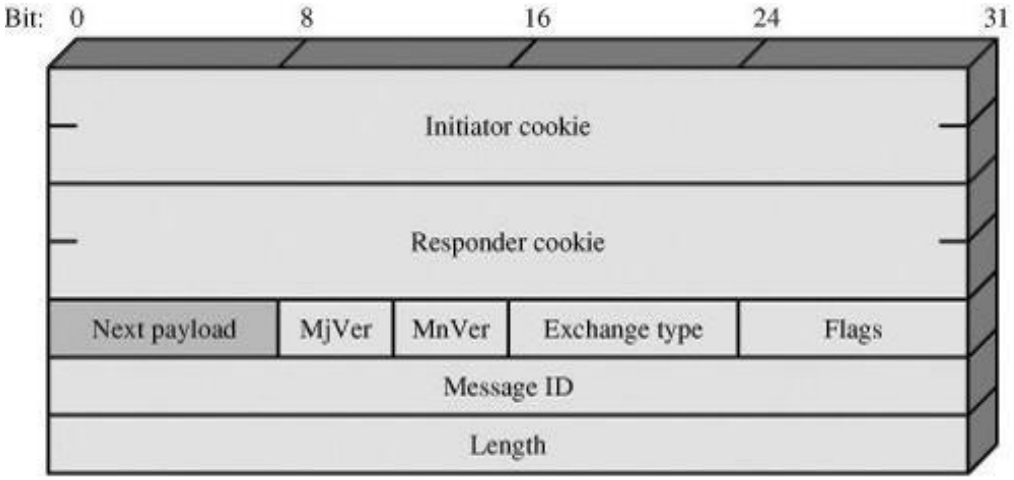
11. Mention the fields of IPSec authentication header. (Apr/May'10)

- Next Header Length
- Security Parameters Index (SPI)
- Sequence Number
- Authentication Data

12. Why the leading two octets of digest are stored in PGP messages along with encrypted message digest? (R-2004) (Apr/May'08)

Leading two octets of message digest: L,to enable the recipient to determine if the correct public key (K(A)e) was used to decrypt the message digest for authentication, by comparing this plain text copy of the f rst two octets with the first two octets of the decrypted digest. These octets also serve as a 16 bit frame check sequence for the message, for the authentication and error detection.

13. Draw the header format for an ISAKMP message. May/June'2007



(a) ISAKMP header

1. PREETY GOOD PRIVACY

Pretty Good Privacy

Definition of PGP:

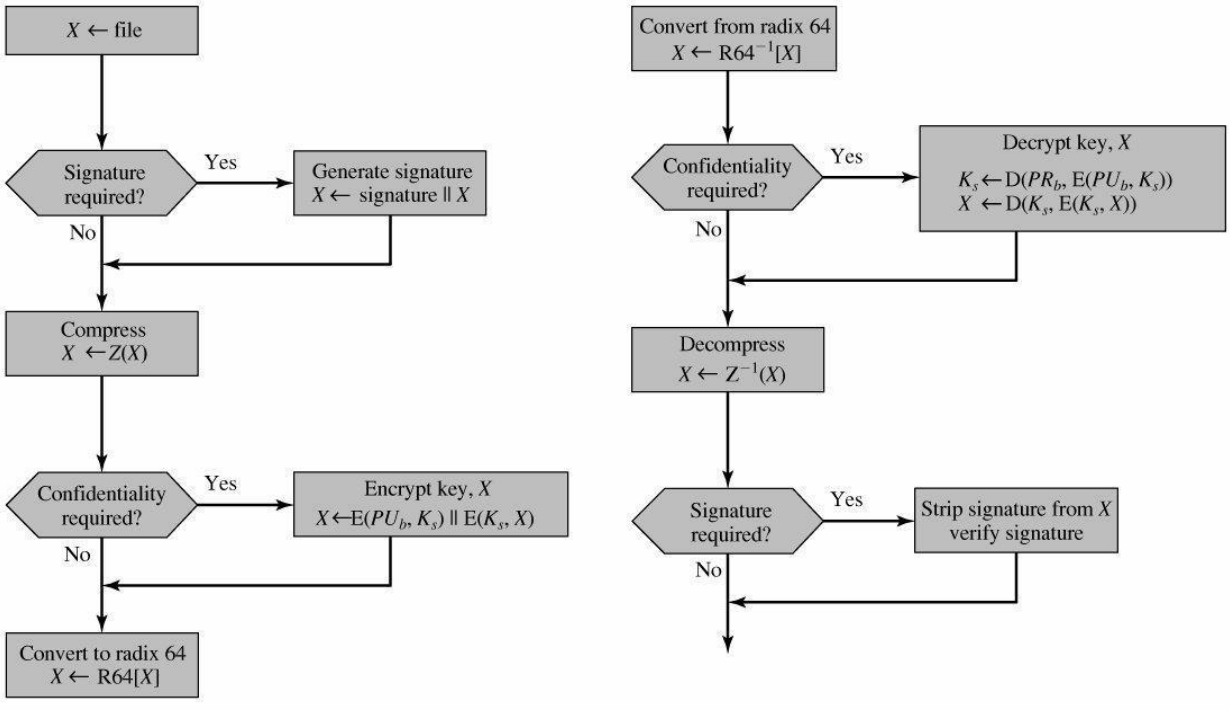
PGP provides confidentiality and authentication service that can be used for electronic mail and file storage applications**.**

Pretty Good Privacy is an open-source freely available software package for e-mail security. It provides authentication through the use of digital signature; confidentiality through the use of symmetric block encryption; compression using the ZIP algorithm; e-mail compatibility using the radix-64 encoding scheme; and segmentation and reassembly to accommodate long e-mails.

PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.

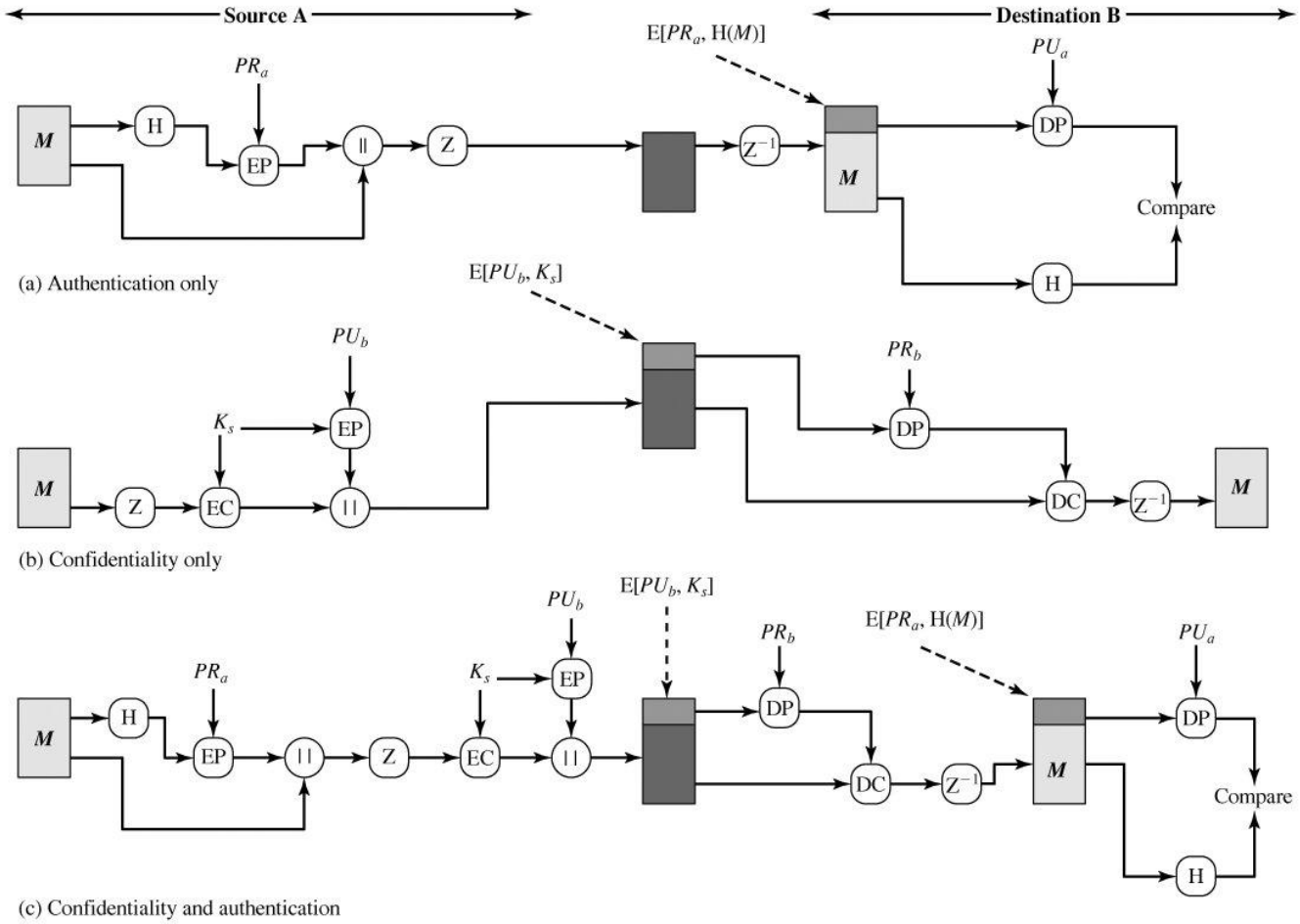
1. Selected the best available cryptographic algorithms as building blocks
2. Integrated these algorithms into a general-purpose application that is independent of operating system and processor and that is based on a small set of easy-to- use commands
3. Made the package and its documentation, including the source code, freely available via the Internet, bulletin boards, and commercial networks such as AOL (America On Line)
4. Entered into an agreement with a company (Viacrypt, now Network Associates) to provide a fully compatible, low-cost commercial version of PGP.

Confidentiality and Authentication



(a) Generic transmission diagram (from A)

(b) Generic reception diagram (to B)



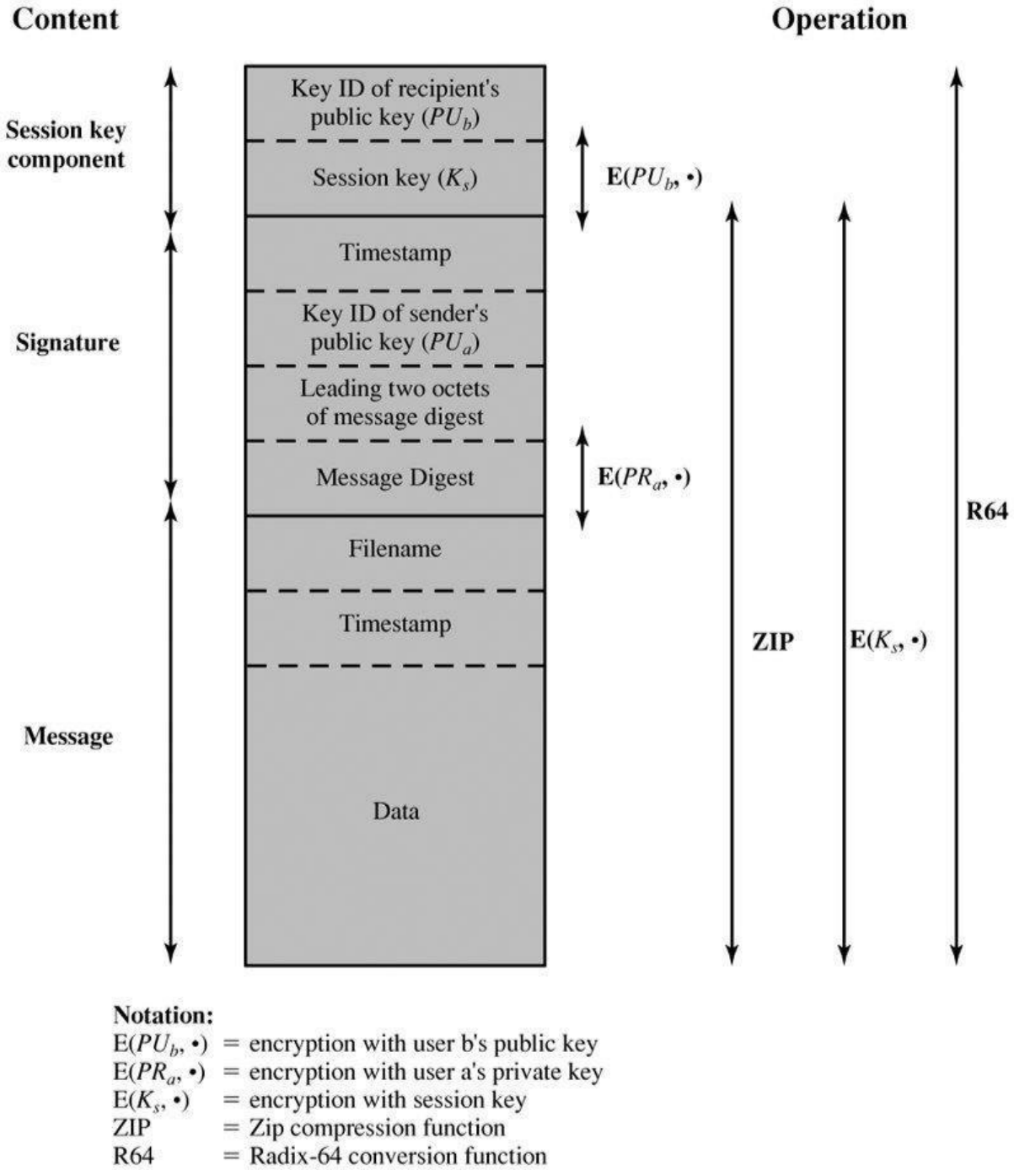
Cryptographic Keys and KeyA means ofType equation here. ge erating unpredictable session keys is needed.

Ri gs

1. We would like to allow a user to have multiple public-key/private-key pairs.
2. Each PGP entity must maintain a file of its own public/private key pairs as well as a file of public keys of correspondents.

General Format of PGP Message (from A to B)

Sketch the general format for PGP message. (2 Marks-Nov/Dec'2014)



Notation:

E(PU_b, •) = encryption with user b's public key
E(PR_a, •) = encryption with user a's private key
E(K_s, •) = encryption with session key
ZIP = Zip compression function
R64 = Radix-64 conversion function

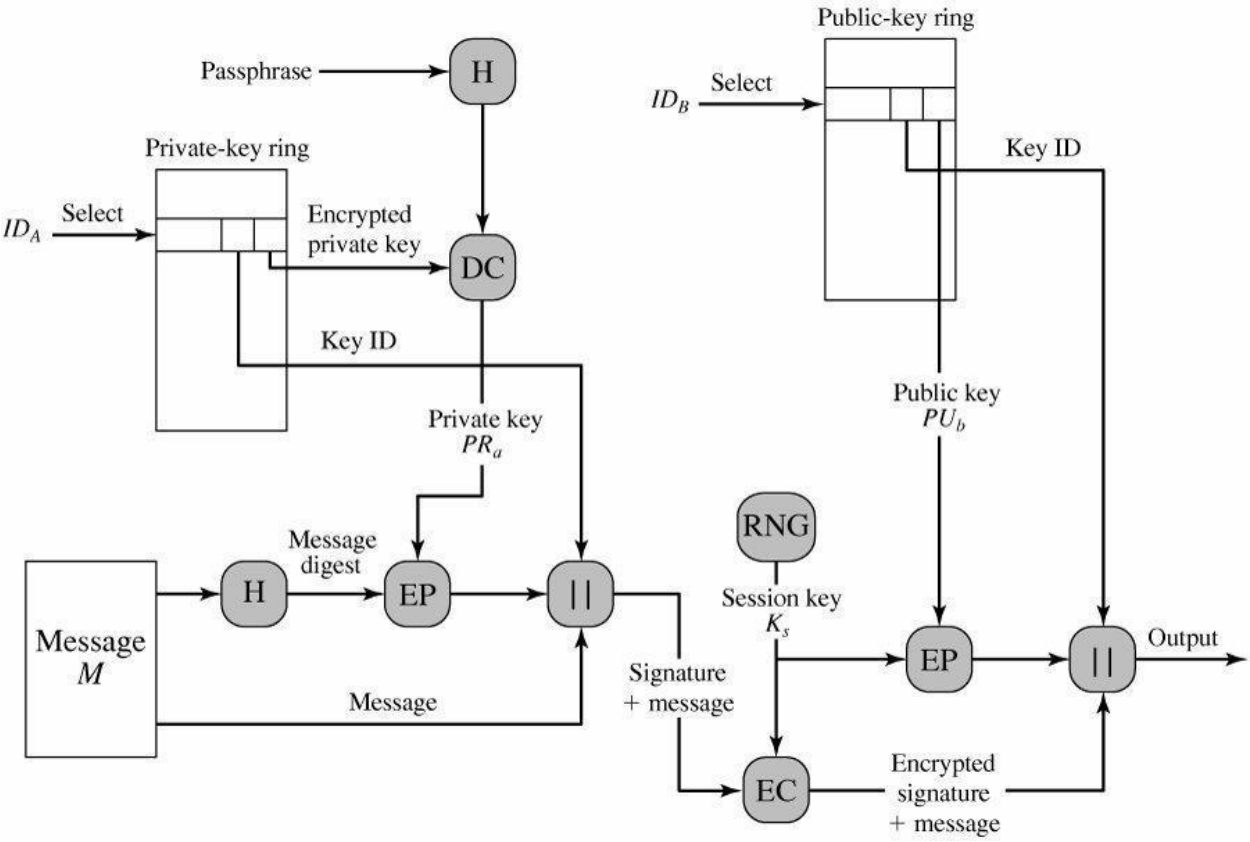


Figure: PGP Message Reception (from User A to User B; no compression or radix 64 conversion)

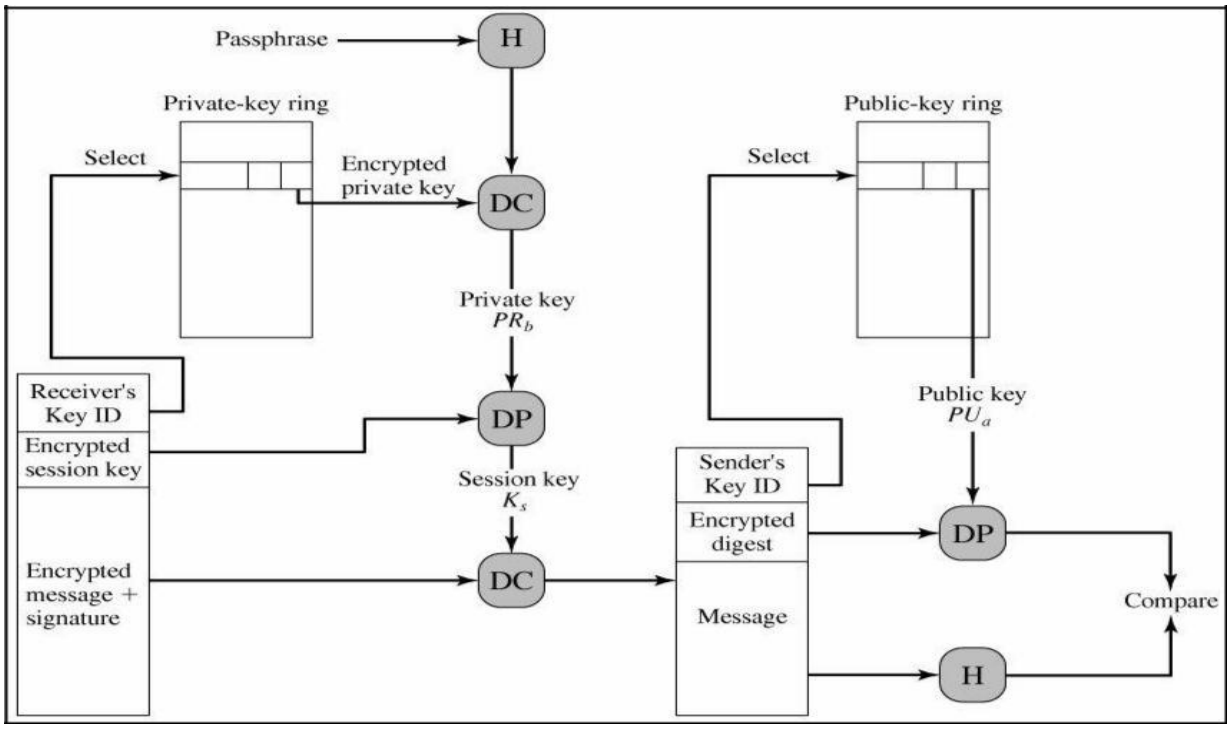
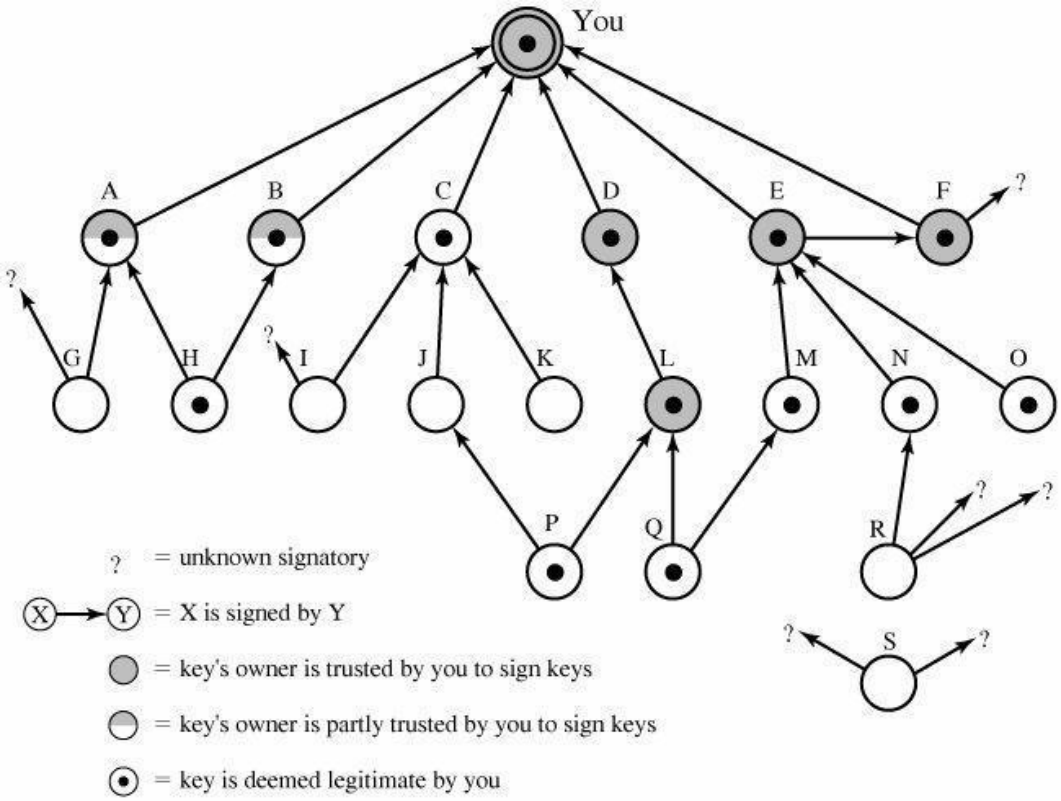


Figure: PGP Trust Model Example


You
A
B
C
D
E
F
?
G
H
I
J
K
L
M
N
O
P
Q
R
S
? = unknown signatory
X
Y
= X is signed by Y
= key's owner is trusted by you to sign keys
= key's owner is partly trusted by you to sign keys
= key is deemed legitimate by you

2. WEB SECURITY

WEB SECURITY:

Web Security Considerations:

The World Wide Web is fundamentally a client/server application running over the Internet and TCP/IP intranets. Secure socket layer (SSL) provides securityervices between TCP and applications that use TCP. The Internet standard version is called transport layer service (TLS).

The Web presents new challenges not generally appreciated in the context of computer and network security:

- The Internet is two way. The electronic publishing systems involving Teledex, voice response, or fax-back, the Web is vulnerable to attacks on the Web servers over the Internet.
- The Web is increasingly serving as a highly visible for corporate, product information and for business transactions. Reputatio s can be damaged and money can be lost if the Web servers are disrupted
- Although Web browsers are very easy to use, Web servers are relatively easy to configure and manage, and Web co te t is increasingly easy to develop, the underlying software is extraord narily complex. This complex software may hide many potential security flaws.
- Casual and untrained (in security matt rs) users are common clients for Web-based services.Such users are not n cessarily aware of the security.

Web Security Threats:

Integrity

- Modification of user data
- Trojan horse browser
- Modification of memory
- Modification of message traffic in transit

Confidentiality

- Eavesdropping on the Net
- Theft of info from server
- Theft of data from client
- Info about network configuration
- Info about which client talks to server

Denial of service

- Killing of user threads
- Flooding machine with bogus requests
- Filling up disk or memory
- Isolating machine by DNS attacks

Authentication

- Impersonation of legitimate users
- Data forgery

b. SSL:

SSL is a layered protocol. It is two layer protocols. At the lower level, the SSL Record Protocol is layered on top of some reliable transport protocol such as TCP.

The Hypertext Transfer Protocol (HTTP), which provides a transfer service for Web client/server interaction, can operate on top of the SSL Record Protocol.

The SSL Record Protocol takes the upper-layer application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies an MAC, encrypts, adds a head r, and transmits the result to TCP.

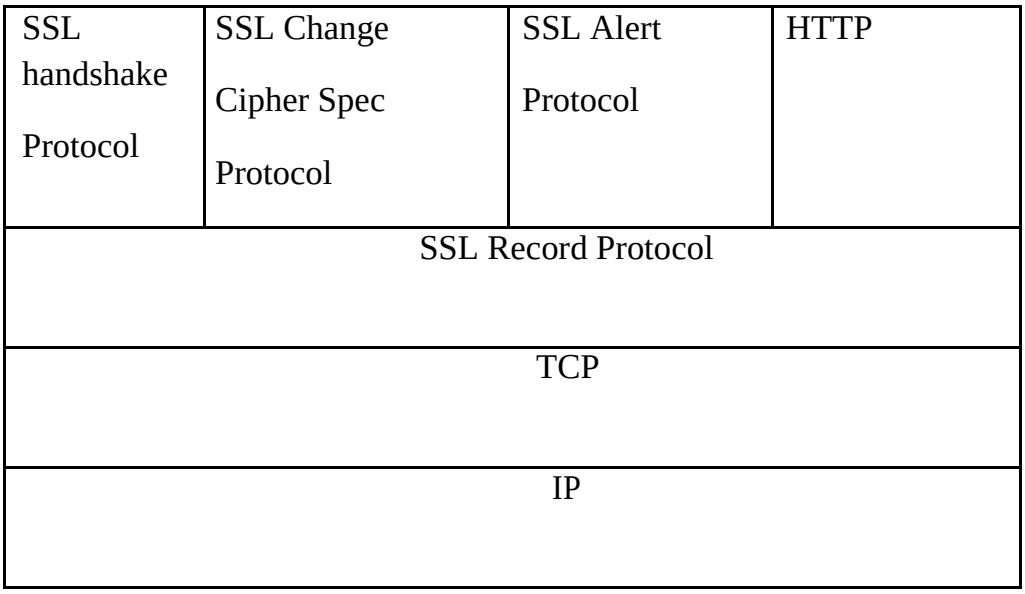


Figure: Two-layered SSL protocols.

Session and Connection States:

There are two defined specifications: SSL session and SSL connection.

SSL session:

An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. They define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection. The session state is defined by the following elements:

- Session identifier
- Peer certificate
- Compression method
- Cipher spec

- Master secret
- Is resumable

SSL connection:

A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. very connection is associated with one session. The connection state is defi ed by the following elements:

- Server and client andom
- Server write MAC secret
- Client write MAC secret
- Server write key
- Client write key
- Initialisation vectors
- Sequence numbers

SSL Record Protocol:

The SSL Record Protocol provides basic security services to various higher-layer protocols. Three upper-layer protocols are defined as part of SSL: the Handshake Protocol, the Change Cipher Spec Protocol and the Alert Protocol.

Content type	Major Version	Minor version	
Plaintext or compressed text			
MAC(0, 16 byte(MD5), 20 byte(SHA-1))			

Figure: SSL Record Protocol format.

The composed fields consist of:

- Content type (8 bits): This field is the higher-layer protocol used to process the enclosed fragment.
- Major version (8 bits): This field indicates the major version of SSL in use. For SSLv3, the value is 3.
- Minor version (8 bits): This field indicates the minor version of SSL in use. For SSLv3, the value is 0.
- Compressed length (16 bits): This field indicates the length in bytes of the

plaintext fragment or compressed fragment if compression is required. The maximum value is 214 + 2048.

SSL Alert Protocol:

One of the content types supported by the SSL Record Layer is the alert type. Alert messages convey the severity of the message and a description of the alert. Alert messages consist of 2 bytes. The first byte takes the value warning or fatal to convey the seriousness of the message. If the level is fatal, SSL immediately terminates the connection.

SSL Handshake Protocol:

The SSL Handshake Protocol operated on top of the SSL Record Layer is the most important part of SSL. This protocol provides three services for SSL connections between the server and client. The Handshake Protocol

1. Allows the client/server to agree on a protocol version.
2. To authenticate each other by forming an MAC.
3. To negotiate an encryption algorithm and cryptographic keys for protecting data sent in an SSL record before the application protocol transmits or receives its first byte of data.

The Handshake Protocol consists of a series of messages exchanged by the client and server.

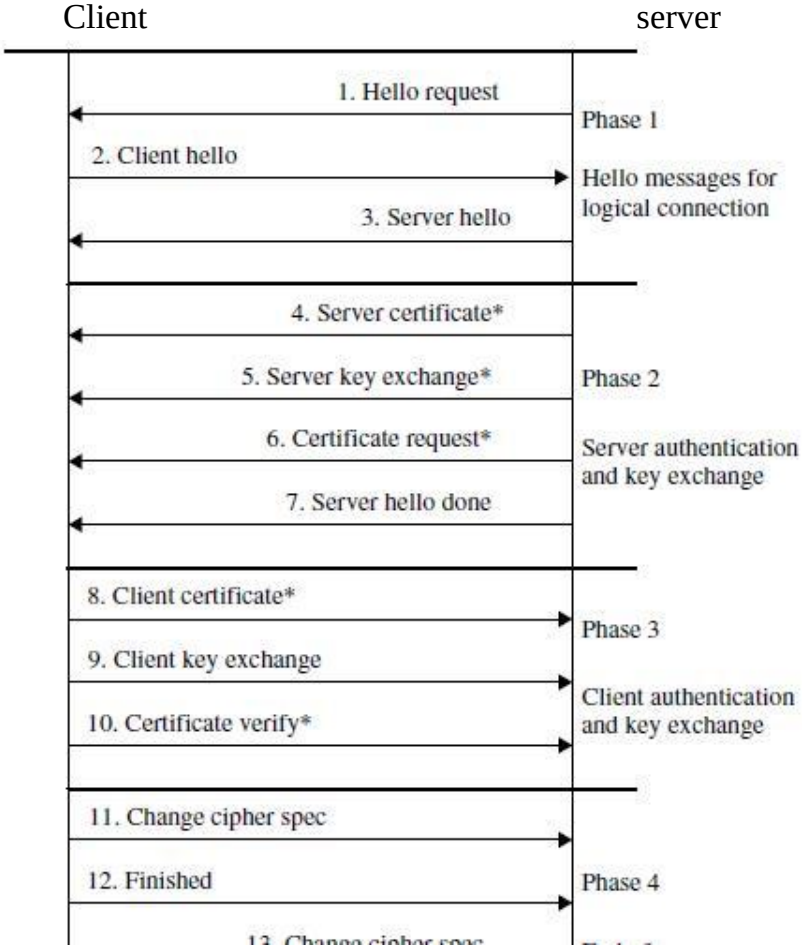


Figure: Handshake Protocol

c. TLS:

TLS is an IETF standardization initiative whose goal is to produce an Internet standard version of SSL.Transport Layer Security is defined as a Proposed Internet Standard in RFC 2246. RFC 2246 is very similar to SSLv3. The TLS Record Format is the same as that of the SSL Record Format, and the fields in the header have the same meanings. The one difference is in version number.

Version Number:

The TLS Record Format is the same as that of the SSL Record Format and the fields in the header have the same meanings. The one difference is in version values. For the current version of TLS, the Major Version is 3 and the Minor Version is 1.

Message Authentication Code:

There are two differences between the SSLv3 and TLS MAC schemes: the actual algorithm and the scope of the MAC calculation. TLS makes use of the HMAC algorithm defined in RFC 2104.

HMAC is defined as follows:

$$HMACK(M) = H[(K+ opad)||H[(K+ ipad)||M]]$$

where

H = embedded hash function (for TLS, either MD5 or SHA-1)

M = message input to HMAC

K+ = secret key padded with zeros on the l ft so that the result is equal to the block length of the hash code(for MD5 and SHA-1, block length = 512 bits)

ipad = 00110110 (36 in hexadecimal) repeated 64 times (512 bits)

opad = 01011100 (5C in hexadec mal) repeated 64 times (512 bits)

SSLv3 uses the same algorithm, except that the padding bytes are concatenated with the secret key.

For TLS, the MAC calculation encompasses the fields indicated in the following expression:

HMAC_hash(MAC_write secret, seq num || TLSCompressed.type ||
TLSCompressed.version || TLSCompressed.length ||
TLSCompr ss d.fragment)

The MAC calculation covers all of the fields covered by the SSLv3 calculation, plus the field T SCompressed.version, which is the version of the protocol being employed.

Pseudorandom Function:

TLS makes use of a pseudorandom function referred to as PRF to expand secrets into blocks of data for purposes of key generation or validation. The objective is to make use of a relatively small shared secret value but to generateonger blocks of data in a way that is secure from the kinds of attacks made on hash functions and MACs.

The PRF is based on the following data expansion

P_hash(secret, seed) = HMAC_hash(secret, A(1) || seed) ||
HMAC_hash(secret, A(2) || seed) ||
HMAC_hash(secret, A(3) || seed) || ...

where A() is defined as

A(0) = seed

A(i) = HMAC_hash (secret, A(i - 1))

The data expansion function makes use of the HMAC algorithm, with either MD5 or SHA.

To make PRF as secure as possible, it uses two hash algorithms in a way that should guarantee its security if either algorithm rema ns secure. PRF is defined as

PRF(secret, label, seed) = P_MD5(S1, label || s d)
P_SHA-1(S2, lab l || seed)

PRF takes as input a secret value, an ide tifying label, and a seed value and produces an output of arbitrary length.

Alert Codes:

TLS supports all of the alert codes defined in SSLv3 with the exception of no_certificate. Additional codes are defined in TLS

- decryption failed: A ciphertext decrypted in an invalid way;
- record_overflow: A TLS record was received with a payload (ciphertext) whose length xceeds 214 + 2048 bytes.
- unknown ca: A valid certificate chain or partial chain was received trusted CA.
- access denied: A valid certificate was received, but when access control as applied, the sender decided not to proceed with the negotiation.
- decode_error: A message could not be decoded because a field was out of its specified range.
- export_restriction: A negotiation not in compliance with export restrictions on key length was detected.
- protocol_version: The protocol version the client attempted to negotiate is recognized but not supported.
- insufficient_security: Returned instead of handshake_failure when a negotiation has failed specifically because the server requires ciphers more secure than those supported by the client.
- internal_error: An internal error unrelated to the peer or the correctness of the protocol makes it impossible to continue.

New alerts include the following:

- decrypt error: A handshake cryptographic operation failed, including being unable to verify a signature, decrypt a key exchange, or validate a finished message.

- user_canceled: This handshake is being canceled for some reason unrelated to a protocol failure.
- no_renegotiation: Sent by a client in r sponse to a hello request or by the server in response to a client hello after initial handshaking.

Cipher Suites:

There are several small differe ces between the cipher suites available under SSLv3 and under TLS:

- Key Exchange: TLS supports all of the key exchange techniques of SSLv3 with the exception of Fortezza.
- Symmetric Encryption Algorithms: TLS includes all of the symmetric encryption algorithms found in SSLv3, with the exception of Fortezza.

Client Certificate Types:

TLS defines the following certificate types to be requested in a certificate_request message: rsa sign,dss_sign, rsa_fixed_dh, and dss_fixed_dh. These are all defined in SSLv3. In addition, SSLv3 includes rsa_ephemeral_dh, dss_ephemeral_dh, and fortezza kea.

Certificate_Verify and Finished Messages:

In the TLS certificate_verify message, the MD5 and SHA-1 hashes are calculated only over handshake_messages.

For TLS, we have

PRF(master_secret, finished_label, MD5(handshake_messages)||

SHA-1(handshake_messages))

where finished_label is the string "client finished" for the client and "server finished" for the server.

Cryptographic Computations:

The pre_master_secret for TLS is calculated in the same way as in SSLv3.The master_secret in TLS is calculated as a hash function of the pre_master_secret and the two hello random numbers. The form of the TLS calculation is different from that of SSLv3 and is defined as follows:

master_secret = PRF(pre master_secret, "master secret",
ClientHello.random || ServerHello.random)

The algorithm is performed until 48 bytes of pseudorandom output are produced. The calculation of the key block material (MAC secret keys, session encryption keys, and IVs) is defined as follows:

key_block = PRF(master_secret, "key expansion",

SecurityParameters.server_random ||

SecurityParameters.client_random)

until enough output has been generated.

Padding:

In SSL, the padding added prior to encryption of user data is the minimum amount required so that the total size of the data to be encrypted is a multiple of the cipher's block length. In TLS, the padding can be any amount that results in a total that is a multiple of the cipher's block length, up to a maximum of 255 bytes.

d. **PKI.**

A public key infrastructure (PKI) is defined as the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography. Typically, PKI implementations make use of X.509 certificates so PKIX model.

Principal objective:

- Develop a PKI is to enable secure, convenient, and efficient acquisition of public keys.

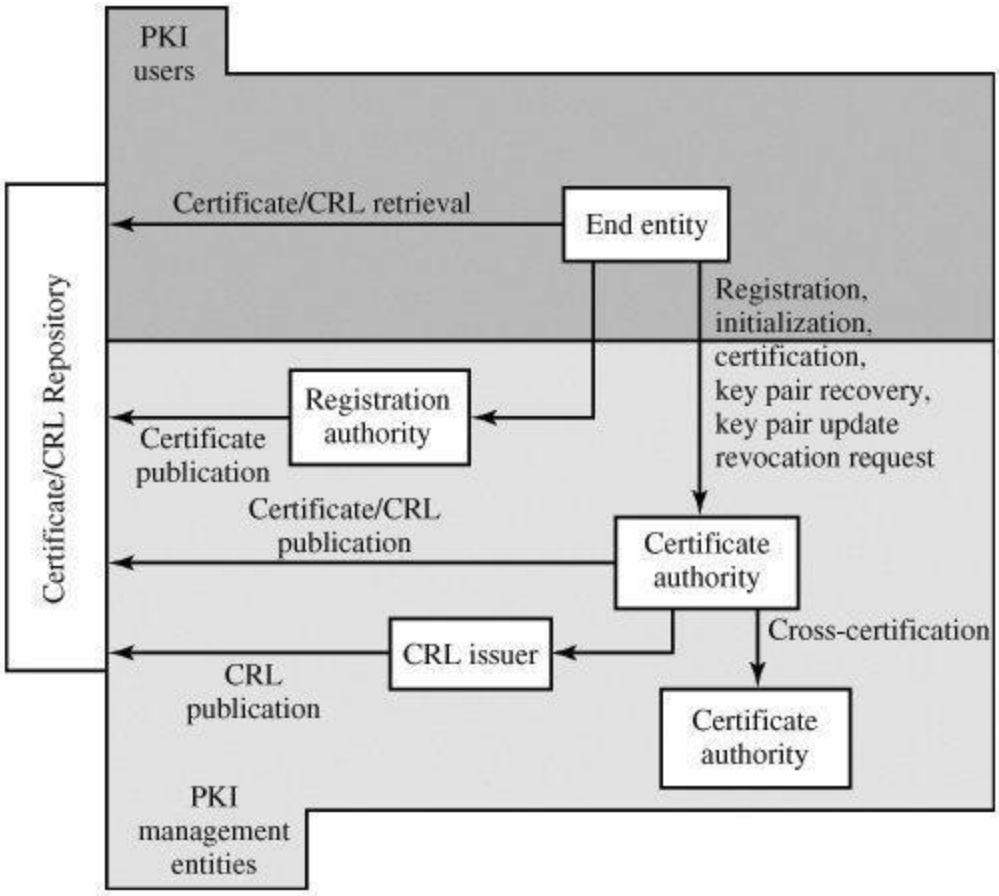
Key elements of the PKIX model:

These elements are

- End entity: A generic term used to de ote end users, devices (e.g., servers, routers).
- Certification authority (CA): The issuer of certificates and (usually) certificate revocation lists (CRLs).
- Registration authority (RA): An optional component that can assume a number of administrative functio s from the CA.

● CRL issuer: An option l component that a CA can delegate to publish CRLs.

● Repository: A g n ric term used to denote any method for storing certificates and CRLs so that they can be retrieved by End Entities.



PKIX Management Functions

PKIX identifies a number of management functions that potentially need to be supported by manag m nt protocols.

Registration: This is the process whereby a user first makes itself known to a CA (directly, or through an RA), prior to that CA issuing a certificate or certificates for that user. Registration begins the process of enrolling in a PKI.

Initialization: Before a client system can operate securely, it is necessary to install key materials.

For example, the client needs to be securely initialized with the public key and other assured information of the trusted CA(s), to be used in validating certificate paths.

- Certification: This is the process in which a CA issues a certificate for a user's public key, and returns that certificate to the user's client system and/or posts that certificate in a repository.
- Key pair recovery: Key pairs can be used to support digital signature creation and verification, encryption and decryption, or both.
- Key pair update: All key pairs need to be updated regularly .Update is required when the certificate lifetime expires and as a result of certificate revocation.

- Revocation request: An authorized person adv ses a CA of an abnormal situation requiring certificate revocation
- Cross certification: Two CAs exchange information used in establishing a cross-certificate. A cross-certificate is a c rtificate issued by one CA to another CA that contains a CA sig ature key used for issuing certificates.

PKIX Management Protocols:

The PKIX has defines two alter ative management protocols between PKIX entities that support the management functions listed in the preceding subsection.

RFC 2510 defines the certificate management protocols (CMP). CMP is designed to be a flexible protocol able to accommodate a variety of technical, operational, and business models.

RFC 2797 defines certificate management messages over CMS (CMC), where CMS refers to RFC 2630, and cryptographic message syntax. CMC is built on earlier work and is intended to leverage existing implementations.

IP SECURITY

IPSec:

IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.

Function areas of IP security:

- ✓ Authentication
- ✓ Confidentiality
- ✓ Key management

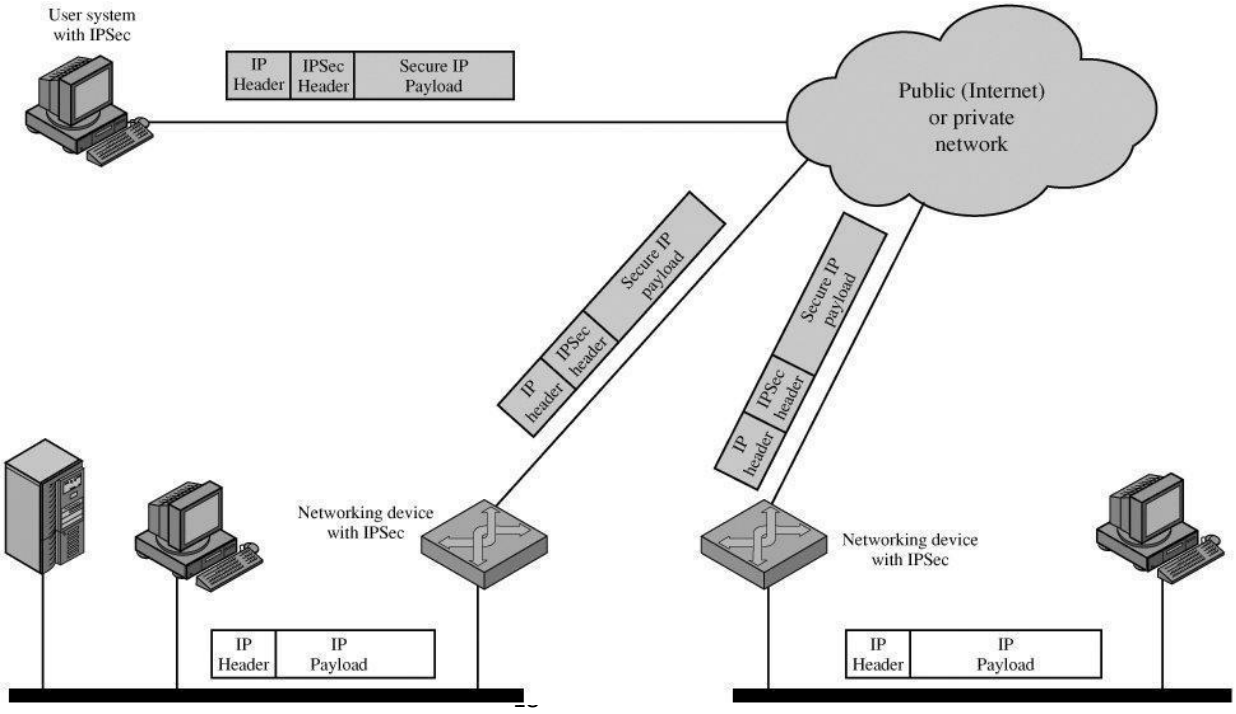


Figure: IPSecurity

Applications of IPSec.

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establishing extranet and intranet connectivity with partners
- Enhancing electronic commerce security

Benefits of IPSec

- When IPSec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.
- IPSec in a firewall is resistant to bypass if all traffic from the outside must use IP, and the firewall is the only means of entrance from the Internet into the organization.
- IPSec is below the transport layer (TCP, UDP) and so is transparent to applications. There is no need to change software on a user or server system when IPSec is implemented in the firewall or router.
- IPSec can be transparent to end users. There s no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.
- IPSec can provide security for individual us rs if needed. This is useful for offsite workers and for setting up a secure virtual sub network within an organization for sensitive applications.

Routing Applications

- A router advertisement (a new router advertises its presence) comes from an authorized router
- A neighbor advertisement (a router seeks to establish or maintain a neighbor relationship with router in another routing domain) comes from an authorized rout r.
- A redirect message comes from the router to which the initial packet was sent.
- A routing update is not forged.

IP Security Architecture

- **Architecture:** Covers the general concepts, security requirements, definitions, and mechanisms defining IPSec technology.

- **Encapsulating Security Payload (ESP):** Covers the packet format and general issues related to the use of the ESP for packet encryption and, optionally, authentication.
- **Authentication Header (AH):** Covers the packet format and general issues related to the use of AH for packet authentication.
- **Encryption Algorithm:** A set of documents that describe how various encryption algorithms are used for ESP.
- **Authentication Algorithm:** A set of documents that describe how various authentication algorithms are used for AH and for the authe tication option of ESP.
- **Key Management:** Documents that describe key management schemes.
- **Domain of Interpretation (DOI):** Contains values needed for the other documents to relate to each other.

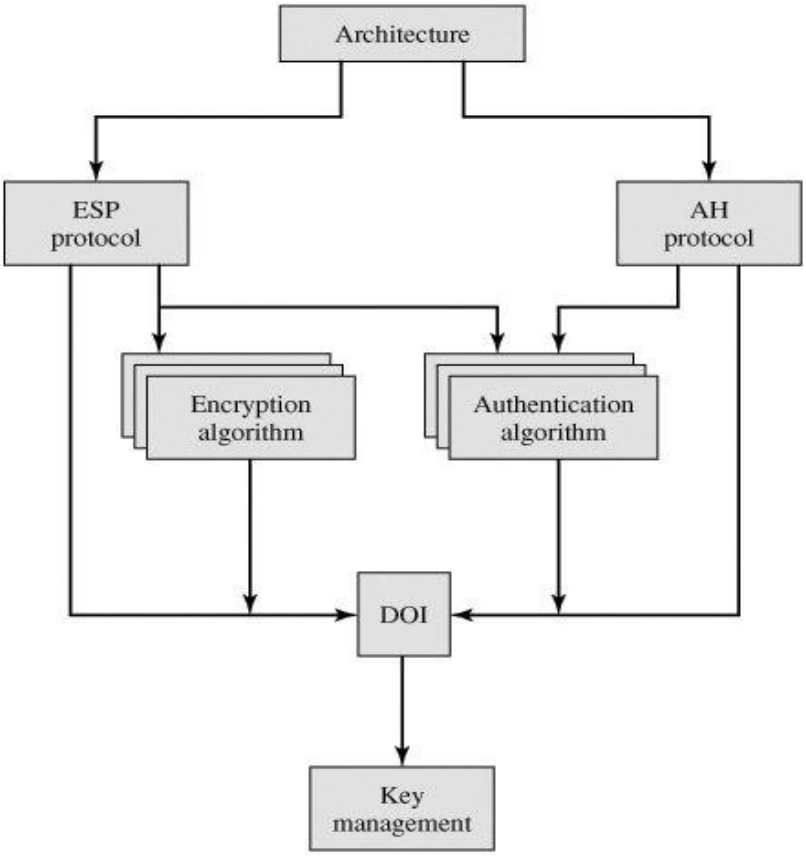


Figure: IPSec Document Overview

IPSec Services

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets (a form of partial sequence integrity)
- Confidentiality (encryption)
- Limited traffic flow confidentiality

Figure: IPSec Services

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✔	✔	✔
Connectionless integrity	✔		✔
Data origin authentication	✔		✔
Rejection of replayed packets	✔	✔	✔
Confidentiality		✔	✔
Limited traffic flow confidentiality		✔	✔

Authentication Header

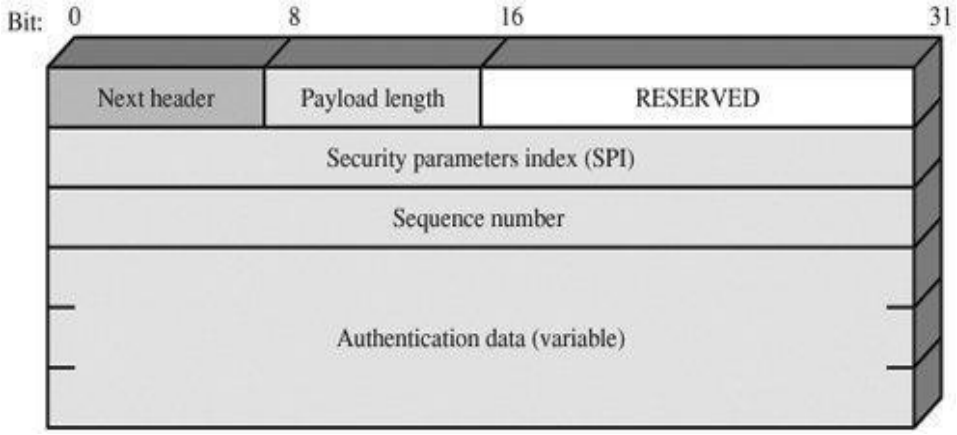


Fig 5.7 IPSec Authentication Header

Anti-Replay Service

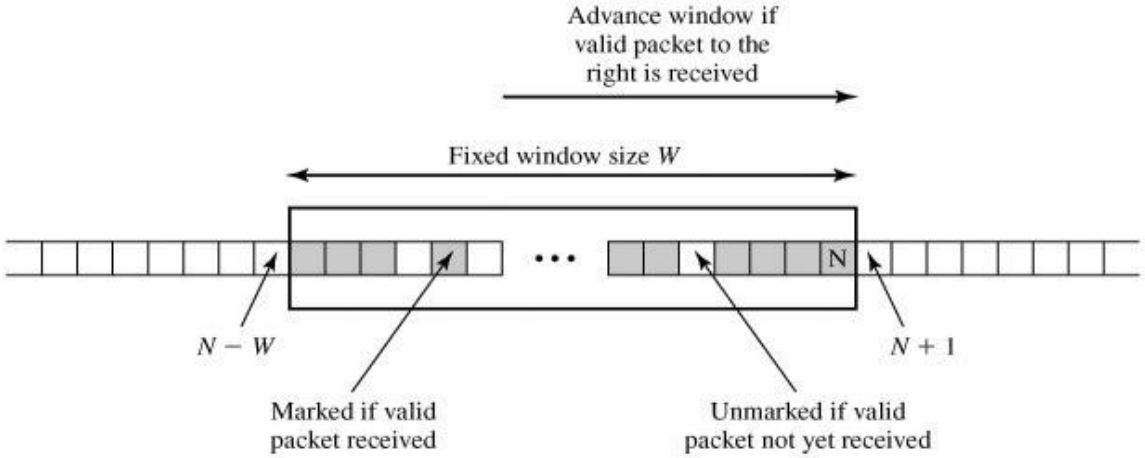


Figure: Anti-replay Mechanism

End-to-End versus End-to-Intermediate Authentication

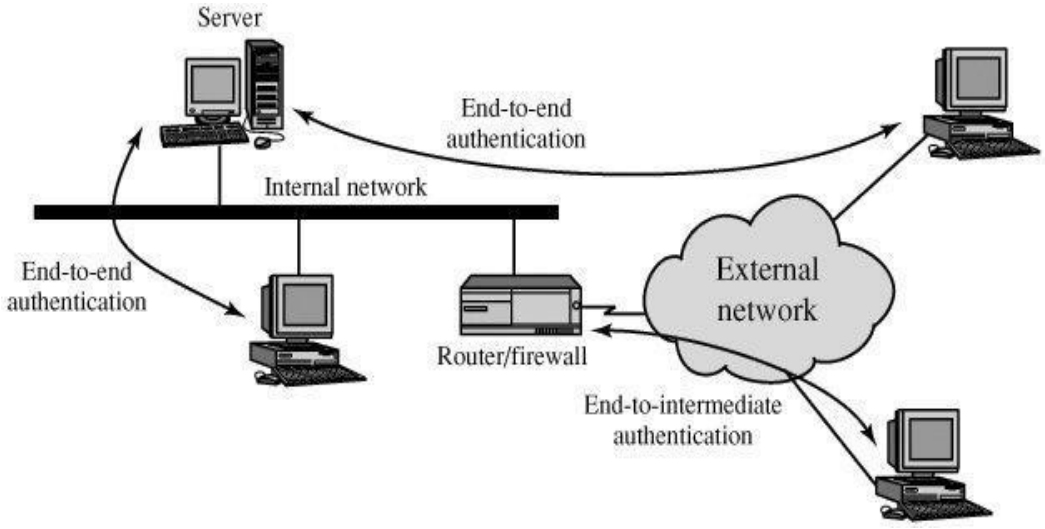


Figure: End-to-End versus End-to-Intermediate Authentication

Scope of AH Authentication

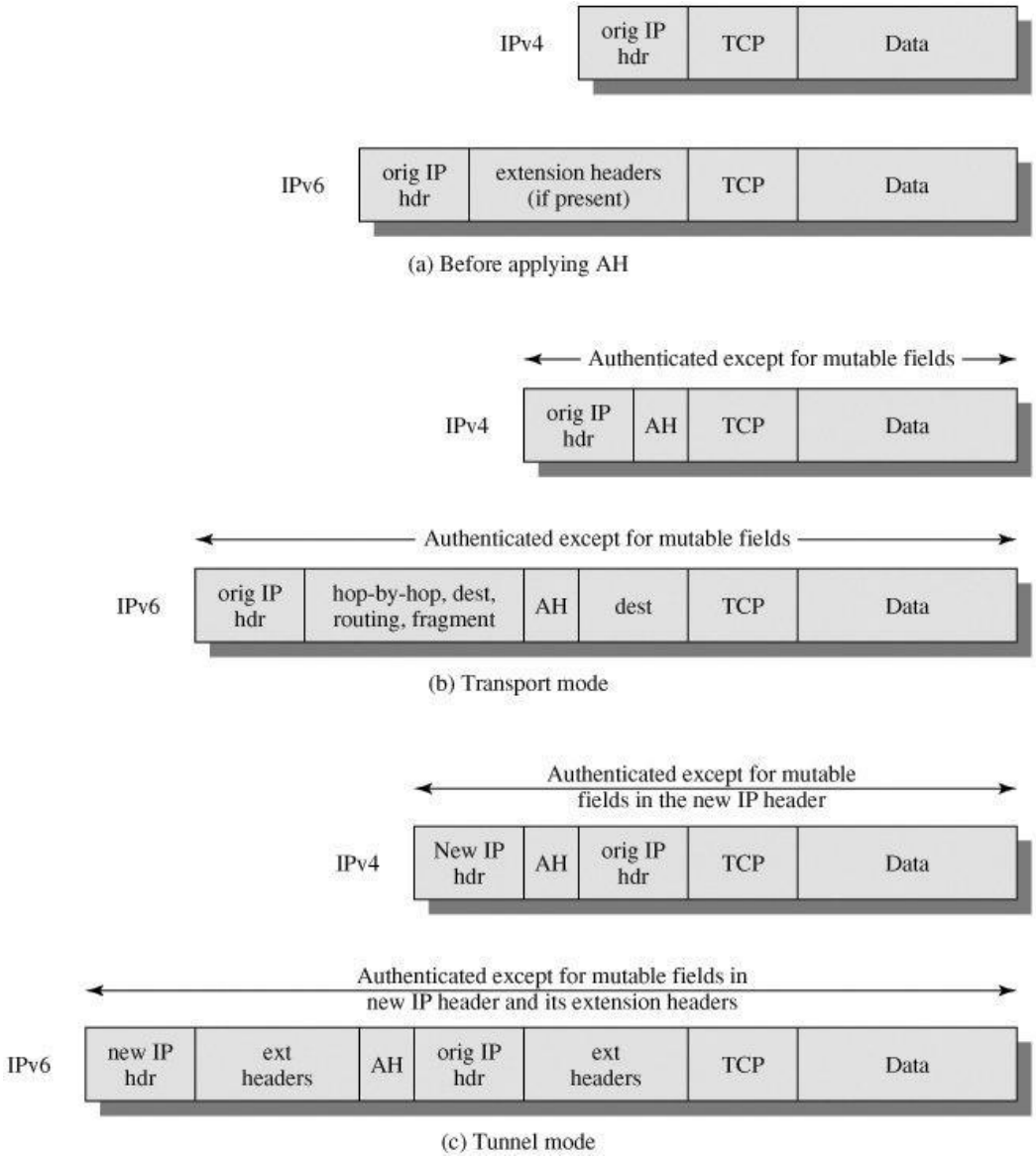


Figure: Scope of AH Authentication

4. SECURE ELECTRONIC TRANSACTION

Secure Electronic Transaction:

Secure Electronic Transaction (SET) is an open encryption a d security specification designed to protect credit card transactions on the Internet.

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication

SET is an open encryption and security sp cification designed to protect credit card transactions on the Internet. The curre t version, SETv1, emerged from a call for security standards by MasterCard and Visa in February 1996.

SET is not itself a payment system. Rather it is a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network (Internet) in a secure fashion.

SET services:

- Provides a secure communications channel among all parties involved in a transaction.
- Provides trust by the use of X.509v3 digital certificates
- Ensures privacy because the information is only available to parties in a transaction when and where necessary.

SET Overview:
Requirements:

Business requirements for secure payment processing with credit cards over the Internet and other networks:

- Provide confidentiality of payment and ordering information: It is necessary to assure cardholders that this information is safe and accessible only to the intended recipient.
- Ensure the integrity of all transmitted data: That is, e sure that no changes in content occur during transmission of SET messages D gital signatures are used to provide integrity.
- Provide authentication that a cardholder is a legitimate user of a credit card account. Digital signatures and certificates are used to verify that a cardholder is a legitimate user of a valid account.
- Provide authentication that a merchant can accept credit card transactions through its relationship with a fi a cial institution.

- Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.

- Create a protocol that neither depends on transport security mechanisms nor prevents their use.

- Facilitate and encourage interoperability among software and network providers.

Key Features of SET

SET incorporates the following features:

- Confidentiality of information.
- Integrity of data.
- Cardholder account authentication
- Merchant authentication

SET Participants:

Cardholder:

In the electronic environment, consumers and corporate purchasers interact with merchants from personal computers over the Internet. A cardholder is an authorized holder of a payment card (e.g., MasterCard, Visa) that has been issued by an issuer.

Merchant:

A merchant is a person or organization that has goods or services to sell to the cardholder.

Issuer:

This is a financial institution, such as a bank, that provides the cardholder with the payment card.

Acquirer:

This is a financial institution that establish s an account with a merchant and processes payment card authorizations and payments. The acquirer also provides electronic transfer of payments to the merchant's account. Payment gateway:

This is a function operated by the acquirer or a designated third party that processes merchant payment messages. The payment gateway interfaces between SET and the existing bankcard payment networks for authorization and payment functions.

Certification authority (CA):

This is an entity th t is trusted to issue X.509v3 public-keycertificates for cardholders, merchants, and payment gateways. The success of SET will depend on the existence of a CA infrastructure available for this purpose.

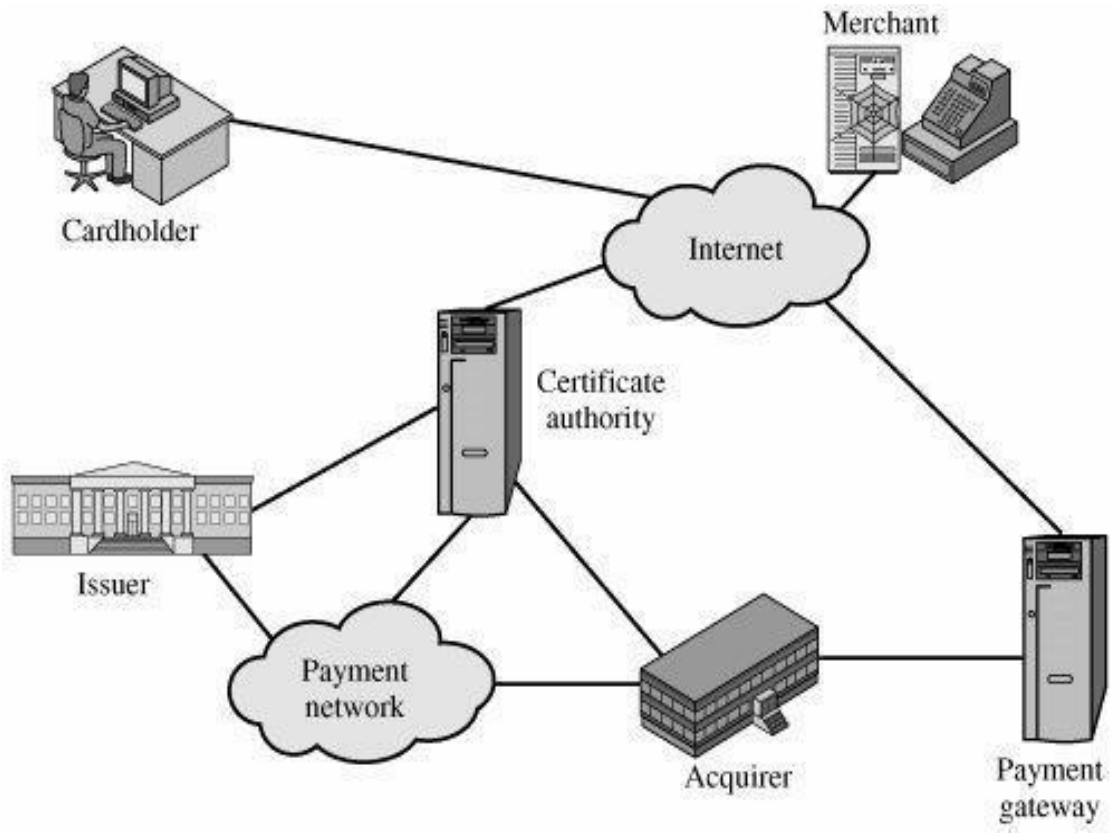


Figure: Secure Electronic Commerce Components

Sequence of events for a transaction:

- The customer ope s an account
- The customer receives a certificate
- Merchants h ve their own certificates
- The custom r places an order
- The merchant is verified.
- The order and payment are sent.
- The merchant requests payment authorization
- The merchant confirms the order.
- The merchant provides the goods or service.
- The merchant requests payment.

Dual Signature:

SET dual signature : The purpose of the dual signature is to link two messages that are intended for two different recipients. In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank. The merchant does not need to know the customer's credit card number, and the bank does not need to know the details of the customer's order. The customer is afforded extra protection in terms of privacy by keeping these two items separate.

The customer takes the hash (using SHA-1) of the PI and the hash of the OI. These two hashes are then concatenated and the hash of the result is taken. Finally, the customer encrypts the final hash with his or her private signature key, creating the dual signature. The operation can be summarized as

DS = E(PRc, [H(H(PI)||H(OI)])

where PRc is the customer's private signature key.

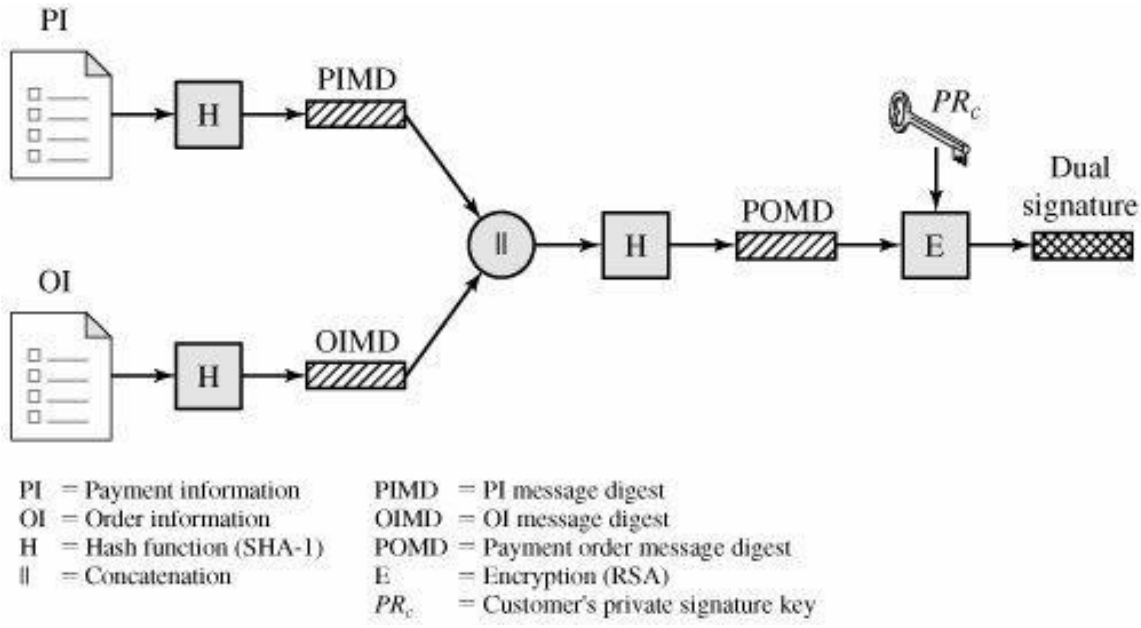


Figure: Construction of Dual Signature

if these two quantities are equal, then the bank has verified the signature.

1.The merchant has received OI and verified the signature.

2.The bank has received PI and verified the signature.

3.The customer has linked the OI and PI and can prove the linkage.

Payment Processing:

- Purchase request
- Payment authorization
- Payment capture

SET Transaction Types:

Cardholder registration:

Cardholders must register with a CA b fore they can send SET messages to merchants.

Merchant registration:

Merchants must register with a CA before they can exchange SET messages with customers and payment gateways.

Purchase request:

Message from customer to merchant containing OI for merchant and PI for bank.

Payment authorization:

Exchange between merchant and payment gateway to authorize a given amount for a purchase on a given credit card account.

Payment capture:

Allows the merchant to request payment from the payment gateway.

Certificate inquiry and status:

The cardholder or merchant sends the Certificate Inquiry message to determine the status of the certificate request and to receive the certificate if the request has been approved.

Purchase inquiry:

Allows the cardholder to check the status of the processing of an order after the purchase response has been received.

Authorization reversal:

Allows a merchant to correct previous authorization requests. If the order will not be completed, the merchant reverses the e t re authorization.

Capture reversal :

Allows a merchant to correct errors in capture requests such as transaction amounts that were entered incorrectly by a clerk.

Credit:

Allows a merchant to issue a credit to a cardholder's account such as when goods are returned or were damaged during shipping.

Credit reversal:

Allows a merch nt to correct a previously request credit. **Payment Gateway certificate r quest**:

Allows a merchant to query the payment gateway and receive a copy of the gateway's current key-exchange and signature certificates.

Batch administration:

Allows a merchant to communicate information to the payment gateway regarding merchant batches.

Error message:

Indicates that a responder rejects a message because it fails format or content verification tests.

S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security. Both PGP and S/MIME are on an IETF standards track. S/MIME will emerge as the industry standard for commercial and or generational use, while PGP will remain the choice for personal e-mail s curity for many users.

S/MIME is defined in a number of docum nts, most importantly RFCs 3369, 3370, 3850 and 3851.

Multipurpose Internet Mail Extensions

1. SMTP cannot transmit executable files or other binary objects. A number of schemes are in use for converting binary files into a text form that can be used by SMTP mail systems, including the popular UNIX UUencode/UUdecode scheme. However, none of these is a standard or even a de facto stand rd.
2. SMTP cannot transmit text data that includes national language characters because these are represented by 8-bit codes with values of 128 decimal or higher, and SMTP is limited to 7-bit ASCII.
3. SMTP servers may reject mail message over a certain size.
4. SMTP gateways that translate between ASCII and the character code EBCDIC do not use a consistent set of mappings, resulting in translation problems.
5. SMTP gateways to X.400 electronic mail networks cannot handle non textual data included in X.400 messages.

6. Some SMTP implementations do not adhere completely to the SMTP standards defined in RFC 821.

Problems in S/MIME:

- Deletion, addition, or reordering of carriage return and linefeed
- Truncating or wrapping lines longer than 76 characters
- Removal of trailing white space (tab and space characters)
- Padding of lines in a message to the same length
- Conversion of tab characters into multiple space characters
- MIME is intended to resolve these problems in a manner that is compatible with existing RFC 822 implementations.

MIME Header Fields:

The five header fields defined in MIME are as follows:

- MIME-Version: Must have the parameter value 1.0. This field indicates that the message conforms to RFCs 2045 and 2046.
- Content-Type: Describes the data contained in the body with sufficient detail that the receiving user agent can pick an appropriate agent or mechanism to represent the data to the user or otherwise deal with the data in an appropriate manner.
- Content-Transfer-Encodi g: I dicates the type of transformation that has been used to represent the body of the message in a way that is acceptable for mail transport.

- Content-ID: Used to id ntify MIME entities uniquely in multiple contexts.
  Content-Description: A text description of the object with the body; this is useful when the object is not readable (e.g., audio data).