Chapter 7

WEB Security

Henric Johnson

Blekinge Institute of Technology, Sweden

http://www.its.bth.se/staff/hjo/

henric.johnson@bth.se

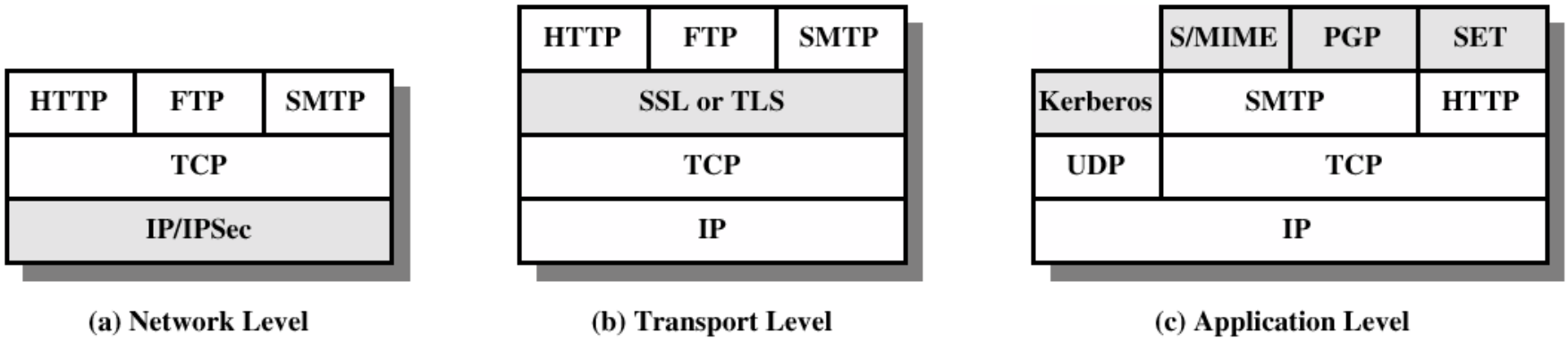
Outline

- Web Security Considerations
- Secure Socket Layer (SSL) and Transport Layer Security (TLS)
- Secure Electronic Transaction (SET)
- Recommended Reading and WEB Sites

Web Security Considerations

- The WEB is very visible.
- Complex software hide many security flaws.
- Web servers are easy to configure and manage.
- Users are not aware of the risks.

Security facilities in the TCP/IP protocol stack



(a) Network Level

(b) Transport Level

(c) Application Level

SSL and TLS

- SSL was originated by Netscape
- TLS working group was formed within IETF
- First version of TLS can be viewed as an SSLv3.1

SSL Architecture

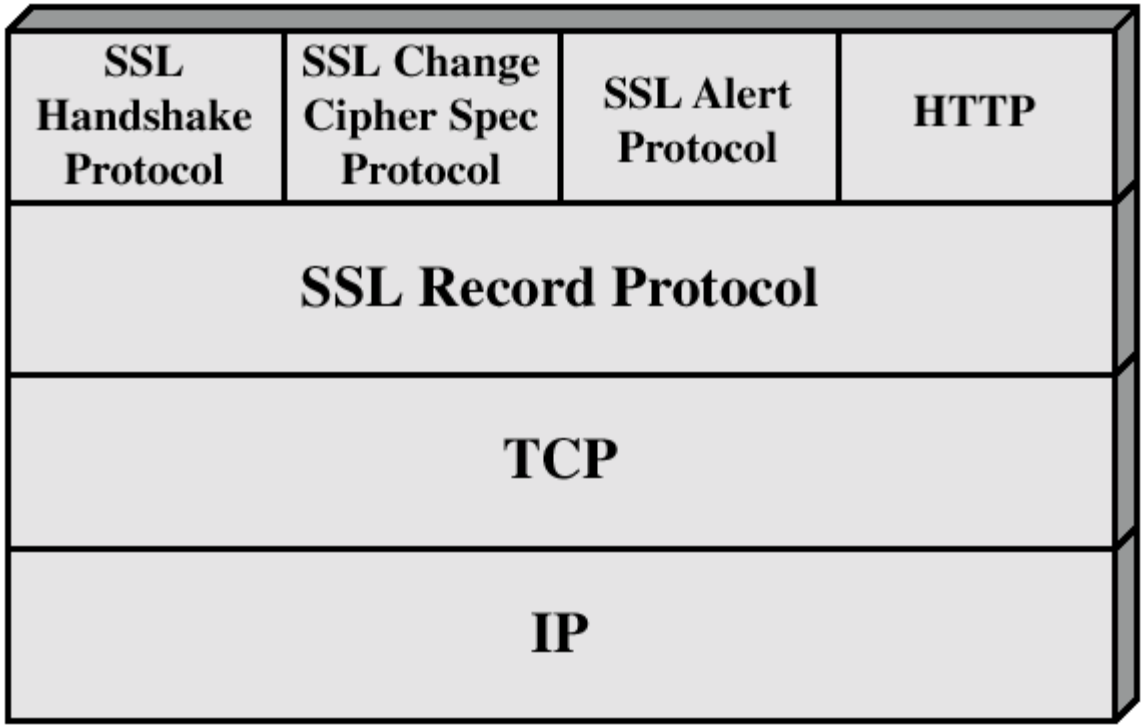
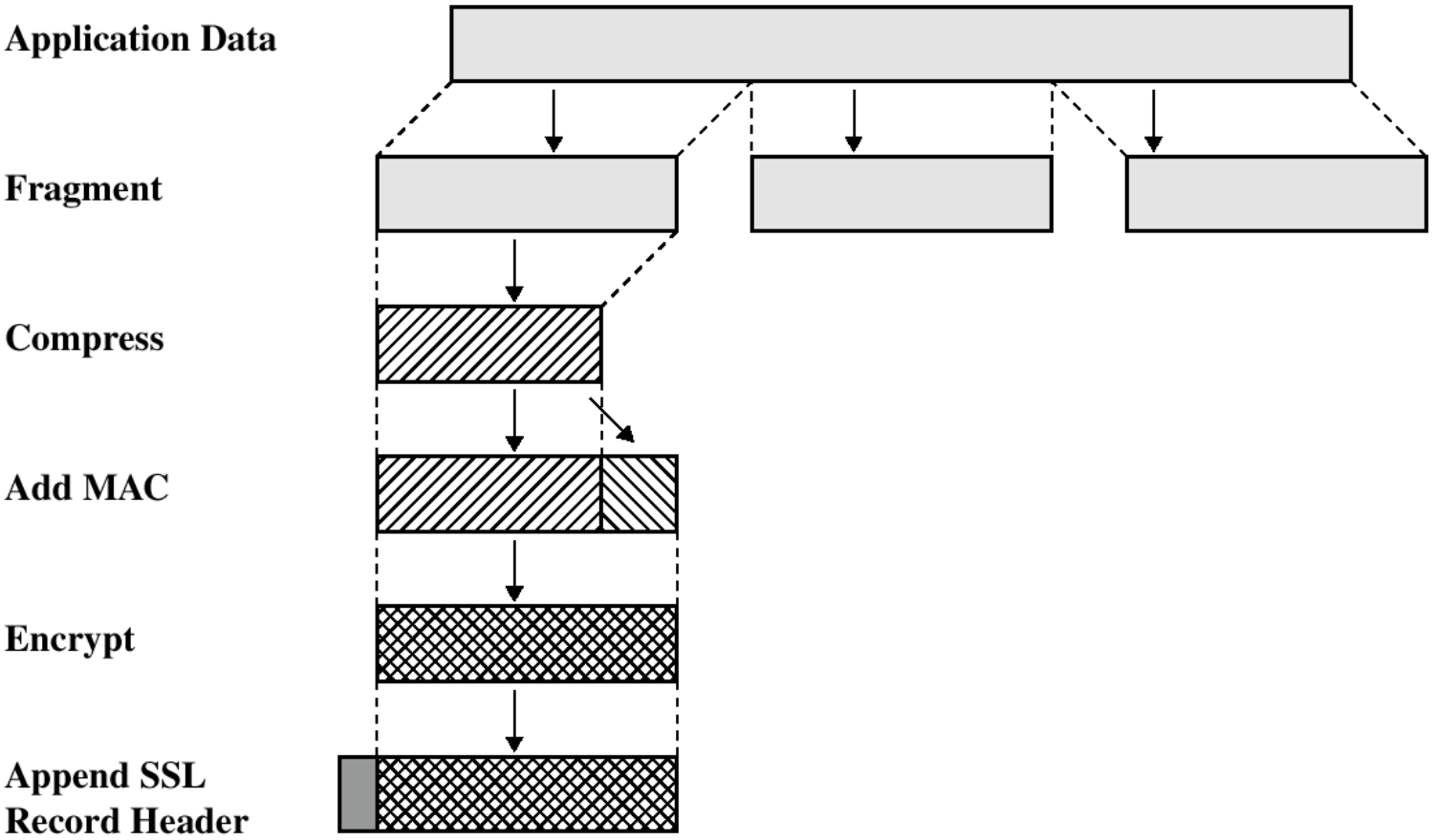
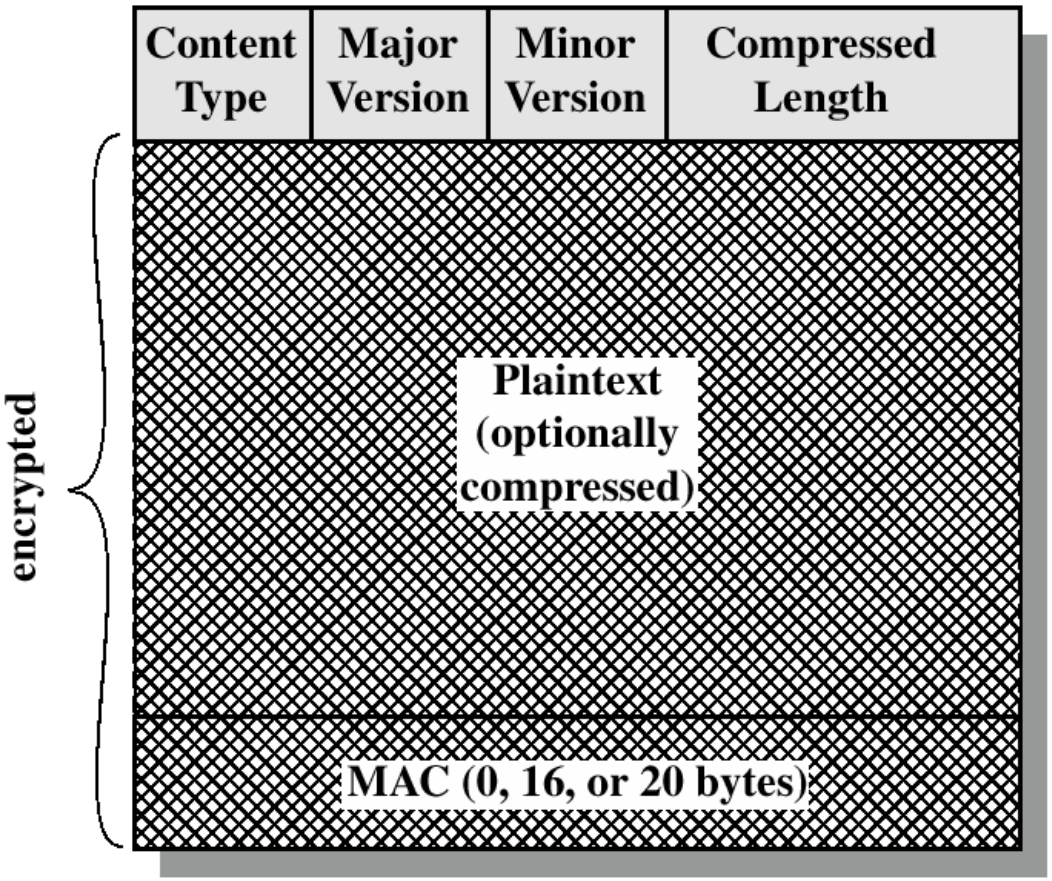


Figure 7.2 SSL Protocol Stack

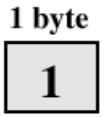
SSL Record Protocol Operation



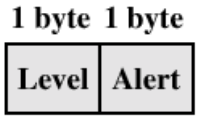
SSL Record Format



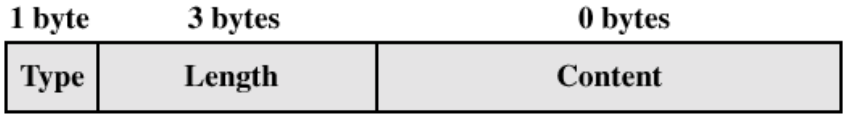
SSL Record Protocol Payload



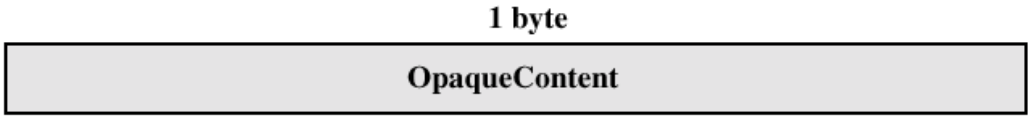
(a) Change Cipher Spec Protocol



(b) Alert Protocol



(c) Handshake Protocol

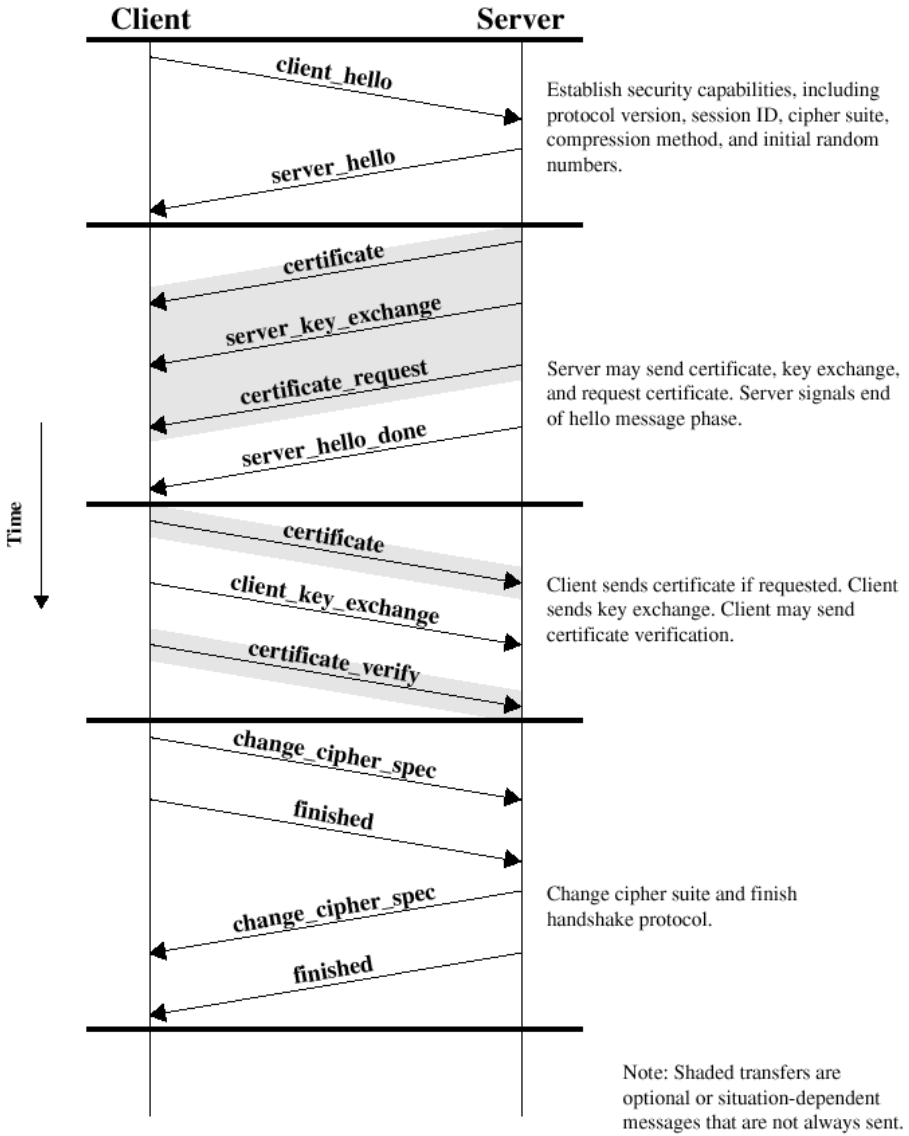


(d) Other Upper-Layer Protocol (e.g., HTTP)

Handshake Protocol

- The most complex part of SSL.
- Allows the server and client to authenticate each other.
- Negotiate encryption, MAC algorithm and cryptographic keys.
- Used before any application data are transmitted.

Handshake Protocol Action



Transport Layer Security

- The same record format as the SSL record format.
- Defined in RFC 2246.
- Similar to SSLv3.
- Differences in the:
  - version number
  - message authentication code
  - pseudorandom function
  - alert codes
  - cipher suites
  - client certificate types
  - certificate_verify and finished message
  - cryptographic computations
  - padding

Secure Electronic Transactions

- An open encryption and security specification.
- Protect credit card transaction on the Internet.
- Companies involved:
  - MasterCard, Visa, IBM, Microsoft, Netscape, RSA, Terisa and Verisign
- Not a payment system.
- Set of security protocols and formats.

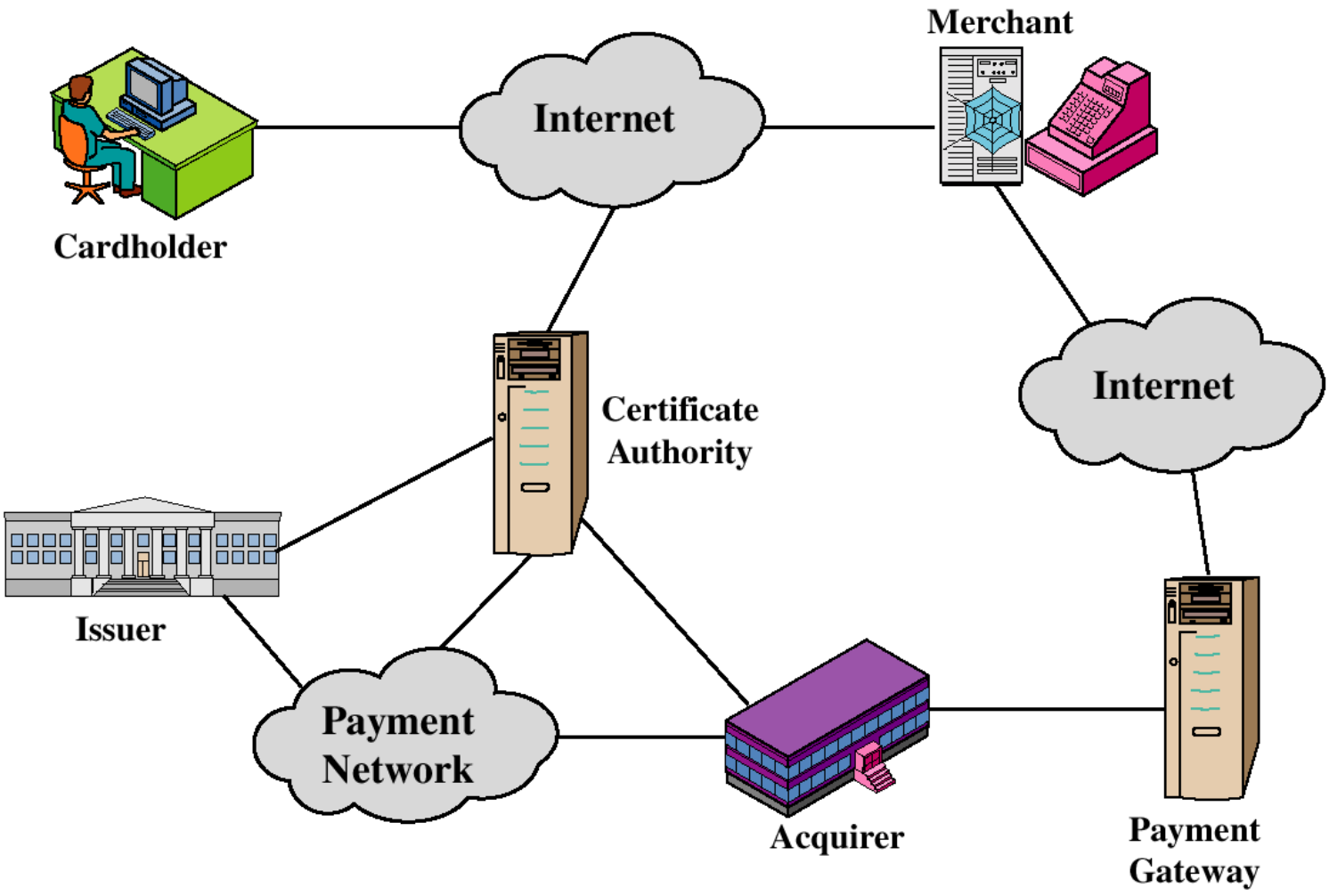
SET Services

- Provides a secure communication channel in a transaction.
- Provides tust by the use of X.509v3 digital certificates.
- Ensures privacy.

SET Overview

- Key Features of SET:
  - Confidentiality of information
  - Integrity of data
  - Cardholder account authentication
  - Merchant authentication

SET Participants

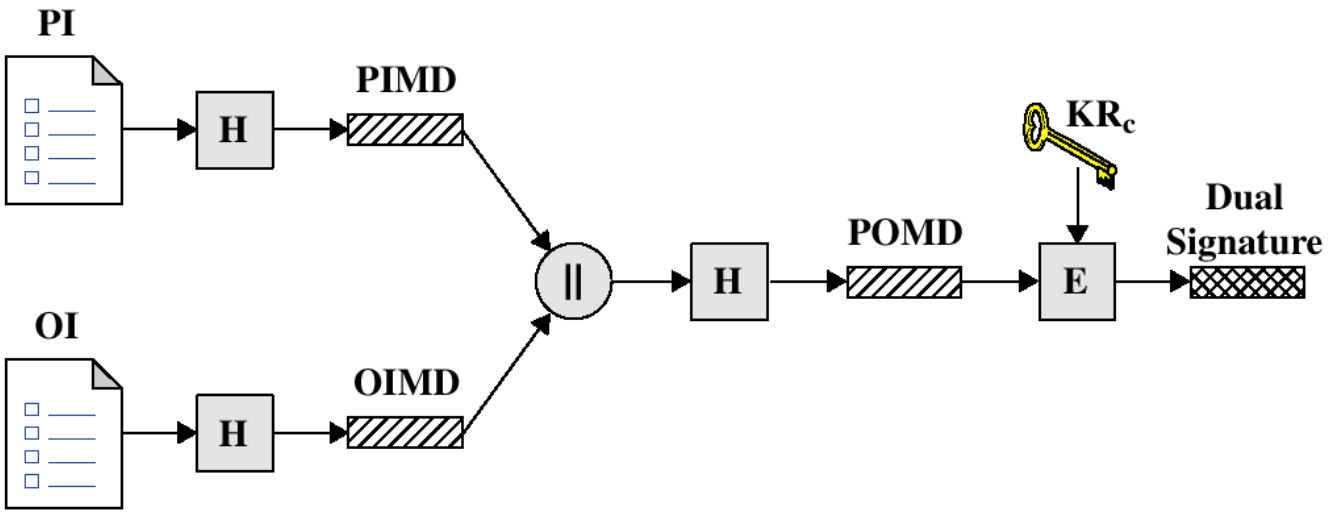


Sequence of events for transactions

1. The customer opens an account.
2. The customer receives a certificate.
3. Merchants have their own certificates.
4. The customer places an order.
5. The merchant is verified.
6. The order and payment are sent.
7. The merchant request payment authorization.
8. The merchant confirm the order.
9. The merchant provides the goods or service.
10. The merchant requests payments.

Dual Signature

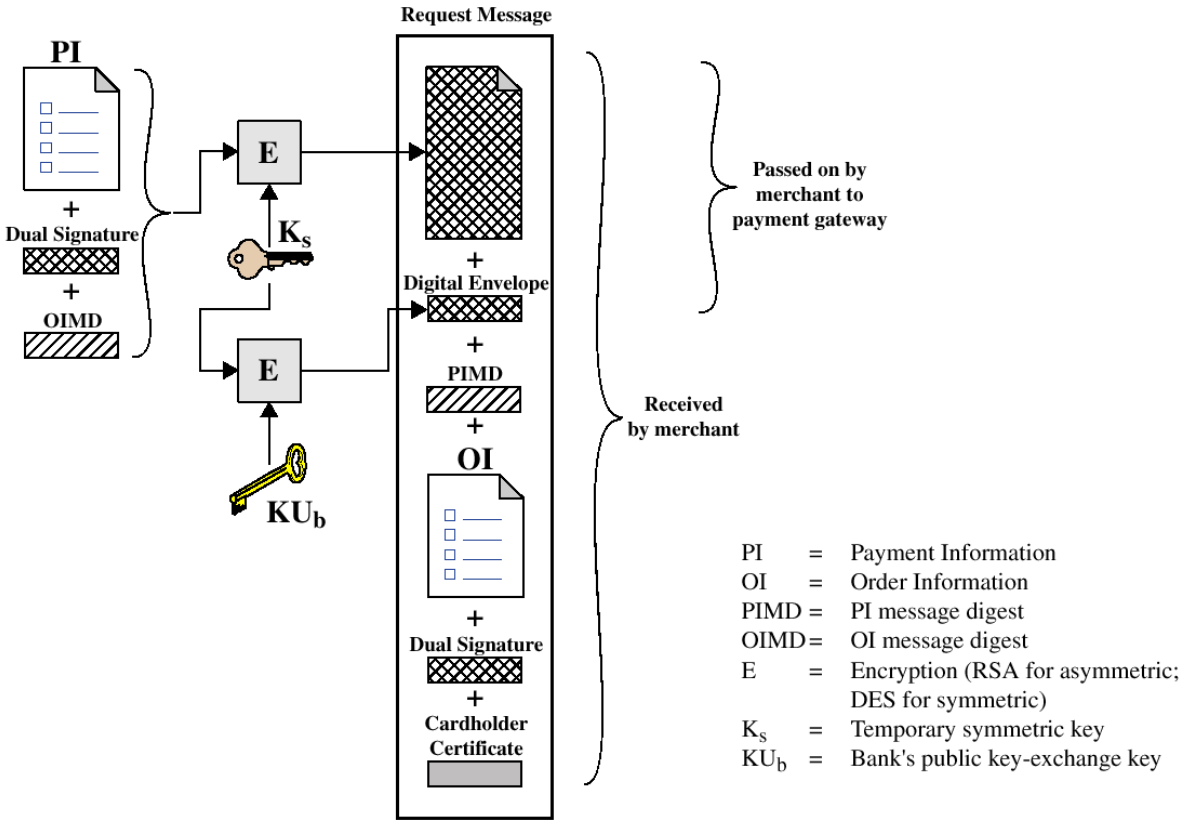
$$DS = E_{KR_c}[H(H(PI) \| \mathrm{H(OI)})]$$



PI = Payment Information
OI = Order Information
H = Hash function (SHA-1)
|| = Concatenation

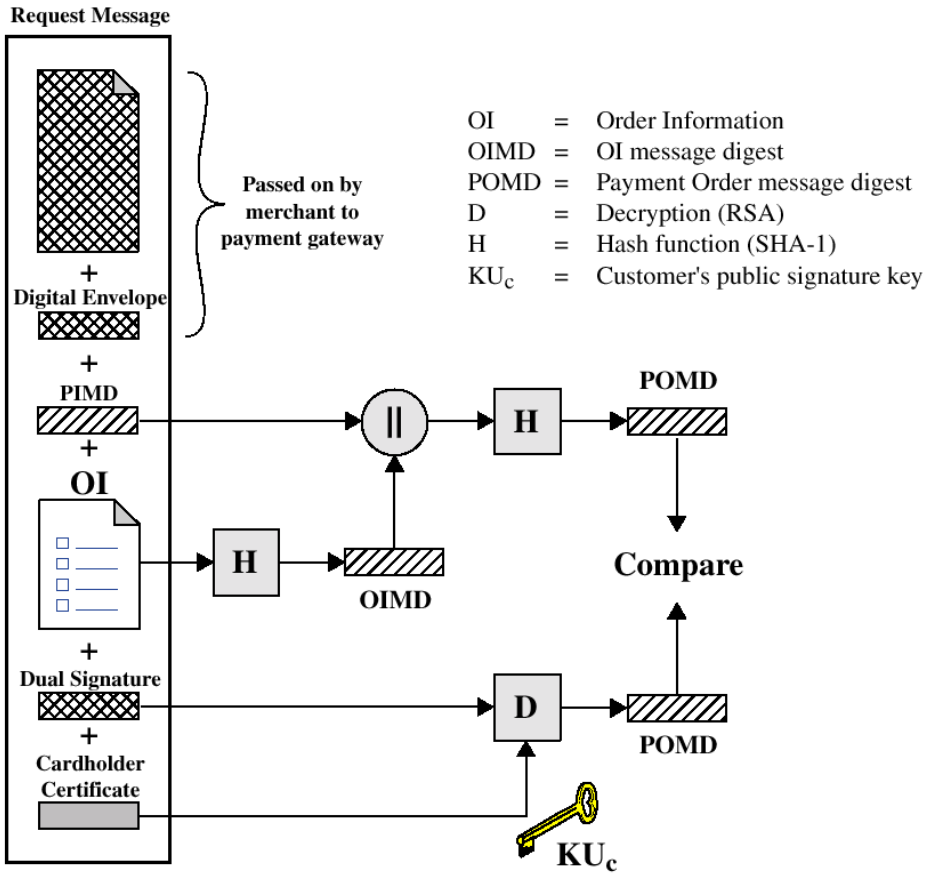
PIMD = PI message digest
OIMD = OI message digest
POMD = Payment Order message digest
E = Encryption (RSA)
KR_c = Customer's private signature key

Payment processing



Cardholder sends Purchase Request

Payment processing



Merchant Verifies Customer Purchase Request

Payment processing

- Payment Authorization:
  - Authorization Request
  - Authorization Response
- Payment Capture:
  - Capture Request
  - Capture Response

Recommended Reading and WEB sites

- Drew, G. *Using SET for Secure Electronic Commerce*. Prentice Hall, 1999
- Garfinkel, S., and Spafford, G. Web Security & Commerce. O'Reilly and Associates, 1997
- MasterCard SET site
- Visa Electronic Commerce Site
- SETCo (documents and glossary of terms)