

ECE-8843

<http://www.csc.gatech.edu/copeland/jac/8813-03/>

Prof. John A. Copeland
john.copeland@ece.gatech.edu
404 894-5177
fax 404 894-0035

Office: GCATT Bldg 579

email or call for office visit, or call Kathy Cheek, 404 894-5696

Chapter 7: 07-WebSec.pdf has PDF copies of slides from Chap. 7 of the text, “Network Security Essentials, Applications and Standards” by William Stallings)

	Threats	Consequences	Countermeasures
Integrity	<ul style="list-style-type: none"> • Modification of data 	<ul style="list-style-type: none"> • Loss of information 	<ul style="list-style-type: none"> • Cryptographic checksums
	<ul style="list-style-type: none"> • Trojan horse browser 	<ul style="list-style-type: none"> • Compromise of machine 	
	<ul style="list-style-type: none"> • Modification of memory 	<ul style="list-style-type: none"> • Vulnerability to all threats 	
	<ul style="list-style-type: none"> • Modification of messages in transit 		
Confidentiality	<ul style="list-style-type: none"> • Eavesdropping on the net 	<ul style="list-style-type: none"> • Loss of information 	<ul style="list-style-type: none"> • Encryption
	<ul style="list-style-type: none"> • Theft of info from server 	<ul style="list-style-type: none"> • Loss of privacy 	<ul style="list-style-type: none"> • Web Proxies
	<ul style="list-style-type: none"> • Theft of data from client 		
	<ul style="list-style-type: none"> • Info about network configuration 		
	<ul style="list-style-type: none"> • Information about which clients talk to server 		
Denial of Service	<ul style="list-style-type: none"> • Killing of user threads 	<ul style="list-style-type: none"> • Disruptive 	<ul style="list-style-type: none"> • Difficult to prevent
	<ul style="list-style-type: none"> • Flooding machine with bogus requests 	<ul style="list-style-type: none"> • Annoying 	
	<ul style="list-style-type: none"> • Filling disk or memory 	<ul style="list-style-type: none"> • Prevent users from getting work done 	
	<ul style="list-style-type: none"> • Isolating machines by DNS attacks 		
Authentication	<ul style="list-style-type: none"> • Impersonate users 	<ul style="list-style-type: none"> • Misrepresentation of user 	<ul style="list-style-type: none"> • Cryptographic techniques
	<ul style="list-style-type: none"> • Data forgery 	<ul style="list-style-type: none"> • Belief that false data is valid 	

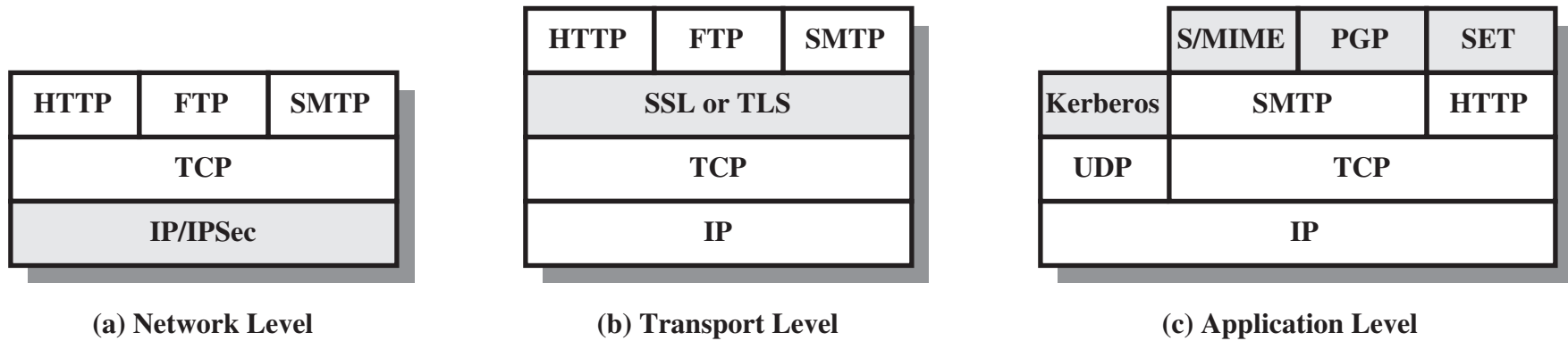


Figure 7.1 Relative Location of Security Facilities in the TCP/IP Protocol Stack

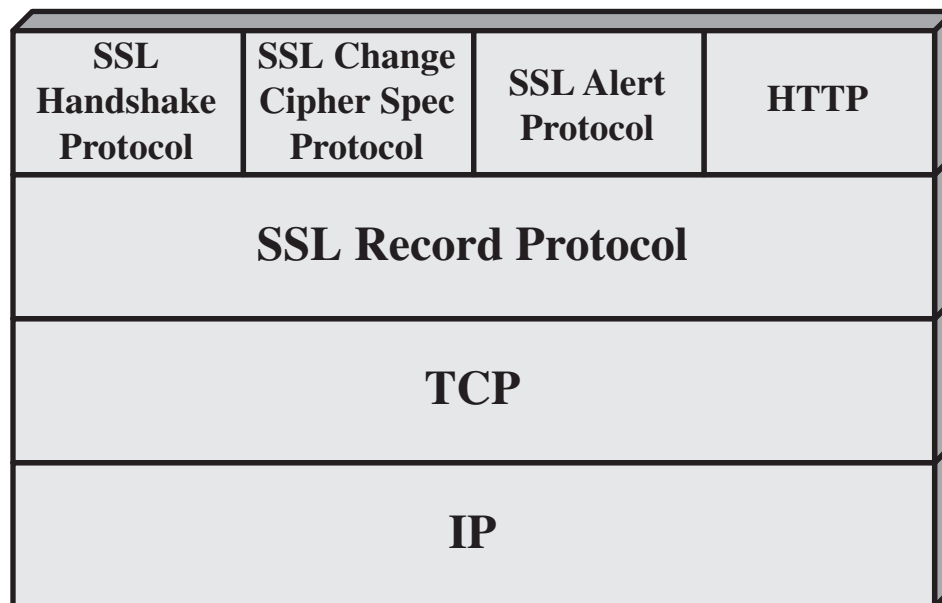


Figure 7.2 SSL Protocol Stack

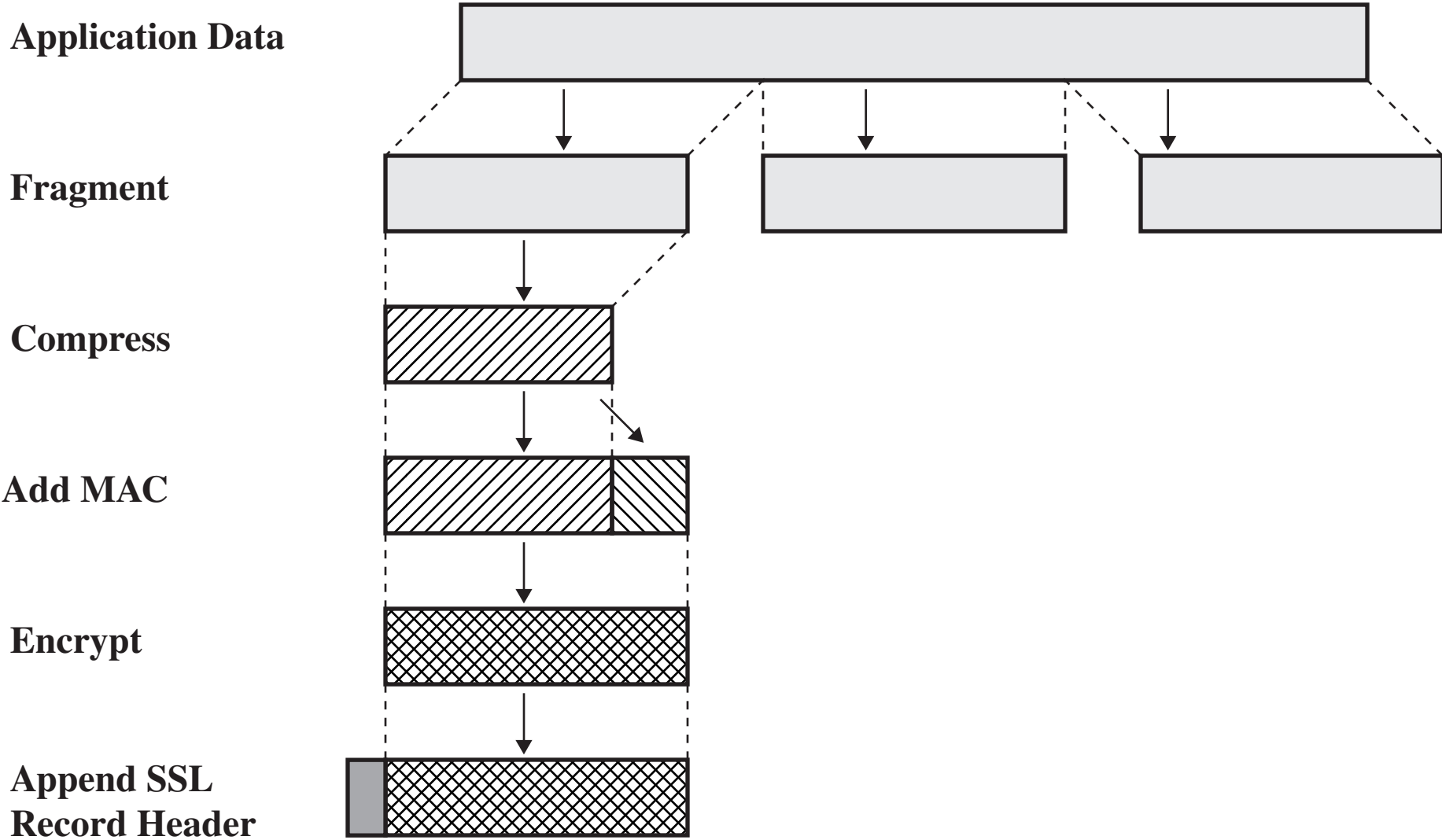


Figure 7.3 SSL Record Protocol Operation

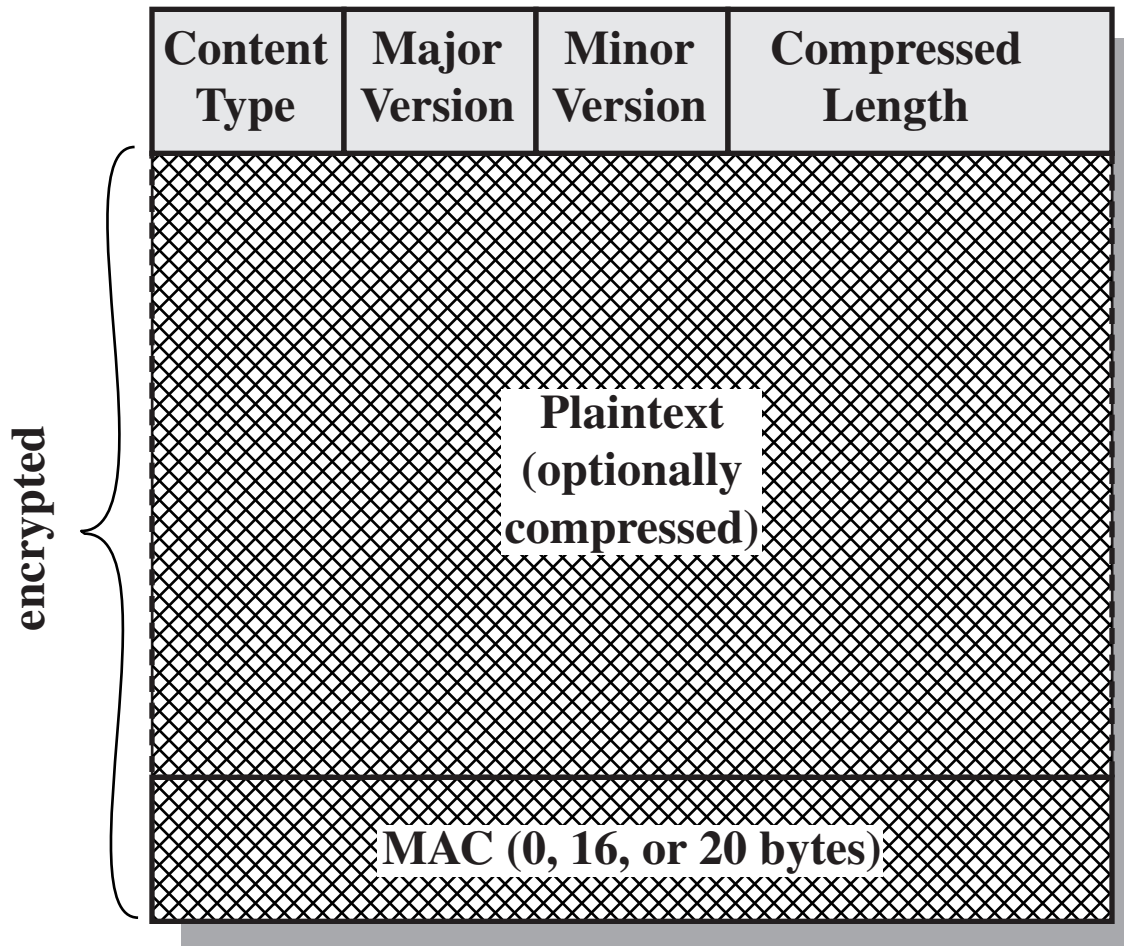
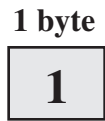
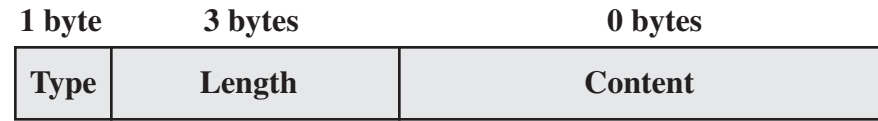


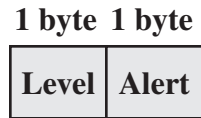
Figure 7.4 SSL Record Format



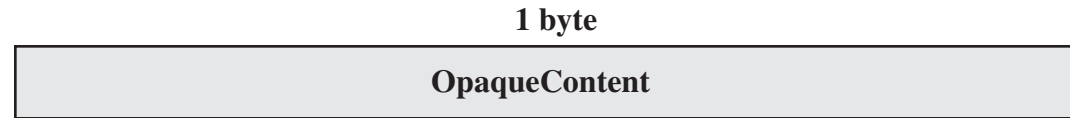
(a) Change Cipher Spec Protocol



(c) Handshake Protocol



(b) Alert Protocol



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

Figure 7.5 SSL Record Protocol Payload

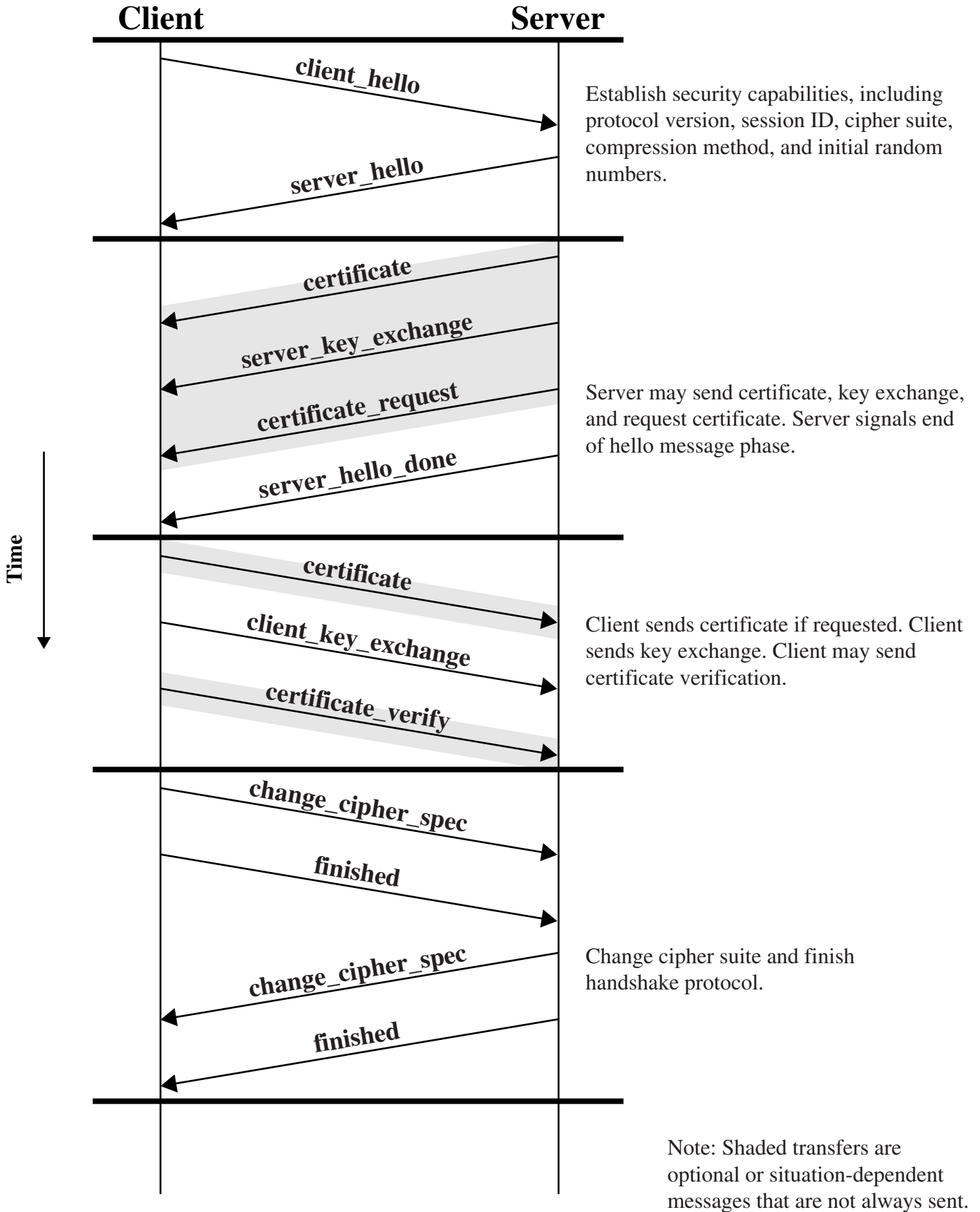


Figure 7.6 Handshake Protocol Action

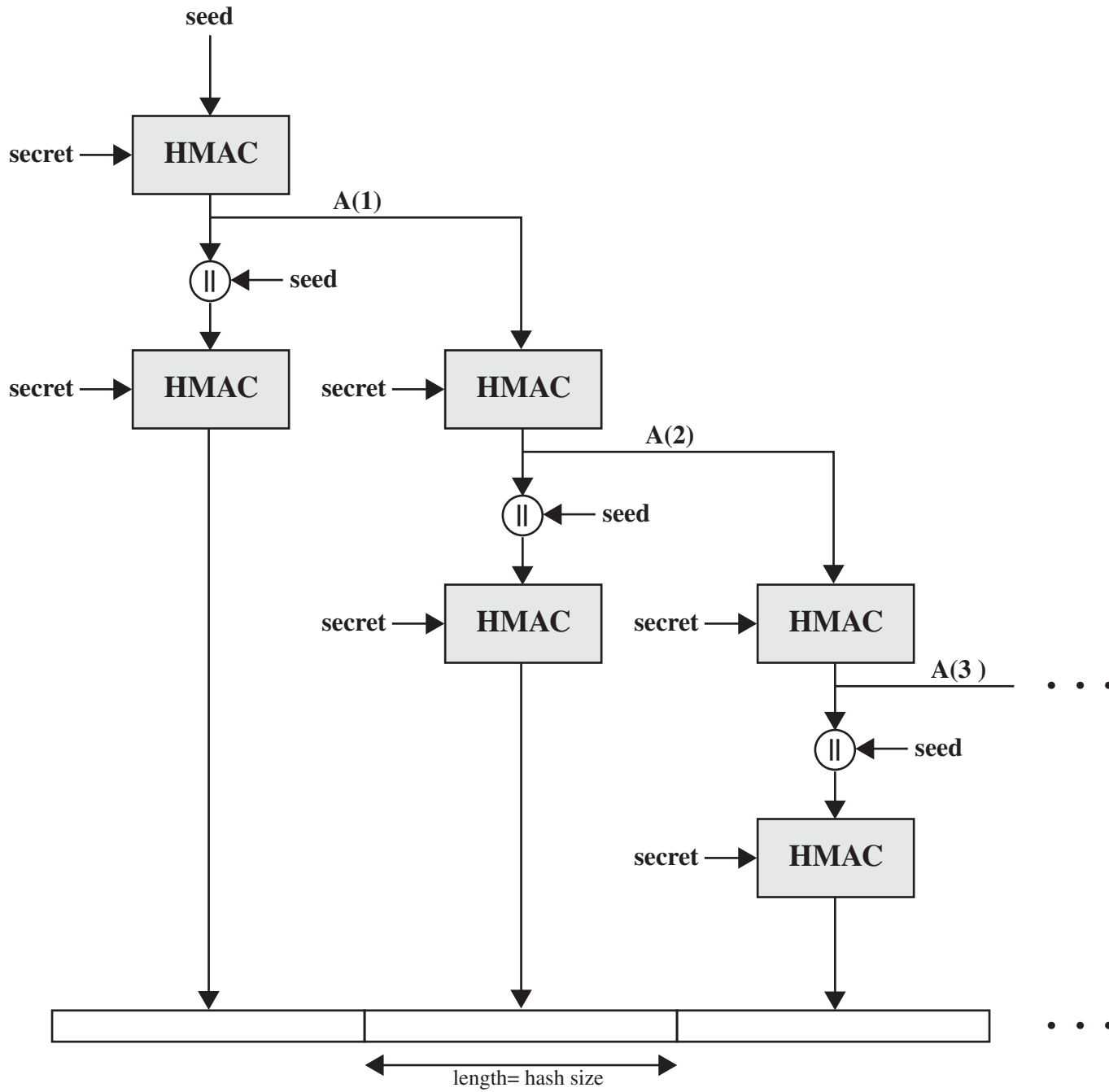


Figure 7.7 TLS Function P_hash (secret, seed)

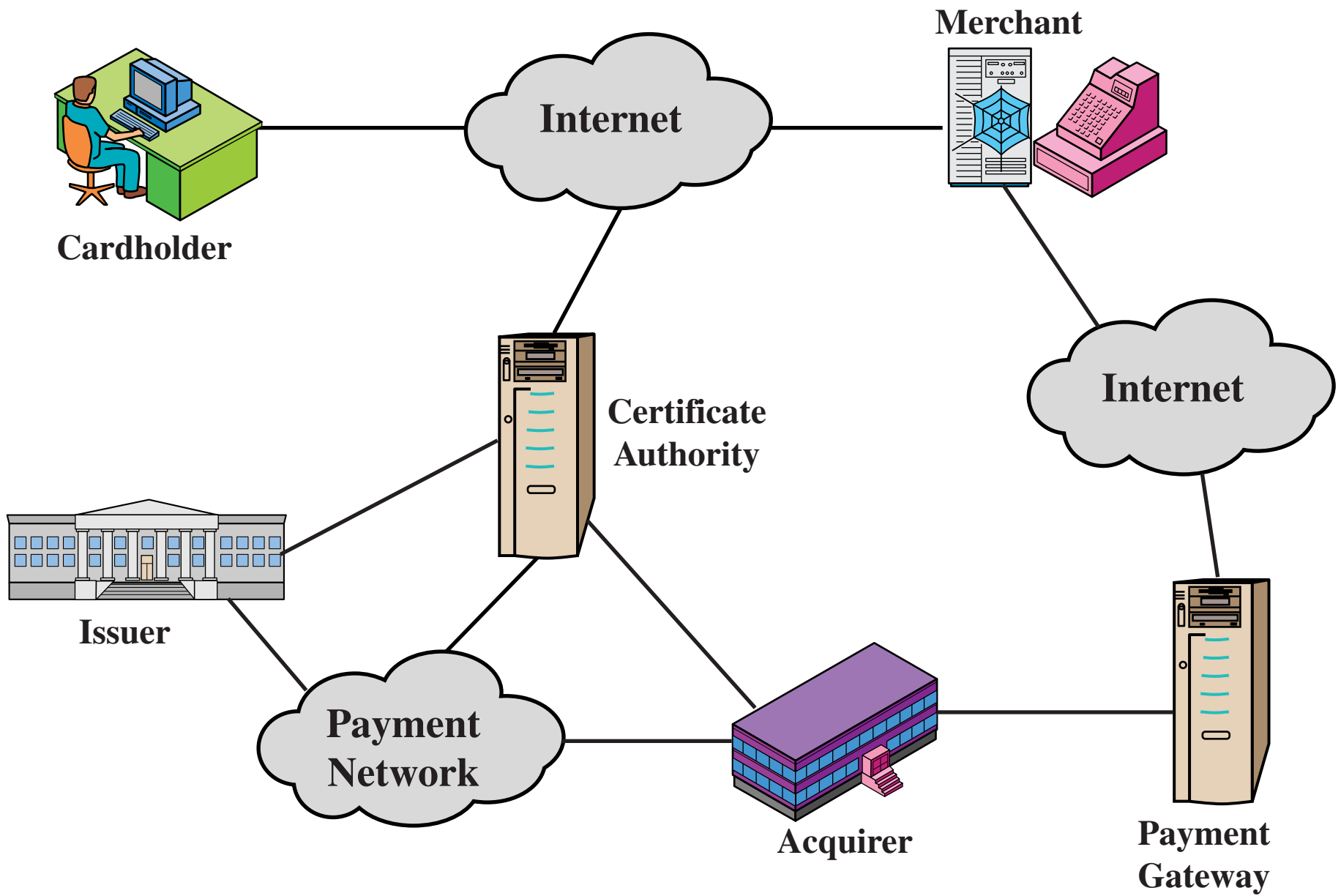
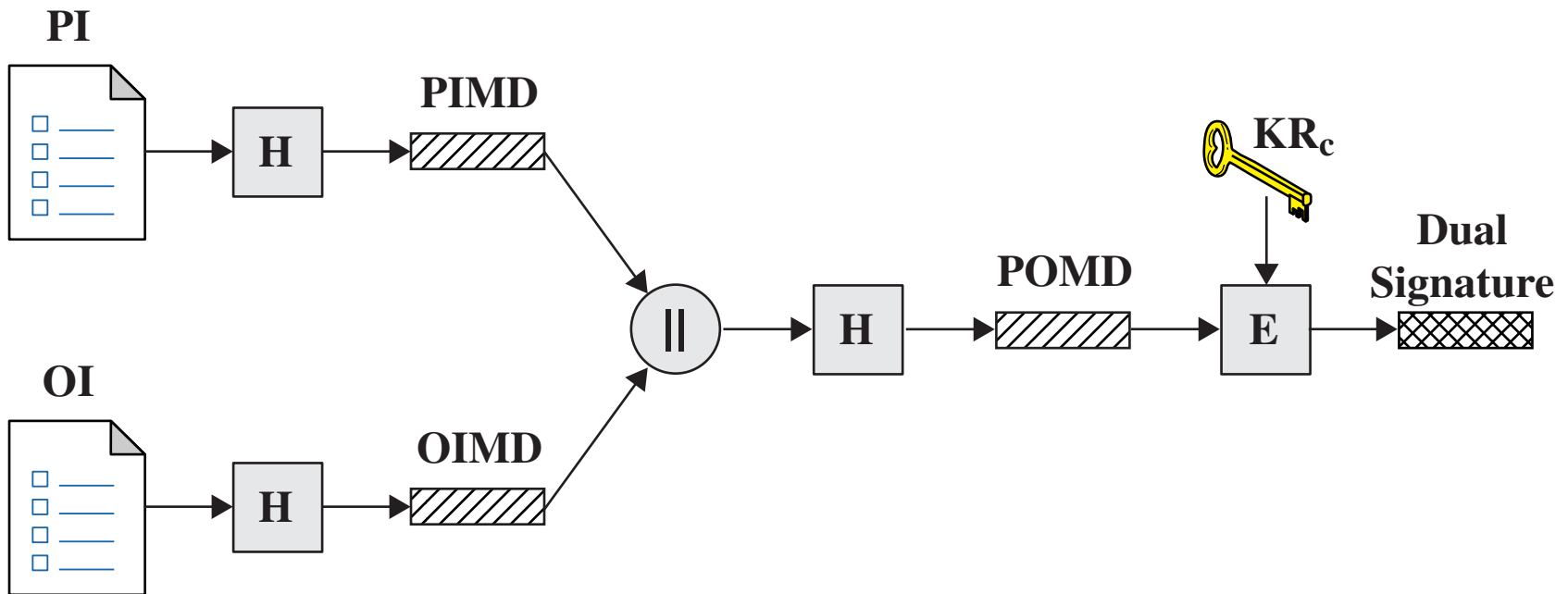


Figure 7.8 Secure Electronic Commerce Components



PI = Payment Information	PIMD = PI message digest
OI = Order Information	OIMD = OI message digest
H = Hash function (SHA-1)	POMD = Payment Order message digest
= Concatenation	E = Encryption (RSA)
	KR _c = Customer's private signature key

Figure 7.9 Construction of Dual Signature

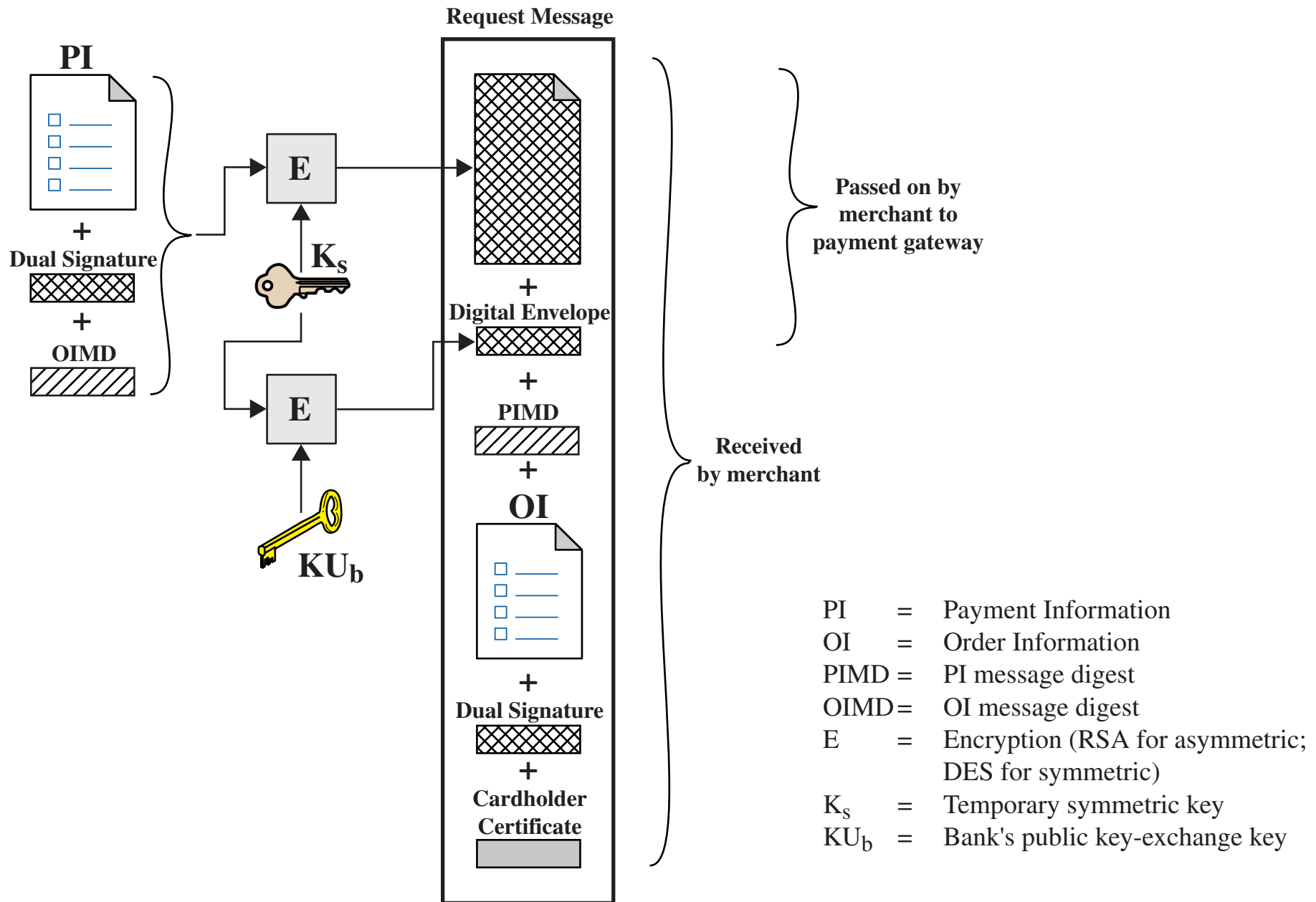


Figure 7.10 Cardholder Sends Purchase Request

Request Message

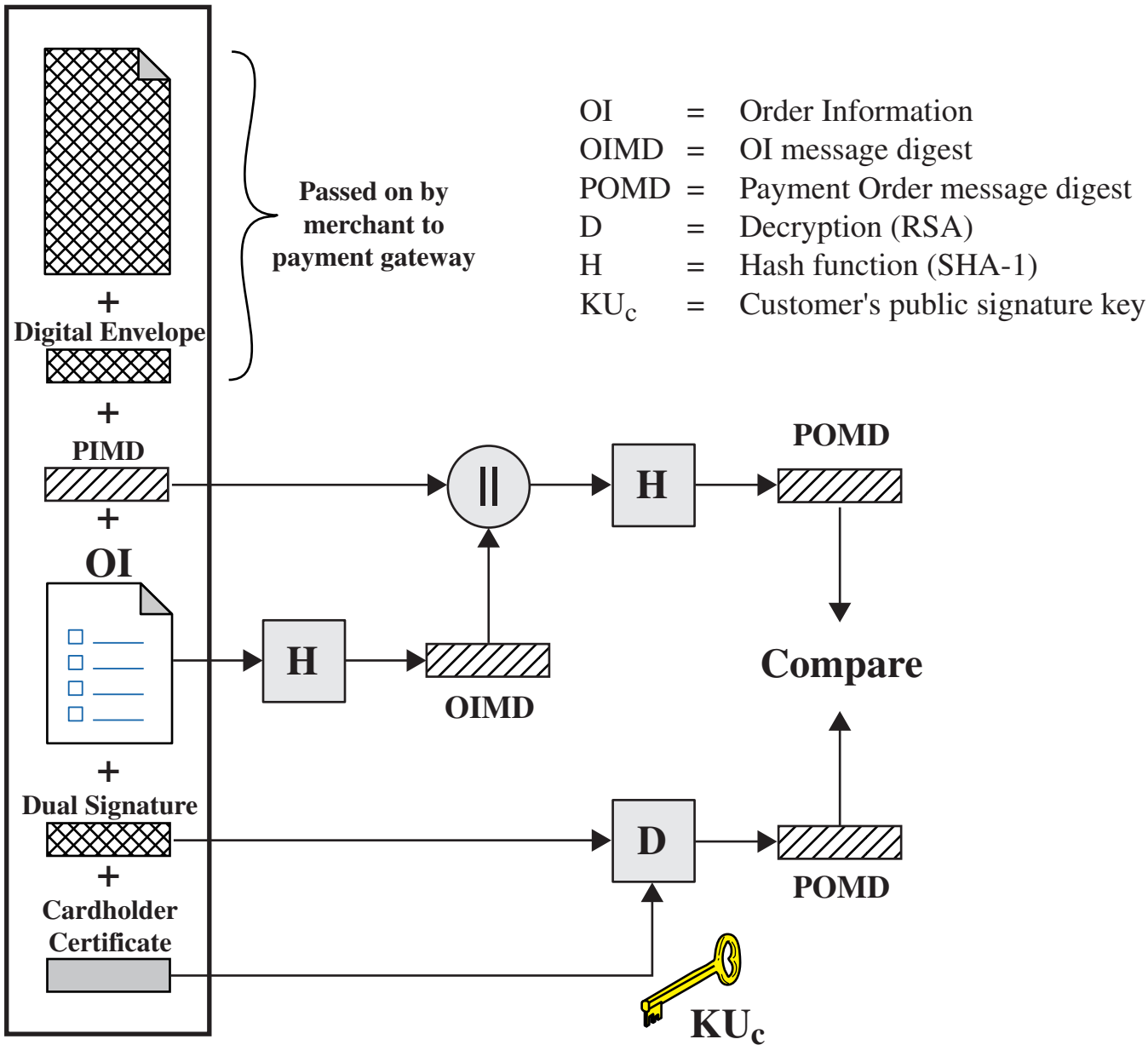


Figure 7.11 Merchant Verifies Customer Purchase Request