



Compliance Component

DEFINITION

<i>Name</i>	Cryptography for Web Servers
<i>Description</i>	<p>Cryptography for Web Servers provides authentication and encrypts the data stream. The most commonly used encryption protocol is Secure Socket Layer (SSL). HTTPS is Hypertext Transport Protocol integrated with SSL. SSL is sometimes referred to as SSL/TLS (Secure Socket Layer/Transport Layer Security).</p> <p>Secure Electronic Transaction (SET) provides a protocol and infrastructure specification for financial transactions that integrates into web servers. The use of SET requires collaboration with financial institutions.</p>
<i>Rationale</i>	Web servers are inherently unsecure and cryptography provides necessary security features.
<i>Benefits</i>	<p>Cryptography for web servers can provide the following:</p> <ul style="list-style-type: none"> • Server authentication • Client authentication • Data integrity • Confidentiality • User authentication (SET only) <p>SSL protects TCP services such as HTTP, FTP, SMTP and telnet.</p>

ASSOCIATED ARCHITECTURE LEVELS

<i>List the Domain Name</i>	Security
<i>List the Discipline Name</i>	Technology Controls
<i>List the Technology Area Name</i>	Cryptography
<i>List Product Component Name</i>	

COMPLIANCE COMPONENT TYPE

<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	

COMPLIANCE DETAIL

<i>State the Guideline, Standard or Legislation</i>	<p><i>Note: S/HTTP (Secure Hypertext Transport Protocol) is not the same as HTTPS. S/HTTP is not recommended because it requires users to install a specific web browser and is not widely accepted.</i></p> <ul style="list-style-type: none"> • When transmitting sensitive or critical information over the web, users shall use SSL with at least: <ul style="list-style-type: none"> ○ Advanced Encryption Standard (AES) 128-bit encryption or Triple Data Encryption Standard (3DES) 168/112-bit encryption, and ○ Digital Signature Standard (DSS) or RSA with 1024 bit
---	---

	keys, and Secure Hash Algorithm-1 (SHA-1). <ul style="list-style-type: none"> • SET shall be used when transferring funds over the web. 		
<i>Document Source Reference #</i>	NIST Special Publications 800-44 – Guidelines for Securing Public Web Servers; and CERT Security Improvement Module http://www.cert.org/security-improvement/practices/p080.html		
Standard Organization			
<i>Name</i>	NIST	<i>Website</i>	http://csrc.nist.gov
<i>Contact Information</i>			
Government Body			
<i>Name</i>		<i>Website</i>	
<i>Contact Information</i>			
KEYWORDS			
<i>List all Keywords</i>	SSL, HTTPS, S/HTTP, FTP, SMTP, AES, 3DES, Digital Signature, SHA-1, TLS, Secure Electronic Transaction, SET, financial transaction, credit card, debit card		
COMPONENT CLASSIFICATION			
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i>	<input checked="" type="checkbox"/> <i>Current</i>	<input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>
Rationale for Component Classification			
<i>Document the Rationale for Component Classification</i>			
Conditional Use Restrictions			
<i>Document the Conditional Use Restrictions</i>			
Migration Strategy			
<i>Document the Migration Strategy</i>			
Impact Position Statement			
<i>Document the Position Statement on Impact</i>			
CURRENT STATUS			
<i>Provide the Current Status</i>	<input type="checkbox"/> <i>In Development</i>	<input type="checkbox"/> <i>Under Review</i>	<input checked="" type="checkbox"/> <i>Approved</i> <input type="checkbox"/> <i>Rejected</i>
AUDIT TRAIL			
<i>Creation Date</i>	04/13/2004	<i>Date Accepted / Rejected</i>	4/13/04
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>		<i>Last Date Updated</i>	
<i>Reason for Update</i>			