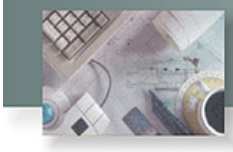

Compliance Component

DEFINITION	
Name	Hardware vs. Software Encryption
Description	Encryption processing (coding or decoding) on the host and/or client system can take place by one of two methods: (1) software using shared processor, or (2) dedicated or auxiliary hardware.
Rationale	A decision on where encryption should take place is needed before deploying an application that requires encrypted transport or storage. Cost, performance, support, and perceived success of the business application will hinge on the analysis used to determine encryption processing capacity needs and methods.
Benefits	• A suitable analysis on encryption method (hardware vs. software) can avert scalability issues. Scalability problems often lead to costly hardware, software, or infrastructure solutions to remedy the problem. • Knowledge of the business application and target audience help staff determine scalability needs and the supporting technology base. • Each approach (hardware vs. software) has unique benefits with relation to cost and support when deployed properly.
ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Cryptography
List Product Component Name	
COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	
COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	**General Encryption Statements** • Encrypted transmissions are processing-intensive functions on the client and/or server endpoints • Encrypted storage is a processing-intensive function on the system side issuing the “save” for the data in question. • The processing load increases with greater key length and more complex algorithm. **Software-based Encryption** • Software-based encryption is normally performed using existing processing capacity in the client/host system. • Software encryption shares processing resources with all other programs/processes on the system, which could impact

	performance of all other functions of the system.
	• Scalability problems may necessitate additional processors in the system, or multiple systems to meet scalability needs.
	• In small application environments (a single workstation or a server with few concurrent users), software-based encryption is normally the most cost-effective approach.
	Distribution
	• The information protected with encryption shall be transmitted over a different communication channel than the keys used to govern the encryption process.
	• Private and secret encryption keys transmitted over communication lines shall be sent in encrypted form with one of the following key exchange algorithms:
	  • RSA
	  • Elliptic Curve
	  • Diffie-Hellman
	Hardware-based Encryption
	• Hardware encryption is normally performed by dedicated hardware in the client/host system.
	• Hardware encryption has minimal impact on other programs/processes because it uses separate processing resources.
	• Scalability is normally achieved by adding more components to an existing device.
	• Hardware-based encryption normally provides much greater throughput capacity and speed in large-scale environments.
	• In medium and larger environments, hardware-based encryption is normally the most scalable, cost-effective solution.

Document Source Reference #	www.cisco.com www.microsoft.com Search criteria: hardware-based encryption

Standard Organization			
Name		*Website*	
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC); U.S. Department of Commerce, Bureau of Industry and Security	*Website*	http://csrc.nist.gov/ http://www.bxa.doc.gov/encryption/

Contact Information	inquiries@nist.gov			
KEYWORDS				
List all Keywords	Encryption, scalability			
COMPONENT CLASSIFICATION				
Provide the Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*
Rationale for Component Classification				
Document the Rationale for Component Classification				
Conditional Use Restrictions				
Document the Conditional Use Restrictions				
Migration Strategy				
Document the Migration Strategy				
Impact Position Statement				
Document the Position Statement on Impact				
CURRENT STATUS				
Provide the Current Status)	☐ *In Development*	☐ *Under Review*	☒ *Approved*	☐ *Rejected*
AUDIT TRAIL				
Creation Date	04/13/2004	*Date Accepted / Rejected*	4/13/04	
Reason for Rejection				
Last Date Reviewed		*Last Date Updated*		
Reason for Update				