Compliance Component

DEFINITION

Name	Message Authentication
Description	Message authentication is a technique used to detect unauthorized changes to, or corruption of, the contents of a transmitted electronic message.
Rationale	Provides a means to validate the integrity of information transmitted over or stored in an unsecured environment.
Benefits	Provides: • Non-Repudiation o When the system provides data integrity a receiver can be sure of both the sender's identity and that he is receiving the data that sender meant to send.

ASSOCIATED ARCHITECTURE LEVELS

List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Identification and Authentication
List Product Component Name	

COMPLIANCE COMPONENT TYPE

Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL

State the Guideline, Standard or Legislation	Message authentication must be considered for applications where there is a security requirement to protect the integrity of the message content such as: • Electronic funds transfer • Specifications • Contracts • Proposals • Other similar electronic data exchanges of high importance An assessment of security risks should be carried out to determine if message authentication is required and to identify the most appropriate method of message authentication. **Recommended methods of message authentication**

	Non-repudiation Non-repudiation should be used where it is necessary to resolve disputes of authenticity such as dispute involving the use of a signature on an electronic contract or payment. **Digital Signatures** Digital signatures provide a means of protecting the authenticity and integrity of electronic documents. • They can be used in electronic commerce where there is a need to verify who signed an electronic document and check whether the contents of the signed document have been changed. (See Digital Signatures CC). These services are based on the use of encryption and digital signature techniques (see Cryptography TA). **Note:** Message authentication is not designed to protect the contents of a message from unauthorized disclosure.		
Document Source Reference #			
Standard Organization			
Name	SP 800-63; FIPS 201, FIPS 198, SP 800-61, ISO 17799-2000 (E)	*Website*	
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
KEYWORDS			
List all Keywords	Encryption, non-repudiation, digital signature, cryptography, validate, integrity.		
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	01/04/2007	*Date Accepted / Rejected*	03/23/2007
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			