Compliance Component

DEFINITION

Name	Secret Key Cryptography
Description	Secret Key Cryptography, also known as Symmetric Key, is a cryptographic method where a single key is shared between the sender and recipient, or is implemented by a single user.
Rationale	Secret Key Cryptography enables confidentiality and integrity.
Benefits	• Secret Key Cryptography is generally faster than Public Key Cryptography because it has a higher rate of data throughput and uses shorter keys, and is most often used for encrypting data. Notes: • Secret key distribution is prone to interception and/or disclosure, which can lead to impersonation and/or unauthorized disclosure or modification of the data. • Secret Key management is more difficult than Public Key because the keys must be changed frequently, and there are many more keys to be managed. • Secret key encryption does not support strong authentication and non-repudiation because both parties share the same key. Therefore, it is possible for one party to create a message with the shared secret key and falsely claim it had been sent by the other party. • Streaming cipher algorithms (such as RC4) are susceptible to compromise and are not recommended.

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	• There are two algorithms suitable for Secret Key Cryptography: o Triple Data Encryption Standard (3DES) o Advanced Encryption Standard (AES) • Approved key length for Secret Key shall be at least: o 168-bits for 3DES o 192-bits for AES

Document Source Reference #	(All found at www.csrc.nist.gov) NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook (Oct 1997) NIST SP 800-21, Guideline for Implementing Cryptography in the Federal Government (Nov 1999) NIST Federal Information Processing Standards (FIPS) 197, Advanced Encryption Standard (AES) (Nov 2001)		
Standard Organization			
Name	NIST	*Website*	www.csrc.nist.gov
Contact Information	inquiries@nist.gov		
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	www.csrc.nist.gov/publications/fips/index.html
Contact Information	inquiries@nist.gov		
KEYWORDS			
List all Keywords	AES, 3DES, RC4, symmetric key, block cipher, stream cipher, algorithm		
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			