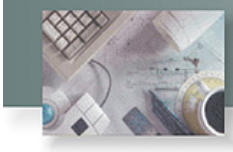

Compliance Component

DEFINITION	
Name	Encryption Key Management
Description	Encryption Key Management encompasses the policies and practices used to protect encryption keys against modification and unauthorized disclosure or export outside the United States.
Rationale	The proper management of encryption keys is essential to the effective use of cryptography for security purposes. The security of information protected by cryptography directly depends on the protection afforded the keys.
Benefits	• Key management provides for the secure generation, storage, distribution, life cycle and export of keys.

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** • State agencies shall control centrally stored keys and system software, even when developed or maintained by a contractor. State agencies shall also control the configuring of the key management hardware and software. • Key management responsibility may only be delegated to a party who has passed a background check and signed a confidentiality agreement. • Encryption systems shall be designed such that no single person has full knowledge of any single encryption key. This is achieved by separation of duties (use of more than one individual to handle a certain important activity) and dual control (two people shall be simultaneously present for an important activity to be accomplished). • Users shall be trained to keep their encryption keys secure and shall be made aware of their liabilities and responsibilities. **Generation** • Encryption algorithms used to protect production information and

	information systems shall adhere to industry standards.
	• Each individual key record shall be signed to enable tamper detection.
	• Encryption keys shall be generated by means which are not practically discernable by an adversary.
	• Materials to develop encryption keys as well as the keys themselves shall be kept secured when not in use and throughout the life cycle of the information.
	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
	Storage
	• Access to encryption keys shall be strictly limited to those who have a need-to-know.
	• Encryption keys shall be prevented from unauthorized disclosure via technical controls such as encryption under a separate key and use of tamper-resistant hardware.
	• Encryption or split knowledge and dual control shall be used to protect centrally stored user secret keys, private keys, master keys, to secure the distribution of user tokens, and to initialize all crypto-modules.
	• If a key is stored on a token and a PIN is used to access the token, then only that token's owner shall have possession of both the token and its corresponding PIN. The token and its PIN shall be distributed via separate secure mailings.
	• Software at the central key management site shall be electronically signed and periodically verified to check the integrity of the code.
	• All centrally stored data that is related to user keys shall be signed for integrity, and encrypted or use dual control and split knowledge for confidentiality.
	• Automated resources that generate keys and initialization vectors require layered physical protection to prevent disclosure, modification or replacement by those without a need to know.
	• Backup copies shall be made of central/root keys and stored off-site.

	• Encryption keys and the data they protect shall be stored on separate physical media. • Automatic backup systems shall not copy the readable version of private keys used for digital signatures and digital certificates. Readable backups are prevented by keeping private keys in smart cards or in encrypted form. • Encryption keys used to conceal backup data shall themselves be backed-up. These keys shall also be stored with security measures comparable to or more stringent than measures applied to the backed-up data. • All encryption processes running on production information systems shall include key recovery functions. Key escrow allows management to recover encrypted information should there be system errors, human errors, or other problems. • Keys used for digital signatures, digital certificates, and user authentication shall not be included in a key escrow arrangement with a third party. **Life Cycle** • The crypto-period (the time a key can be used for signature verification or decryption) shall be determined based on the sensitivity of the information and the risk of key compromise. • All encryption keys shall have a stated life and shall be changed on or before the stated expiration date. • Key lifetime (the time during which a key can be used to generate a signature or perform encryption) is dependent upon the user's roles, responsibilities, the applications used, and the security services provided by the key. • Reissuing keys shall be performed often enough to minimize the loss caused by compromise, but not so often that it becomes a burden. • The secrecy of any encryption key used for confidentiality purposes shall be maintained until all of the protected information is no longer considered confidential. • Private digital signature keys shall be kept confidential and accessible for at least the number of years that they might be used in a legal challenge. • All supplies used for the generation, distribution, and storage of keys shall be protected from disclosure to unauthorized persons. When they are not longer needed, they shall be destroyed by pulping, shredding, burning, or other approved methods. **Key Change or Compromise** • State agencies shall have a plan for handling the compromise or suspected compromise of central/root keys or key components at a central site before the system goes live. This includes key recovery capabilities for terminated users.

	• Encryption keys that have been compromised shall immediately be revoked retroactively to the last known time when the keys were safe. • Key management systems shall be capable of designating a key as “lost” or “compromised”, so that signatures generated prior to a specified date can still be verified. • If a public encryption key has been posted on a publicly accessible location, all regular correspondents shall be notified whenever there is a change in the public key. **Export** • The U.S Government controls the export of cryptographic implementations. For the current rules, refer to Title 15 of the Code of Federal Regulations. • "Mass market" encryption commodities and software with symmetric key lengths exceeding 64-bits may be exported following a 30-day review by the U.S. Department of Commerce.
Document Source Reference #	NIST SP 800-18 (www.csrc.nist.gov/publications/nistpubs); CERT Guide to System and Network Security Practices (www.cert.org/security-improvement/); 15 CFR 740.17; 15 CFR Part 742; and 15 CFR Part 774, Category 5, Part 2.

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	Export, dual control, separation of duties, key life-cycle, crypto-period, key distribution, key storage, key escrow, key recovery, RSA, elliptic curve, Diffie-Hellman

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*	4/13/2004
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			