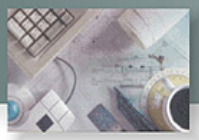

Technology Area

DEFINITION	
Name	Cryptography
Description	Cryptography transforms data into a secured format. It is a critical tool for protecting information and is used to provide many security services, such as keeping data secret, enabling digital signatures, and ensuring that data has not been modified. Cryptography both depends on and supports other security controls, including physical security, identification and authentication, logical access controls, and audit trails.
Rationale	Data needs special protection if it is sensitive, has a high value, or is vulnerable to unauthorized disclosure or undetected modification. Cryptographic methods protect against intentional or accidental compromise and alteration of data.
Benefits	• Protects data confidentiality. • Protects data integrity. • Enables authentication of user identity. • Protects data during transmission and in storage.
ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls
Associated Compliance Components	

List the Compliance Component Names	• Secret Key Cryptography
	• Public Key Infrastructure
	• Hashing
	• Crytography Design/Implementation
	  o Hardware vs. Software Encryption
	  o Encryption Key Management
	• Cryptography Uses
	  o Digital Signature
	  o Cryptography for Stored Data
	  o Cryptography for VPN
	  o Cryptography for Email
	  o Cryptography for Wireless
	  o Cryptography for Web Servers

Associated Product Components	
List the Product Component Names	• Entrust Secure Messaging Solution • VeriSign Digital Certificates
TECHNOLOGY AREA DETAIL	
Supporting Documentation	NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST SP 800-21, Guideline for Implementing Cryptography in the Federal Government, FIPS 140-2, Security Requirements for Cryptographic Modules

Document Source Reference #	www.csrc.nist.gov/publications/nistpubs		
Standard Organization / 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		
Name		*Website*	
Contact Information			
KEYWORDS			
List Keywords	PKI, encryption, digital certificate, AES, DES, Skipjack, block cipher, DSA, RSA, ECDSA, digital signature, SHA-1, SHA-256, SHA-384, SHA-512, public key, secret key, symmetric key, asymmetric key, PRING, random number generator, DAC, MAC, HMAC		
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			