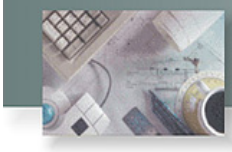

Compliance Component

DEFINITION	
Name	Cryptography for Email
Description	Cryptography for Email is accomplished through the implementation of S/MIME (Secure / Multipurpose Internet Mail Extensions) specifications for securing electronic mail. MIME (Multipurpose Internet Mail Extensions) allows the use of multiple-text effects (e.g., bold, italic, various font sizes, and colors) as well as the transfer of digital information. S/MIME is based upon the MIME standard, and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and/or encrypted objects.
Rationale	Email is inherently unsecure. Cryptography allows the user to add a set of security features to email.
Benefits	• The basic security services offered by S/MIME are: o authentication, o non-repudiation of origin, o message integrity, and o message confidentiality. • Optional security services include: o signed receipts, o security labels, o secure mailing lists, and o an extended method of identifying the signer's certificate(s). *NOTE: Interoperability may not be possible due to differing S/MIME choices of options selected by different vendors. Standards developers allow many options within communications systems, even if all standards are rigidly followed.* *NOTE: An alternative to an integrated email encryption system is to encrypt the sensitive data separately (see Cryptography for Stored Data) and email the encrypted files as attachments.* *NOTE: The use of PGP (Pretty Good Privacy) is **not** recommended as a statewide standard since the control of certificates is not centralized. PGP is suitable only for small groups or single users.*

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technical Controls

List the Technology Area Name	Cryptography		
List Product Component Name	• VeriSign • Entrust		
COMPLIANCE COMPONENT TYPE			
Document the Compliance Component Type	Guideline		
Component Sub-type			
COMPLIANCE DETAIL			
State the Guideline, Standard or Legislation	• S/MIME shall be used when emailing sensitive or critical information requiring confidentiality, reliability, authentication and/or non-repudiation over a public access line, such as the Internet or wireless. • S/MIME requires a Public Key Infrastructure (PKI) with X.509 (PKIX) Certificates, either purchased from a Certificate Authority vendor or created by an internal Certificate Authority. • S/MIME compliant implementations shall process both "clear" and "opaque" signed messages. o "Clear" signed messages can be read by non-S/MIME clients, although signatures cannot be automatically processed and verified by such clients. o "Opaque" signed messages are encoded such that the recipient requires an S/MIME email client to automatically read the message. • S/MIME compliant implementations shall use the Lightweight Directory Access Protocol (LDAP) to obtain certificates and Certificate Revocation Lists (CRLs) to check that the proper fields within each certificate match the sender's name.		
Document Source Reference #			
Standard Organization			
Name	NIST SP 800-49	*Website*	http://csrc.nist.gov/publications/nistpubs/800-49/sp800-49.pdf
Contact Information			
Government Body			
Name	NIST	*Website*	http://csrc.nist.gov
Contact Information			
KEYWORDS			
List all Keywords	MIME, S/MIME, LDAP, opaque, clear, X.509, certificate, PKI, PGP		
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	04/13/04	*Date Accepted / Rejected*	4/13/04
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			