Compliance Component

DEFINITION	
Name	Public Key Infrastructure (PKI)
Description	Public Key Infrastructure (PKI) is a cryptography method that provides a mathematical identification of a specific resource. In public key systems, there are two encryption keys: a *public* key and a *private* key. The public key is different from the private key, but they are mathematically related.
Rationale	PKI enables confidentiality, authentication, digital signatures, and integrity.
Benefits	• Provides a means of identification and authentication • Provides non-repudiation (entity integrity) • Provides confidentiality • Provides data integrity • Provides the means to read encrypted documents through key recovery • PKI is best suited for a multi-user environment • Greater ease of distributing encryption 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	• Functional elements of a public key infrastructure should include: 1. A Certification Authority (CA) which confirms the identities of parties sending and receiving communications. The CA also issues and processes Certificate Revocation Lists (CRLs), which are lists of certificates that have been revoked. 2. Registration Authorities which are entities trusted by the CA to register or vouch for the identity of users to a CA. 3. Repositories which are databases of active digital certificates for a PKI system. 4. Archives which store and protect sufficient information to determine if an inactive digital signature on a document should be trusted. 5. PKI users. • Certificates must adhere to the IETF (Internet Engineering Task Force) X.509 standard.

	• Each entity in an authentication exchange must use an approved digital signature algorithm to generate and/or verify digital signatures (see the MAEA Digital Signatures Compliance Component). • There are two algorithms suitable for asymmetric key certificate generation and verification: o Rivest-Shamir-Adleman, a reversible Digital Signature Algorithm (RSA). o Elliptic Curve Digital Signature Algorithm (ECDSA). • Encryption key length shall be at least 512-bits for RSA and ECDSA. • Public key certificates must be generated prior to the authentication exchange. • Public key certificates must be readily accessible to any entity that wishes to authenticate another entity. • Organizations may either purchase a PKI product and become their own Certification Authority or subscribe to a PKI service. • A private key must remain accessible only to its owner.		
Document Source Reference #			
Standard Organization			
Name	NIST SP 800-12 and 800-32	*Website*	http://csrc.nist.gov/publications/
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	Asymmetric, Digital Signature, RSA, ECDSA, elliptic curve, key length		
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			