# COMPLIANCE COMPONENT

## DEFINITION

| | |
|---|---|
| *Name* | Digital Signature |
| *Description* | The digital signature is based on Public Key Infrastructure (PKI) and is a result of a cryptographic operation that guarantees signer authenticity, data integrity and non-repudiation of signed documents. The digital signature cannot be copied, tampered or altered. In addition, because they are based on standard PKI technology, digital signatures made within one application can be validated by others using the same applications. |
| *Rationale* | The purpose of a digital signature is to provide a means for an entity to bind its identity to data, and to detect unauthorized modifications to data. |
| *Benefits* | • Digital signatures eliminate the need for transmitting passwords for authentication, which reduces the threat of their compromise<br>• Using a private key to generate digital signatures for authentication prevents an attacker from using the same information to masquerade as another entity and authenticate repeatedly.<br>• Digital signatures provide security for electronic mail, electronic funds transfer (EFT), electronic data interchange (EDI), software distribution, data storage, and other applications that require data integrity assurance and data origin authentication.<br>• Digital signatures provide a cost savings by eliminating the need to print and store hard copies. |

## ASSOCIATED ARCHITECTURE LEVELS

| | |
|---|---|
| *Specify the Domain Name* | Security |
| *Specify the Discipline Name* | Technical Controls |
| *Specify the Technology Area Name* | Cryptography |
| *Specify the 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 three algorithms suitable for digital signature generation and verification:<br>o Digital Signature Algorithm (DSA)<br>o Rivest-Shamir-Adleman, a reversible Digital Signature Algorithm (RSA)<br>o Elliptic Curve Digital Signature Algorithm (ECDSA)<br>• Digital signatures require a Public Key Infrastructure (PKI)<br>• Users must guard against the unauthorized acquisition of their private keys, because the security of a digital signature system is dependent on maintaining the confidentiality of users' private keys |
| *Document Source Reference #* | NIST SP 800-135 Rev. 1, **Recommendation for Existing Application-Specific Key Derivation Functions** |

| | |
|---|---|
| | |

## Compliance Sources

| | | | |
|---|---|---|---|
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC) | *Website* | www.csrc.nist.gov/publications/fips/index.html<br>http://csrc.nist.gov/publications/nistpubs/800-135-rev1/sp800-135-rev1.pdf |
| *Contact Information* | inquiries@nist.gov | | |
| *Name* | | *Website* | |
| *Contact Information* | | | |

## Keywords

| | |
|---|---|
| *List Keywords* | Public key, private key, PKI, DSA, RSA, ECDSA, authenticate, integrity, electronic funds transfer (EFT), electronic data interchange (EDI), Cryptography |

## Component Classification

| | | | | |
|---|---|---|---|---|
| *Provide the Classification* | ☐ *Emerging* | ☒ *Current* | ☐ *Twilight* | ☐ *Sunset* |
| *Sunset Date* | | | | |

## Component Sub-Classification

| Sub-Classification | Date | Additional Sub-Classification Information |
|---|---|---|
| ☐ *Technology Watch* | | |
| ☐ *Variance* | | |
| ☐ *Conditional Use* | | |

## Rationale for Component Classification

| | |
|---|---|
| *Document the Rationale for Component Classification* | |

## 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 Approved / Rejected* | 04/13/2004 |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | 02/26/2015 | *Last Date Updated* | 7/15/2015 |
| *Reason for Update* | Vitality | | |