# COMPLIANCE COMPONENT

| DEFINITION | |
|---|---|
| *Name* | Cryptography for Web Servers |
| *Description* | Cryptography for Web Servers provides authentication and encrypts the data in transit. |
| *Rationale* | Web servers are inherently unsecured and cryptography provides necessary security features to protect the data. |
| *Benefits* | • Server authentication<br>• Client authentication<br>• Data integrity<br>• Confidentiality<br>• User authentication |

| ASSOCIATED ARCHITECTURE LEVELS | |
|---|---|
| *Specify the Domain Name* | Security |
| *Specify the Discipline Name* | Technology 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* | The most commonly used encryption protocol is Secure Socket Layer (SSL). HTTPS is Hypertext Transport Protocol integrated with SSL. SSL is sometimes referred to as SSL/TLS (Secure Socket Layer/Transport Layer Security).<br>• When transmitting sensitive or critical information over the web, users shall use SSL with at least:<br>o Advanced Encryption Standard (AES) 256-bit encryption<br>o Secure Hash Algorithim-2 (SHA-2) |
| *Document Source Reference #* | NIST Special Publications 800-44 V2 – Guidelines for Securing Public Web Servers; IRS Publication 1075 |

| Compliance Sources | | | |
|---|---|---|---|
| *Name* | National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC), IRS | *Website* | http://csrc.nist.gov |

| | | | |
|---|---|---|---|
| *Contact Information* | inquiries@nist.gov | | |
| *Name* | | *Website* | |
| *Contact Information* | | | |

## KEYWORDS

| | |
|---|---|
| *List Keywords* | SSL, HTTPS, FTP, SMTP, AES, Digital Signature, SHA-2,TLS, Cryptology, Web Server |

## 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* | 10/27/2016 | *Date Approved / Rejected* | 10/27/2016 |
| *Reason for Rejection* | | | |
| *Last Date Reviewed* | | *Last Date Updated* | 10/27/2016 |
| *Reason for Update* | Vitality | | |