UNIVERSITY OF CENTRAL FLORIDA

University Standards

Subject:	SSL/TLS Standards
Standards Number:	702
Effective Date:	12/14/18
Revised Date:	
Responsible Authority:	Information Security Office
Pages:	5

ACCOUNTABILITY/APPLICABILITY:

This standard applies to any system that utilizes TLS, SSL and other technologies to confirm identity, secure communications between devices, and/or ensure integrity and confidentiality of transmissions. It is particularly important for those systems that are publicly available on campus or to the Internet. Systems Administrators, Web Developers, and IT leadership for the University of Central Florida should be aware of these standards and ensure they are in place.

STANDARDS STATEMENT:

The purpose of this standard is to define how TLS certificates (commonly known as SSL certificates), protocols, and cipher suites are to be configured to confirm identity, secure communications between devices via encryption in transit, and ensure the integrity and confidentiality of transmissions for Information Technology (IT) services provided by the University of Central Florida.

BACKGROUND:

Cryptographic protocols such as TLS are constantly being updated to address vulnerabilities and to support stronger, more secure cipher suites and algorithms. For example, the Internet Engineering Task Force deprecated SSL 2.0 and 3.0 in 2011 and 2015 respectively due to publicly known flaws and weaknesses. Maintaining up-to-date network protocols is important to protecting the privacy and security of our users.

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476

STANDARDS:

1. Certificates

- All digital certificates are to be RSA 2048-bit or greater.
- It is recommended that Administrators also request a 256-bit Elliptical Curve (ECDSA) certificate in addition to the RSA certificate.
    - The newer, faster, and more secure certificates enable the use of ECDSA cipher suites below.
    - To ensure compatibility with legacy clients that might only support RSA-based cipher suites, The EC certificate should be enabled in a hybrid mode with the traditional RSA 2048-bit certificate.
- When a certificate is needed for multiple domains, a Multi-Domain (SAN) certificate should be used. Wildcard certificates are not recommended and should not be used.
- Self-signed certificates should only be used in the following situations:
    - Development and test services, or services that will NOT be publicly accessible.
    - Lab environments that will NOT be publicly accessible (e.g., labs used for educational purposes that are only accessible by students/instructors.)
- The UCFIT Certificate Request Process is recommended when acquiring TLS certificates to ensure consistent issuance (Key Strength, Protocols, and Certificate Authority.)

2. Protocols

Recommended

- TLS 1.3
- TLS 1.2
- TLS 1.1

Not Recommended, but acceptable for compatibility purposes with valid business reason

- TLS 1.0
    - Contingent on the mitigation of BEAST vulnerability via disabling TSL compression option on the server.

Unacceptable

- All versions of SSL (SSL v2, SSL v3, etc.)

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

3. Secure Cipher Suites

Whitelist

- The following cipher suites should be used in this order so that faster and more secure suites, such as ECDSA, and AES-GCM, are preferred.
    - ECDHE_ECDSA+AES-GCM
    - ECDHE+AES-GCM
    - ECDHE_ECDSA+AES
    - ECDHE+AES

Blacklist

- The following cipher suites are insecure and must be disabled:
    - Anonymous Diffie-Hellman (ADH)
    - NULL cipher suites
    - EXPORT cipher suites
    - RC4
    - 3DES
    - RSA-Based Key Exchange
    - MD5
    - SSL v2 Ciphers
    - SSL v3 Ciphers

4. Force Encryption

- Encryption should be forced on all connections that support it.
    - For example, for websites that support both HTTP (port 80) and HTTPS (port 443), the website should force all unencrypted HTTP connections to redirect to the HTTPS version.
    - HTTPS is required for all services that communicate Restricted and Highly Restricted Data

5. Testing and Validation

- It is recommended to configure and test these settings on a non-production system first. Administrators should be aware of the clients that would connect to the server in question and perform tests to ensure the configuration will work for these clients.
- After configuring these changes, Administrators should validate the security and compatibility of their configurations with a tool such SSLLab's SSL Server Test. UCF servers should achieve an 'A' or 'A+' grade:
    - https://www.ssllabs.com/ssltest/

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

DEFINITIONS:

Cryptography: The process of reconstructing data into an unreadable format that must be decrypted to read as a method of data protection.

ECDHE: Elliptic Curve Diffie-Hellman Ephemeral key exchange. When no other authentication algorithm is defined, such as ECDSA, it is implied that traditional RSA authentication will be used.

ECDHE_ECDSA: Elliptic Curve Diffie-Hellman Ephemeral key exchange, paired with Elliptic Curve Digital Signature Algorithm for Authentication (instead of traditional RSA)

Extended Validation: This type of certificate requires the requester to go through more in-depth identity verification process by the Certificate Authority. These types of certificates are more trusted because the Certificate Authority verified that the requester is who they claim to be.

HTTPS: Short for "Hyper Text Transfer Protocol- Secure." This is a protocol that ensures an encrypted connection and communicates via port 443.

SAN: Short for "Subject Alternative Name." This type of certificate allows a single TLS certificate to protect more than one domain. This is commonly referred to as a "Multi-Domain (SAN) certificate."

Self-Signed Certificates: Self-Signed Certificates are certificates that are not validated or signed-for by a third-party Certificate Authority. The CA's outside verification is responsible for the recognition of whether a site is genuine or has been tampered with; it is because of this lack of verification in Self-Signed certificates that they are considered insecure in most cases.

SSL: Short for "Secure Sockets Layer." This is protocol establishes an encrypted connection between server and browser, known as a 'Socket.' This protocol is vulnerable to a plethora of exploits and is considered 'insecure.'

TLS: Short for "Transport Layer Security." This protocol replaced SSL after the cryptographic flaws became evident. This protocol uses a handshake between two 'talking' devices to establish a secure cipher suite by which they communicate.

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

RELATED DOCUMENTS:

1. 4-008.1 *Data Classification and Protection* policy
2. US-CERT SSL 3.0 Protocol Vulnerability and POODLE Attack
    a. https://www.us-cert.gov/ncas/alerts/TA14-290A
3. NIST NVD CVE 2014-3566
    a. https://nvd.nist.gov/vuln/detail/CVE-2014-3566
4. Internet Engineering Task Force: Prohibiting Secure Sockets Layer (SSL) Version 2.0
    a. https://tools.ietf.org/html/rfc6176
5. Internet Engineering Task Force: Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)
    a. https://tools.ietf.org/html/rfc7525
6. SSL Server Test
    a. https://ssllabs.com/ssltest/index.html

CONTACTS:

Information Security Office https://infosec.ucf.edu infosec@ucf.edu	Security Incident Response Team (SIRT) https://infosec.ucf.edu/incident-response/ sirt@ucf.edu
Identity Access Management (IAM) https://infosec.ucf.edu/iam iam@ucf.edu	UCF IT Support Center (407) 823-5117 https://ucf.service-now.com/ucfit itsupport@ucf.edu

INITIATING OFFICE: Information Security Office

STANDARDS APPROVAL
(For use by the Information Security Office)

Standards Number: *702*

Initiating Office: Information Security Office

Chief Information Security Officer: *Chris Vakhordjian*

Signature: chrisv Digitally signed by chrisv Date: 2019.02.22 14:24:25 -05'00' Date: _____

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution