Certificate Authority Policy

TEC 13.0

Office of Information Technology

Institutional Type: Operational
Applies to: Office of Information Technology staff who manages Certificate Authorities.

POLICY DATES

Issued: 11/15/2019
Revised Last: 3/6/2020
Edited by: Tina Stuchell
Reviewed: 3/6/2020

This policy guides the procedures relating to the use of authorized certificate authorities (CA) to establish protected sessions between web clients and web servers and to verify that the certifications are obtained from trusted sources. Reliance on certificate authorities for the entablement of secure sessions includes, for example, the use of Secure Socket Layer (SSL) and/or Transport Layer Security (TLS) certificates.

Trusted authorities, known as Certificate Authorities (CA), sign and distribute certificates for use by entities that need to assure identities and when establishing encrypted communications. Certificate Authorities are typically third-party commercial service providers.

The need for parties to communicate securely over an insecure medium such as the internet necessitated the creation of the Public Key infrastructure (PKI) framework. PKI frameworks utilize public-key cryptography and digital certificates in order to provide integrity and/or confidentiality to communications between parties.

Certificates are most used for secure (HTTPS) web sites. Web browsers inspect signed server-side certificates to verify that a Web server is authentic, using a specific Uniform Resource Locator (URL), and that the URL has been publicly verified with the identity of the institution it has been issued against (this verification is performed by the CA). Using a server certificate in this manner helps assure that integrity and confidentiality of the encrypted communications through use of cryptographic protocols more commonly known as SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security). SSL is no longer considered secure, and its use is no longer recommended.

Other types or classes of certificates may be installed on the client-side web browser and used for the legal non-repudiation of transactions and multi-factor authentication, such as when the specific identity of individuals needs to be validated when connecting the server. Acknowledging that all vendors are “not equal”, this policy recognizes those providers that are professional and prevalent within the marketplace.

Table of Contents

Definitions

Term	Definition
Certificate Authorities (Cas)	A certification authority is a system that issues digital certificates. These digital certificates are based on cryptography and follow the X.509 standards defined for information security. ... Federal Common Policy Certification Authority.
Secure Socket Layer (SSL) and Transport Layer Security (TLS)	Protocols used to authenticate servers and clients and to encrypt messages between the authenticated parties.
HTTPS:	A combination of the Hypertext Transfer Protocol (HTTP) with the SSL/TLS protocol to provide encryption and secure identification of the server.
Public Key Infrastructure (PKI)	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store and revoke digital certificates.

Certificate Authority Policy

TEC 13.0

Office of Information Technology

Applies to: Office of Information Technology staff who manages Certificate Authorities.

Term	Definition

Policy Details

Any University system, application, appliance or site that uses the NetID/password combination for purposes of authentication, or that transmits/receives data classified as "Legally/Contractually Restricted is required to:

1. Employ Transport Layer Security (TLS) or their equivalent cryptographic protocols for authenticating and establishing identities, and maintaining encrypted communications channels between endpoints; and
2. Use a Secure Hypertext Transport Protocol (HTTPS) connection based on server-side SSL certificates signed by a recommended trusted third-party certificate provider.

Self-signed certificates are permitted for these systems and conditions:

- Development and testing systems, with no "legally/contractually Restricted" data, segregated from the production network and resources, and prohibited from connecting to external resources
- Application server to database server connections behind an approved firewall.
- Internally hosted infrastructure systems (LDAP servers, load balancers, etc.)

The University of Mount Union participates in the InCommon certificate program. InCommon serves the U.S. education and research communities, supporting a common framework of trust services for the safe sharing of online resources. InCommon operates the InCommon Federation – the U.S. trust federation for research and education – and the community-driven InCommon Certificate Service. The InCommon Certificate Service provides unlimited SSl certificates (including extended validation certificates), client certificates, and code signing certificates for one fixed annual fee. This program offers a true site license and truly unlimited certificates for all of the domains you own or control (.edu, .net, .com,.org, etc.).

All certificates are handled by the Office of Information Technology. All departments needing certificates must go through the Office of Information Technology for digital certificates.

PROCEDURE

The following steps must be followed:

1. Certificate Authorities are reviewed by the Office of Information Technology and approved for use in University systems according to their certificate issuance procedures and criteria.
2. Anyone needing a Certificate Authority must go through the Office of Information Technology.
3. Solutions must be installed and maintained in strict adherence to the providers instructions to help ensure that security and integrity of the certificate processes are preserved. Any deviation from provider instructions or recommended use must be approved before implementation or changes are affected.
4. The transport Layer Security 1.2 protocol is the minimum installation permitted. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
5. Mount Union systems that participate as Certificate Authorities must implement appropriate security controls in order to ensure their integrity in the role of facilitating encrypted web communications.
6. System administrators must track certificate expiration dates to ensure that certificates are kept current to avoid adverse impact to operations.
7. Strict adherence to provider instructions for implementation and maintenance is required. Individuals who discover or strongly suspect a violation of this policy or standards must promptly notify the Office of Information Technology Director of IT for Security.

Certificate Authority Policy

TEC 13.0

Office of Information Technology

Applies to: Office of Information Technology staff who manages Certificate Authorities.

Responsibilities

Position or Office	Responsibilities
Office of Information Technology (Network Services)	Management of Certificate Authorities (CA)

Resources

Contacts

Subject	Office	Telephone	E-mail/URL
	Office of Information Technology	330.823.2854	IT@mountunion.edu

History

Issued: 11/18/2019

Revised: 3/6/2020

Edited: Tina Stuchell

Reviewed: 3/6/2020