Digital Certificates

Background

The purpose of this standard is to identify the acceptable use and implementation of digital certificates at the University of Cincinnati (UC).

Digital certificates ("certificates") are used to confirm identity, secure communications between parties, and ensure integrity of transmissions. The use of certificates is one method of encrypting sensitive (Export Controlled, Restricted, Controlled, etc…) data while in transit.

Digital certificates can include, but are not limited to the following:

- SSL Certificates (Single-Domain)
- Multi-Domain Certificates (SAN Certificate)
- Wildcard Certificates
- Code-Signed Certificates
- Self-Signed Certificates
- Client Certificates (Digital Signature)

Standard

This section outlines the acceptable use of digital certificates at UC. The University of Cincinnati uses InCommon as the official Certificate Authority (CA). All certificates issued on behalf of the university to university-covered domains must be issued through InCommon.

All exceptions to this standard must complete a Risk Acceptance Form (RAF).

Additional strength, configuration, and validity requirements are included in the Appendix.

Requests for certificates that do not meet minimum requirements will be denied. Previously issued certificates that do not meet the requirements will be revoked.

Table of Contents

A. Acceptable Use Requirements

1. SSL Certificates (Single-Domain)

A SSL Certificate is a single-domain webserver certificate needed to enable SSL operation on a server.

When To Use SSL Certificates

These certificates will secure a fully-qualified domain name (FQDN). For example, “example.uc.edu” would be secured by a single-domain certificate. This certificate would not be valid for any other FQDN than example.uc.edu.

2. Multi-Domain Certificates (SAN Certificate)

A SAN (Subject Alternative Name) certificate has a field that specifies alternate FQDN’s that can use the certificate on the same domain. These certificates will secure up to 100 different FQDN’s on a single certificate.

When to Use Multi-Domain Certificates

These certificates will secure up to 100 different FQDN’s on a single certificate. For example, a multi-domain certificate could be requested for “example.uc.edu” but have SAN’s for “www.example.uc.edu,” example1.uc.edu,” etc…

3. Wildcard Certificates

A “wildcard” SSL certificate is a certificate that matches any FQDN of a sub-domain. For example, “example.uc.edu” is a sub-domain of “uc.edu.”

The certificate that contains “*.example.uc.edu” is an example of a wildcard certificate. This certificate can be used on any server whose hostname is in the “example.uc.edu” domain, e.g, “www.example.uc.edu,” “mail.example.uc.edu,” or “ftp.example.uc.edu.” Note that only

one level of sub-domain is matched, so "*.example.uc.edu" does not match "www.email.example.uc.edu."

When to Use Wildcard Certificates

In many industries there are time and cost considerations when purchasing digital certificates, thus making wildcard certificates more appealing as they cover an unlimited number of sub-domains. Since UC is a member of the InCommon Federation, the individual cost per certificate is not a concern.

There is also a security consideration when using a wildcard certificate: if the private key associated with that wildcard certificate is compromised, then *all* servers using that wildcard certificate are vulnerable. Due to these concerns, UC has implemented the following restrictions on wildcard certificates:

- Cannot be used for one of UC's top-level domains (e.g., *.uc.edu)
- Must be limited to a period of 1 year
- Are not permitted on sub-domains that handle, transmit, or store Export Controlled/Restricted/Controlled data
- Are not permitted on sub-domains with production data
- Are not permitted on sub-domains that handle, transmit, or store production credentials
- Must be recreated with new keypairs, not renewed
- May only be used when more than 100 FQDNs are involved. (If fewer than 100 FQDNs are needed, request a Multi-Domain SSL certificate instead).

Exception to Restrictions on Wildcard Certificates

It is recommended that a multi-domain certificate be used rather than a wildcard certificate. In the event that a multi-domain certificate is not appropriate, an exception may be granted. However, exceptions to these restrictions require approval by the Office of Information Security who will require a documented and approved RAF.

4. Self-Signed Certificates

1. Self-signed certificates are not permitted on systems with Export Controlled/Restricted/Controlled data
2. Self-signed certificates are only permitted under the following circumstances:
    a. Technical, contractual, or vendor requirements preclude using a certificate issued by a trusted Certificate Authority
    b. Temporary development on a host that is not public-facing
    c. Factory-installed certificates on devices that are not public-facing

5. Client Certificates

Also known as personal certificates or digital signatures, these certificates are associated with a person using their UC e-mail address for the following purposes:

- Signing Email
- Encrypting Email
- Digitally Signing Documents

B. Exceptions

Any exceptions to this standard will require approval by the Office of Information Security who will require a documented and approved RAF.

C. Requesting Certificates

The sections below will outline the process for requesting various types of certificates. The Office of Information Security handles requests and can typically review/approve within 5 business days.

SSL/Multi-Domain Certificate Request Process

1. Create a certificate signing request (CSR)
2. Go to the SSL Request Form and submit your request
    a. OIS receives the request
    b. OIS obtains verbal verification from requestor
    c. OIS obtains email approval from supervisor of the requestor*
3. Certificates are typically approved/issued within 4 business days when verification and approval are received in a timely manner

If the request comes from Central IT, the Office of Information Security will verify details with the requestor, approve the request, and forward the approval information to the supervisor of the requestor as an FYI.

Wildcard Certificate Request Process

1. Create a certificate signing request (CSR)
2. Go to the SSL Request Form and submit your request
    a. OIS receives the request
    b. OIS will contact the requestor to obtain additional information and initiate the RAF
3. Certificates are approved following a documented and approved RAF

Client Certificates

1. Navigate to https://www.uc.edu/infosec/services/cert.html
2. Click the red button in the top-right "*Request Personal or Server Certificate*"

3. Login with your CLS credentials
4. Select *Request Client Certificate*
5. Fill out all of the required information in the form
6. Your certificate will be emailed to you

D. Private Key Management

1. Private keys must be protected to the same standard as Restricted Data per the Data Governance & Classification Policy 9.1.1.B – Minimum Safeguards
2. When an employee who has access to private keys protecting restricted data leaves the organization, private keys and associated certificates must be replaced
3. Units may not install the same private key on multiple hosts, except for clustered and load-balanced services.

E. Renewing, Replacing, and Revoking Certificates

1. Certificates must be renewed or replaced before expiration
    a. See Appendix B for specific renewal requirements
2. Certificates must be revoked if any of the following occur:
    a. A private key has been compromised
    b. The service is being retired or decommissioned
    c. When the private key is no longer in use
    d. An employee with access to the certificate/private key leaves the university

Contact Information

IT@UC Office of Information Security 513-558-ISEC(4732) Infosec@uc.edu

Related Links

Risk Acceptance Policy
Data Governance & Classification Policy

History

Issued: 05/03/2017

Appendix A – Definitions

Digital Certificates – A means by which consumers and businesses can utilize the security applications of Public Key Infrastructure (PKI). PKI comprises of the technology that enables secure e-commerce and Internet based communication.

Certificate Authority – A trusted entity that issues electronic documents that verify a digital entity's identity on the Internet. The electronic documents, which are called digital certificates, are an essential part of secure communication and play an important part in the PKI.

FQDN – The complete domain name for a specific computer, or host, on the Internet. The FQDN consists of two parts: the hostname and the domain name. For example, an FQDN for a hypothetical mail server might be mymail.somecollege.edu.

SSL – The standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

CSR – A message sent from an applicant to a Certificate Authority in order to apply for a digital identity certificate.

Appendix B – Server Certificate and Related Configuration Requirements

Please note: Requirements in this appendix are subject to change in response to changes in industry standards, law, or UC policy, as identified by the Office of Information Security. The affected community will be notified of significant changes.

Certificates issued through the OIS Digital Certificate Service meet or support the requirements in this appendix and are available at no cost to UC individuals or departments.

An exception is required if an implementation cannot meet these standards. Compensating controls may be required if an exception is granted.

1. Implementations must meet Qualys SSL Labs "SSL/TLS Deployment Best Practices" described at https://www.ssllabs.com/projects/best-practices/index.html
    a. Note: The InCommon certificate service meets the CA requirements outlined in these Best Practices
    b. Servers that achive a "Grade A" or higher rating on the Qualys SSL Labs Server Test at https://www.ssllabs.com/ssltest/ are considered to meet these Best Practices
    IMPORTANT: Always check: "Do not show the results on the boards" when running the SSL Labs Server Test so results are not posted publicly.
    c. Re-validation/re-testing should be done at least annually
2. Significant findings from UC security scans must be addressed
3. Certificate Renewal:
    a. Keys must be regenerated and certificates re-signed when renewing a certificate
    b. Annual renewal is required for systems handling restricted data
    c. Certificates for systems that do not handle restricted data must be renewed after no longer than three years. It is recommended that all certificates be renewed annually

Appendix C – Request/Approval Process Diagram for SSL, Multi-Domain, and Wildcard Certificates