Obtain a UW Services CA Certificate For a UW Application

Purpose

This page describes the steps required to establish an identity and X.509 certificate credential for a UW application.

The intended audience is application developers, system owners, system operators, support staff, and possibly even application business owners.

Overview

There are two main steps involved in establishing an identity and credential for a UW application.

1. Establish a Domain (DNS) name for your application. This provides it an identity.
2. Request a client certificate from the UW Services Certificate Authority for your application.

Step 1: Establish DNS Name

To establish a DNS name for your application, refer to Managing DNS Names For Infrastructure Services Access.

Step 2: Request Client Certificate

To request a client certificate for your application, refer to section 1.5.2 "Requesting certificates for systems without static IPs" on UW Services CA Technical Information.

You will enter the application DNS name you established above as the first step, "1. Enter your host's fully qualified domain name" in requesting a certificate.

Frequently Asked Questions

Q: Why do I need a DNS name?

A: Your application will be identified to the Web Service (and perhaps other UW infrastructure services) by a domain name. Unlike the domain names used by hosts, an application domain name is not associated with an IP address and its DNS entry is not used for routing. Your application DNS name will be used in Step 2 to request a client certificate.

Q: How should I choose a name?

A: Although you have a great deal of leeway choosing your application domain name, some basic guidance is:

- Choose a DNS name that reflects the business name or purpose of your application.
- Use a subdomain (e.g., *cac*.washington.edu or *cs*.washington.edu) managed by support staff that also support the hosts on which your application will run.
- For example: employee-charity-donations.cac.washington.edu

Q: When might I need more than one name? Can multiple applications share a name?

A: UW web services identify and authenticate your application using the DNS name in your X.509 certificate. Once authenticated, and with the right authorizations, your application can access privileged data and operations. Thus, your application name will appear in audit logs reflecting the sensitive activity your application has engaged in. Where you want the access granted, or the audit log references, to identify a single application uniquely for security, diagnostic, or forensic purposes, do not share an application DNS name amongst multiple apps. Many application developers request separate domain names for their Production and Development instances of their application. On the other hand, we recommend using the same application name for multiple instances of the same application that run simultaneously for high availability. There's no need for redundant service instances to each have their own unique domain name. See also section 1.10 "When to use multiple certificates" on UW Services CA Technical Information.

Q: Why do I need a certificate?

A: Your application will use its certificate and associated private key to authenticate (i.e., prove its identity) to a SSL/TLS protected Web Service and to encrypt communications, which may include sensitive data.

Q: Can I use a certificate issued by Thawte, InCommon, or some other external CA?

A: No. UW Web Services and many other UW infrastructure services only trust the UW Services CA to authenticate UW applications. Therefore, you must obtain a client certificate from the UW Services CA.

For additional guidance, please email iam-support@uw.edu.

Q: What if my legacy application requires a SHA-1 certificate?

A: SHA-1 certificates for legacy applications can be requested by sending email to help@uw.edu. SHA-1 Support will be reduced over the next few years–see UW CA SHA-1 Sunset for details.