UW Services CA Technical Information

Status

Included on this page:

Certificate Use Guidelines

Supported uses of UW Services CA certificates

The UW Services Certificate Authority (CA) issues certificates for various kinds of services, the two most typical being:

- traditional web server certificates to provide SSL/TLS (https) access to browsers
- certificates for systems and services acting as clients to other SSL/TLS-protected services.

In general, it issues certificates for secure web servers and other kinds of SSL-secured services, such as email servers (IMAP, POP, etc). It also issues certificates for services that need to access other secure services, such as a web server that needs to access a secure directory.

Policy on scope of supported applications

Certificates issued by the UW Services CA are appropriate for many uses and applications, but not all applications. A key issue is that the UW Services CA root certificate is not installed in browsers by default, which can increase support costs associated with the use of UW Services CA certificates. While many other CA root certificates are pre-installed, the UW Services CA root certificate must be installed by the user (see section 1.4 on getting the root certificate) or by automated desktop configuration strategies (e.g. Windows group policy). Many UW users have installed the root certificate in their browsers, but most users outside of UW have not.

For this reason it is not advisable to use UW Services CA certificates on web applications with large numbers of users (10,000 or more), or where many users are not from the regular UW community. Web applications using UW Services CA certificates with more than a small number of users (over 100) should have support staff who can help users with any questions that may come up about certificate warnings and use.

A certificate issued by InCommon may be an appropriate alternative for securing applications whose scope exceeds that supported by the UW CA. The new UW Certificate Service website supports issuing InCommon certificates in addition to UW CA certificates. Please see the UW Certificate Services page for more information on the two certificate authorities.

Deploying on a web server

Administrators should weigh several factors before choosing the UW Services CA over other well-established public CAs, particularly when SSL-enabling a web server. These factors include:

- number of website visitors
- type of visitors (UW vs non-UW)
- technical knowledge of visitors
- platform used by visitors (Windows vs. Macintosh)
- ability to pre-install root cert beforehand
- volume of SSL connections
- cost of supporting visitors
- cost of purchasing a certificate

Users who haven't installed the root certificate into their browsers will see warning messages when your web server presents a certificate issued by the UW Services CA. If you don't help them install the root certificate beforehand, visitors may think there is a problem with, or become frustrated by, your website.

Although pre-installing the root certificate on systems within your department that you manage can significantly reduce the support burden, it probably won't eliminate it. Therefore, if you plan to deploy a certificate issued by the UW Services CA you should be prepared to support your user community and answer some questions (see UW Services CA FAQ).

If the size and nature of your user community suggests that this support is going to be difficult, it might be better to purchase a certificate from a well-known public CA, such as Thawte, and wait until such a time that the UW Services CA root certificate is better deployed within your user community. An In Common-issued certificate may also be a good option in some cases.

Getting the root certificate

The UW Services CA's root certificate can be obtained by visiting the UWCA site website to obtain it in PEM or DER format.

Requesting a certificate

The UW Services CA issues service certificates quickly and automatically to contacts of DNS names with UW NetIDs registered in the Domain Name Service maintained by UW Technology. The certificate request process depends on the purpose of the certificate:

- If the certificate is for a DNS name that already has a static IP address assigned, refer to section 1.5.1.
- If the certificate is for use by a DNS name that identifies a service, application, or process, rather than a physical host machine, and there is no associated static IP address, refer to section 1.5.2.

Requesting certificates for systems with a static IP address

To request a certificate for a system with a DNS name and an assigned static IP address:

1. Verify that you are registered as a contact for your DNS name. Your UW NetID may not have been added to the DNS record when the DNS name was established. If need be, update the contact information. For help with this step, refer to Managing DNS Names For Infrastructure Services Access
2. Go to the UW Certificate Services website.
3. Click "New Certificate"
4. Click the "Verify DNS Ownership" tab.
5. Enter the fully qualified domain name (e.g. `<hostname>.<subdomain>.washington.edu` or `<appname>.<subdomain>.washington.edu`) and click "Verify ownership." If the response confirms your ownership, go to the next step. Otherwise go back to step 1.
6. Click on either the "New UWCA Certificate" or the "New InCommon Certificate" tab.
    a. Additional details specific to an InCommon certificate can be found here.
7. Paste your certificate request into the CSR window. The request must be in PEM format. PEM is a text encoding (base-64) of the binary certificate request.
    a. A CSR includes information that is used to create a certificate. This includes but is not limited to:
        i. Attributes of the certificate like state and country where it will be used. These two values must be set to Washington and US respectively. These values are part of the Subject property of the certificate.
        ii. The common name (CN) which for a web site or service is its DNS name.
        iii. The certificate public key. The public/private key pair are generated as part of the CSR creation.
        Note: InCommon Certificates require 2048 bit public/private keys.
    b. There are a number of different tools that can be used to generate a CSR. One popular tool is openSSL. openSSL can be obtained (in source code form) from the openSSL.org website. It is also installed as part of a Shibboleth installation and with most Linux distributions.
8. Choose the appropriate certificate type from the Type drop-down.
9. Choose the type of web server you will be using along with the number of servers.
10. Choose a certificate lifetime. Certificates used for testing should have a short lifetime. Production certificates are usually valid for 2 or 3 years.
11. Click "Submit" to finish your request. You should receive a confirmation within 10 min.

Note: If your DNS name is not in a DNS subdomain managed by UW Technology, your subdomain contact will have to submit and manage the certificate request.

Requesting certificates for systems without static IPs

To request a certificate for a service, application, or process without an assigned static IP address:

1. If you do not already have a DNS name registered for your service, register one in a DNS subdomain for which you are allowed to register DNS names (e.g. `<application name>.<subdomain>.washington.edu`). Application developers working with web services will often request a DNS name of the form `<uwnetid>.<subdomain>.washington.edu`.
2. Verify that you are registered as a contact for your DNS name. Your UW NetID may not have been added to the DNS record when the DNS name was established. If need be, update the contact information. For help with this step, refer to Managing DNS Names For Infrastructure Services Access
3. Go to step #2 under the section in this document titled "Requesting certificates for systems with a static IP address".

With keyUsage extensions

The UW Services CA asserts several keyUsage extensions if they are specified in a given certificate signing request: Digital Signature, Non Repudiation, Key Encipherment, and Data Encipherment. If you need a certificate with any of these keyUsage extensions, generate and submit a request including those extensions you need. (See Section 4.2.1.3 of RFC 3280 to learn more about keyUsage extensions.)

Note: Don't include keyUsage extensions unless you are certain you need them. Under usual circumstances you will be better off without them.

With subjectAltName extensions

The UW Services CA asserts all Subject Alternative Name (subjectAltName) extensions specified in a request if you are a registered contact of each name in UW DNS. The issued certificate contains each subjectAltName you specify, plus the value of the request's CN element as a subjectAltName if it wasn't already in the list.

Changing Certificate Ownership

The UW Services CA manages certificate requests using contact information from the Domain Name Service maintained by UW Technology. Registered contacts for your DNS name can request changes. For help, refer to Managing DNS Names For Infrastructure Services Access

Expiration Notification

The UW Services CA notifies all registered contacts for your DNS name when your certificate is approaching its expiration date. This expiration notification is sent via email approximately a month before expiration.

Note: The UW Services CA discards requests corresponding with expired certificates about a month after the expiration date. At that time, you will no longer see the request and certificate listed in the management interface and you will have to generate and submit a new request to obtain a new certificate.

When to revoke a certificate

You should only revoke a certificate if you have reason to believe its private key has been stolen and could be misused. Please do not revoke a certificate just because you do not want an application to accept the certificate any longer. Instead, please remove the certificate's access rights to the application. Each revoked certificate becomes listed on the UW Services CA Certificate Revocation List (CRL) which is downloaded and checked several times a day by multiple systems. Keeping the CRL short reduces resource utilization on all the systems.

How to revoke a certificate

Email help@uw.edu with the CN (DNS Name) and expiration date of the certificate.

When to use multiple certificates

Hosting multiple applications on the same server introduces a dilemma: should you use one certificate for all the applications or one certificate for each application?

As a guideline, use distinct certificates when the applications or processes using certificates for access to other services have a distinct function, or distinct administration, or are likely to need different levels of access. A rule of thumb might be if you would run the processes under different local accounts or userids, then you should use distinct certificates.

Requesting a wildcard certificate

The UW Services CA supports wildcard certificates. To request a wildcard certificate you must be a registered contact for the UW DNS subdomain specified in the request's Common Name field. For example, to request a certificate for `*.<subdomain>.washington.edu` you must be a subdomin contact for `<subdomain>.washington.edu`.

Requesting a SHA-1 Certificate

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.

Application Development Guidelines

Client certificates vs server certificates

The common usage of "client-server" in networking terminology defines the client as the initiator of a connection and the server as the target system of that connection.

A server (such as a web server) can provide a server certificate to a client during secure SSL connections. This server certificate contains information that the client can verify so it can trust the host it has connected with is the desired server. For example, the web servers for _https://www.washington.edu_ have server certificates to indicate they are authorized to use that DNS name. Server certificates also allow a client to send encrypted data to the server which only that server can decrypt.

Client certificates can be used to identify the client to the server. They provide the server with verifiable information about the client. Note the term "client" is not clearly defined; it may identify and authenticate a system or service, a user, or even a process running on a machine. The UW Services CA currently issues client certificates for system and service identification only, based on DNS names.

UW Services CA certificates can be used either as client or server certificates, but only to identify systems and services with DNS names. The UW Services CA does not issue certificates used to identify people.

Verifying client certificates

Here are some considerations if you are verifying a UW Services CA certificate used within client authentication:

- Although UW Services CA certificates are issued to a system or service based on its DNS name, there is no guarantee that the certificate is only installed on a machine with the corresponding DNS name. Certificates and private keys can be exported and then installed on any number of systems. If your server wants to verify a client is connecting from a system that matches the DNS name found in the client certificate, it must verify this by looking at the IP source of the client connection.
- Any given certificate may be installed on numerous machines. This may be desired or not, depending on your server and application, but you may need to be aware of this.
- Certificates are good for a specified time period. However, if your server or application wants to make sure a certificate has not been revoked (proclaimed bad and untrustworthy) before its expiration date, your application must check the certificate against the UW Services CA's certificate revocation list (CRL). Each issued certificate contains the CRL location. The CRL can also be found on the UW Services CA website. The CRL contains certificates that should no longer be trusted because they have been revoked by the UW Services CA.

Using Certificates With Microsoft Windows

Certificates storage

On Windows 2000 and Windows XP, certificates can be stored in a variety of locations. The various storage locations are not equivalent, and a certificate must be stored in the proper location for its intended use or else it won't be usable.

The Windows operating system itself provides several significant certificate storage locations. Applications such as IE and IIS use these locations for certificate storage and retrieval. The locations include a separate **User Store** for each user account, as well as a **Local Machine Store** for the computer's system processes. Both stores have numerous sub-folders which contain the actual certificates of varying types.

The User Store typically contains certificates that a user can use to authenticate to web servers. It may also contain certificates that can be used for S /MIME, encrypting files, signing software, etc. These certificates are usually located in the Personal subfolder of the User Store.

To display the current User Store, run certmgr.msc. This program includes help information that explains certificates and stores in detail. Note: this tool's utilities to "request a certificate" cannot be used with the UW Services CA because it is a standalone, third-party CA. This feature only works with Active Directory Integrated Microsoft Enterprise CAs.

The Local Machine Store (also provided by the Windows operating system) contains certificates that identify the machine to other machines. The Windows operating system uses these certificates to serve web pages with SSL, negotiate IPSEC, etc. These certificates are usually located in the Personal subfolder of the Local Machine Store.

Using the MMC with the Certificates add-in allows you to choose the Local Machine store for viewing. You must have local Administrator rights on the machine to do so.

Applications may also provide their own certificate stores and tools to manage them. Examples would include Sun's Java VM which uses its own store and is managed with its keytool application. Netscape software also uses its own certifcate storage and provides a manage UI for it. Please refer to specific application documentation to understand these non-OS based certificate stores and how to use their own tools to manage them.

Exporting certificates to a different certificate store

If a certificate is created with an exportable private key, you can use the certmgr and/or MMC GUI tools to export the certificate to a different storage location. Right-click the certificate and choose All Tasks > Export...

If a certificate is created with a non-exportable private key, you can export the public key of the certificate, but not the private key.

To import a certificate, double-click the .crt file, and select which store for installing the certificate. UW Services CA certificates are typically placed in the LocalMachine/Personal store, so if you want to use one as a client certificate, export it using the mmc and then import it into the "user/personal" storage location.

Adding the UW Services CA to a Windows domain's group policy

To add the UW Services CA root certificate to a Windows domain's group policy:

1. Get the UW Services CA root certficiate from the UW Services CA web site and save it to a file such as uwroot.crt
2. As Domain Administrator, use the Active Directory Users and Computer tool to edit the Group Policy for the OU you want to install the root cert in. Use the "Default Domain Policy" for the whole domain.
3. In the GPO Editor user interface, under Computer Configuration > Windows Settings > Security Settings > Public Key Policies, right click on "Trusted Root Certification Authorities" and choose Import. Then choose the file containing the UW Services CA root you made in step 1 (e.g. uwroot.crt).

The new CA root certificate should now be visible in the Group Policy Editor/Viewer, and machines in the affected OU will have and trust the new root certificate after a group policy refresh cycle (usually 24 hours, or after their next reboot).

Certificate requests using the Web Server Certificate Wizard

To request a certificate for use with IIS using the IIS's Web Server Certificate Wizard:

Note: the following instructions were tested on a Windows 2000 Server SP4, with Internet Explorer 6.0.2800.1106, and all critical updates as of 29 Apr 2004. Be sure your system has all critical Windows updates and IE updates installed by visiting Windows Update.

1. Verify your system has the UW Services CA root installed.
2. Log on to your Windows server as Administrator.
3. Start the IIS Internet Services Manager.
4. Display your web site properties.
5. Select Directory Security > Server Certificate to run the Web Server Certificate Wizard.

6. Select "Create a new certificate", click Next.
7. Select "Prepare the request now, but send later", click Next.
8. Type in any simple name (e.g. "MyExampleUWSCAcert") for the certificate, 1024 is a good bit length, click Next.
9. Type in Organization = "UW", Organization Unit = "" (actual text doesn't matter), click Next.
10. Type your full DNS name for the Common Name, to conform to our DN policy.
11. Select US for Country, type in "Washington" for state, and "Seattle" for city, click Next.
12. Save the certificate request to a file (e.g. c:\certreq.txt).
13. Finish the IIS Certificate Wizard.
14. Open the certificate request file (e.g. in Notepad).
15. Select the contents and copy it to the clipboard.
16. Start a web browser, go to the UW Service CA web site (https://iam-tools.u.washington.edu/cs/), log in with your UW NetID, and select "New UWCA certificate".
17. Choose the PEM method as you walk thru the request process.
18. Paste the contents of your certificate request file (e.g. c:\certreq) into the "CSR" text field and submit your request.
19. Wait for email acknowledging that your certificate has been issued.
20. Go back to the UW Service CA web site, select the number corresponding with your current request from the list of Favorites, and click "Get PEM" or "Get PKCS 7" from the details display to the right.
21. Copy, paste, and save the PEM certificate into a new file (e.g. c:\certfile.txt).
22. Return to the Web Server Certificate Wizard.
23. Process the pending request to install the new certificate (e.g. c:\certfile.txt).

Certificate requests on Windows without using IIS

- Obtain a Certificate on Windows 2008 (without using IIS)
- Obtain a Certificate on Windows Server 2008 R2 and 2012 (Without Using IIS)