UW Services CA FAQ

Status

Included on this page:

About Certificates and Public-Key Infrastructure

What is Public-Key Infrastructure (PKI)?

The term "Public-key infrastructure" refers to a set of services that use the methods of public-key cryptography to provide security functions for an organization, a group of cooperating organizations, or the Internet as a whole. The basic security services are assurance of the identity of a sender of information, assurance of the integrity of information, and protection of information from disclosure to unauthorized persons. A certificate authority such as the UW Services CA is one component of a PKI.

Where can I learn more about certificates and PKI?

There is a lot of information available. One source of introductory documents is http://www.oasis-pki.org/whitepapers.html, from the OASIS PKI Forum. There are lots of good books about PKI and related security issues; one comprehensive book is: "Understanding the Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations" by Carlisle Adams, Steve Lloyd, Stephen Kent (ISBN: 157870166X)
Note that in the field of PKI there are many technologies, and many differing opinions about how to use them.

What is a digital certificate?

A digital certificate contains the name of the entity that is being identified, the entity's public key, the name of the issuer, and other information such as validity dates and the cryptographic data that proves that the certificate is authentic. Your browser lets you view the certificates that it has stored.

What is a Certificate Authority?

A digital certificate is issued by a special service called a Certificate Authority (CA). There are many commercial CA's whose verification information comes pre-installed on many personal computers and browsers. This permits the secure use of Web sites that use certificates issued by those authorities.

What is a CA certificate?

A CA certificate establishes the name and public key of a certificate authority. Upon installing a CA certificate, your browser can verify the identity of web sites and other entities whose certificates were issued by that CA.

A CA certificate contains the name of the CA, the CA's public key, and other information such as validity dates. Upon installing a CA certificate, your browser can verify the identity of web sites whose web server certificates were issued by that CA.

Should I accept and install a CA certificate when asked?

No. If you install a CA certificate issued by a malicious or negligent CA, your browser could accept as valid fraudulent identities presented by web sites. This could lead to stolen passwords or other kinds of fraud. You should only accept CA certificates from sites you trust, and only for legitimate purposes.

About the UW Services CA

How do I request a certificate?

Our technical information section describes how to request a certificate for your server or service.

Where do administrators go for further technical information?

Refer to the section on technical information for issues related to requesting and using certificates issued by the UW Services CA.

Does the UW Services CA issue certificates to individuals, e.g. for use with secure email?

No, it does not provide this service. Certificates that identify individuals, rather than machines and services, might be offered in the future. In the meantime if you require such a certificate various commercial services, such as Thawte offer certificates for individuals, for secure (i.e., S/MIME) email and other purposes.

How do I let UW Information Technology know about a particular need for certificates that I have?

Send mail to help@u.washington.edu. We'll be happy to discuss it with you.

Washington state law, in RCW 19.34.231, says that state agencies may not act as certificate authorities. Is the UW Services CA in violation?

This provision was removed from the RCWs in 2015, but the previous answer is preserved below.

RCW 19.34 sets requirements for certificate authorities that issue certificates to identify people for use in conducting official public business using digitally-signed documents. The UW Services CA issues certificates only for servers and other system processes, and so is not covered by this legislation.

Will the UW Services CA ever be in browsers via a parent.edu root CA?

No. With the advent of free CAs like Let's Encrypt, and the University's subscription to the InCommon Certificate Service (which gives us an unlimited number of certs for very low cost), there's no reason to pursue this.

Does the UW Services CA issue certificates signed with the SHA-2 algorithm?

Yes, beginning 2016-04-27. 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.