UW Services Certificate Authority Certification Practices Statement

1. Introduction

A Certificate Authority (CA) is maintained by the University of Washington (UW) to facilitate secure communication between clients and services at the University of Washington by issuing IETF X.509 client and server certificates to authorized applications.

These certificates allow the applications to positively identify themselves and to authenticate their peers in a communications network.

This Certificate Practices Statement (CPS) describes the policies in place for the CA identified by the following certificates:

Common Name	Fingerprint
UW Services CA	MD5: 04:41:05:F2:32:5D:25:2C:00:97:46:C2:FE:00:17:51 SHA1: B9:76:8F:DA:34:54:56:46:9A:0B:AE:38:64:FE:00:55:C9:E6:35:7F

It is expected that a majority of the University community will install the UW Services CA root certificate into their browsers or email clients as a trusted certificate authority, thereby allowing UW issued certificates to seamlessly and securely authenticate UW web and email applications.

Intended Use

Certificates issued by the CA may be used only by authorized administrators of services provided by the University of Washington. They may be used to identify web servers and IMAP servers to their clients. They may also be used to identify each peer of an application to application communication.

2. Infrastructure

The CA maintains one or more secure root certificates along with: tools to securely sign, renew, and revoke certificate requests; a database of issued certificates; a list of revoked certificates; and a log of activity.

CA Root Certificate

Certificate

The "UW Services CA" certificate is available for installation into any browser or application.

Key

The root certificate key is maintained on a secure system housed in a locked area of the University of Washington's computing facility and is accessible only through remote procedures by CA administrators and other authorized personnel for issuance and revocation of certificates and creation of Certificate Revocation Lists (CRL).

Certificate Issuance and Renewal

1. Requests for certificates are received via authenticated https transactions and entered into a database. A request consists of the applicant's identity (UW NetID, as provided by the UW "weblogin" service); the certificate request (CR) in PEM format; and commentary notes. Requests for renewal do not include the CR text.
2. We require that the Common Name (CN) and any Subject Alternative Names specified in the request identify a domain name within DNS. If the requestor is recognized as a contact for that DNS name, as reported by the Network Operations Center (NOC), the request is signed automatically. Otherwise a CA administrator intervenes, determines the validity of the request, and signs or rejects it. Certificates will only be issued to names in DNS domains managed by the UW NOC.
3. The applicant retrieves the signed certificate from the CA's web service.
4. Reasons for refusal of a request are logged and are provided to the requester.
5. Any owner of a certificate's CN and Subject Alternative Name(s) may request certificate renewal anytime within a month of its expiration.

Certificate Lifetime and Content

Certificates issued by the CA contain:

Certificate Field	Certificate Value
Subject	Standard clients and servers: C=US, ST=WA (or Washington) O and OU fields are optional CN=*domain name of the service*
Validity	Not Before: *The date of issuance* Not After: *Up to three years from the date of issuance*

X.509 v3 Certificate Extensions	Basic Constraints: CA:FALSE Key Usage: *Digital Signature* *Non Repudiation* *Key Encipherment, and* *Data Encipherment; if requested in Certificate Signing Request* Extended Key Usage: Client Authorization Server Authorization

Certificate Revocation

Certification revocation is also by authenticated web transaction, and may be instigated only by the certificate holder. The CA maintains a publicly available Certificate Revocation List (CRL) for each root certificate.

Transaction Logs

The CA maintains logs of all transactions.

3. Customer Requirements

Certificates are available only for authorized services of the University. Application administrators requesting one or more certificates are expected to:

- Be able to securely generate a certificate request, and store and use the resultant certificate and key;
- Be aware that clients of the application will have to load or install the UW Server CA certificate as a trusted certificate authority in their programs, and be willing to assist them in that effort;
- Inform their clients of the existence and use of the CA's Certificate Revocation List;
- Notify us if either the private key has been compromised; and
- Keep the contact list for DNS names up to date.

4. Amendment

UW reserves the right to modify the services of this CA, including, but not limited to:

- Issuance of client certificates for personal identification,
- Creation of additional root certificates for special circumstances not covered by the present CAs.

Additions to service will be accompanied by corresponding documentation in this CPS. Current certificate holders will be notified by email to the certificate owner prior to any modifications which may adversely affect their applications.

5. Contact Information

Send inquiries to help@uw.edu.

See also: IT Connect and the University of Washington home page.

6. Disclaimer

THE UNIVERSITY OF WASHINGTON MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THESE SERVICES, INCLUDING ANY WARRANTIES OF TITLE, NONINFRINGEMENT OF COPYRIGHT OR PATENT RIGHTS OF OTHERS, MERCHANTABILITY, OR FITNESS OR SUITABILITY FOR ANY PURPOSE.