UW Services CA Certificates for 3rd Party Use

Problem Statement

You're working with a non-employee (3rd party) and would like them to use a UW Service CA certificate. However, they can't submit a certificate signing request (CSR) to the UW Service CA. What can you do?

Solution

You can submit the request on their behalf and send them the signed X.509 certificate. Here's how:

1. Register a new UW DNS name in your current subdomain for the 3rd party client or server application, e.g.

   <application name>.<subdomain>.washington.edu.

2. Be sure to include your UW NetID when requesting the new DNS name. The UW Services CA authorizes users again UW NetIDs registered as UW DNS name contacts. Refer to Managing DNS Names For Infrastructure Services Access.

3. Ask the non-employee (3rd party) to generate a new RSA private key and CSR for the DNS name you've registered.

Note: When generating the certificate request advise them to use the UW Services CA guidelines for the Distinguished Name:

Country (C)	US
State (ST)	WA or Washington
Organization (O)	*Optional*
Organizational Unit (OU)	*Optional*
Common Name (CN)	*Your fully qualified DNS name*

4. Ask them to send you the CSR in PEM format.

5. Submit the CSR to the UW Services CA.

6. Retrieve your X.509 certificate once it has been signed.

7. Send the certificate to the non-employee (3rd party).

8. Direct the third party to install the UW Services CA root certificate too. Refer to http://www.washington.edu/itconnect/security/ca/.

9. Manage the lifecycle of the certificate as needed over time.

Result

By establishing a DNS name for your non-employee (3rd party) application, you can obtain a UW Services CA certificate for them without having to send any private keys via insecure email. They send you the CSR; you send them the signed certificate.