SSL Certificate and Subject Alternative Names (SAN)

This article assumes you are using InCommon-Comodo Certificate Service, and that you intend to use openssl to generate your Certificate Signing Request (CSR). If you are using other Cert providers, please check with your vendor

If your host name has multiple DNS entries or your Web site has multiple names, you don’t need a separate SSL certificate for each one. If you include “Subject Alternative Names” (SAN) in your CSR , you need only one SSL certificate. The SAN lists the names that you want your certificate to cover.

When you have no certificate, you can include the SAN information in your CSR. This process has been automated via a python script by the technical staff at UC Berkeley. More information can be found here: https://wikihub.berkeley.edu/display/calnet/CalNet+InCommon-Comodo+Certificate+Service#CalNetInCommon-ComodoCertificateService-GenFAQ

Note: If you use the python script, please customize the [req_distinguished_name] section in the script. For more information on openSSL input parameters, you can use the reference here: http://www.openssl.org/docs/apps/req.html. For example, if I wanted to add emailAddress to the CSR, I would edit the script and added emailAddress=xxx@xxx.xxx.xxx right below the [req_distinguished_name]

If you already have an SSL certificate in use, you can add a SAN to it without generating a new CSR and revoking the existing cert. In this case, contact your CERT authority to make this arrangement.

Revision #3
Created 2011-03-04 16:05:43 UTC by Tran, Daniel
Updated 2012-08-03 21:52:58 UTC by Rom, Gloria