

UC Berkeley - CCS Managed PKI for SSL Subscriber Services

General Information

CCS has pre-purchased the right to issue Verisign SSL certificates and to manage the distribution and renewal of these certificates. If you previously purchased a Verisign certificate independently, you must obtain a new certificate, rather than renew. Future renewals of the cert can then be made through this service.

Information needed when generating your CSR (Certificate Signing Request) on the server

Common Name

The Common Name is the Host + Domain Name. It looks like "www.berkeley.edu" or "bfs.berkeley.edu".

VeriSign certificates can only be used on Web servers using the Common Name specified during enrollment. For example, a certificate for the domain "domain.com" will receive a warning if accessing a site named "www.domain.com" or "secure.domain.com", because "www.domain.com" and "secure.domain.com" are different from "domain.com".

If you have a load balanced name or alias (e.g. reportportal.berkeley.edu) that runs on multiple servers (e.g. act-pa04.berkeley.edu and act-pa05.berkeley.edu) you should use the load-balanced name for the certificate, and specify quantity 2 on the order (because it will be applied to 2 servers).

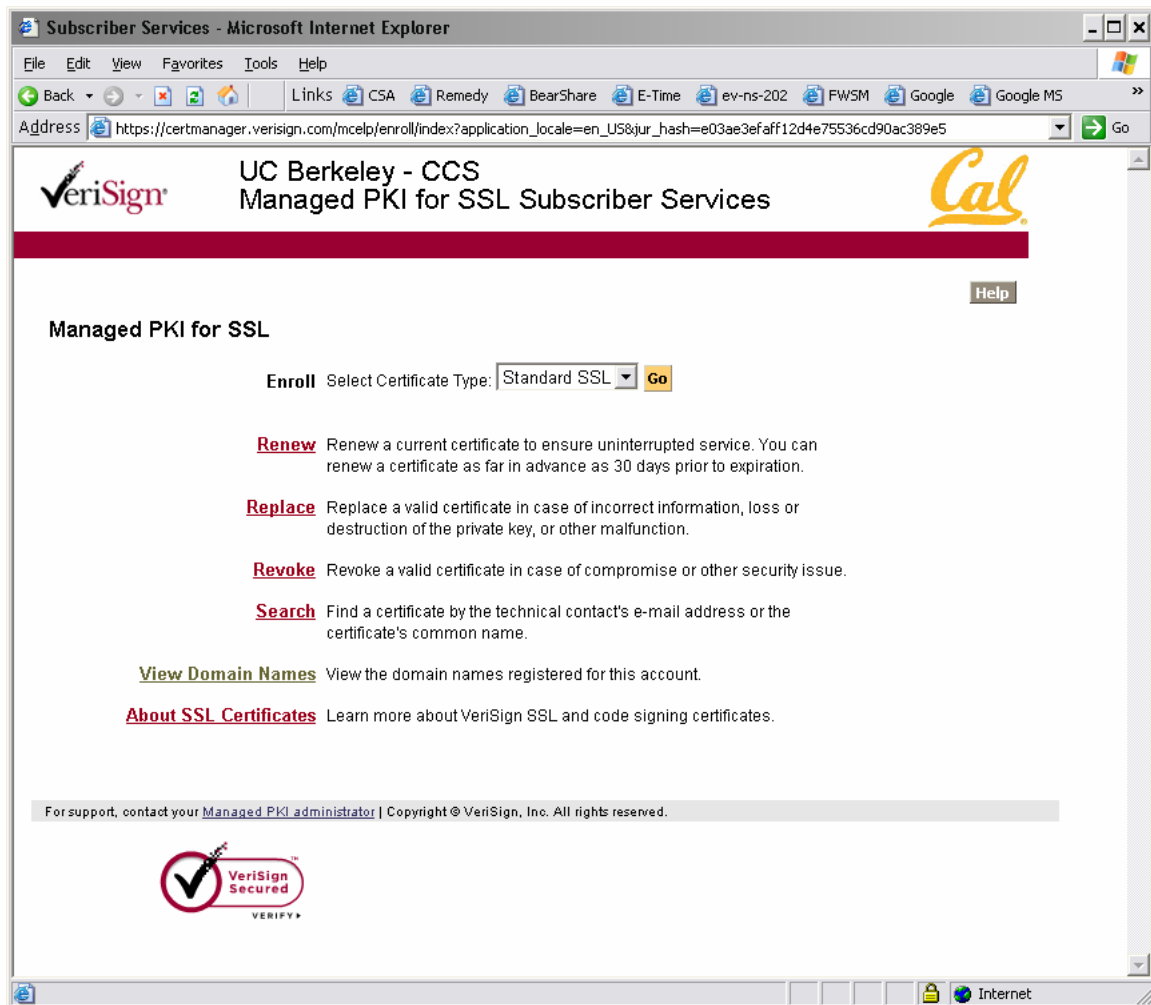
Organization Information

- The organization field should read: UC Berkeley (**Not** U.C. Berkeley or University of California, Berkeley)
- The "Org Unit" field is the name of the department or organization unit making the request.
- The Locality field should read: Berkeley.
- The state or province name, should read: California.
- Country code should read: US

Requesting your Certificate

1. Browse to the URL:

https://certmanager.verisign.com/mcelp/enroll/index?application_locale=en_US&jur_hash=e03ae3efaff12d4e75536cd90ac389e5




2. Click the "Go" Button

Subscriber Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Links CSA Remedy BearShare E-Time ev-ns-202 FW5M Google Google MS

Address https://certmanager.verisign.com/mcelp/enroll/enroll?application_locale=en_US&jur_hash=e03ae3efaff12d4e75536cd90ac389e5&certProdu Go

VeriSign UC Berkeley - CCS Managed PKI for SSL Subscriber Services 

[Help](#)

Enroll for a Standard SSL Certificate

Complete and submit this form to request a new SSL certificate from **UC Berkeley - CCS**.

If you have questions about this enrollment form, click the **Help** button at right or contact your [Managed PKI administrator](#).

* Required Field

Your Contact Information

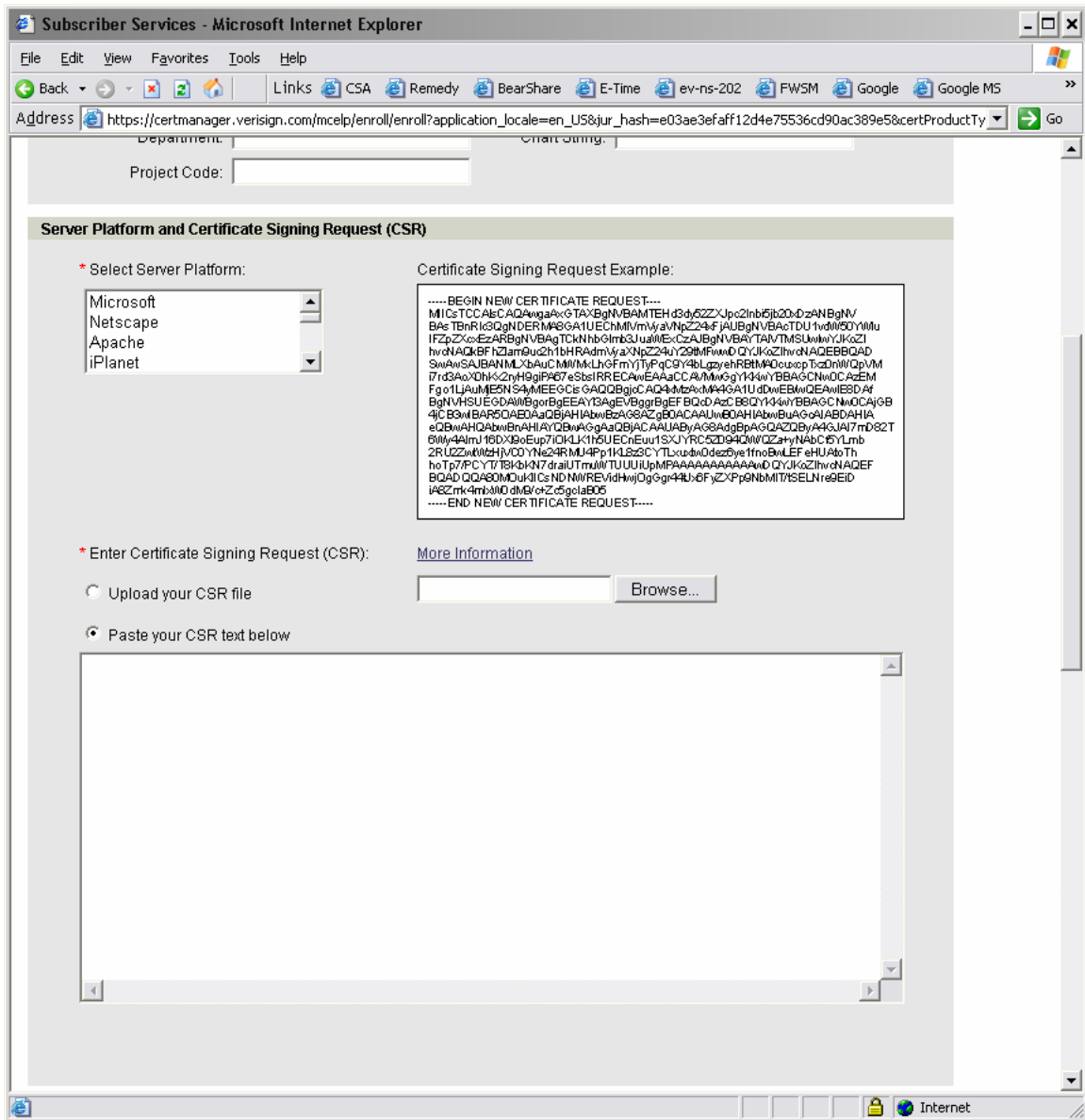
Fill in all required contact and other enrollment information configured by your Managed PKI administrator. Your Managed PKI administrator uses this information to approve your certificate request.

* First Name:	<input type="text"/>	Middle Initial:	<input type="text"/>
* Last Name:	<input type="text"/>	* E-mail Address:	<input type="text"/>
* Department:	<input type="text"/>	* Chart String:	<input type="text"/>
Project Code:	<input type="text"/>		

Server Platform and Certificate Signing Request (CSR)

* Select Server Platform:	<input type="text"/>	Certificate Signing Request Example:	<input type="text"/>
---------------------------	----------------------	--------------------------------------	----------------------

3. Enter the Contact information, the following fields are required:
 - a. First Name
 - b. Last Name
 - c. Email Address (where you want notifications and the certificate to be sent)
 - d. Department owning the certificate
 - e. Chart string against which the certificate fee will be charged



4. Select Server Platform (e.g. Microsoft for IIS, BEA Weblogic, Apache, etc.)
5. Paste or attach the Certificate Signing Request (CSR) generated on the server.

Subscriber Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Links CSA Remedy BearShare E-Time ev-ns-202 FWSM Google Google MS

Address https://certmanager.verisign.com/mcelp/enroll/enroll?application_locale=en_US&jur_hash=e03ae3efaff12d4e75536cd90ac389e5&certProduct Go

Certificate Options

If you have multiple servers hosting a single domain, you can secure all of them with a single SSL certificate.

Server Licenses:

Validity Period: One Year Two Years

Challenge Phrase

Enter a new challenge phrase. The challenge phrase is a certificate password used to renew or revoke your certificate. This password is not your server's private key password.

* Challenge Phrase:

* Re-enter Challenge Phrase:

Comments to Administrator

Enter any comments to your Managed PKI administrator as needed. These comments are not included in your SSL certificate.


Subscriber Agreement

[Printable Version](#)

VeriSign Class 3 Organizational Certificate Subscriber Agreement

YOU MUST READ THIS SUBSCRIBER AGREEMENT ("SUBSCRIBER AGREEMENT") BEFORE APPLYING FOR, ACCEPTING, OR USING A VERISIGN SECURE SITE CERTIFICATE, SECURE SITE PRO CERTIFICATE, OFX SSL CERTIFICATE, SHARED HOSTING SECURITY SERVICE CERTIFICATE, WLAN SERVER CERTIFICATE, MANAGED PKI FOR SSL CERTIFICATE, OR MANAGED PKI FOR SSL PREMIUM EDITION CERTIFICATE, MANAGED PKI FOR SSL INTRANET CERTIFICATE, OR MANAGED PKI FOR INTRANET SSL PREMIUM EDITION CERTIFICATE (COLLECTIVELY A "CERTIFICATE" AS FURTHER

For support, contact your [Managed PKI administrator](#) | Copyright © VeriSign, Inc. All rights reserved.



Internet

6. Enter number of server licenses needed
7. Choose whether the cert is to be valid for one or two years
8. Enter your challenge phrase (this is used to authenticate that you have right to see or change information about the certificate, such as contact information)
9. Accept the Subscriber agreement.



Thank you for completing your order!

Congratulations, you have successfully enrolled for an SSL Certificate for *UC Berkeley*. You will soon receive an e-mail confirming your order.

Your administrator will review your request. When your request is approved, you will receive an e-mail from your administrator with your SSL Certificate and instructions for installing it.

If you have questions about your order, please contact your [Managed PKI for SSL administrator](#).

Subscriber Services

For support, contact your [Managed PKI administrator](#) | Copyright © VeriSign, Inc. All rights reserved.



This screen shows that the submission was successful.

Completion of the Process

Email will be auto-generated from Verisign to the address you specified in the order form confirming the order. The CCS administrators get similar notification email. When your certificate request is approved, Verisign will mail your public key. You will then apply this key to your server(s).

When the certificate is close to expiration, you will receive notification from Verisign at your specified email address. It is important to keep your contact information current for timely notification of renewal.