InCommon ®

InCommon
Certificate Manager

SSL Certificates
Enrollment, Collection, Installation and Renewal

InCommon
c/o Internet2
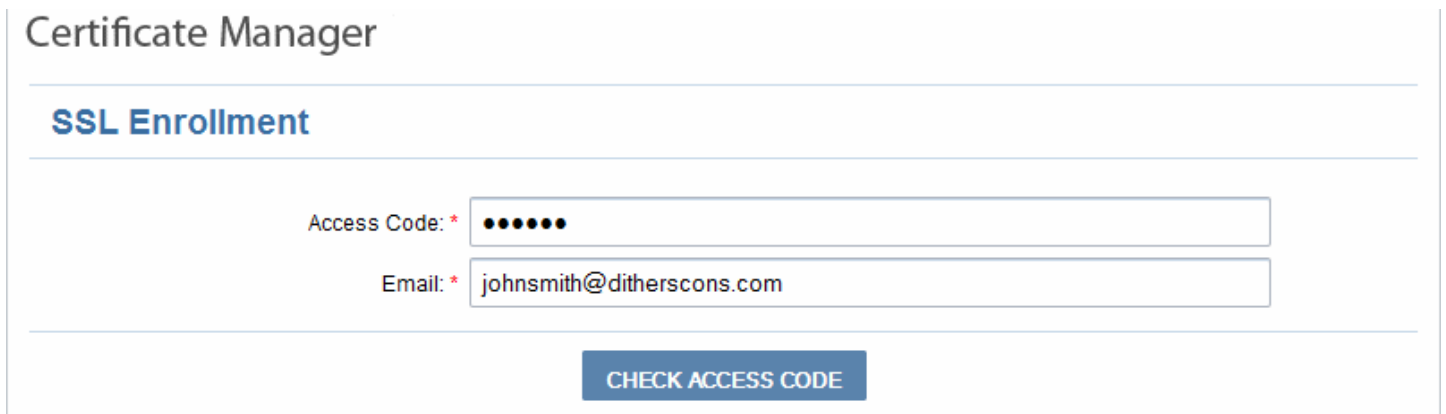1000 Oakbrook Drive, Suite 300
Ann Arbor MI, 48104

Enrolling For Your Certificate

This is step-by-step guide will explain how to enroll for then collect and install an SSL certificate on your web server.

Step 1: The provisioning email and authentication

Firstly, your SSL administrator should have sent you a certificate provisioning email. This email will contain two important items:

- A link to the certificate enrollment pages. The URL will be *similar* to https://cert-manager.com/customer/InCommon/ssl

- An access code which will be used to authenticate you before you can proceed to the enrollment form.

- Click the enrollment link in your mail. You will be taken to the SSL certificate management page.
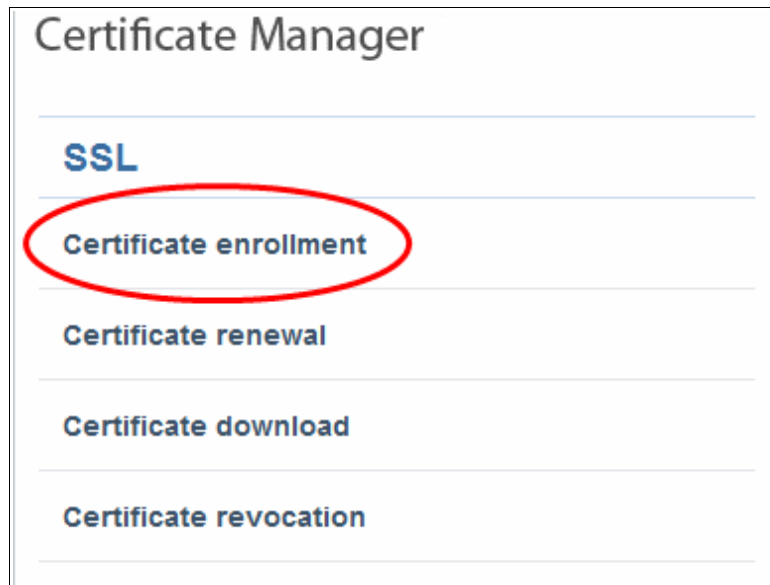
- Click the 'Certificate enrollment' link will open the self enrollment form

- Copy and paste the code from your email into the 'Access Code' field.

- Enter your email address in the space provided. This email address must be on the same domain as the certificate for which you are applying. For example, if you are applying for a certificate for www.company.com, then the email address entered here must be something like yourname@company.com. You must also be able to receive mail at this address.

- Click 'Check access code' to verify your application. Please contact your SSL administrator if authentication fails.

- If authentication is successful, you will proceed to Step 2: The self-enrollment form:

Step 2: The Self-Enrollment Form

You need to fill out all fields in order to submit the form. After submitting, your application will be sent to your SSL administrator for approval and issuance. Advice on all fields on this form is available directly below the screenshot.

InCommon ® Certificate Manager

SSL Enrollment

Access Code: * ••••••

Email: * john@ccmqa.com

The external applicant need not be an existing user in the CM, but the person's email address must be from the same domain as the common name, else the application cannot proceed.

Click here to edit address details

Certificate Type: * Instant SSL

Certificate Term: * 1 year

Server Software: * AOL

CSR: *

GET CN FROM CSR   UPLOAD CSR   Max CSR size is 32K

Common Name: *

Renew: ☐ Auto renew [____] days before expiration

Please provide a pass-phrase. A pass-phrase is necessary for certificate revocation and renewal.

Pass-phrase:

Re-type pass-phrase:

External Requester:

Acceptable format:
- email@domain.com
- email.1@domain.com, email.2@domain.com

Comments:

Subscriber Agreement: Predefined test SSL license text for test customer[2]...

PRINT

☐ I Agree. *

Scroll to bottom of the agreement to activate check box.

ENROLL   RESET

Clicking 'Get Common Name from CSR' will automatically populate the 'Common Name' field and if relevant, the 'SAN' field with the domian name(s) in the CSR - Helping to avoid errors. This feature is especially useful while applying for MDCs where the application could contain upto 100 domains in the SAN field.

The applicant can directly upload the CSR saved as .txt file by clicking 'Upload CSR'. The CSR field will be auto-populated with the CSR from the text file.

The applicant can configure for auto-renewal of the certificate, upon its expiry.

The Passphrase entered here is required for the purposes of certificate revocation.

The applicant must accept the 'Terms and Conditions' before submitting the form. The 'I Agree' checkbox becomes active only on scrolling down the page till the end.
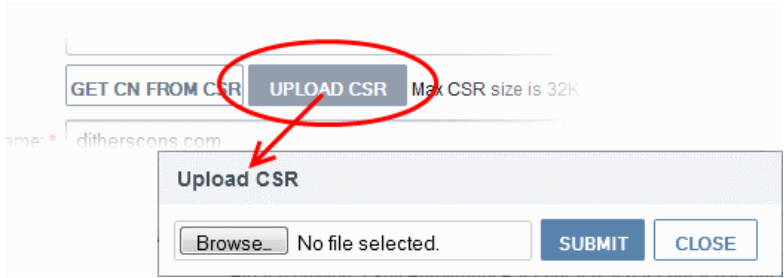
Form notes and advice

- The 'Access Code' and 'E-mail' address fields will be pre-populated as you entered them previously.

- The EV application form contains additional fields related to Incorporating Agency and certificate requester, approver and signer. The MDC form contains an additional SAN field so you can add multiple domain names.

- InCommon's partner Comodo provides a range of CSR generation documents designed to assist with the CSR creation process at https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=33&pcid=1&nav=0,96,1

- After you have successfully submitted the form, your application will go for approval by your SSL administrator. Once approved, your certificate request will be forwarded to InCommon CA for issuance and you will be notified by email when it is ready for collection. Help on certificate collection and installation are in the section that comes after this table:

Form Element	Type	Description
Access Code *(required)*	*Text Field*	An access code is used to authenticate certificate requests that are made using the self-enrollment form. This code should have been supplied by your SSL administrator. Please contact him/her if this has not been provided to you.
Email *(required)*	*Text Field*	Please enter the contact email address for this application. The email address must be from the same domain as the common name and you must be able to receive mails at this address.
Address Details Displayed on clicking the Click here to edit address details link. Address 1: Address 2: Address 3: City: State or Province: Postal Code: (all auto-populated)	*Text Fields*	Clicking the link Click here to edit address details displays the address fields. The address fields are auto-populated from the details in the 'General Settings' tab of the Organization or Department on whose behalf this certificate request is being made. These fields cannot be modified but, in the case of OV level certificates, the applicant can choose to omit them from the certificate by selecting the 'Remove' checkbox next to the fields. The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted". For EV level certificates, it is mandatory to include and display address details of the Organization, Incorporation or Registration Agency, Certificate Requester and the Contract Signer. Therefore text fields for entering the these address details will be displayed and the option to remove certain fields is not available on the EV self-enrollment form on selecting Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate from the 'Certificate Type' drop-down.
Certificate Type *(required)*	*Drop-down list*	Please choose the type of certificate you need. For an explanation of certificate types, please refer to Appendix: Certificate Types
Certificate Term *(required)*	*Drop-down list*	*Applicant should select the life time of the certificate chosen from the 'Certificate Type ' drop-down.*

Form Element	Type	Description
		The available term lengths for different certificate types displayed in the drop-down list (and therefore available to the applicant) can be customized according to the needs of the Organization. Please refer to sections Creating a new Organization, Customize an Organization's SSL Certificate Types and SSL Types for more details.
Server Software **(required)**	*Drop-down list*	*Applicant should select the server software that is used to operate their web server (for example, Apache, IIS etc). Installation support documentation is available from the Comodo's support portal here:* https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=1&pcid=0&nav=0
CSR **(required)**	*Text Field*	A Certificate Signing Request (CSR) is required to be entered into this field in order forInCommon CA to process your application and issue the certificate for the domain. The CSR can be entered in two ways: • Pasting the CSR directly into this field • Uploading the CSR saved as a .txt file by clicking the 'Upload CSR' button **Background:** In public key infrastructure systems, a certificate signing request (also CSR or certification request) is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate. Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The CSR contains information identifying the applicant (such as a directory name in the case of an X.509 certificate), and the public key chosen by the applicant. The corresponding private key is not included in the CSR, but is used to digitally sign the entire request. The CSR may be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate authority may contact the applicant for further information. Upon uploading or pasting the CSR, the form will automatically parse the CSR. Administrators that require assistance to generate a CSR should consult the Comodo knowledge article for their web server type here: https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=33&pcid=1&nav=0,1 **Special Note regarding MDC applications:** The CSR you generate only needs to be for the single 'Common Name' (aka the 'Primary Domain Name'). You should type the additional domains that you require in the 'Subject Alternative Name' field' on this form.
Get CN from CSR **(optional)**	*Control*	Once the CSR has been entered correctly, clicking this button will auto-populate the Common Name (CN) field. Using this method helps to avoid human error by ensuring the domain name mentioned in the application form exactly match that in the CSR. If the domain name mentioned in this application form do not match that in

| Form Element	Type	Description
		the CSR, then InCommon CA will not be able to issue the certificate. **Special Note regarding MDC applications:** In order to successfully order a Multi-Domain Certificate, the applicant need only list the additional domains in the SAN field on this form. In certain circumstances, however, the applicant may have created a CSR that already contains these Subject Alternative Names. In this case, clicking the 'Get CN from CSR' button will also auto-populate the 'Subject Alternative Names' form fields as well as the 'Common Name' field.
Upload CSR *(optional)*	*Control*	The applicant can upload the CSR saved as a .txt file in the local computer, instead of copying and pasting the CSR into the CSR field - helping to avoid errors.
Common Name *(required)*	*Text Field*	Applicants should enter the correct fully qualified domain name for the Organization or Department Single Domain certificates - enter domain name using the form: domain.com. Wildcard Certificates - enter domain name using the form: *.domain.com. Multi-Domain Certificates - enter the primary domain name using the form: domain.com.
Renew	Check box	Allows applicants to specify whether the certificate should be automatically renewed when it is nearing expiry. Applicants can also choose the number of days in advance of expiry that the renewal process should start. On the scheduled day, CCM will automatically submit the renewal application to the CA with a CSR generated using the same parameters as the existing certificate.
Subject Alternative Names *(required for Multi-Domain certificates)*	*Text Field*	If the certificate 'Type' is a Multi-Domain Certificate (MDC) then the applicant should list the 'Subj Alt Name' additional domains here. Each domain listed in this field should be separated by a comma.
Pass Phrase *(optional)*	*Text Field*	This phrase is needed to revoke the certificate when using the external revocation page at: https://cert-manager.com/customer/InCommon/ssl?action=revoke
Re-type Pass Phrase *(required if specified in the field above)*	*Text Field*	Confirmation of the above.

Form Element	Type	Description
External Requester (*optional*)	Text Field	Applicants should enter the full email address of the user on behalf of whom the application is made. The email address must be from the same domain name for which the certificate is applied. The certificate collection email will be sent to this email address.

| Form Element	Type	Description
Comments *(optional)*	*Text Field*	Applicant can enter information for the administrator.
Subscriber Agreement	*Checkbox*	Applicant must accept the terms and conditions before submitting the form by reading the agreement and clicking the 'I Agree' checkbox. **Note**: The Subscriber Agreement will differ depending on the type of SSL certificate selected from the 'Certificate Type' drop-down. If Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate is selected, The 'I Agree' checkbox will not be shown and the agreement will be taken as accepted, when the user submits the application.
Enroll	*Control*	Submits the application and enrolls the new certificate request.
Reset	*Control*	Clears all data entered on the form.

Certificate Collection and Installation

The next stage of the process is to download your certificate then install it on your web-server.

Once your certificate has been validated and issued you will receive a certificate collection email. The email will contain a summary of certificate details and a link to the certificate download page. This link also contains a unique ID that will be used to verify the download.
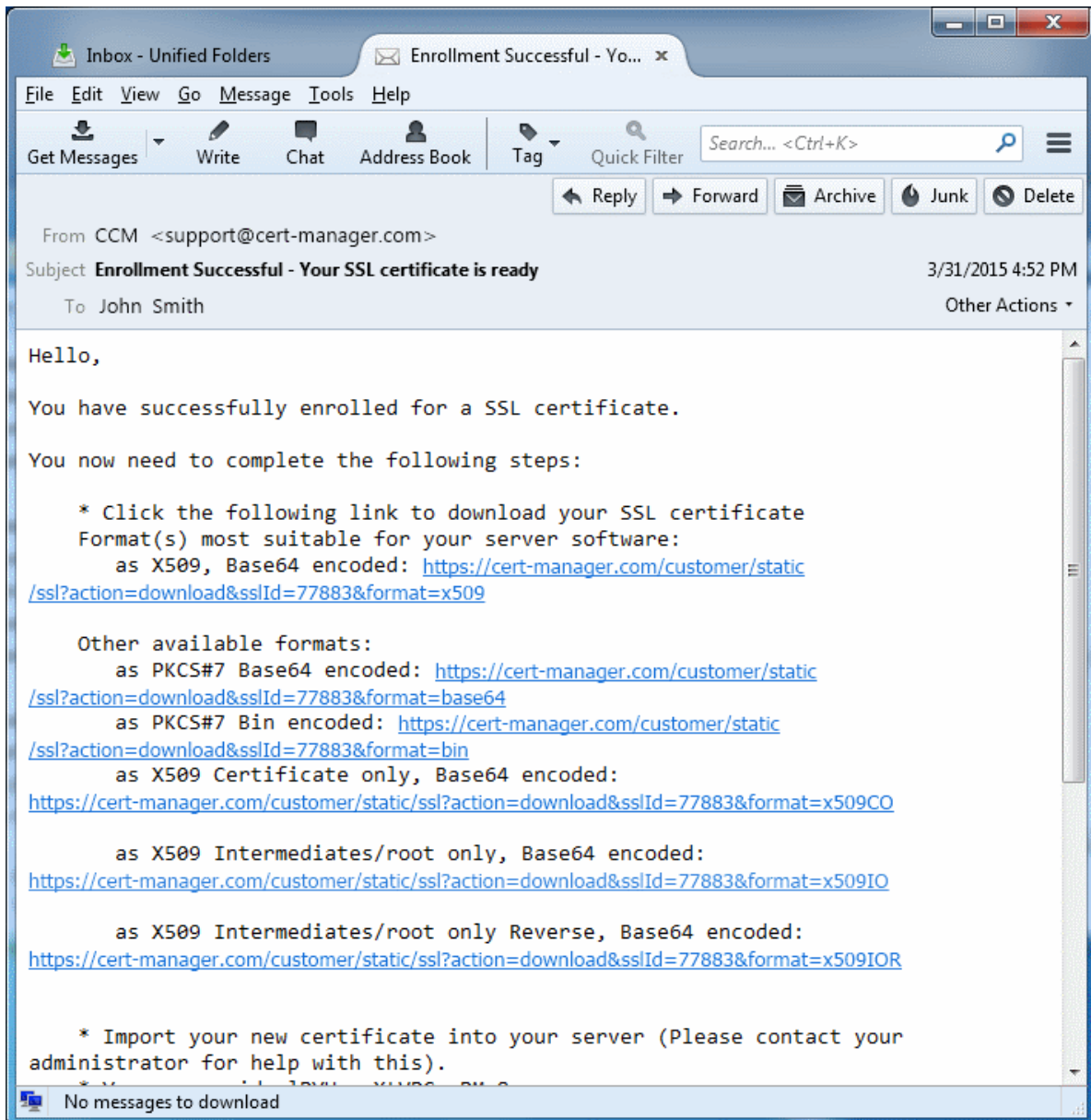
Having clicked the link in the mail, you will be taken to the certificate download form:
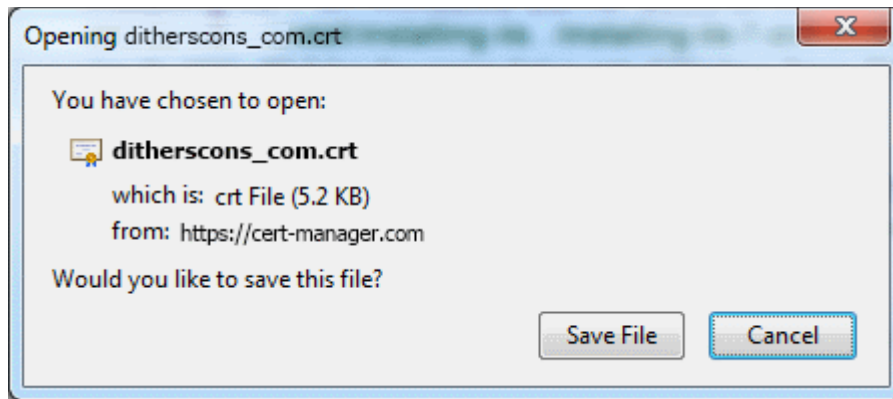
Next, you need to install the certificate. The precise installation process will depend on which type of web server you use to host your site. The following page contains a list of tutorials covering certificate installation on a wide range of web servers:

https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=1&pcid=0&nav

Renewing Your Certificate

You can renew certificates which are about to expire by entering the Self Enrollment Certificate ID and the renewal pass-phrase of the certificate in the Self-Renewal form. The Self Enrollment Certificate ID can be found in the certificate collection email you received during enrollment. The renewal pass-phrase is the one you entered in the self-enrollment form, while enrolling for the certificate. Please contact your administrator if you do not have access to either of these pieces of information.

Accessing the Self Renewal Form

The Self Renewal form is available at the same URL of the Self Enrollment form. The URL will be *similar* to https://cert-manager.com/customer/InCommon/ssl
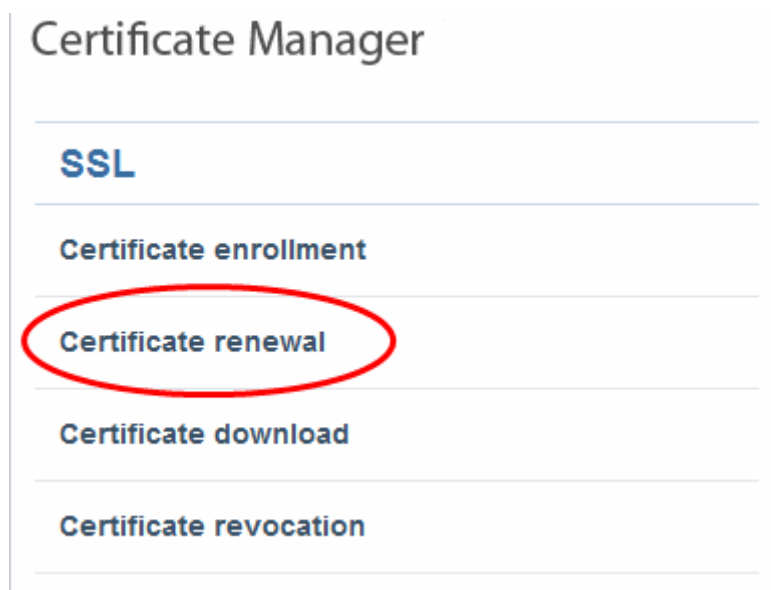
- Clicking the 'Certificate renewal' link will open the self renewal form

Certificate Manager

SSL Renew

Your Certificate ID: *	77881
Pass-phrase: *	●●●●●●

RENEW

Form Element	Description
Your Certificate ID *(required)*	Please enter the correct self enrollment certificate ID. The certificate ID is available from certificate collection email received during enrollment. Tip: If you do not have the certificate collection email or the self enrollment ID, you can request your SSL administrator for the same, by providing your certificate details. The administrator can refer to the InCommon CM interface and can communicate the ID to you.
Pass-phrase *(required)*	Please enter renewal/revocation passphrase you entered in the self-enrollment form, while enrolling for the certificate.

- Filling up the 'SSL Renew' form and clicking 'Renew' will automatically renew the certificate with the same details as in the existing certificate.

- Once issued, the renewal certificate can be collected and installed. Refer to the section Certificate Collection and Installation for more details.

Appendix - Certificate Types

If you do not know which type of certificate to choose then we recommend that you first contact your SSL admin who should be able to advise you. This appendix is provided only to give applicants an understanding of the different types of certificate that are available but does not cover pricing or warranty levels. The appendix opens with a definition of terms that should provide an insight into SSL terminology and concludes with a table listing all certificates offered by InCommon CA. Note – this is a *complete* list of InCommon certificates. You might not see all of these certificate types if your administrator hasn't made them available.

Validation Levels

OV: Organization **V**alidated certificates include full business and company validation from a certificate authority using currently established and accepted manual vetting processes.

EV: Extended **V**alidation certificates provide the highest levels of trust and reassure web site visitors that it is safe to trade by turning the address bar green during https sessions. EV's are generally more expensive than OV level certificates and require a more in-depth validation process prior to issuance. However, because the green bar has become a hallmark of security seen on the Internet's largest and most prestigious websites, placing an EV on your website can often lead to increased customer conversion.

Certificate Types

SDC: Single **D**omain **C**ertificates - will secure a single fully qualified domain name such as www.company.com

WC: Wildcard **C**ertificates - will secure the domain and unlmited sub-domains of that domain

MDC: Multi-**D**omain **C**ertificates - will secure up to 100 different domain names on a single certificate

Additional Technologies

SGC: **S**erver **G**ated **C**ryptography. SGC technology upgrades the encryption capabilities of older browsers to modern day standards

Certificate Name	Type	Validation Level	Description	Maximum Term Length
InCommon SSL Certificate	SDC	OV	Secures a single domain	1 year – 3

Certificate Name	Type	Validation Level	Description	Maximum Term Length
				years
InCommon Wildcard SSL Certificate	WC	OV	Secures domain and unlimited sub-domains of that domain	1 year – 3 years
InCommon Multi-Domain SSL Certificate (MDC)	MDC	OV	Secures multiple Fully Qualified domains on a single certificate	1 year – 3 years
InCommon Unified Communication Certificate (UCC)	MDC	OV	Secures multiple Fully Qualified domains on a single certificate. Specifically designed for use with Microsoft Exchange and Microsoft Office Communications servers	1 year – 3 years
InCommon Intranet SSL Certificate	SDC	OV	Secures a single internal host	1 year – 3 years
Comodo Extended Validation (EV) SSL Certificate	SDC	EV	Secures a single domain	1 year – 2 years
Comodo EV Multi-Domain SSL Certificate (EVMDC)	MDC	EV	Secures multiple Fully Qualified domains on a single certificate	1 year – 2 years