InCommon® SSL Certificates

2022 Winter Workshop

David Albrecht
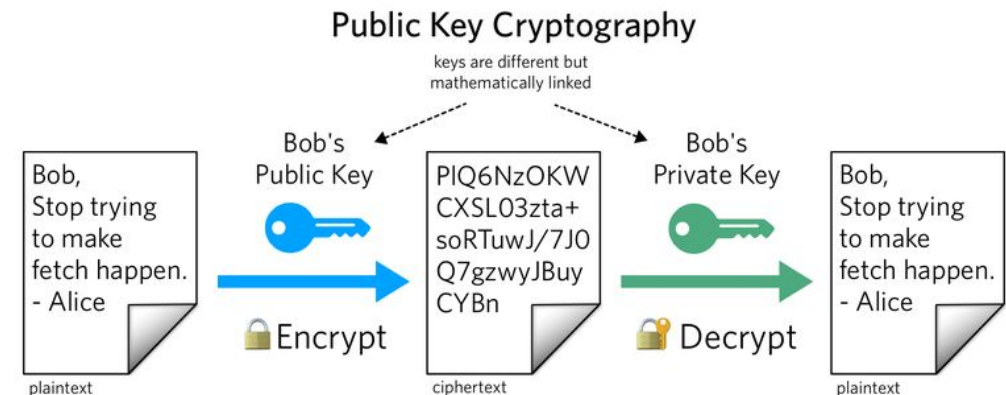
California Community Colleges

Topics we will cover:

❏ What is an SSL certificate?

❏ How does it work?

❏ What types of certificates are available?

❏ How much do they cost?

❏ Which certificate type is right for me?

❏ How do you use the interface?

❏ Additional resources

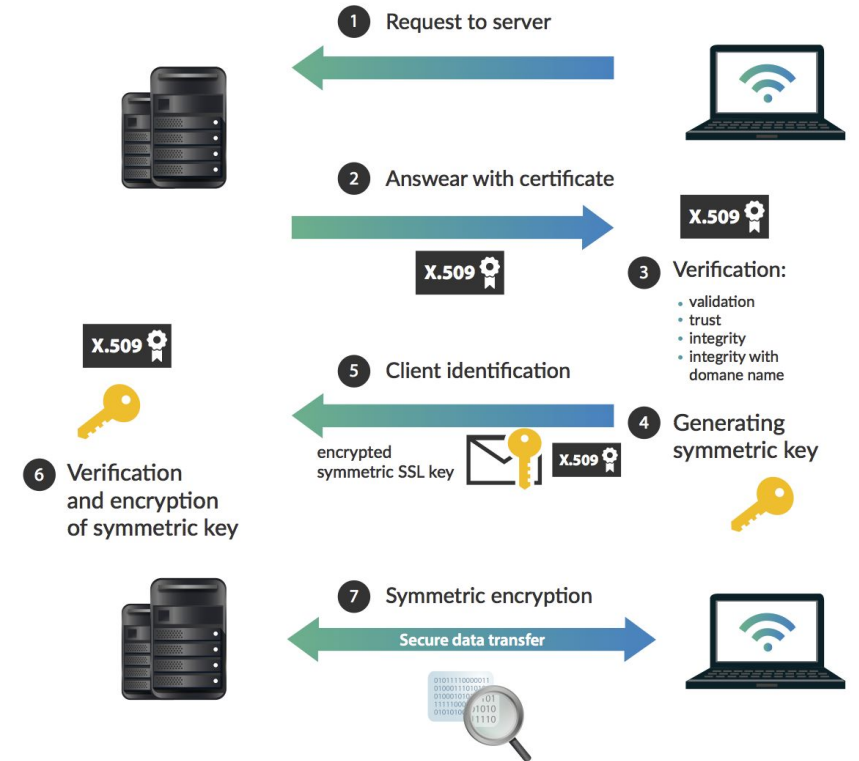❏ Benefits of InCommon membership

California Community Colleges

What is an SSL certificate?

❑ Stands for Secure Socket Layer

❑ Is not actually SSL, is technically TLS or Transport Layer Security

❑ Verifies a website identity through public/private key cryptography

❑ Secures private information through encryption in transit

❑ Usually begins with the https:// prefix

❑ Is a defense against man in the middle attacks

❑ Required by most modern web browsers

❑ Would take about 300 trillion years to brute force

Public Key Cryptography

keys are different but mathematically linked

Bob's Public Key

Bob,
Stop trying to make fetch happen.
- Alice

plaintext

🔒Encrypt

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn

ciphertext

Bob's Private Key

🔓Decrypt

Bob,
Stop trying to make fetch happen.
- Alice

plaintext

How does it work?

❑ Verifies the server instance and the chain of trust

❑ Allows the connection to be encrypted

❑ Easy to add primes, hard to guess used primes

❑ Allows the connection to be encrypted

❑ Is a defense against man in the middle attacks

❑ Required by most modern web browsers

1 Request to server

2 Answear with certificate

X.509

3 Verification:
- validation
- trust
- integrity
- integrity with domane name

5 Client identification

4 Generating symmetric key

encrypted symmetric SSL key

X.509

6 Verification and encryption of symmetric key

7 Symmetric encryption

Secure data transfer

www.internetum.com

California Community Colleges

What types of certificates are available?

☑ Self-Signed

What types of certificates are available?

☑ Self-Signed

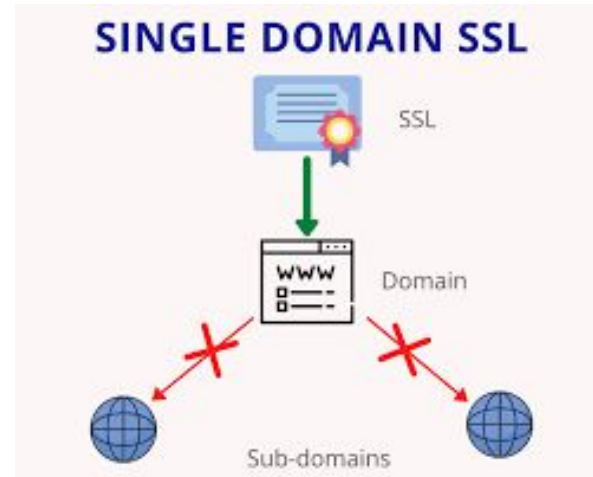☑ Let's Encrypt

What types of certificates are available?

☑ Self-Signed

☑ Let's Encrypt
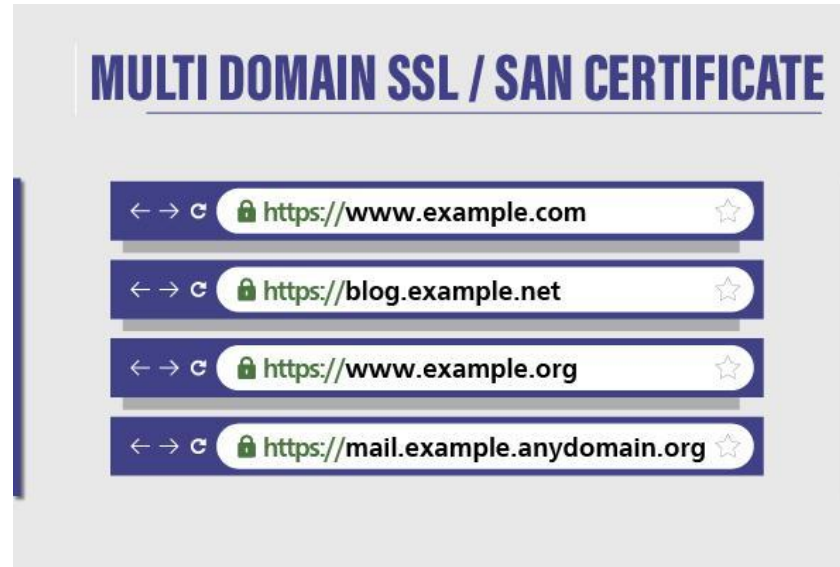
☑ Comodo Elite

California
Community
Colleges

What types of certificates are available?

- ☑ Self-Signed

- ☑ Let's Encrypt

- ☑ Comodo Elite

- ☑ Single Domain

California Community Colleges

What types of certificates are available?

- Self-Signed

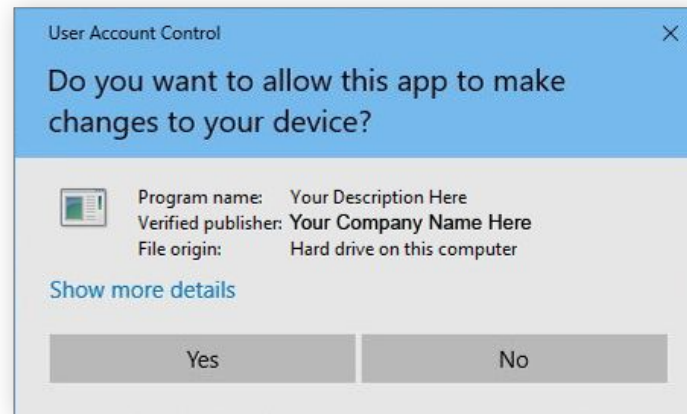- Let's Encrypt

- Comodo Elite

- Single Domain

- Multi-Domain

MULTI DOMAIN SSL / SAN CERTIFICATE

🔒 https://www.example.com

🔒 https://blog.example.net

🔒 https://www.example.org

🔒 https://mail.example.anydomain.org

California Community Colleges

What types of certificates are available?

- ⌨ Self-Signed

- ⌨ Let's Encrypt

- ⌨ Comodo Elite

- ⌨ Single Domain

- ⌨ Multi-Domain

- ⌨ Wildcard

What types of certificates are available?

- Self-Signed

- Let's Encrypt

- Comodo Elite

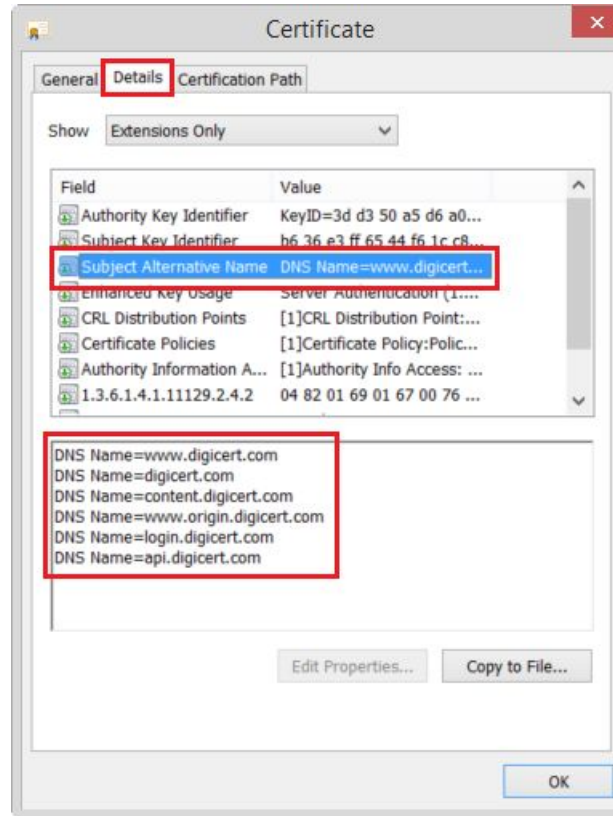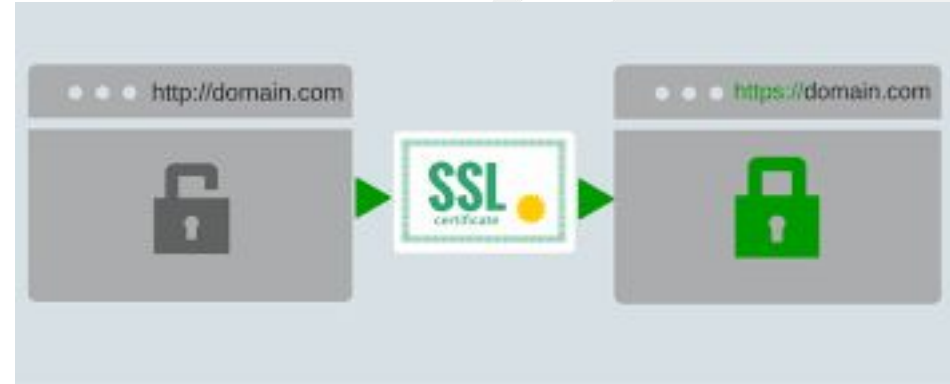- Single Domain

- Multi-Domain

- Wildcard

- Code Signing

User Account Control

Do you want to allow this app to make changes to your device?

Program name: Your Description Here
Verified publisher: Your Company Name Here
File origin: Hard drive on this computer

Show more details

Yes   No

California Community Colleges

What types of certificates are available?

- ☑ Self-Signed

- ☑ Let's Encrypt

- ☑ Comodo Elite

- ☑ Single Domain

- ☑ Multi-Domain

- ☑ Wildcard

- ☑ Code Signing

- ☑ Short Life

California
Community
Colleges

What types of certificates are available?

- Self-Signed
- Let's Encrypt
- Comodo Elite
- Single Domain
- Multi-Domain
- Wildcard
- Code Signing
- Short Life
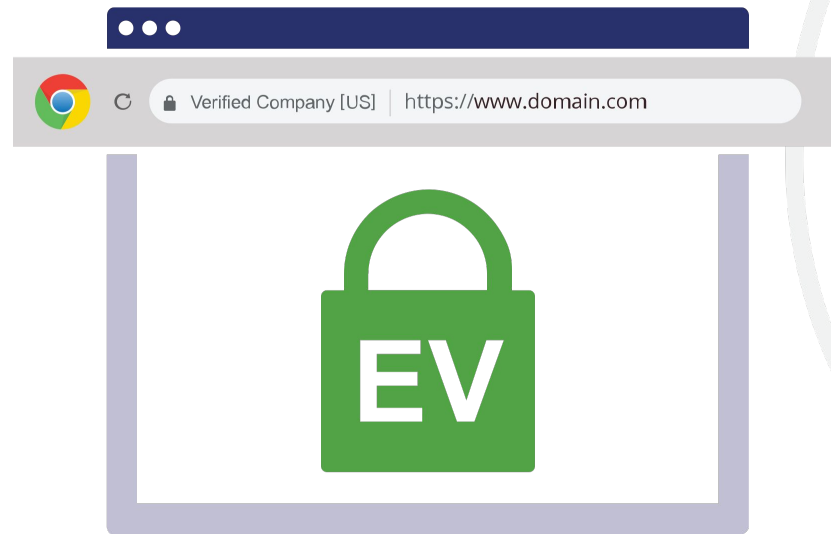- Unified Communications

What types of certificates are available?

- Self-Signed

- Let's Encrypt

- Comodo Elite

- Single Domain

- Multi-Domain

- Wildcard

- Code Signing

- Short Life

- Unified Communications

- Domain Validated (DV)

What types of certificates are available?

- Self-Signed   ☑
- Let's Encrypt   ☑
- Comodo Elite
- Single Domain
- Multi-Domain
- Wildcard
- Code Signing
- Short Life
- Unified Communications
- Domain Validated (DV)
- Organization Validated (OV)

What types of certificates are available?

- ☑ Self-Signed   ☑
- ☑ Let's Encrypt   ☑
- ☑ Comodo Elite   ☑
- ☑ Single Domain
- ☑ Multi-Domain
- ☑ Wildcard
- ☑ Code Signing
- ☑ Short Life
- ☑ Unified Communications
- ☐ Domain Validated (DV)
- ☐ Organization Validated (OV)

Verified Company [US] | https://www.domain.com

EV

What types of certificates are available?

- ☑ Self-Signed   ☑
- ☑ Let's Encrypt   ☑
- ☑ Comodo Elite   ☑
- ☑ Single Domain   ☑
- ☑ Multi-Domain
- ☑ Wildcard
- ☑ Code Signing
- ☑ Short Life
- ☑ Unified Communications
- ☐ Domain Validated (DV)
- ☐ Organization Validated (OV)

Attribute	Value
Organization	<Organization_Requiring_Extended_Validation>
Certificate Type	EV Anchor Certificate
Common Name	<something>.<domain>.<extension>
Subject Alternative Names	contoso.com, contosoc.ca, acme.com, acme.org, test.ca, test.co.uk, abc123.nl

California Community Colleges

What types of certificates are available?

- ☑ Self-Signed ☑
- ☑ Let's Encrypt ☑
- ☑ Comodo Elite ☑
- ☑ Single Domain ☑
- ☑ Multi-Domain ☑
- ☑ Wildcard
- ☑ Code Signing
- ☑ Short Life
- ☑ Unified Communications
- ☐ Domain Validated (DV)
- ☐ Organization Validated (OV)

What types of certificates are available?

- Self-Signed ☑
- Let's Encrypt ☑
- Comodo Elite ☑
- Single Domain ☑
- Multi-Domain ☑
- Wildcard ☑
- Code Signing
- Short Life
- Unified Communications
- Domain Validated (DV)
- Organization Validated (OV)

IGTF
International Grid Trust Federation
AP | EU | TAG

What types of certificates are available?

☑ Self-Signed   ☑

☑ Let's Encrypt   ☑

☑ Comodo Elite   ☑

☑ Single Domain   ☑

☑ Multi-Domain   ☑

☑ Wildcard   ☑

☑ Code Signing   ☑

☑ Short Life

☑ Unified Communications

☐ Domain Validated (DV)

☐ Organization Validated (OV)

What types of certificates are available?

- ☑ Self-Signed   ☑
- ☑ Let's Encrypt   ☑
- ☑ Comodo Elite   ☑
- ☑ Single Domain   ☑
- ☑ Multi-Domain   ☑
- ☑ Wildcard   ☑
- ☑ Code Signing   ☑
- ☑ Short Life   ☑
- ☑ Unified Communications
- ☐ Domain Validated (DV)
- ☐ Organization Validated (OV)

How much do they cost?

❑ Single domain, Comodo basic SSL SHA 128 bit ($62/yr)

❑ Code signing ($85/yr)

❑ Wildcard certificates SHA2 2048-4096 bit ($199/yr)

❑ Multi-Domain certificates SHA2 2048-4096 bit ($250/yr)

❑ Extended Validation certificates SHA2 2048-4096 bit ($450-$1000/yr)

❑ All of the above, and much more available through InCommon – for free!

Which Certificate is right for me?

❏ Depends on use case, but try to keep it simple

❏ Use auto-renew whenever possible

❏ 2048 bit keys are plenty strong

❏ Most colleges use either InCommon SSL, Multi-domain or Wildcard

❏ Summary of most recent 3000 certificates issued;

❏ 68% InCommon SSL (single domain)

❏ 24% InCommon Multi-Domain

❏ 7% InCommon Wildcard

California Community Colleges

David Albrecht

Dashboard

Certificates ⌄

Discovery ⌄

Domains

Organizations

Reports

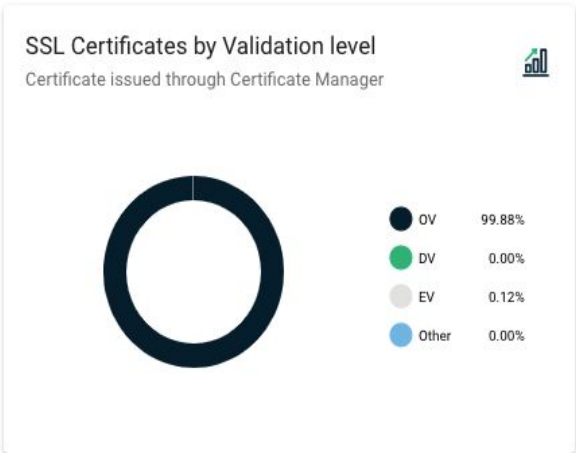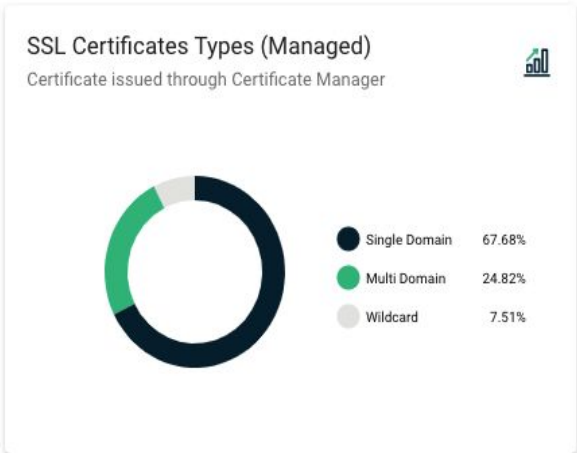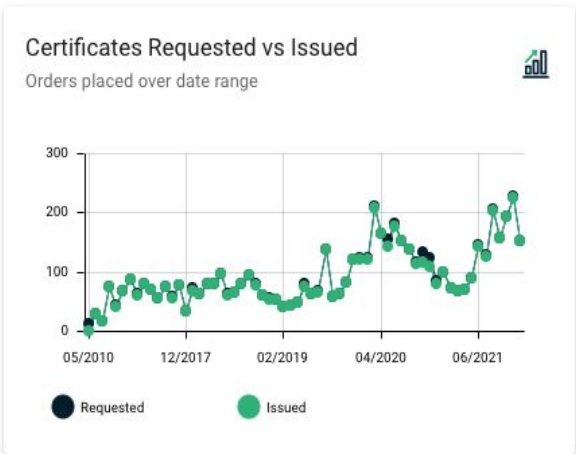Enrollment ⌄

Integrations ⌄

Settings ⌄

About

🔒 SSL Certificates
+ 207 Since Last Month

3,224 Total | **2,478** Active | **746** Revoked

✎ Code Signing Certificates
+ 0 Since Last Month

7 Total | **7** Active | **0** Revoked

Expiring Certificates
Within 180 days

- Sectigo Limited
- Self-Signed
- Trusted

Expiring Domain Validation
Within 180 days

Certificates Requested vs Issued
Orders placed over date range

05/2010   12/2017   02/2019   04/2020   06/2021

- Requested
- Issued

Certificate Requests
Orders placed over date range

05/2010   12/2017   02/2019   04/2020   06/2021

- SSL
- Client Certificate
- Code Signing
- Device

SSL Certificates Types (Managed)
Certificate issued through Certificate Manager

- Single Domain — 67.68%
- Multi Domain — 24.82%
- Wildcard — 7.51%

SSL Certificates by Validation level
Certificate issued through Certificate Manager

- OV — 99.88%
- DV — 0.00%
- EV — 0.12%
- Other — 0.00%

California Community Colleges

Admins

Add IdP User   Add Template   +

	NAME	EMAIL	USERNAME	TYPE ↓	ROLE	ACTIVE
−	**STANDARD**					
☐	Patrick Plagens	pplagens@sdccd.edu	pplagens@sdccd.edu	Standard	DRAO Admin - SSL, DRAO A⋯	✅
☐	Jon Ambrosia	jambrosi@sdccd.edu	jambrosi@sdccd.edu	Standard	DRAO Admin - SSL, DRAO A⋯	✅
☐	David Albrecht	albrechtda@cccnext.net	albrechtda@cccnext.net	Standard	DRAO Admin - SSL, DRAO A⋯	✅
☐	Larry Hsieh	lhsieh@ivc.edu	lhsieh@ivc.edu	Standard	DRAO Admin - SSL, DRAO A⋯	✅
☐	Robert Ford	rford@ivc.edu	rford@ivc.edu	Standard	DRAO Admin - SSL, DRAO A⋯	✅
☐	Kevin Quinn	kquinn@socccd.edu	kquinn@socccd.edu	Standard	DRAO Admin - SSL, DRAO A⋯	✅
☐	Hsiawen Hull	hsiawen.hull@canyons.edu	hsiawen.hull@canyons.e⋯	Standard	DRAO Admin - SSL, DRAO A⋯	✅
☐	Kevin Du	kdu13@saddleback.edu	kdu13@saddleback.edu	Standard	DRAO Admin - SSL, DRAO A⋯	✅
☐	Hai Nguyen	HNguyen@fullcoll.edu	hnguyen@fullcoll.edu	Standard	DRAO Admin - SSL, DRAO A⋯	✅
☐	Michael Cortez	mcortez@fullcoll.edu	mcortez@fullcoll.edu	Standard	DRAO Admin - SSL, DRAO A⋯	✅

Sidebar navigation:
- Dashboard
- Certificates
- Discovery
- Domains
- Organizations
- Reports
- Enrollment
- Integrations
- Settings
  - Email Notifications
  - Admins
- About

David Albrecht

Page 1   Rows per page 10   1-10 of 224

California Community Colleges

David Albrecht

Domains

Domains

Name	Status
> ☐ cccassess.org	EXPIRED
> ☐ ccccco.edu	VALIDATED
> ☐ ccccco.net	EXPIRED
> ☐ cccd.edu	VALIDATED
> ☐ cccedplan.org	EXPIRED
> ☐ ccchelp.info	EXPIRED
> ☐ cccmypath.org	EXPIRED
> ☐ cccnext.net	VALIDATED
> ☐ cccnext.org	ACTION REQUIRED
> ☐ ccc-sac.org	EXPIRED
> ☐ cccsecuritycenter.org	EXPIRED
> ☐ cccsurvey.org	EXPIRED
> ☐ ccctc.network	EXPIRED
> ☑ ccctechcenter.org	VALIDATED
> ☐ ccctechedge.org	EXPIRED
> ☐ ccctechnology.info	EXPIRED
> ☐ ccctechplan.org	EXPIRED
> ☐ ccsf.edu	VALIDATED
> ☐ cerritoscollege.us	EXPIRED
> ☐ cerritos.edu	VALIDATED
> ☐ cerrocoso.edu	VALIDATED
> ☐ chaffey.edu	VALIDATED

Total: 479

🌐 ccctechcenter.org   ID 42563   PUBLIC APEX

Created Date	11/10/2016
Created by	Jeff Holden

Delegate

🛡 Domain Control Validation (DCV)
SECTIGO Public CA

DCV method	CNAME
Expires	05/10/2022
DCV Status	VALIDATED ↻

Revalidate

California Community Colleges

David Albrecht

SSL Certificates

	COMMON NAME	DEPARTMENT	RENEWAL STATE
	CALIFORNIA COMMUNITY COLLEGE TECHNOLOGY CENTER		
☐	splunk.ccctechcenter.org	California Community C...	Not scheduled
☐	splunk-utility.ccctechcenter.org	California Community C...	Not scheduled
☐	splunk-indexer.ccctechcenter.org	California Community C...	Not scheduled
☐	splunk-deployment.ccctechcenter.c	California Community C...	Not scheduled
☐	splunk-search.ccctechcenter.org	California Community C...	Scheduled
☐	checkmarx.ccctechcenter.org	California Community C...	Scheduled
☐	splunk-search.ccctechcenter.org	California Community C...	Scheduled
☐	checkmarx.ccctechcenter.org	California Community C...	Not scheduled
☐	openvpn-hubtools.ccctechcenter.o	California Community C...	Scheduled
☐	splunk.ccctechcenter.org	California Community C...	Scheduled
☐	openvpn-mypath-tools-test.ccctech	California Community C...	Scheduled
☐	gp.ccctechcenter.org	California Community C...	Not scheduled
☐	cccvpn.ccctechcenter.org	California Community C...	Not scheduled
☐	cccvpn.ccctechcenter.org	California Community C...	Scheduled
☐	gp.ccctechcenter.org	California Community C...	Scheduled
☐	openvpn-mypath-ops.ccctechcente	California Community C...	Scheduled
☐	openvpn-database-nonprod.ccctec	California Community C...	Scheduled

Dashboard

Certificates ∧

SSL Certificates

Code Signing Certificates

Discovery ∨

Domains

Organizations

Reports

Enrollment ∨

Integrations ∨

Settings ∨

About

Page 1   Rows per page 25   1-25 of 88

Additional Resources

❑ Sectigo Certificate Manager Guide: https://docs.sectigo.com/scm/scm-guides/1/scm-admin-guides/_attachments/Sectigo_Certificate_Manager_Administrator_Guide_V21.11_November_2021.pdf

❑ Sectigo Rest API reference; https://sectigo.com/knowledge-base/detail/Sectigo-Certificate-Manager-SCM-REST-API/kA01N000000XDkE

❑ InCommon Documentation; https://spaces.at.internet2.edu/display/ICCS/Documentation

❑ InCommon Certificate Service FAQ; https://spaces.at.internet2.edu/display/ICCS/InCommon+Cert+Service+FAQ

❑ InCommon Code Signing Certificates; https://spaces.at.internet2.edu/download/attachments/141820811/InCommon_CM_Code_Signing_Certificate_End_User_Guide.pdf?version=1&modificationDate=1547734802117&api=v2

❑ Obtaining seals; http://www.trustlogo.com/install

California Community Colleges

Benefits of InCommon membership

❑ Federation and single-sign on access across hundreds of EDU's

❑ Edu-Roam global roaming wireless access

❑ Trusted platform and Identity and Access Management

❑ Workshops, camps, software training, IAM webinars and collaboration

❑ A large, diverse community of education professionals

❑ For on-boarding contact our Enabling Services Program Manager; Warren Whitmore at (530) 332-8185 or wwhitmore@ccctechcenter.org

❑ Enabling Services can also be reached via e-mail: crms@ccctechcenter.org or our website: https://ccctechcenter.org/services

California Community Colleges

Thank you!

If you have questions or comments regarding this presentation, e-mail:
Omer Usmani ousmani@ccctechcenter.org for follow-up.

If you are having trouble with the InCommon interface or need additional
Certificate Manager Admin accounts at your institution, e-mail or call:
David Albrecht dalbrecht@ccctechcenter.org Cell: (530) 566-2367