InCommon® SSL Certificates

2022 Winter Workshop

David Albrecht
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
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
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
What types of certificates are available?

- Self-Signed

- Paid SSL
- Free SSL
What types of certificates are available?

- Self-Signed
- Let’s Encrypt
What types of certificates are available?

- Self-Signed
- Let’s Encrypt
- Comodo Elite
What types of certificates are available?

- Self-Signed
- Let's Encrypt
- Comodo Elite
- Single Domain
What types of certificates are available?

- Self-Signed
- Let’s Encrypt
- Comodo Elite
- Single Domain
- Multi-Domain
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
What types of certificates are available?

- Self-Signed
- Let’s Encrypt
- Comodo Elite
- Single Domain
- Multi-Domain
- Wildcard
- Code Signing
- Short Life
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)
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)
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)
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
<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Username</th>
<th>Type</th>
<th>Role</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patrick Plagens</td>
<td><a href="mailto:pplagens@sdcccd.edu">pplagens@sdcccd.edu</a></td>
<td><a href="mailto:pplagens@sdcccd.edu">pplagens@sdcccd.edu</a></td>
<td>Standard</td>
<td>DRAD Admin - SSL, DRAO</td>
<td>✔</td>
</tr>
<tr>
<td>Jon Ambrosia</td>
<td><a href="mailto:jambrosi@sdcccd.edu">jambrosi@sdcccd.edu</a></td>
<td><a href="mailto:jambrosi@sdcccd.edu">jambrosi@sdcccd.edu</a></td>
<td>Standard</td>
<td>DRAD Admin - SSL, DRAO</td>
<td>✔</td>
</tr>
<tr>
<td>David Albrecht</td>
<td><a href="mailto:albrecht@cccnext.net">albrecht@cccnext.net</a></td>
<td><a href="mailto:albrecht@cccnext.net">albrecht@cccnext.net</a></td>
<td>Standard</td>
<td>DRAD Admin - SSL, DRAO</td>
<td>✔</td>
</tr>
<tr>
<td>Larry Hsieh</td>
<td><a href="mailto:lhsieh@ivc.edu">lhsieh@ivc.edu</a></td>
<td><a href="mailto:lhsieh@ivc.edu">lhsieh@ivc.edu</a></td>
<td>Standard</td>
<td>DRAD Admin - SSL, DRAO</td>
<td>✔</td>
</tr>
<tr>
<td>Robert Ford</td>
<td><a href="mailto:rford@ivc.edu">rford@ivc.edu</a></td>
<td><a href="mailto:rford@ivc.edu">rford@ivc.edu</a></td>
<td>Standard</td>
<td>DRAD Admin - SSL, DRAO</td>
<td>✔</td>
</tr>
<tr>
<td>Kevin Quinn</td>
<td><a href="mailto:kquinn@soccccd.edu">kquinn@soccccd.edu</a></td>
<td><a href="mailto:kquinn@soccccd.edu">kquinn@soccccd.edu</a></td>
<td>Standard</td>
<td>DRAD Admin - SSL, DRAO</td>
<td>✔</td>
</tr>
<tr>
<td>Hsiawen Hull</td>
<td><a href="mailto:hsiawen.huil@canyons.edu">hsiawen.huil@canyons.edu</a></td>
<td><a href="mailto:hsiawen.huil@canyons.edu">hsiawen.huil@canyons.edu</a></td>
<td>Standard</td>
<td>DRAD Admin - SSL, DRAO</td>
<td>✔</td>
</tr>
<tr>
<td>Kevin Du</td>
<td><a href="mailto:kdu13@saddleback.edu">kdu13@saddleback.edu</a></td>
<td><a href="mailto:kdu13@saddleback.edu">kdu13@saddleback.edu</a></td>
<td>Standard</td>
<td>DRAD Admin - SSL, DRAO</td>
<td>✔</td>
</tr>
<tr>
<td>Hai Nguyen</td>
<td><a href="mailto:hnguyen@fullcoll.edu">hnguyen@fullcoll.edu</a></td>
<td><a href="mailto:hnguyen@fullcoll.edu">hnguyen@fullcoll.edu</a></td>
<td>Standard</td>
<td>DRAD Admin - SSL, DRAO</td>
<td>✔</td>
</tr>
<tr>
<td>Michael Cortez</td>
<td><a href="mailto:mcortez@fullcoll.edu">mcortez@fullcoll.edu</a></td>
<td><a href="mailto:mcortez@fullcoll.edu">mcortez@fullcoll.edu</a></td>
<td>Standard</td>
<td>DRAD Admin - SSL, DRAO</td>
<td>✔</td>
</tr>
<tr>
<td>Name</td>
<td>Status</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ccassess.org</td>
<td>EXPIRED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cccoo.edu</td>
<td>VALIDATED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cccoo.net</td>
<td>EXPIRED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cccd.edu</td>
<td>VALIDATED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cccedplan.org</td>
<td>EXPIRED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ccchelp.info</td>
<td>EXPIRED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cccmypath.org</td>
<td>EXPIRED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ccnext.net</td>
<td>VALIDATED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ccnext.org</td>
<td>ACTION REQUIRED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ccc-ac.org</td>
<td>EXPIRED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cccsecuritycenter.org</td>
<td>EXPIRED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cccsurvey.org</td>
<td>EXPIRED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ccctechnetwork</td>
<td>EXPIRED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cctechcenter.org</td>
<td>VALIDATED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cctechedge.org</td>
<td>EXPIRED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cctechology.info</td>
<td>EXPIRED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cctechplan.org</td>
<td>VALIDATED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ccsf.edu</td>
<td>EXPIRED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cernitoscollege.us</td>
<td>EXPIRED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cernitos.edu</td>
<td>VALIDATED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cernroocoaso.edu</td>
<td>VALIDATED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chaffey.edu</td>
<td>VALIDATED</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total: 479
<table>
<thead>
<tr>
<th>COMMON NAME</th>
<th>DEPARTMENT</th>
<th>RENEWAL STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>splunk.ccctechcenter.org</td>
<td>California Community C...</td>
<td>Not scheduled</td>
</tr>
<tr>
<td>splunk-utility.ccctechcenter.org</td>
<td>California Community C...</td>
<td>Not scheduled</td>
</tr>
<tr>
<td>splunk-indexes.ccctechcenter.org</td>
<td>California Community C...</td>
<td>Not scheduled</td>
</tr>
<tr>
<td>splunk-deployment.ccctechcenter.org</td>
<td>California Community C...</td>
<td>Not scheduled</td>
</tr>
<tr>
<td>splunk-search.ccctechcenter.org</td>
<td>California Community C...</td>
<td>Scheduled</td>
</tr>
<tr>
<td>checkmarx.ccctechcenter.org</td>
<td>California Community C...</td>
<td>Scheduled</td>
</tr>
<tr>
<td>splunk-search.ccctechcenter.org</td>
<td>California Community C...</td>
<td>Scheduled</td>
</tr>
<tr>
<td>checkmarx.ccctechcenter.org</td>
<td>California Community C...</td>
<td>Not scheduled</td>
</tr>
<tr>
<td>openvpn-hubs.ccctechcenter.org</td>
<td>California Community C...</td>
<td>Scheduled</td>
</tr>
<tr>
<td>splunk.ccctechcenter.org</td>
<td>California Community C...</td>
<td>Scheduled</td>
</tr>
<tr>
<td>openvpn-mpath-tools-fast.ccctech</td>
<td>California Community C...</td>
<td>Scheduled</td>
</tr>
<tr>
<td>gp.ccctechcenter.org</td>
<td>California Community C...</td>
<td>Not scheduled</td>
</tr>
<tr>
<td>ccppri.ccctechcenter.org</td>
<td>California Community C...</td>
<td>Not scheduled</td>
</tr>
<tr>
<td>ccppri.ccctechcenter.org</td>
<td>California Community C...</td>
<td>Not scheduled</td>
</tr>
<tr>
<td>gp.ccctechcenter.org</td>
<td>California Community C...</td>
<td>Scheduled</td>
</tr>
<tr>
<td>openvpn-mpath-ops.ccctechcenter</td>
<td>California Community C...</td>
<td>Scheduled</td>
</tr>
<tr>
<td>openvpn-database-nonprod.ccctech</td>
<td>California Community C...</td>
<td>Scheduled</td>
</tr>
</tbody>
</table>
**Additional Resources**

- Sectigo Certificate Manager Guide:  

- Sectigo Rest API reference;  

- InCommon Documentation;  
  [https://spaces.at.internet2.edu/display/ICCS/Documentation](https://spaces.at.internet2.edu/display/ICCS/Documentation)

- InCommon Certificate Service FAQ;  
  [https://spaces.at.internet2.edu/display/ICCS/InCommon+Cert+Service+FAQ](https://spaces.at.internet2.edu/display/ICCS/InCommon+Cert+Service+FAQ)

- InCommon Code Signing Certificates;  

- Obtaining seals;  
  [http://www.trustlogo.com/install](http://www.trustlogo.com/install)
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
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