Managing Enterprise Cybersecurity
MIS 4596

Unit #10

Agenda

- Public Key Infrastructure
- Digital Certificate
- Public key Certificates
- Roles in PKI: Certificate Authority (CA)
- Roles in PKI: Registration Authority (RA)
- PKI Steps
- Chain of Trust
- Root Programs
- Certificate Revocation List (CRL)
- PKI Roles / Workflows…

Public Key Infrastructure (PKI)

Public key cryptography enables entities previously unknown to each other to verify the identity of each other, validate the information being transferred, and securely communicate on an insecure public network

- **Public key infrastructure**
  - Enables online activities requiring more trust and proof of identity than simple passwords
  - Provides a hierarchy of trust relationships that:
    - Enable knowing a public key really belongs to the person/system you want to communicate with
    - Are necessary for hybrid cryptography
    - Facilitate secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email

Public Key Infrastructure (PKI)

Is a system for creating, storing, distributing, validating, revoking and managing **digital certificates** used to verify the identity the owner of a public key contained within the certificate

- Assumes
  - Receiver's and Sender's identities can be positively ensured through digital certificates
  - Asymmetric algorithm will automatically carry out the process of key exchange
- Contains components that
  - Identify users
  - Creates and distributes certificates
  - Maintains and revokes certificates
  - Distributes and maintains encryption keys
  - Enables information technologies to communicate and work together to achieve confidentiality, authentication, integrity, and non-repudiation

Public Key Infrastructure (PKI)

Consists of:

- **Public key certificates (“digital certificates”)** are electronic documents used to prove the ownership of public keys
- ***Roles***
  - ***Certificate Authorities*** (CA) store, issue and sign the digital certificates
  - ***Registration Authorities*** (RA) verify identities of entities requesting their digital certificates be stored at the CA
- ***Technologies***
  - ***Central directory*** provides a secure location in which keys are stored and indexed
  - ***Certificate management system***
    - Creates and delivers new certificates to be issued
    - Searches, retrieves and accesses to stored certificates
- ***Certificate policy*** states procedures for allowing outsiders to analyze the PKI's trustworthiness

Digital Certificate

One of the most important pieces of a PKI

- Associates a public key with information for uniquely identifying its owner

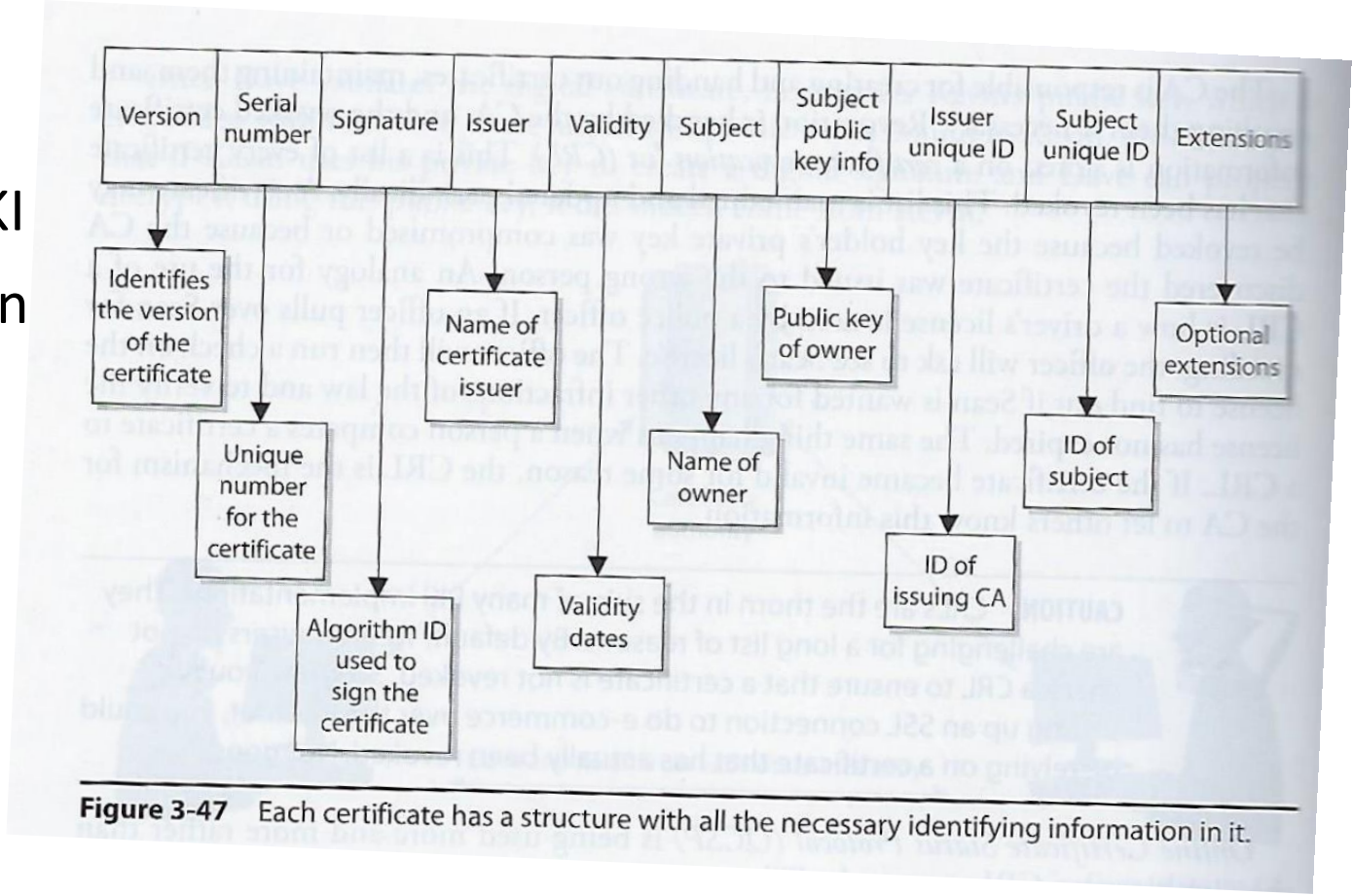


Figure 3-47 Each certificate has a structure with all the necessary identifying information in it.

- X.509 standard defines the format of public key certificates used in many Internet cryptographic protocols for HTTPS for servers & clients, secure email, code signing, digital signatures…

Public Key Certificate

Electronic documents used to prove ownership of a public key

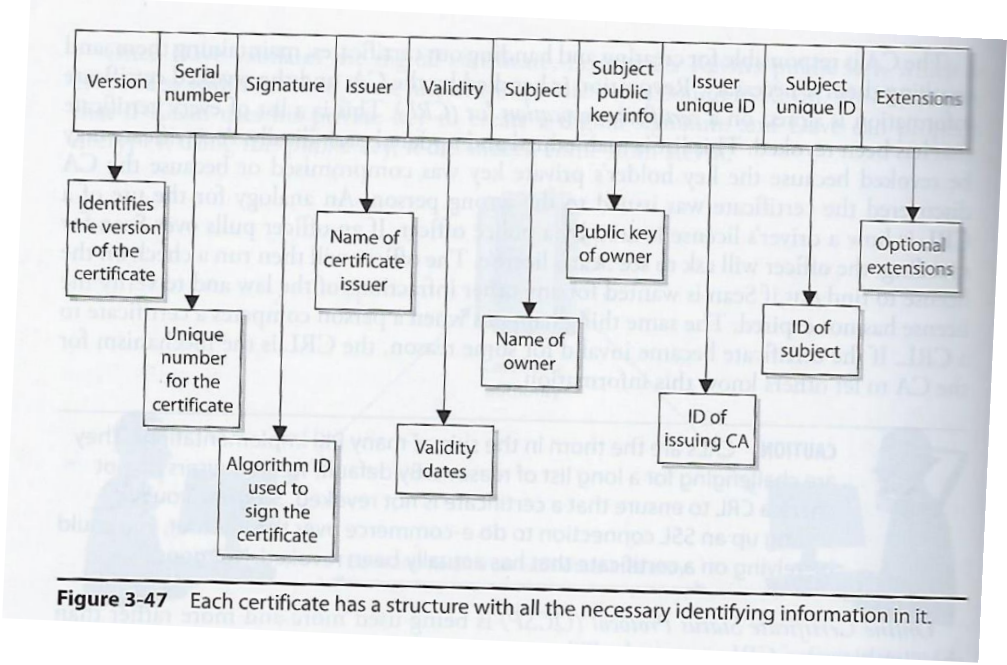


Figure 3-47 Each certificate has a structure with all the necessary identifying information in it.

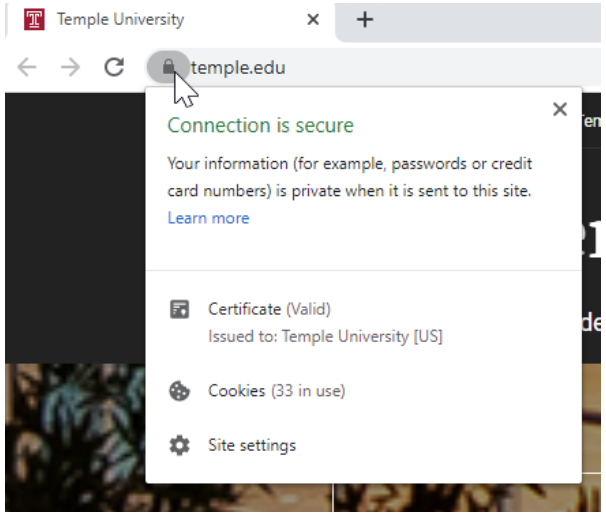
A certificate includes the following common fields:

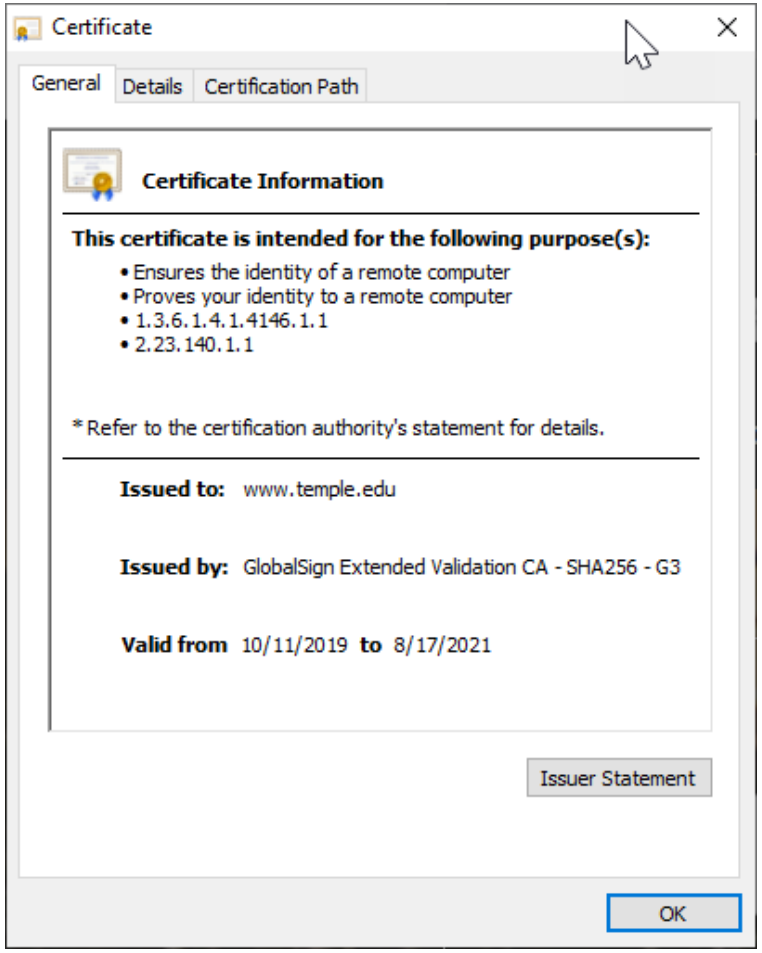
- Information about the certificate
  - **Serial Number:** Used to uniquely identify the certificate
  - **Issuer:** Entity that verified the information and signed the certificate
  - **Signature Algorithm**: The algorithm used to sign the public key certificate
  - **Signature**: A signature of the certificate body by the issuer's private key

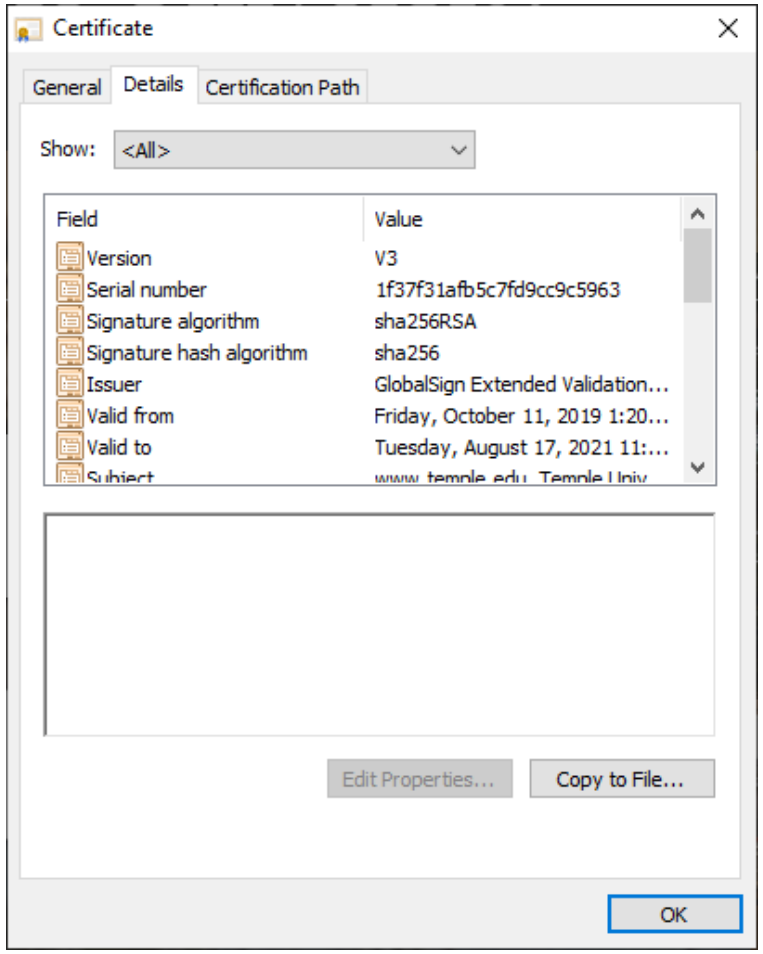
- Information about the public key
  - **Not Before**: Earliest time and date on which the certificate is valid.
  - **Not After**: Time and date past which the certificate is no longer valid
  - **Key Usage**: Valid cryptographic uses of the certificate's public key, e.g. digital signature validation, key encipherment, and certificate signing
  - **Extended Key Usage**: Applications the certificate may be used for, e.g. TLS server authentication, email protection, code signing, or electronic signature

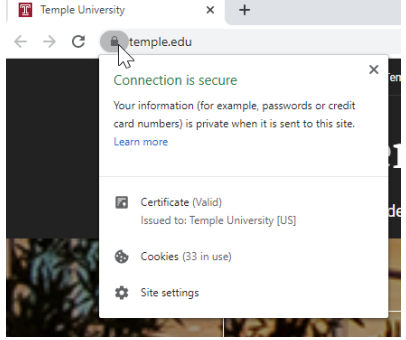
- Information about the identity of its owner (called the subject)
  - **Subject: E**ntity a certificate belongs to, e.g. individual, machine, or organization

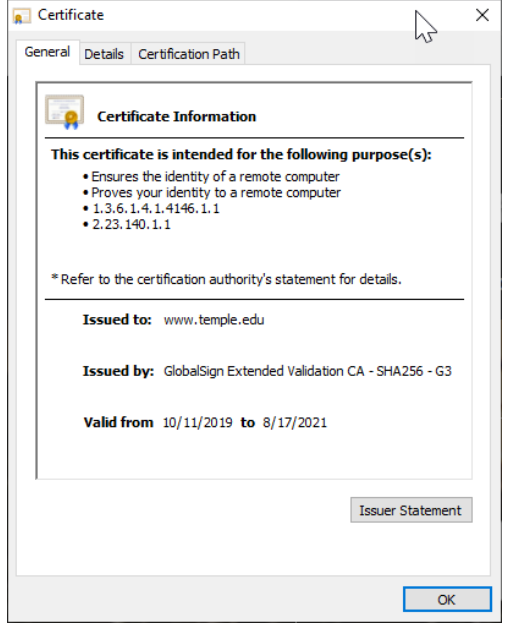
Certificate

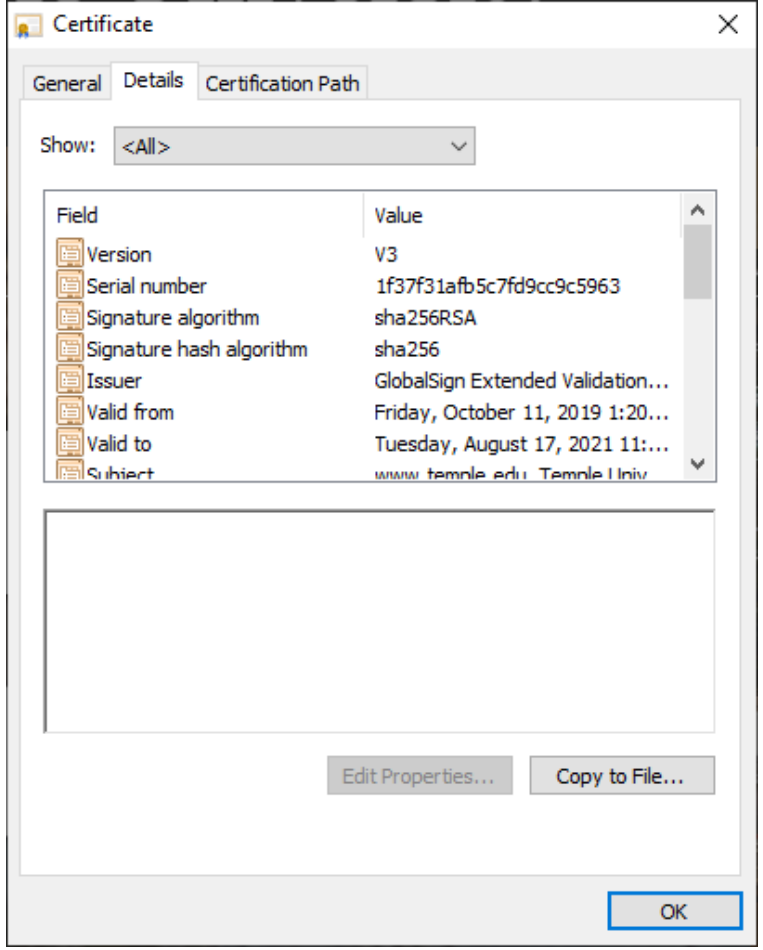


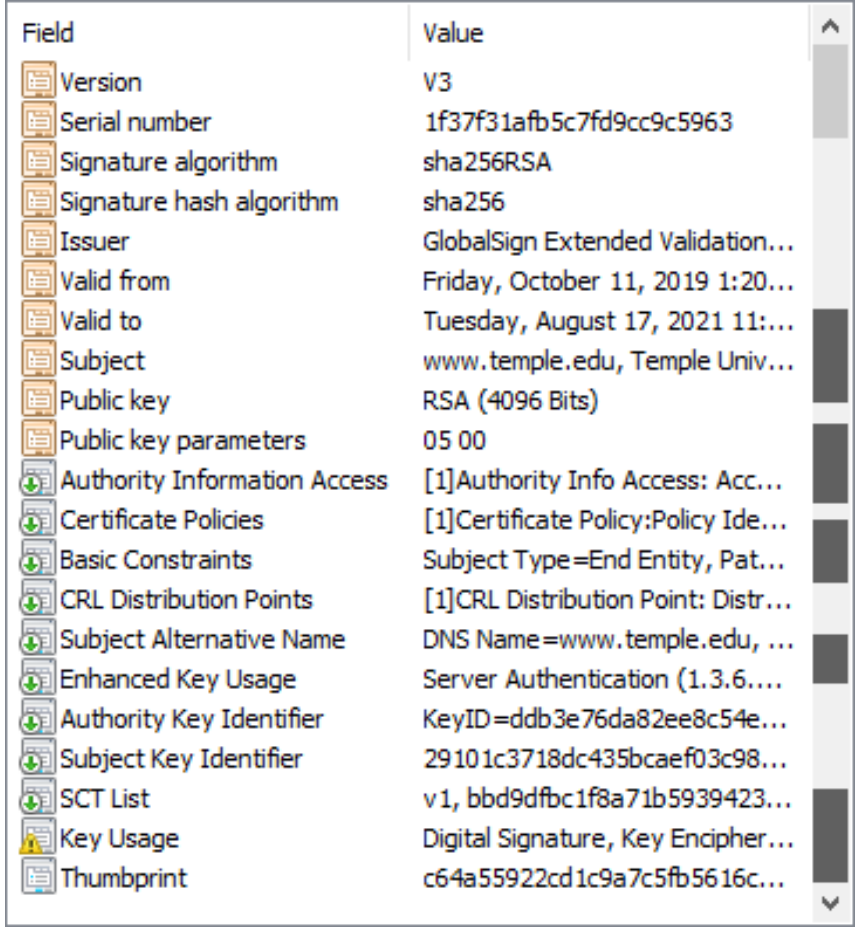


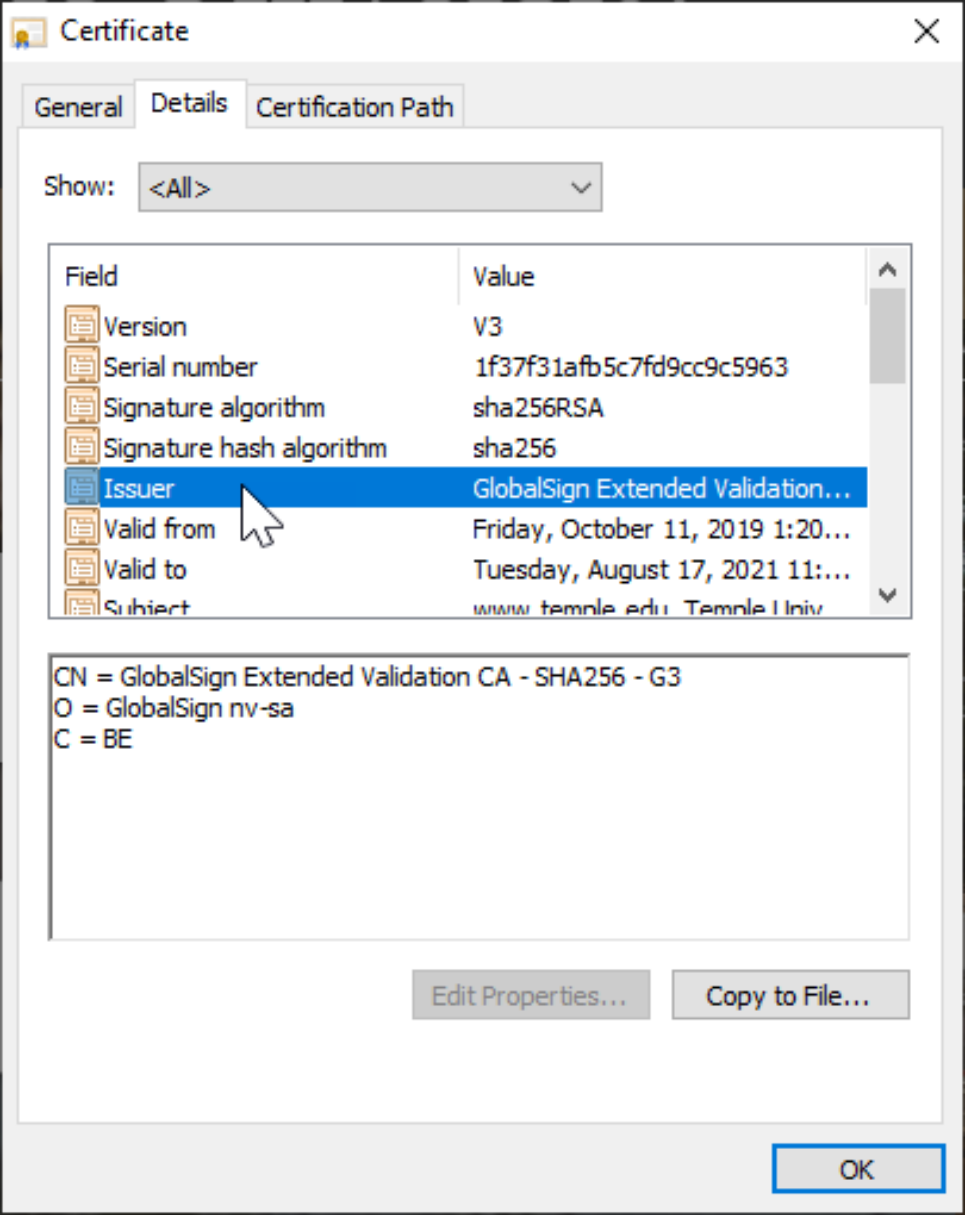


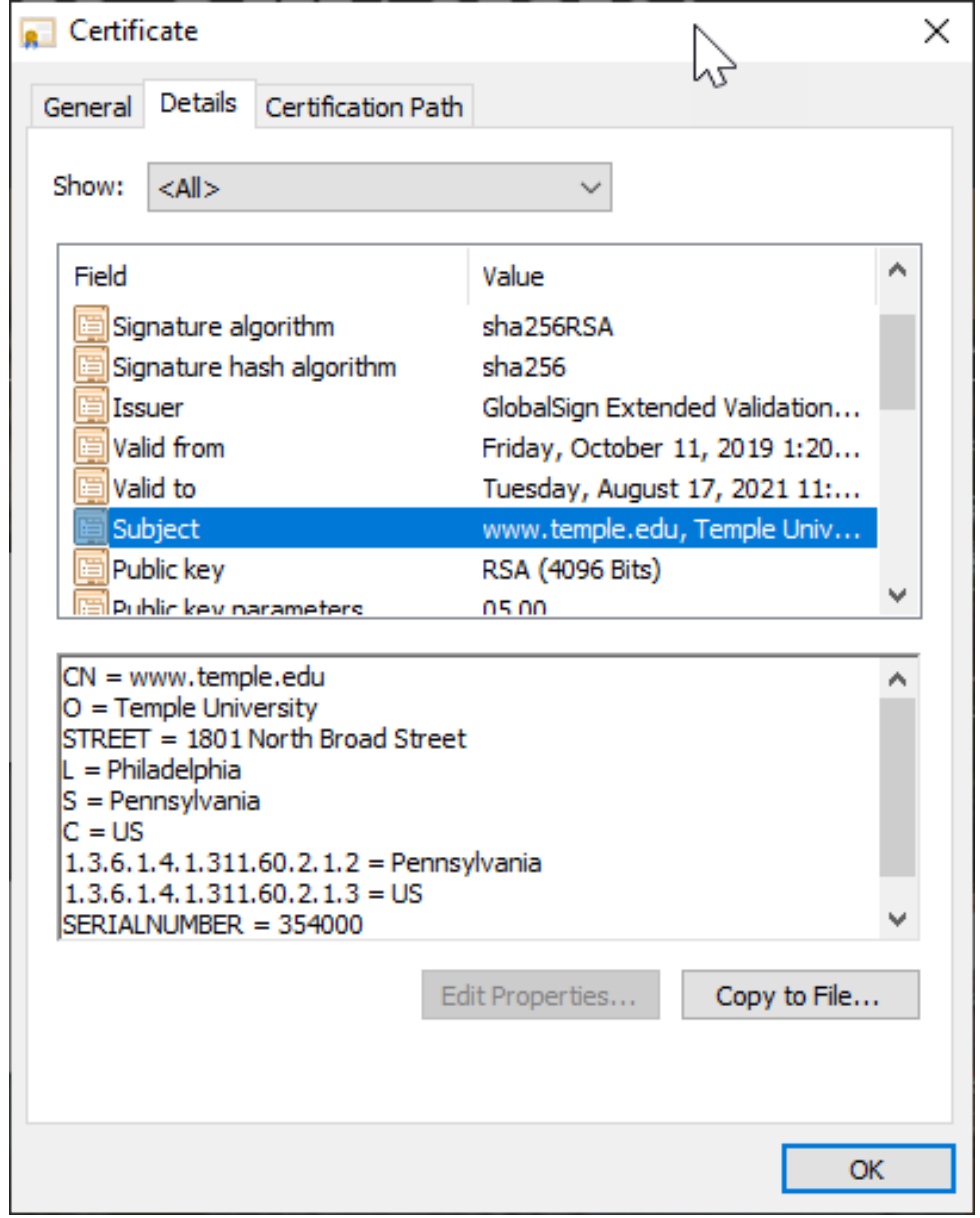

Temple University
temple.edu
Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site.
Learn more
Certificate (Valid)
Issued to: Temple University [US]
Cookies (33 in use)
Site settings

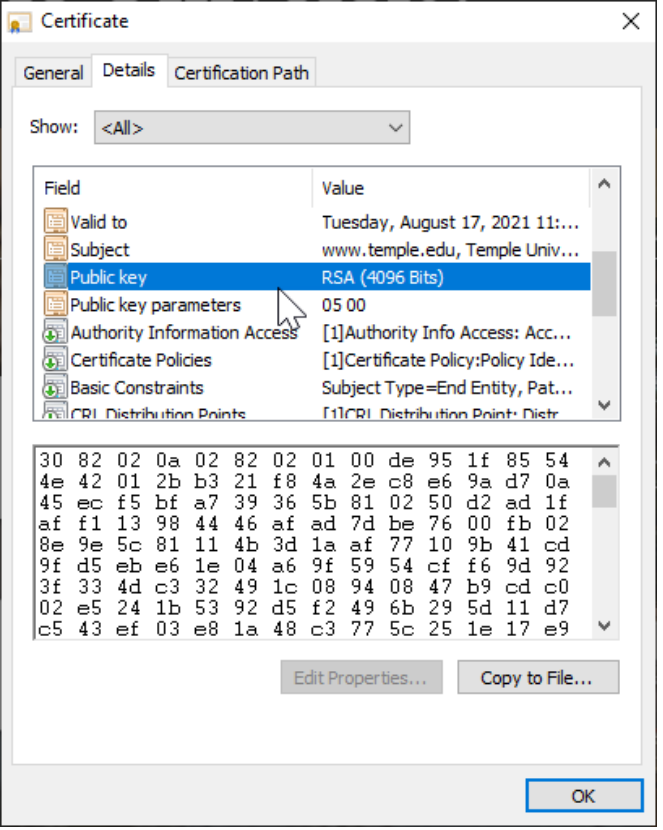

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Proves your identity to a remote computer
• 1.3.6.1.4.1.4146.1.1
• 2.23.140.1.1
* Refer to the certification authority's statement for details.
Issued to: www.temple.edu
Issued by: GlobalSign Extended Validation CA - SHA256 - G3
Valid from 10/11/2019 to 8/17/2021
Issuer Statement
OK


Certificate
General
Details
Certification Path
Show: <All>
Field
Value
Version V3
Serial number 1f37f31afb5c7fd9cc9c5963
Signature algorithm sha256RSA
Signature hash algorithm sha256
Issuer GlobalSign Extended Validation...
Valid from Friday, October 11, 2019 1:20...
Valid to Tuesday, August 17, 2021 11:...
Edit Properties...
Copy to File...
OK


Field
Value
Version V3
Serial number 1f37f31afb5c7fd9cc9c5963
Signature algorithm sha256RSA
Signature hash algorithm sha256
Issuer GlobalSign Extended Validation...
Valid from Friday, October 11, 2019 1:20...
Valid to Tuesday, August 17, 2021 11:...
Subject www.temple.edu, Temple Univ...
Public key RSA (4096 Bits)
Public key parameters 05 00
Authority Information Access [1]Authority Info Access: Acc...
Certificate Policies [1]Certificate Policy:Policy Ide...
Basic Constraints Subject Type=End Entity, Pat...
CRL Distribution Points [1]CRL Distribution Point: Distr...
Subject Alternative Name DNS Name=www.temple.edu, ...
Enhanced Key Usage Server Authentication (1.3.6....
Authority Key Identifier KeyID=ddb3e76da82ee8c54e...
Subject Key Identifier 29101c3718dc435bcaef03c98...
SCT List v1, bbd9dfbc1f8a71b5939423...
Key Usage Digital Signature, Key Encipher...
Thumbprint c64a55922cd1c9a7c5fb5616c...


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
1f37f31afb5c7fd9cc9c5963
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
GlobalSign Extended Validation...
Valid from
Friday, October 11, 2019 1:20...
Valid to
Tuesday, August 17, 2021 11:...
CN = GlobalSign Extended Validation CA - SHA256 - G3
O = GlobalSign nv-sa
C = BE
Edit Properties...
Copy to File...
OK


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Signature algorithm
sha256RSA
Signature hash algorithm
sha256
Issuer
GlobalSign Extended Validation...
Valid from
Friday, October 11, 2019 1:20...
Valid to
Tuesday, August 17, 2021 11:...
Subject
www.temple.edu, Temple Univ...
Public key
RSA (4096 Bits)
CN = www.temple.edu
O = Temple University
STREET = 1801 North Broad Street
L = Philadelphia
S = Pennsylvania
C = US
1.3.6.1.4.1.311.60.2.1.2 = Pennsylvania
1.3.6.1.4.1.311.60.2.1.3 = US
SERIALNUMBER = 354000
Edit Properties...
Copy to File...
OK



VIEW

Text

```
30 82 02 0a 02 82 02 01 00 de 95 1f 85 54 4e 42 01 2b b3
21 f8 4a 2e c8 e6 9a d7 0a 45 ec f5 bf a7 39 36 5b 81 02
50 d2 ad 1f af f1 13 98 44 46 af ad 7d be 76 00 fb 02 8e
9e 5c 81 11 4b 3d 1a af 77 10 9b 41 cd 9f d5 eb e6 1e 04
a6 9f 59 54 cf f6 9d 92 3f 33 4d c3 32 49 1c 08 94 08 47
b9 cd c0 02 e5 24 1b 53 92 d5 f2 49 6b 29 5d 11 d7 c5 43
ef 03 e8 1a 48 c3 77 5c 25 1e 17 e9 96 8b 1f c8 05 7f 64
3e 82 a6 b0 30 37 18 c1 ab 6c 1e 50 c4 9d dc 7d df 51 7c
81 86 f0 e5 94 bb ef b9 04 5b dd 0a 63 ec b9 94 0e b1 c3
92 8a a7 92 ea b1 96 4f 89 c1 58 38 34 71 cf 48 10 29 f0
af e4 c3 a7 e0 dd e9 f3 28 98 06 35 96 c7 37 38 cf ef c8
a7 b9 74 ff 48 e7 f2 2d 52 a2 9f 96 b0 b0 ce 15 a8 ab 7b
72 96 3b 3e bb ee 5e af d4 bd ce 78 09 7c fb 56 c9 19 d8
ca 0c f4 4b 91 93 ed 68 ca 5d 19 00 31 9f e9 38 ad 06 bd
b7 dc 83 82 1e c9 fd 4f 24 40 c8 23 55 48 ac 47 87 8e 95
6c 32 8e cd 99 c2 fa 0c 94 67 ee 16 e4 68 23 a6 a3 d7 ac
4f 03 bd b0 5b a6 6a 4e c3 a8 b3 90 8b a9 07 49 ee 9c 85
6f 61 62 2a 13 f9 95 73 ae f0 45 50 62 2b 55 bb 75 2d 76
c5 64 d7 d3 ad 2f 65 1c 78 b8 79 5e fe b8 74 b7 f8 b2 d9
1e 32 4f f5 fe f9 6e c4 27 37 cc be 09 ec f5 5f 87 68 76
4d a3 d7 b9 99 e4 c5 ec ad d4 05 4a 9f 41 b6 72 dd 2a 53
d8 e6 ec a6 59 cf 79 7e a2 05 36 b6 fa 59 cf 09 04 d1 10
4c 29 3c 44 c7 ca 86 06 17 bb d2 5e bf 0d 66 39 f2 6c 4f
2e c0 83 f5 83 c3 67 76 61 eb ab aa ab c1 43 ca 7a c0 3e
3b 02 91 38 64 78 ab b0 54 ca b9 63 30 6b 8f e6 22 81 91
e1 a9 f6 3f db 1d a5 06 92 3c ce c9 d5 d0 48 b7 ab 0d 76
63 d3 52 7e 5a d9 fd 06 94 ae a8 8f c3 2d ff c9 56 75 2a
90 03 34 9e b6 81 86 a1 02 03 01 00 01
```

ENCODE DECODE

Numeral system

READ

- Binary (2)
- Octal (8)
- Decimal (10)
- Hexadecimal (16)
- Roman numerals

CONVERT TO

- Binary (2)
- Octal (8)
- Decimal (10)
- Hexadecimal (16)
- Roman numerals

→ Encoded 1865 chars

VIEW

Text

```
48 130 2 10 2 130 2 1 0 222 149 31 133 84 78 66 1 43 179
33 248 74 46 200 230 154 215 10 69 236 245 191 167 57 54
91 129 2 80 210 173 31 175 241 19 152 68 70 175 173 125
190 118 0 251 2 142 158 92 129 17 75 61 26 175 119 16
155 65 205 159 213 235 230 30 4 166 159 89 84 207 246
157 146 63 51 77 195 50 73 28 8 148 8 71 185 205 192 2
229 36 27 83 146 213 242 73 107 41 93 17 215 197 67 239
3 232 26 72 195 119 92 37 30 23 233 150 139 31 200 5 127
100 62 130 166 176 48 55 24 193 171 108 30 80 196 157
220 125 223 81 124 129 134 240 229 148 187 239 185 4 91
221 10 99 236 185 148 14 177 195 146 138 167 146 234 177
150 79 137 193 88 56 52 113 207 72 16 41 240 175 228 195
167 224 221 233 243 40 152 6 53 150 199 55 56 207 239
200 167 185 116 255 72 231 242 45 82 162 159 150 176 176
206 21 168 171 123 114 150 59 62 187 238 94 175 212 189
206 120 9 124 251 86 201 25 216 202 12 244 75 145 147
237 104 202 93 25 0 49 159 233 56 173 6 189 183 220 131
130 30 201 253 79 36 64 200 35 85 72 172 71 135 142 149
108 50 142 205 153 194 250 12 148 103 238 22 228 104 35
166 163 215 172 79 3 189 176 91 166 106 78 195 168 179
144 139 169 7 73 238 156 133 111 97 98 42 19 249 149 115
174 240 69 80 98 43 85 187 117 45 118 197 100 215 211
173 47 101 28 120 184 121 94 254 184 116 183 248 178 217
30 50 79 245 254 249 110 196 39 55 204 190 9 236 245 95
135 104 118 77 163 215 185 153 228 197 236 173 212 5 74
159 65 182 114 221 42 83 216 230 236 166 89 207 121 126
162 5 54 182 250 89 207 9 4 209 16 76 41 60 68 199 202
134 6 23 187 210 94 191 13 102 57 242 108 79 46 192 131
245 131 195 103 118 97 235 171 170 171 193 67 202 122
192 62 59 2 145 56 100 120 171 176 84 202 185 99 48 107
143 230 34 129 145 225 169 246 63 219 29 165 6 146 60
206 201 213 208 72 183 171 13 118 99 211 82 126 90 217
253 6 148 174 168 143 195 45 255 201 86 117 42 144 3 52
158 182 129 134 161 2 3 1 0 1
```

https://cryptii.com/

Types of Certificates: Different cryptographic protocols (“applications”)

X.509 is a standard of the International Telecommunications Union which defines the format of public key certificates used in many Internet cryptographic protocols, including:

1. **Transport Layer Security** (TLS/SSL) HTTPS protocol for securely browsing the web

   Certificate's subject is typically a computer or other device, but may also identify organizations or individuals

   - **Server certificate**
     - A server is required to present a certificate as part of the initial connection setup. A client connecting to that server will validate the certificate by checking that
       1. The certificate’s subject matches the hostname (i.e. domain name) to which the client is trying to connect
       2. The certificate is signed by a trusted certificate authority
   - **Client certificate** (less common than server certificates)
     - Used to authenticate the client connecting to a TLS service (e.g. for access control)
     - Most client certificates contain an email address or personal name rather than a hostname

2. **Email encryption certificate**
   - A certificate's subject is typically a person or organization
   - For secure email, senders use an email certificate to discover which public key to use for any given recipient

3. **Code signing certificate**
   - A code signing certificate is used to validate signatures on programs to ensure they were not tampered with during delivery

4. **Qualified digital certificate**
   - A “Qualified digital certificate” identifies an individual for electronic signature purposes

Roles in PKI - Certificate Authority (CA)

Serves as a trusted third party responsible for verifying identities and signing digital certificates of identity ("digital signature") which are exchanged between two parties introducing themselves to each other

Each person wanting to participate in a PKI requires a digital certificate

- Digital certificate is a credential containing the public key for that individual along with other identifying information

A CA is a trusted organization (or server) responsible for:

- Issuing (creating and handing) out digital certificates
- Maintaining digital certificates
- Revoking digital certificates

Use of PKI and exchanging digital certificates is intended to block Man-in-the-Middle attacks where 2 users are not working in PKI environment do not truly know the identity of the owners of public keys

Roles in PKI - Certificate Authority (CA)

Each person wanting to participate in a PKI requires a digital certificate

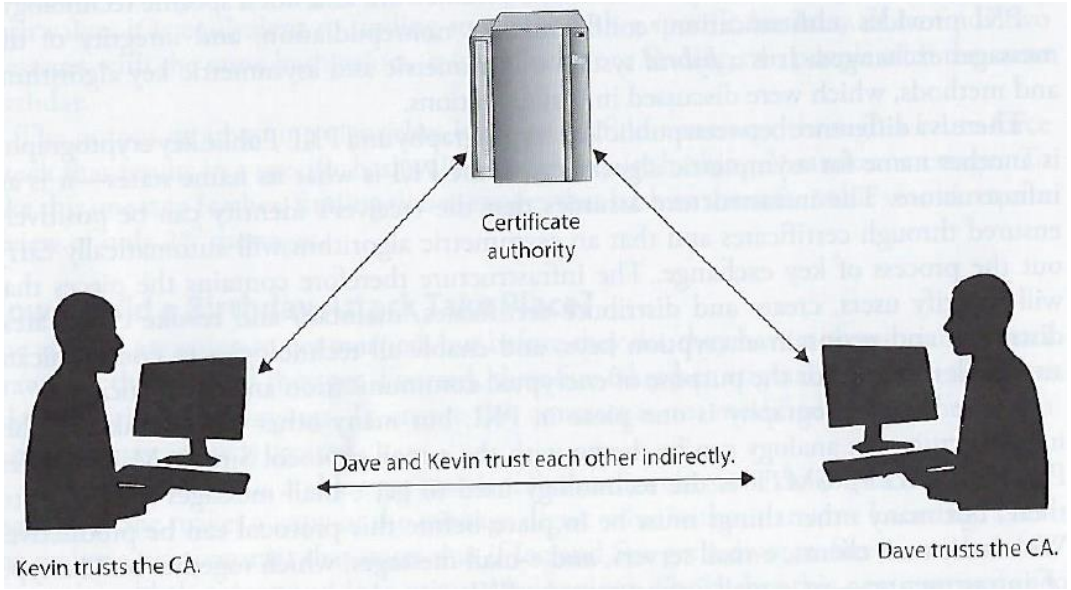
- Digital certificate is a credential containing the public key for that individual, computer or organization along with other identifying information

When a CA signs the certificate, it binds the individual's, computer's or organization' identity to the public key

- The CA takes liability for the authenticity of the identity
  - *Making a CA the "trusted 3rd party" that allows people who have never met to use their public keys to authenticate each other and communicate in a secure way*

Certificate Revocation Information

CA's are also responsible for maintaining up-to-date revocation information about certificates they have issued, indicating when certificates of identity are no longer valid

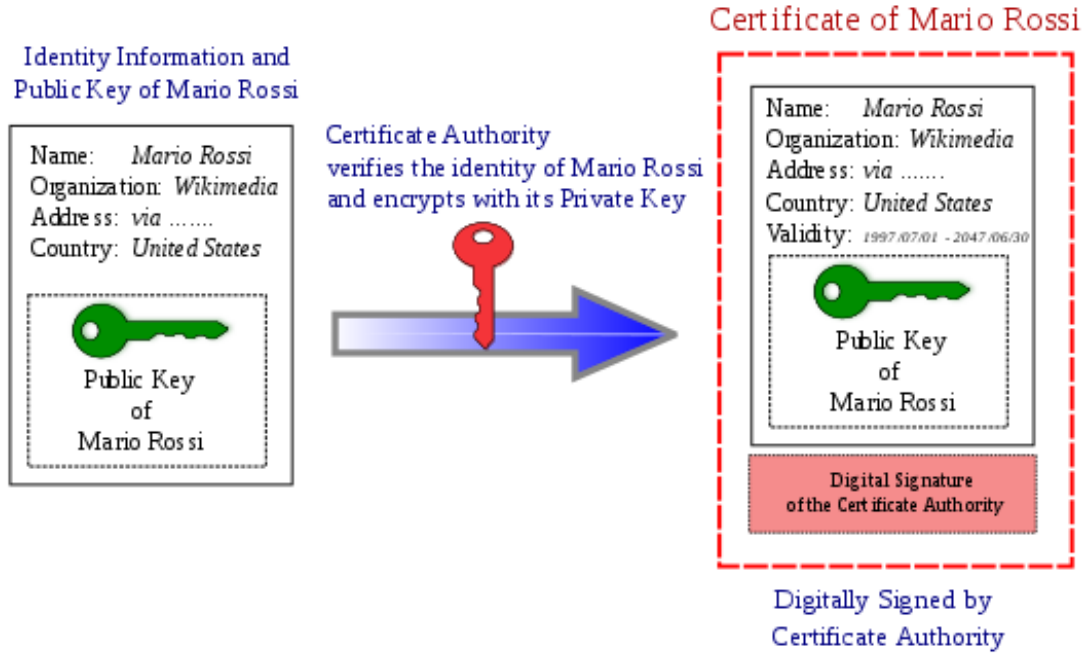


Roles in PKI – Certificate Authority (CA)

New Certificate Requests

A CA processes requests from people or organizations requesting certificates (called “subscribers”)

1. Verifies the subscriber’s information
2. Potentially signs an end-entity certificate based on the subscriber’s information



Registration Authority (RA)

When a user needs a new certificate, the user makes a request to the RA

RA serves as a broker between the user and the CA, and performs certain certification registration tasks

- Performs the certificate life-cycle management functions
- Establishes and confirms the identity of the individual
  - The RA verifies all the necessary identification information before allowing a request to go to the CA
- Initiates the certification process with the CA for the end user

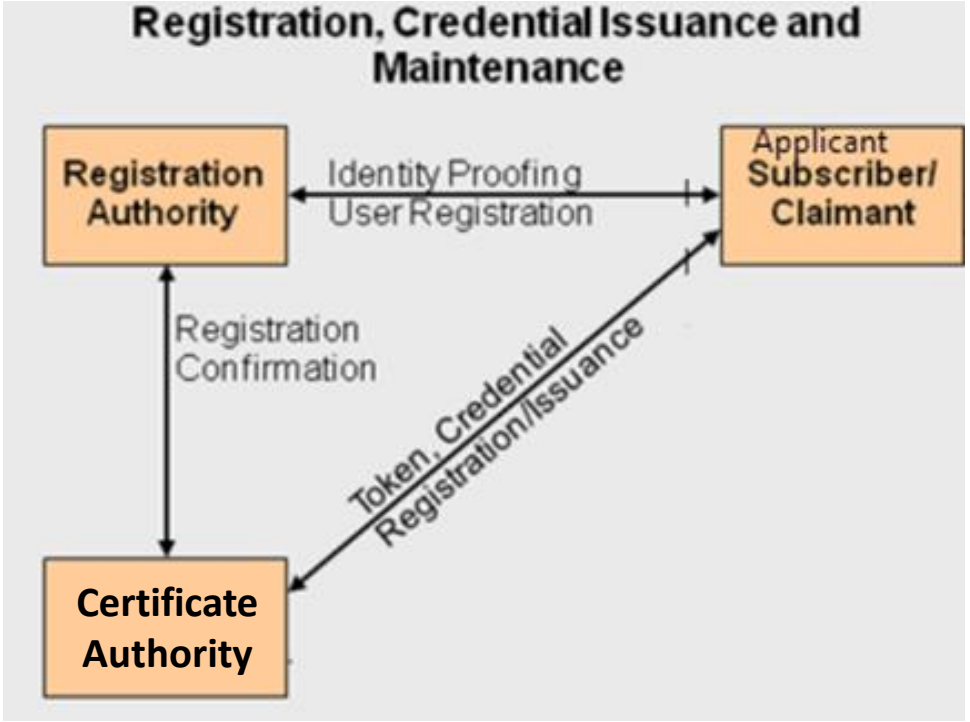
RA cannot issue certificates

PKI Steps

Suppose: John needs to obtain a digital certificate to participate in PKI

1. John requests a digital certificate from a RA
2. The RA requests John's identification information
   - E.g. driver's license, address, phone number, email, …
3. RA receives John's information, verifies it, and sends his certificate request to CA
4. CA creates a certificate with John's public key and embedded identity information
   - Private/Public key pair is generated on John's machine or by the CA (depends on system configuration)
     - Usually – user generates this pair and sends his public key in as part of registration process
     - If CA creates key pair, John's private key needs to be sent to him via secure means

Now John is registered and is able to participate in PKI

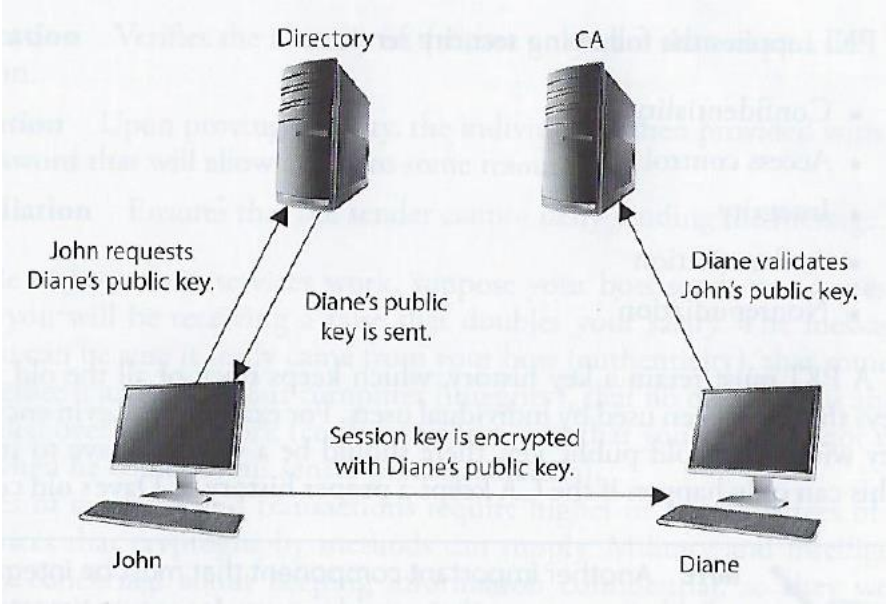


Token, Credential = Public Key

PKI Steps

John and Diane decide to communicate securely using PKI…

1. John requests Diane's public key form a public directory
2. The directory (a.k.a. repository) sends Diane's digital certificate
3. John verifies the digital certificate…
   - extracts her public key, uses the public key to encrypt a session key that will be used to encrypt their messages
   - John sends the encrypted session key to Diane
   - John also sends his certificate, containing his public key to Diane
4. Diane browser receives John's certificate, **looks to see if it trusts the CA** that digitally signed the certificate
   - Diane's browser trusts this CA
   - After verifying the certificate, both John and Diane can communicate using encryption

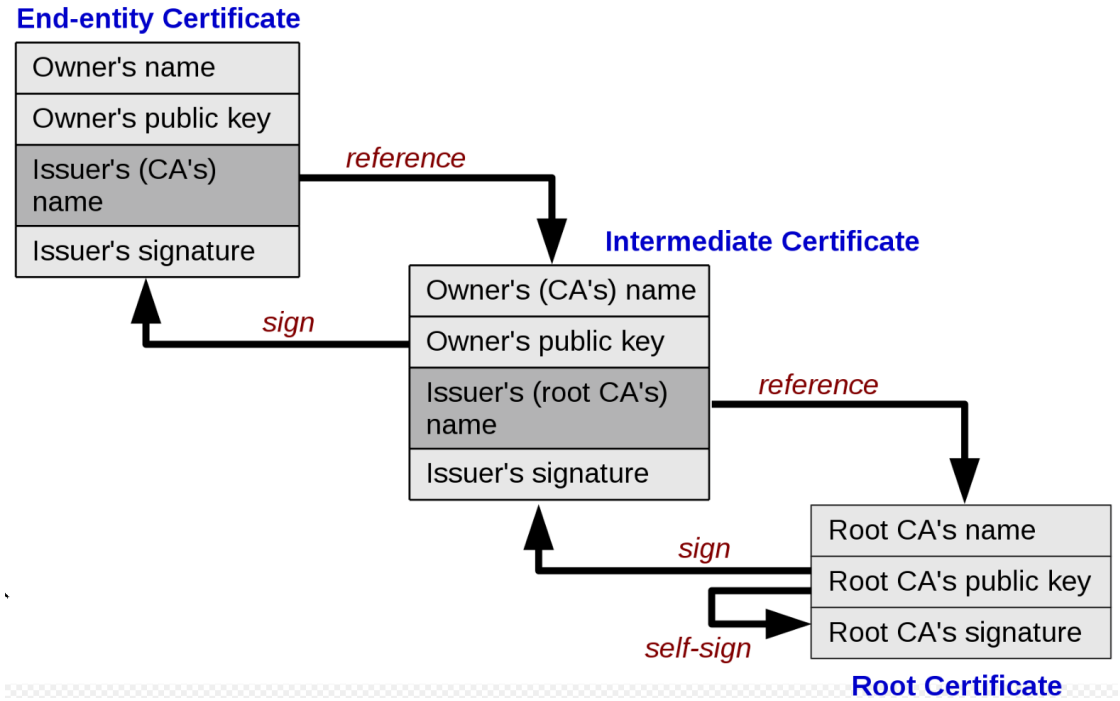


Types of certificates: Chain of trust

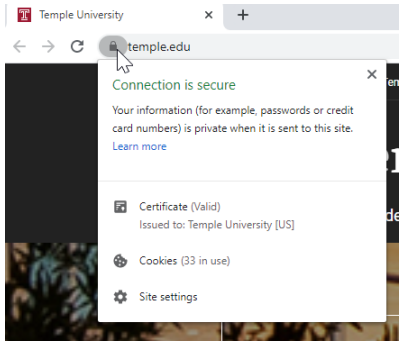
A PKI is often set up with multiple levels of CAs, for practical reasons:

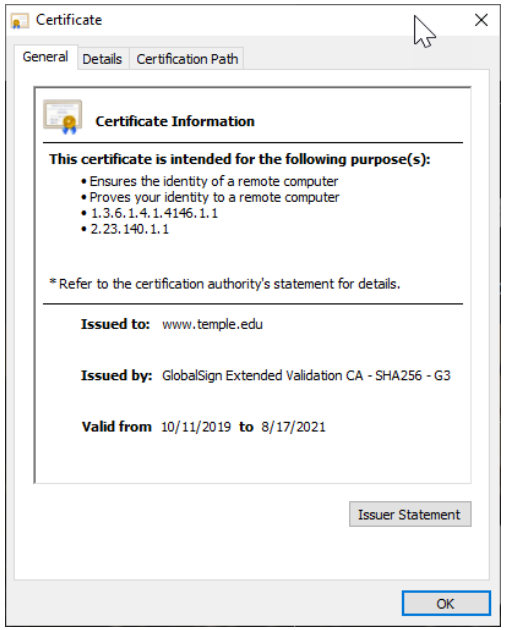
- There is a top-level CA, called the root, which issues certificates on the keys of lower-level CAs, which in turn certify the user keys
- The system of identity validation still behaves in the same way, but now Diane has to check two certificates to verify John's key

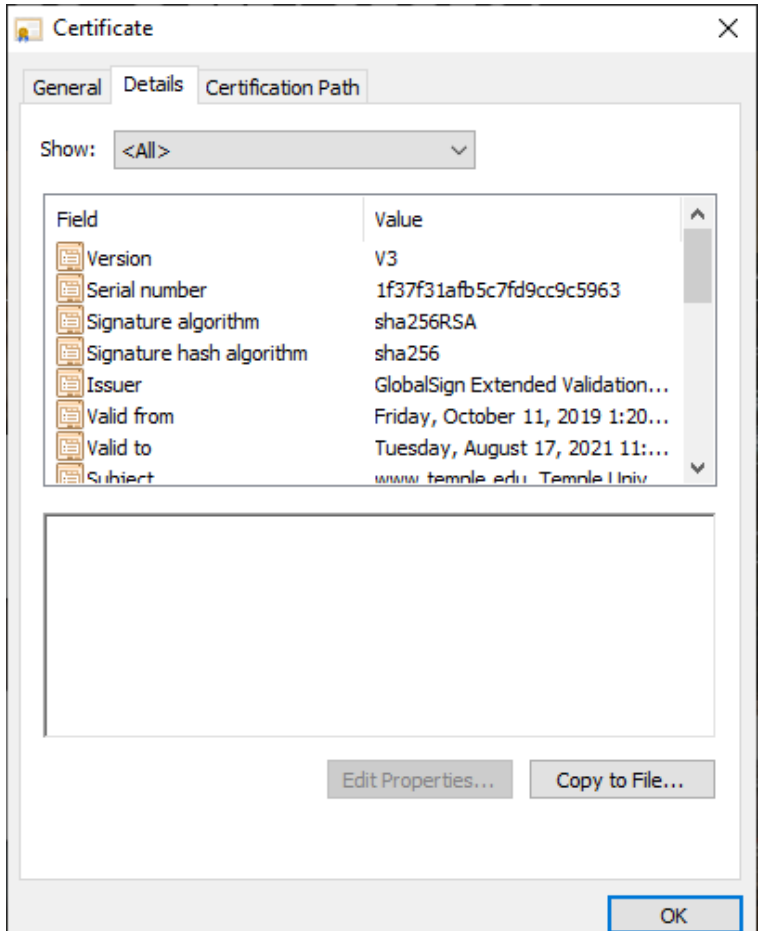
- **Root certificate**
  - Self-signed certificate used to sign other certificates
- **Intermediate certificate**
  - A certificate used to sign other certificates.
  - Must be signed by either a root certificate or another intermediate certificate
- **End-entity ("leaf") certificate**
  - Cannot be used to sign other certificates
  - Include:
    - TLS/SSL server and client certificates
    - Email certificates
    - Code signing certificates
    - Qualified certificates

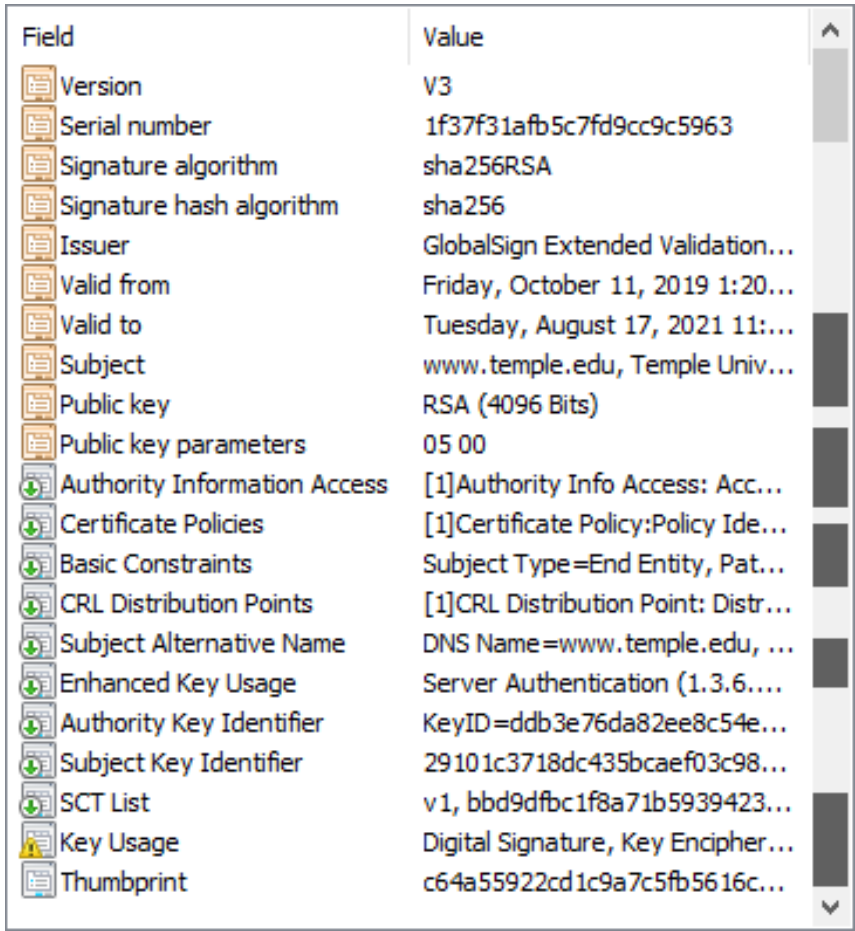


Recall… Temple.edu's certificate…

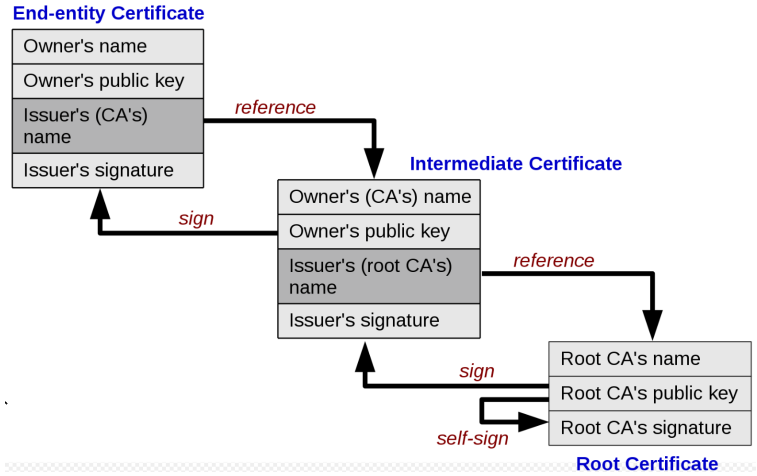


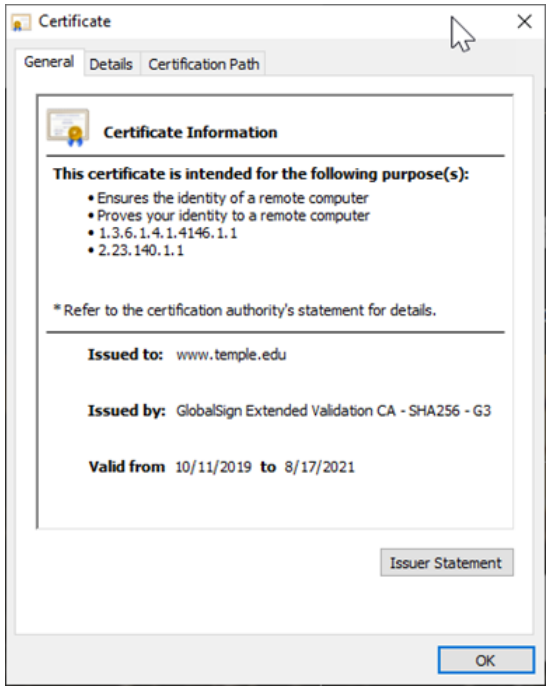


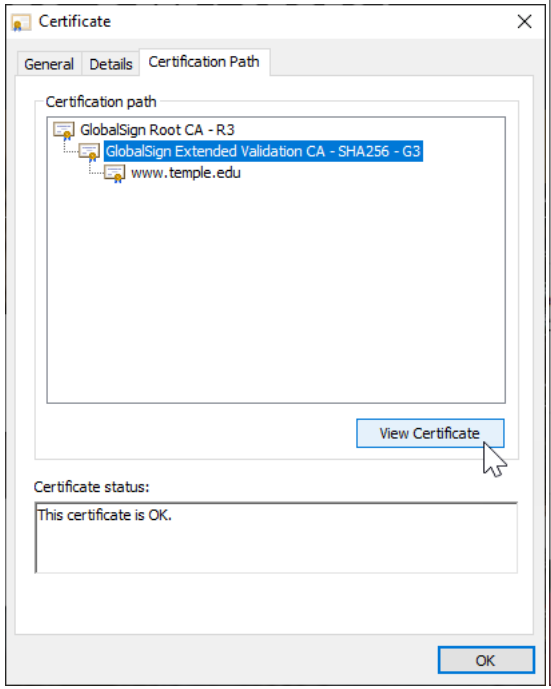


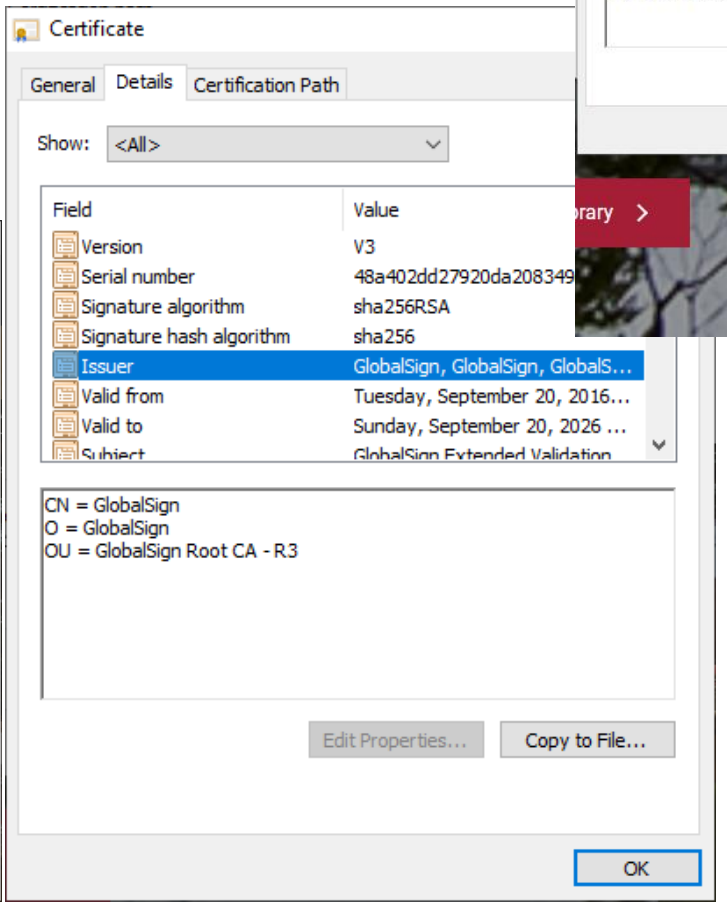


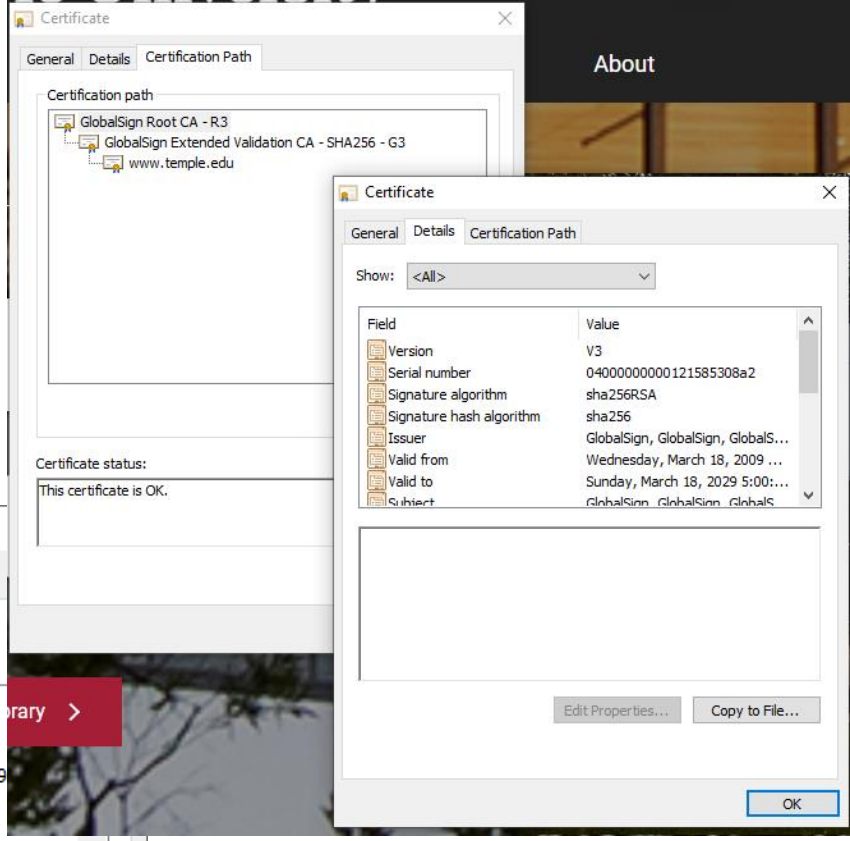
Types of certificates: Chain of trust



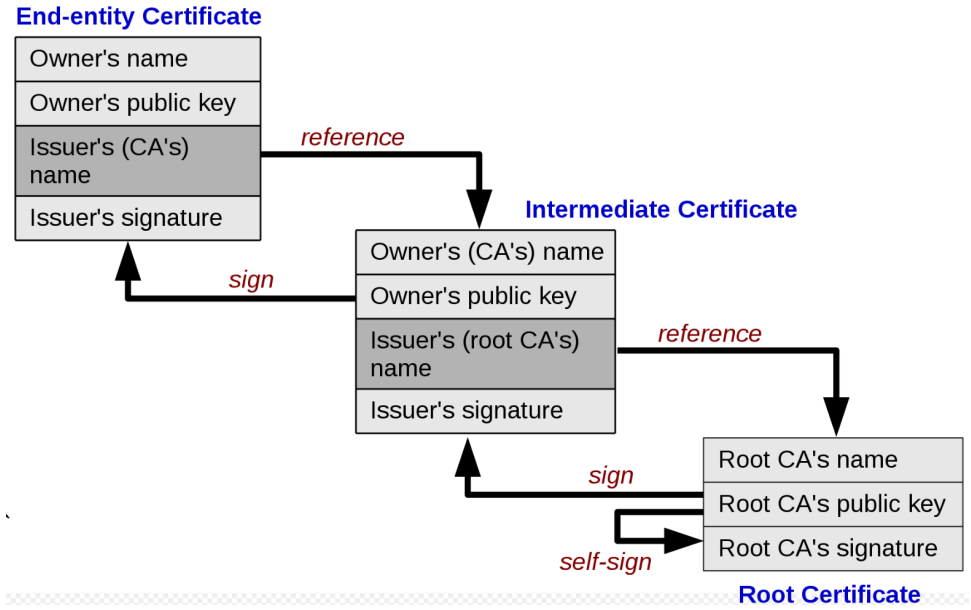


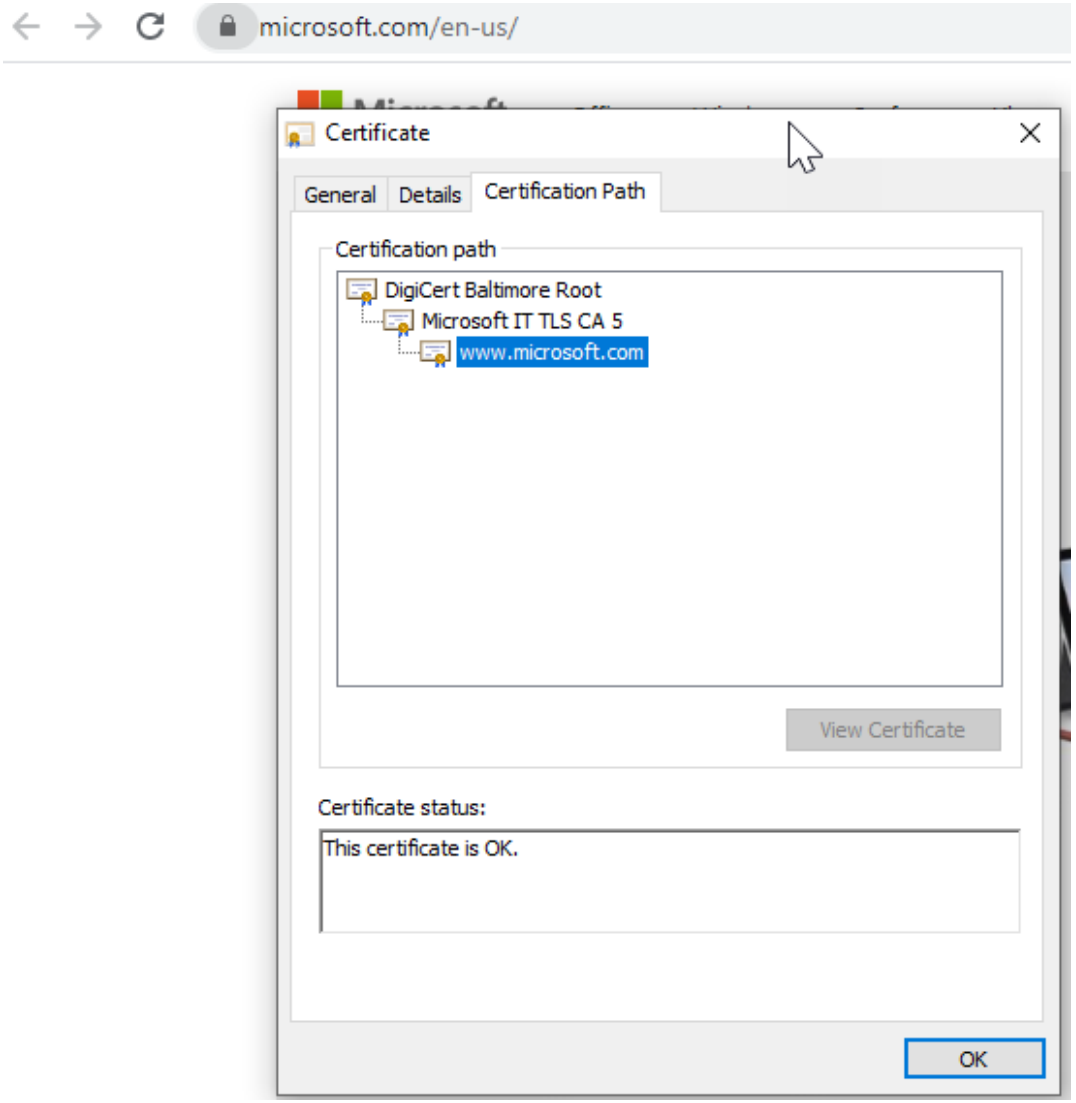




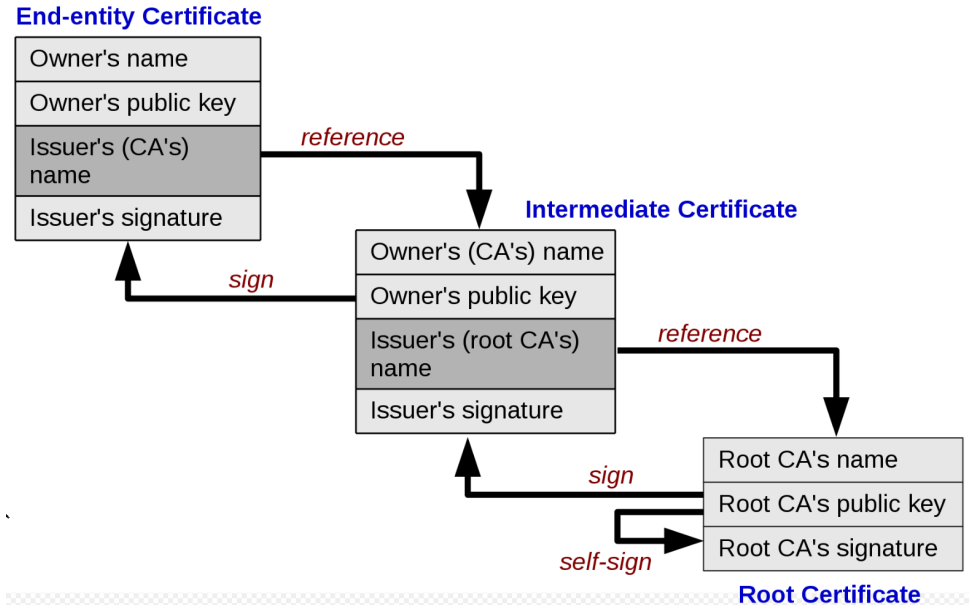


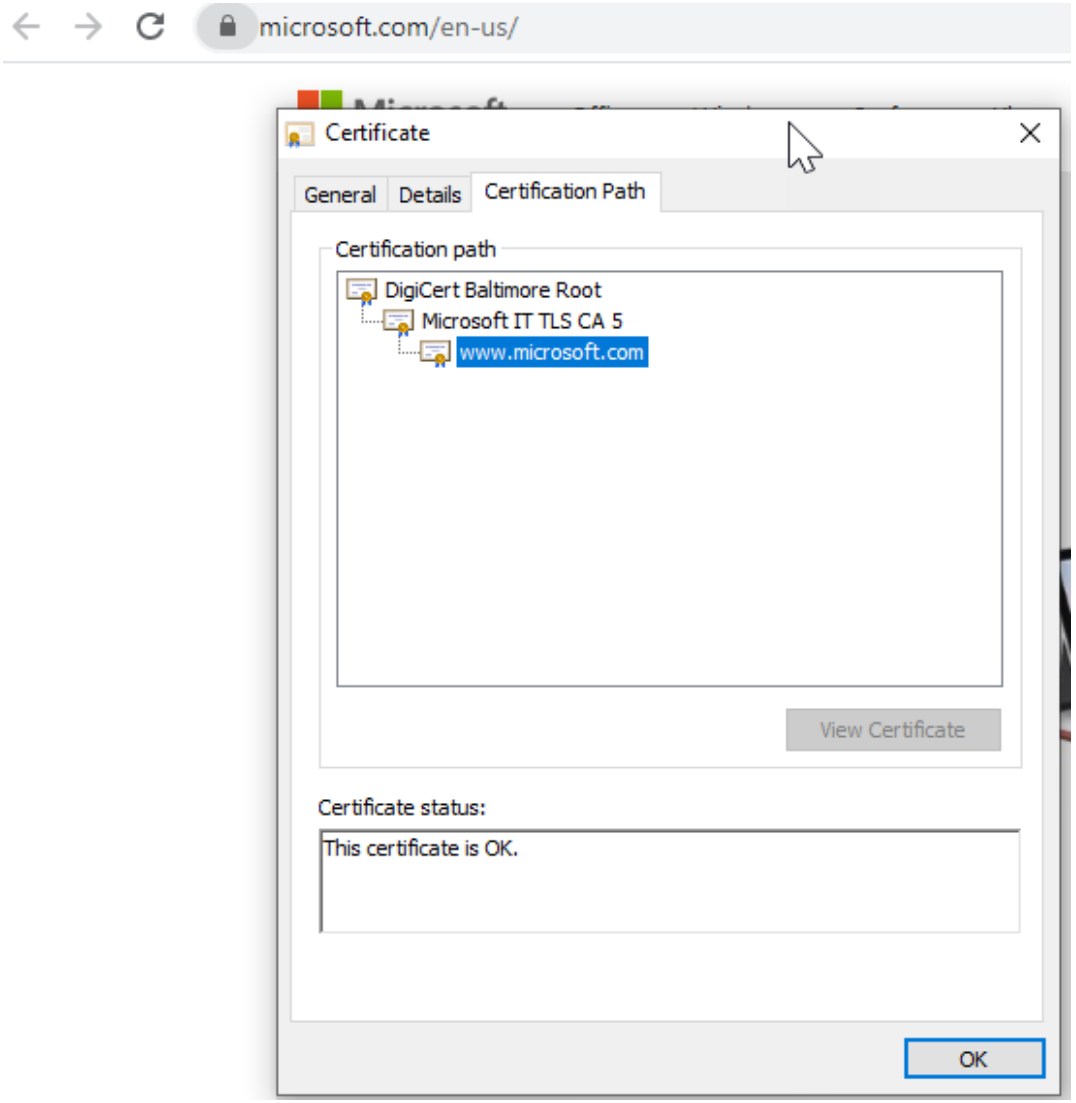
Types of certificates: Chain of trust



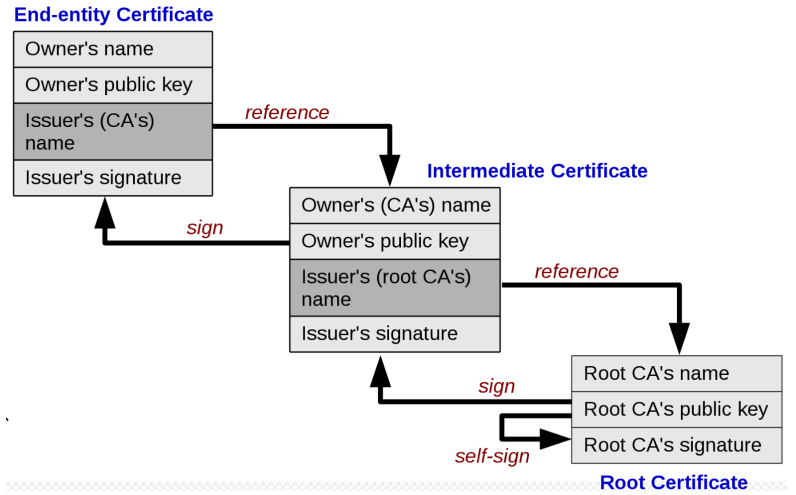


Types of certificates: Chain of trust





Types of certificates: Chain of trust



To perform its role effectively, a CA needs to have one or more broadly trusted root certificates or intermediate certificates and the corresponding private keys

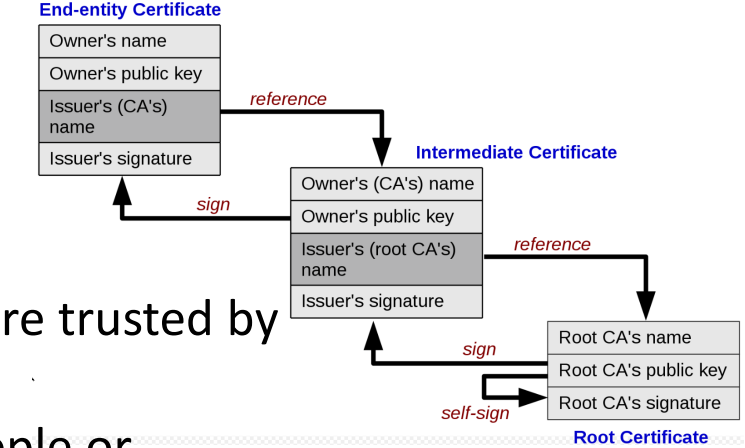
A CA may achieve broad trust by:

- Having its root certificates included in popular software
- Obtaining a cross-signature from another CA delegating trust

Or a CA may be trusted within a relatively small community, like a business

- In which its root certificates are distributed by other mechanisms like Windows Group Policy

Types of certificates: Chain of trust



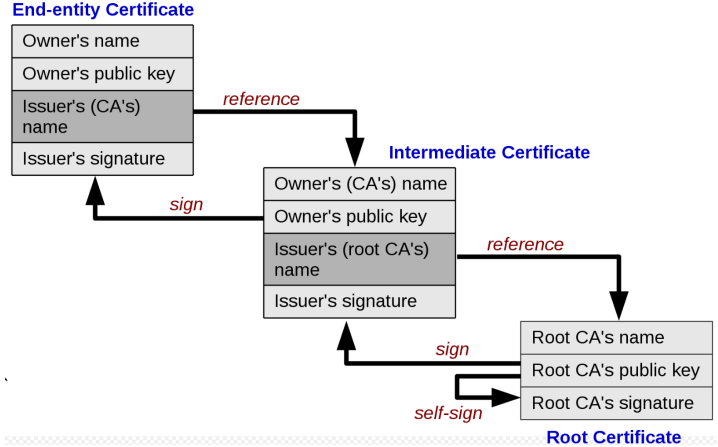
Root programs:

- Some major software products contain a list of certificate authorities that are trusted by default
- This makes it easier for end-users to validate certificates, and easier for people or organizations that request certificates to know which certificate authorities can issue a certificate that will be broadly trusted
- This is particularly important in HTTPS, where a web site operator generally wants to get a certificate that is trusted by nearly all potential visitors to their web site

The most influential root programs are:

- Microsoft Root Program
- Apple Root Program
- Mozilla Root Program
- Oracle Java root program
- Adobe Approved Trust List and EUTL root programs (used for document signing)

Types of certificates: Chain of trust



Root programs:

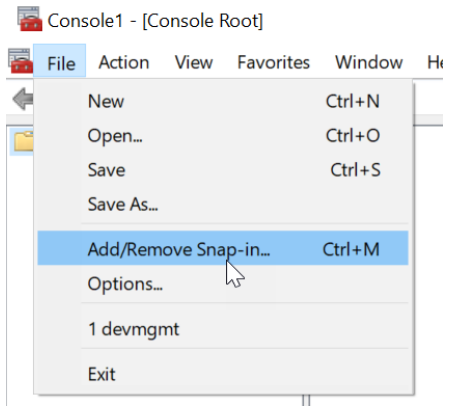
Browsers generally use the operating system's facilities to decide which certificate authorities are trusted:

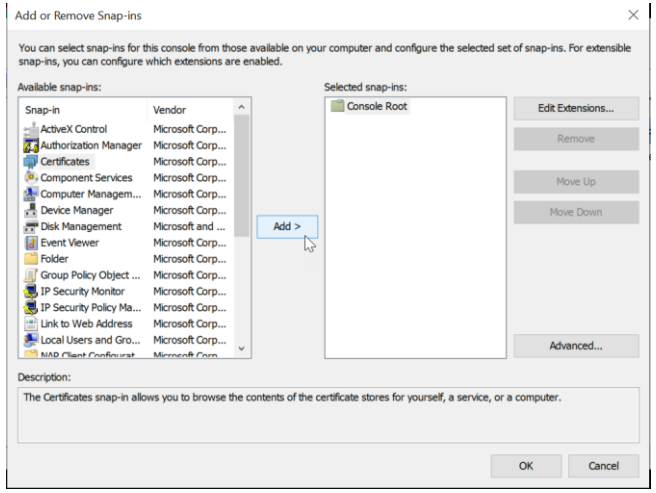
- Google Chrome on Windows trusts certificate authorities included in Microsoft Root Program
- Google Chrome on macOS or iOS trusts certificate authorities in Apple Root Program
- Edge and Safari use their respective operating system trust stores as well, but each is only available on a single OS.

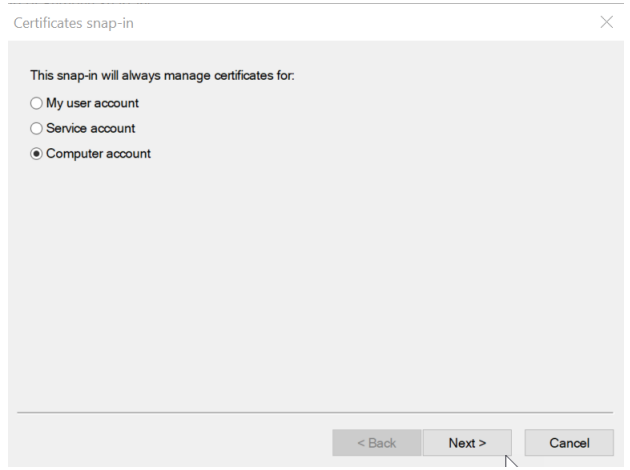
- Firefox, in contrast, uses the Mozilla Root Program trust store on all platforms

Microsoft Windows Root Program's Trust Stores

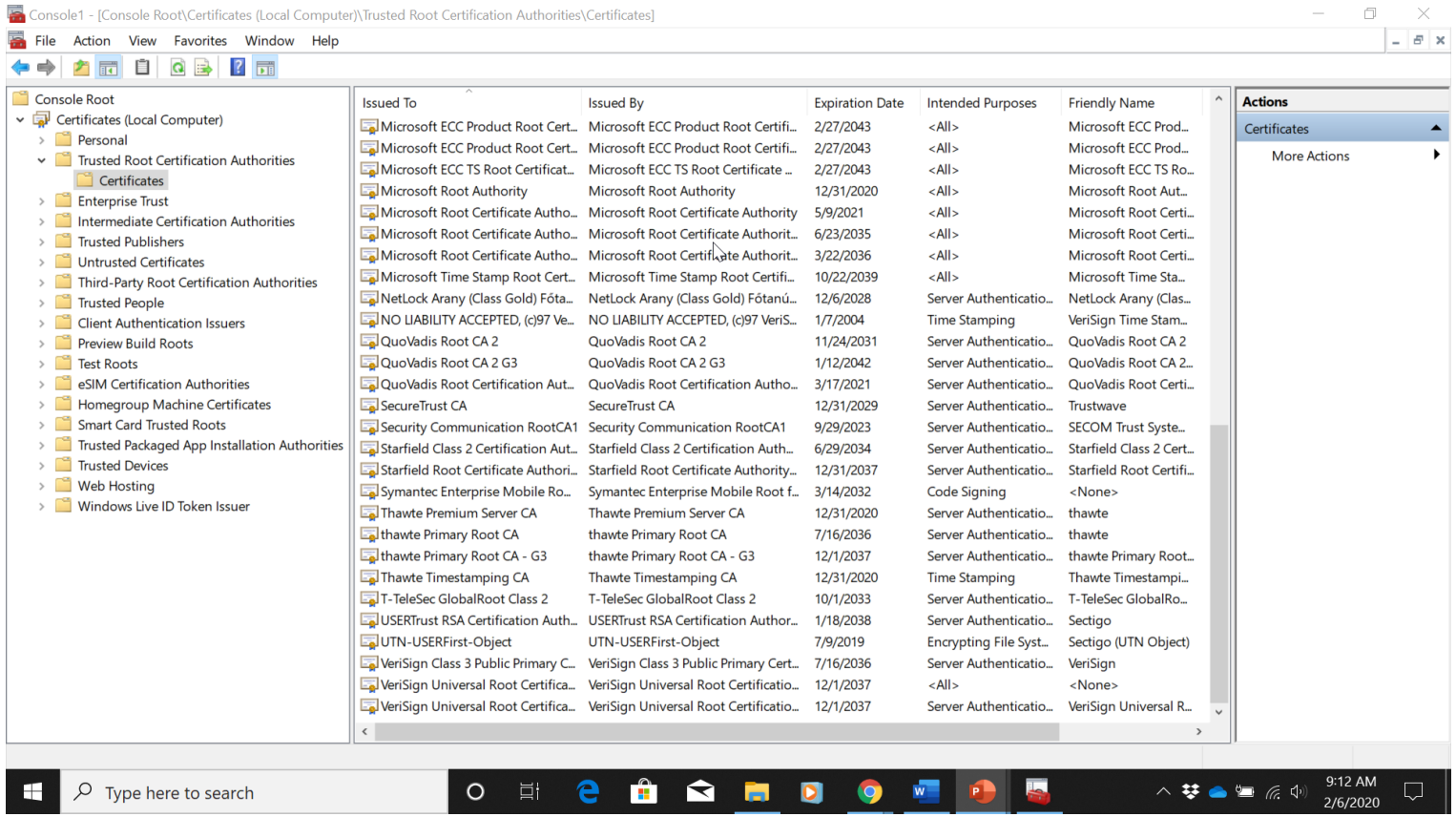
1. Run **mmc.exe**
2. Select **File -> Add/Remove Snap-in**
3. Select **Certificates**, click **Add**
4. Select **Computer Account,** click **next,** click **Finish**
5. Expand the **Certificates** node -> **Trusted Root Certificate Authorities Store**





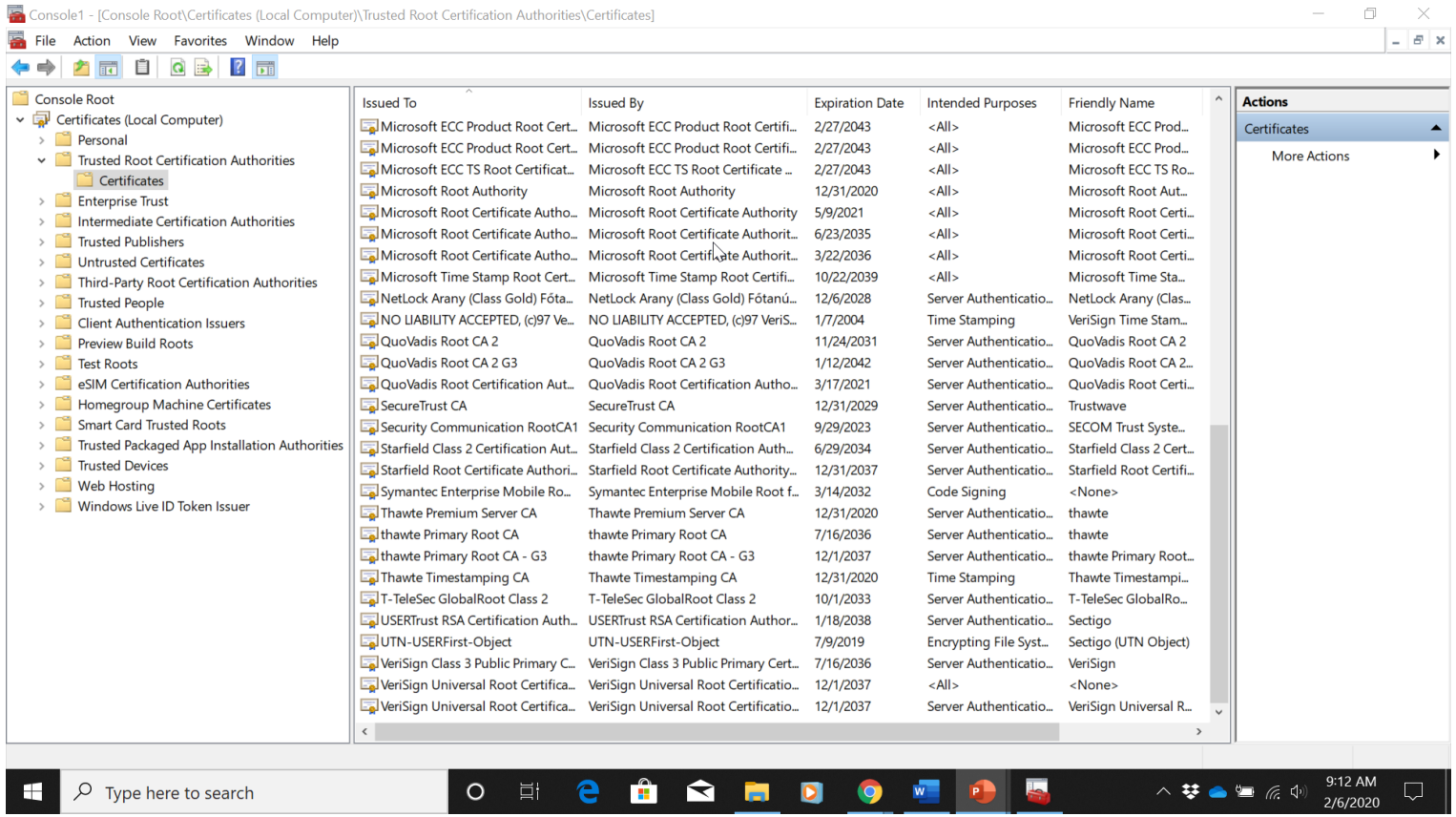


Microsoft Windows Root Program's Trust Stores



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
AAA Certificate Services	AAA Certificate Services	12/31/2028	Server Authenticatio...	Sectigo (AAA)
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticatio...	Sectigo (AddTrust)
AffirmTrust Commercial	AffirmTrust Commercial	12/31/2030	Server Authenticatio...	AffirmTrust Commer...
Amazon Root CA 1	Amazon Root CA 1	1/16/2038	Server Authenticatio...	Amazon Root CA 1
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticatio...	DigiCert Baltimore R...
Certum CA	Certum CA	6/11/2027	Server Authenticatio...	Certum
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Server Authenticatio...	Certum Trusted Net...
Class 3 Public Primary Certificati...	Class 3 Public Primary Certification ...	8/1/2028	Server Authenticatio...	VeriSign Class 3 Pub...
COMODO RSA Certification Aut...	COMODO RSA Certification Autho...	1/18/2038	Server Authenticatio...	Sectigo (formerly Co...
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timestam...
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticatio...	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenticatio...	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Server Authenticatio...	DigiCert Global Roo...
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Server Authenticatio...	DigiCert Global Roo...
DigiCert High Assurance EV Roo...	DigiCert High Assurance EV Root CA	11/9/2031	Server Authenticatio...	DigiCert
DST Root CA X3	DST Root CA X3	9/30/2021	Secure Email, Server ...	DST Root CA X3
Entrust Root Certification Autho...	Entrust Root Certification Authority	11/27/2026	Server Authenticatio...	Entrust
Entrust Root Certification Autho...	Entrust Root Certification Authorit...	12/7/2030	Server Authenticatio...	Entrust.net
Entrust.net Certification Authorit...	Entrust.net Certification Authority (...	7/24/2029	Server Authenticatio...	Entrust (2048)
Equifax Secure Certificate Autho...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Server ...	GeoTrust
GeoTrust Global CA	GeoTrust Global CA	5/20/2022	Server Authenticatio...	GeoTrust Global CA
GeoTrust Primary Certification A...	GeoTrust Primary Certification Aut...	1/18/2038	Server Authenticatio...	GeoTrust Primary Ce...
GeoTrust Primary Certification A...	GeoTrust Primary Certification Aut...	12/1/2037	Server Authenticatio...	GeoTrust Primary Ce...
GlobalSign	GlobalSign	3/18/2029	Server Authenticatio...	GlobalSign Root CA ...
GlobalSign	GlobalSign	12/15/2021	Server Authenticatio...	Google Trust Service...
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticatio...	GlobalSign Root CA ...
Go Daddy Class 2 Certification A...	Go Daddy Class 2 Certification Aut...	6/29/2034	Server Authenticatio...	Go Daddy Class 2 C...
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Authori...	12/31/2037	Server Authenticatio...	Go Daddy Root Cert...
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client ...	DigiCert Global Root
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	12/8/2043	Server Authenticatio...	Hotspot 2.0 Trust Ro...
Intel(R) Technology Access	Intel(R) Technology Access	12/1/2022	<All>	<None>
Microsoft Authenticode(tm) Roo...	Microsoft Authenticode(tm) Root ...	12/31/1999	Secure Email, Code ...	Microsoft Authentic...
Microsoft ECC Product Root Cert...	Microsoft ECC Product Root Certifi...	2/27/2043	<All>	Microsoft ECC Prod...
Microsoft ECC Product Root Cert...	Microsoft ECC Product Root Certifi...	2/27/2043	<All>	Microsoft ECC Prod...
Microsoft ECC TS Root Certificat...	Microsoft ECC TS Root Certificate ...	2/27/2043	<All>	Microsoft ECC TS Ro...
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authority	5/9/2021	<All>	Microsoft Root Certi...
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authorit...	6/23/2035	<All>	Microsoft Root Certi...
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authorit...	3/22/2036	<All>	Microsoft Root Certi...
Microsoft Time Stamp Root Cert...	Microsoft Time Stamp Root Certifi...	10/22/2039	<All>	Microsoft Time Sta...
NetLock Arany (Class Gold) Főta...	NetLock Arany (Class Gold) Főtanú...	12/6/2028	Server Authenticatio...	NetLock Arany (Clas...
NO LIABILITY ACCEPTED, (c)97 Ve...	NO LIABILITY ACCEPTED, (c)97 VeriS...	1/7/2004	Time Stamping	VeriSign Time Stam...
QuoVadis Root CA 2	QuoVadis Root CA 2	11/24/2031	Server Authenticatio...	QuoVadis Root CA 2
QuoVadis Root CA 2 G3	QuoVadis Root CA 2 G3	1/12/2042	Server Authenticatio...	QuoVadis Root CA 2...
QuoVadis Root Certification Aut...	QuoVadis Root Certification Autho...	3/17/2021	Server Authenticatio...	QuoVadis Root Certi...
SecureTrust CA	SecureTrust CA	12/31/2029	Server Authenticatio...	Trustwave
Security Communication RootCA1	Security Communication RootCA1	9/29/2023	Server Authenticatio...	SECOM Trust Syste...
Starfield Class 2 Certification Aut...	Starfield Class 2 Certification Auth...	6/29/2034	Server Authenticatio...	Starfield Class 2 Cert...
Starfield Root Certificate Authori...	Starfield Root Certificate Authority...	12/31/2037	Server Authenticatio...	Starfield Root Certifi...
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root f...	3/14/2032	Code Signing	<None>
Thawte Premium Server CA	Thawte Premium Server CA	12/31/2020	Server Authenticatio...	thawte
thawte Primary Root CA	thawte Primary Root CA	7/16/2036	Server Authenticatio...	thawte
thawte Primary Root CA - G3	thawte Primary Root CA - G3	12/1/2037	Server Authenticatio...	thawte Primary Root...
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestampi...
T-TeleSec GlobalRoot Class 2	T-TeleSec GlobalRoot Class 2	10/1/2033	Server Authenticatio...	T-TeleSec GlobalRo...
USERTrust RSA Certification Auth...	USERTrust RSA Certification Author...	1/18/2038	Server Authenticatio...	Sectigo
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Encrypting File Syst...	Sectigo (UTN Object)
VeriSign Class 3 Public Primary C...	VeriSign Class 3 Public Primary Cert...	7/16/2036	Server Authenticatio...	VeriSign
VeriSign Universal Root Certifica...	VeriSign Universal Root Certificatio...	12/1/2037	<All>	<None>
VeriSign Universal Root Certifica...	VeriSign Universal Root Certificatio...	12/1/2037	Server Authenticatio...	VeriSign Universal R...

Microsoft Windows Root Program's Trust Stores



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
AAA Certificate Services	AAA Certificate Services	12/31/2028	Server Authenticatio...	Sectigo (AAA)
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticatio...	Sectigo (AddTrust)
AffirmTrust Commercial	AffirmTrust Commercial	12/31/2030	Server Authenticatio...	AffirmTrust Commer...
Amazon Root CA 1	Amazon Root CA 1	1/16/2038	Server Authenticatio...	Amazon Root CA 1
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticatio...	DigiCert Baltimore R...
Certum CA	Certum CA	6/11/2027	Server Authenticatio...	Certum
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Server Authenticatio...	Certum Trusted Net...
Class 3 Public Primary Certificati...	Class 3 Public Primary Certification ...	8/1/2028	Server Authenticatio...	VeriSign Class 3 Pub...
COMODO RSA Certification Aut...	COMODO RSA Certification Autho...	1/18/2038	Server Authenticatio...	Sectigo (formerly Co...
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timestam...
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticatio...	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenticatio...	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Server Authenticatio...	DigiCert Global Roo...
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Server Authenticatio...	DigiCert Global Roo...
DigiCert High Assurance EV Roo...	DigiCert High Assurance EV Root CA	11/9/2031	Server Authenticatio...	DigiCert
DST Root CA X3	DST Root CA X3	9/30/2021	Secure Email, Server ...	DST Root CA X3
Entrust Root Certification Autho...	Entrust Root Certification Authority	11/27/2026	Server Authenticatio...	Entrust
Entrust Root Certification Autho...	Entrust Root Certification Authorit...	12/7/2030	Server Authenticatio...	Entrust.net
Entrust.net Certification Authorit...	Entrust.net Certification Authority (...	7/24/2029	Server Authenticatio...	Entrust (2048)
Equifax Secure Certificate Autho...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Server ...	GeoTrust
GeoTrust Global CA	GeoTrust Global CA	5/20/2022	Server Authenticatio...	GeoTrust Global CA
GeoTrust Primary Certification A...	GeoTrust Primary Certification Aut...	1/18/2038	Server Authenticatio...	GeoTrust Primary Ce...
GeoTrust Primary Certification A...	GeoTrust Primary Certification Aut...	12/1/2037	Server Authenticatio...	GeoTrust Primary Ce...
GlobalSign	GlobalSign	3/18/2029	Server Authenticatio...	GlobalSign Root CA ...
GlobalSign	GlobalSign	12/15/2021	Server Authenticatio...	Google Trust Service...
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticatio...	GlobalSign Root CA ...
Go Daddy Class 2 Certification A...	Go Daddy Class 2 Certification Aut...	6/29/2034	Server Authenticatio...	Go Daddy Class 2 C...
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Authori...	12/31/2037	Server Authenticatio...	Go Daddy Root Cert...
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client ...	DigiCert Global Root
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	12/8/2043	Server Authenticatio...	Hotspot 2.0 Trust Ro...
Intel(R) Technology Access	Intel(R) Technology Access	12/1/2022	<All>	<None>
Microsoft Authenticode(tm) Roo...	Microsoft Authenticode(tm) Root ...	12/31/1999	Secure Email, Code ...	Microsoft Authentic...
Microsoft ECC Product Root Cert...	Microsoft ECC Product Root Certifi...	2/27/2043	<All>	Microsoft ECC Prod...
Microsoft ECC Product Root Cert...	Microsoft ECC Product Root Certifi...	2/27/2043	<All>	Microsoft ECC Prod...
Microsoft ECC TS Root Certificat...	Microsoft ECC TS Root Certificate ...	2/27/2043	<All>	Microsoft ECC TS Ro...
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authority	5/9/2021	<All>	Microsoft Root Certi...
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authorit...	6/23/2035	<All>	Microsoft Root Certi...
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authorit...	3/22/2036	<All>	Microsoft Root Certi...
Microsoft Time Stamp Root Cert...	Microsoft Time Stamp Root Certifi...	10/22/2039	<All>	Microsoft Time Sta...
NetLock Arany (Class Gold) Főta...	NetLock Arany (Class Gold) Főtanú...	12/6/2028	Server Authenticatio...	NetLock Arany (Clas...
NO LIABILITY ACCEPTED, (c)97 Ve...	NO LIABILITY ACCEPTED, (c)97 VeriS...	1/7/2004	Time Stamping	VeriSign Time Stam...
QuoVadis Root CA 2	QuoVadis Root CA 2	11/24/2031	Server Authenticatio...	QuoVadis Root CA 2
QuoVadis Root CA 2 G3	QuoVadis Root CA 2 G3	1/12/2042	Server Authenticatio...	QuoVadis Root CA 2...
QuoVadis Root Certification Aut...	QuoVadis Root Certification Autho...	3/17/2021	Server Authenticatio...	QuoVadis Root Certi...
SecureTrust CA	SecureTrust CA	12/31/2029	Server Authenticatio...	Trustwave
Security Communication RootCA1	Security Communication RootCA1	9/29/2023	Server Authenticatio...	SECOM Trust Syste...
Starfield Class 2 Certification Aut...	Starfield Class 2 Certification Auth...	6/29/2034	Server Authenticatio...	Starfield Class 2 Cert...
Starfield Root Certificate Authori...	Starfield Root Certificate Authority...	12/31/2037	Server Authenticatio...	Starfield Root Certifi...
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root f...	3/14/2032	Code Signing	<None>
Thawte Premium Server CA	Thawte Premium Server CA	12/31/2020	Server Authenticatio...	thawte
thawte Primary Root CA	thawte Primary Root CA	7/16/2036	Server Authenticatio...	thawte
thawte Primary Root CA - G3	thawte Primary Root CA - G3	12/1/2037	Server Authenticatio...	thawte Primary Root...
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestampi...
T-TeleSec GlobalRoot Class 2	T-TeleSec GlobalRoot Class 2	10/1/2033	Server Authenticatio...	T-TeleSec GlobalRo...
USERTrust RSA Certification Auth...	USERTrust RSA Certification Author...	1/18/2038	Server Authenticatio...	Sectigo
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Encrypting File Syst...	Sectigo (UTN Object)
VeriSign Class 3 Public Primary C...	VeriSign Class 3 Public Primary Cert...	7/16/2036	Server Authenticatio...	VeriSign
VeriSign Universal Root Certifica...	VeriSign Universal Root Certificatio...	12/1/2037	<All>	<None>
VeriSign Universal Root Certifica...	VeriSign Universal Root Certificatio...	12/1/2037	Server Authenticatio...	VeriSign Universal R...

Mac OS X

The root store is in the Keychain.app

1. Search Finder (Spotlight) for “keychain”
2. Double-click Keychain Access app
3. Select “System Roots” in the left-hand pane

Certificate Revocation List (CRL) – in principal

CRL is the mechanism for the CA to let others know that a certificate has become invalid for some reason

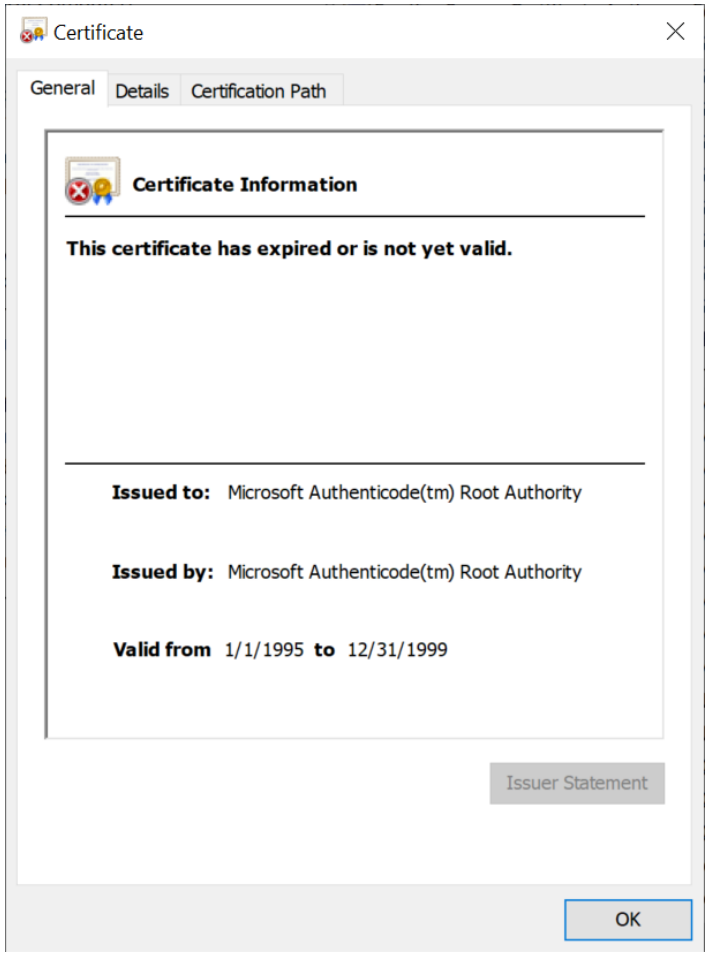
A certificate may be revoked because

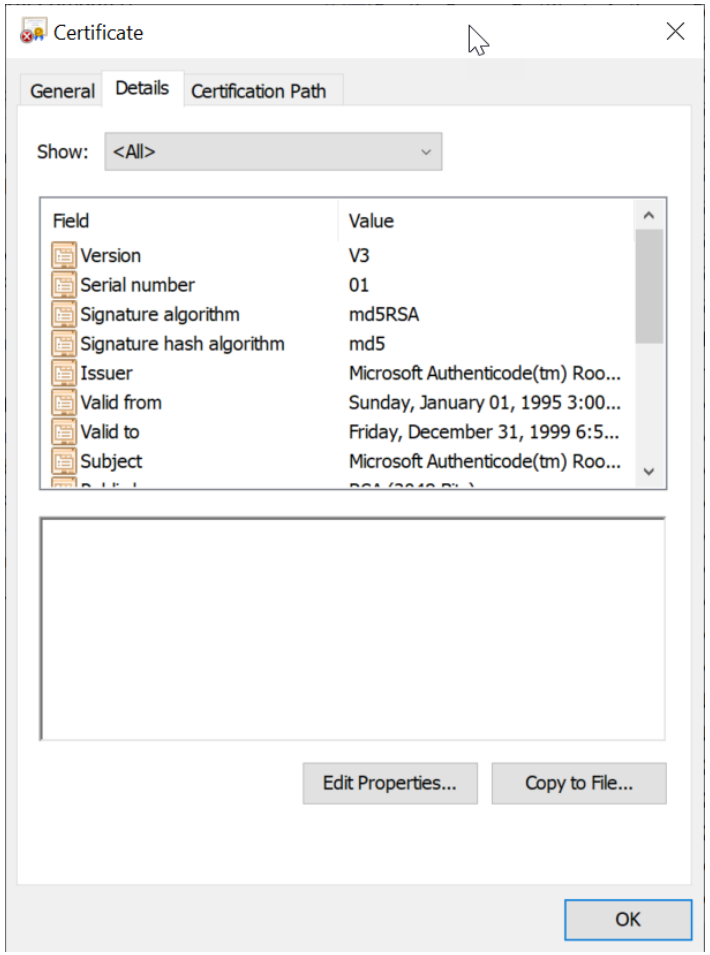
- The key holder's private key was compromised
- CA discovered the Certificate was issued to the wrong person
- The certificate expired
- The certificate became invalid for other reasons…

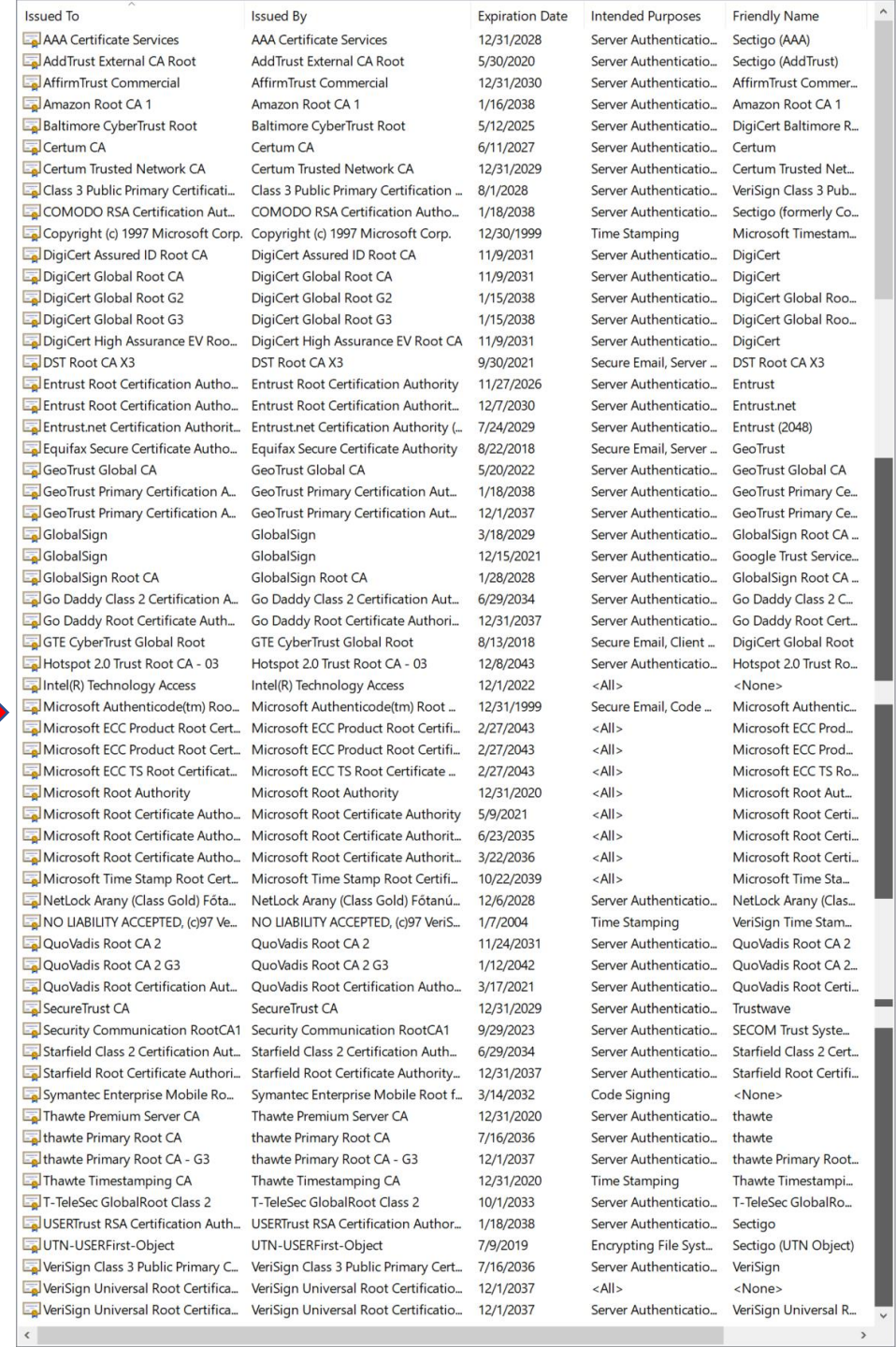
The CA handles revocation by putting the revoked certificate's information on a ***certificate revocation list*** (CRL)

- The CRL is a list of every certificate that has been revoked
- The CRL is maintained and updated

Microsoft Windows Root Program's Trust Stores



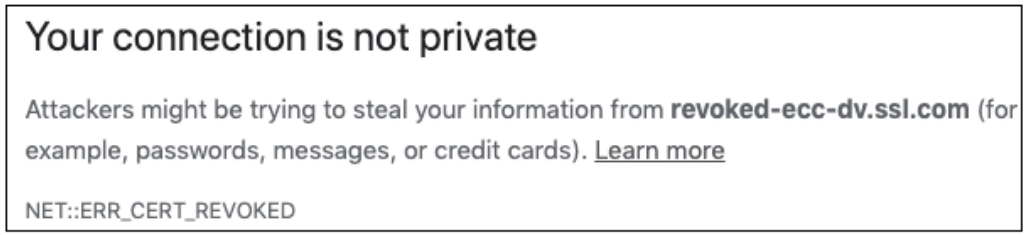




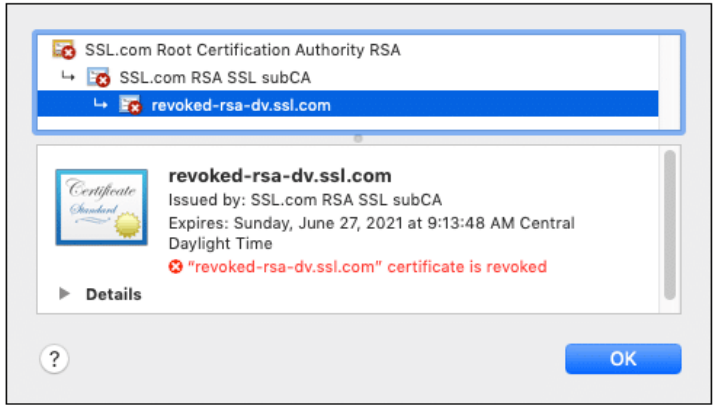
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
AAA Certificate Services	AAA Certificate Services	12/31/2028	Server Authenticatio...	Sectigo (AAA)
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticatio...	Sectigo (AddTrust)
AffirmTrust Commercial	AffirmTrust Commercial	12/31/2030	Server Authenticatio...	AffirmTrust Commer...
Amazon Root CA 1	Amazon Root CA 1	1/16/2038	Server Authenticatio...	Amazon Root CA 1
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticatio...	DigiCert Baltimore R...
Certum CA	Certum CA	6/11/2027	Server Authenticatio...	Certum
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Server Authenticatio...	Certum Trusted Net...
Class 3 Public Primary Certificati...	Class 3 Public Primary Certification ...	8/1/2028	Server Authenticatio...	VeriSign Class 3 Pub...
COMODO RSA Certification Aut...	COMODO RSA Certification Autho...	1/18/2038	Server Authenticatio...	Sectigo (formerly Co...
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timestam...
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Server Authenticatio...	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenticatio...	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Server Authenticatio...	DigiCert Global Roo...
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Server Authenticatio...	DigiCert Global Roo...
DigiCert High Assurance EV Roo...	DigiCert High Assurance EV Root CA	11/9/2031	Server Authenticatio...	DigiCert
DST Root CA X3	DST Root CA X3	9/30/2021	Secure Email, Server ...	DST Root CA X3
Entrust Root Certification Autho...	Entrust Root Certification Authority	11/27/2026	Server Authenticatio...	Entrust
Entrust Root Certification Autho...	Entrust Root Certification Authorit...	12/7/2030	Server Authenticatio...	Entrust.net
Entrust.net Certification Authorit...	Entrust.net Certification Authority (...	7/24/2029	Server Authenticatio...	Entrust (2048)
Equifax Secure Certificate Autho...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Server ...	GeoTrust
GeoTrust Global CA	GeoTrust Global CA	5/20/2022	Server Authenticatio...	GeoTrust Global CA
GeoTrust Primary Certification A...	GeoTrust Primary Certification Aut...	1/18/2038	Server Authenticatio...	GeoTrust Primary Ce...
GeoTrust Primary Certification A...	GeoTrust Primary Certification Aut...	12/1/2037	Server Authenticatio...	GeoTrust Primary Ce...
GlobalSign	GlobalSign	3/18/2029	Server Authenticatio...	GlobalSign Root CA ...
GlobalSign	GlobalSign	12/15/2021	Server Authenticatio...	Google Trust Service...
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticatio...	GlobalSign Root CA ...
Go Daddy Class 2 Certification A...	Go Daddy Class 2 Certification Aut...	6/29/2034	Server Authenticatio...	Go Daddy Class 2 C...
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Authori...	12/31/2037	Server Authenticatio...	Go Daddy Root Cert...
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client ...	DigiCert Global Root
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	12/8/2043	Server Authenticatio...	Hotspot 2.0 Trust Ro...
Intel(R) Technology Access	Intel(R) Technology Access	12/1/2022	<All>	<None>
Microsoft Authenticode(tm) Roo...	Microsoft Authenticode(tm) Root ...	12/31/1999	Secure Email, Code ...	Microsoft Authentic...
Microsoft ECC Product Root Cert...	Microsoft ECC Product Root Certifi...	2/27/2043	<All>	Microsoft ECC Prod...
Microsoft ECC Product Root Cert...	Microsoft ECC Product Root Certifi...	2/27/2043	<All>	Microsoft ECC Prod...
Microsoft ECC TS Root Certificat...	Microsoft ECC TS Root Certificate ...	2/27/2043	<All>	Microsoft ECC TS Ro...
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authority	5/9/2021	<All>	Microsoft Root Certi...
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authorit...	6/23/2035	<All>	Microsoft Root Certi...
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authorit...	3/22/2036	<All>	Microsoft Root Certi...
Microsoft Time Stamp Root Cert...	Microsoft Time Stamp Root Certifi...	10/22/2039	<All>	Microsoft Time Sta...
NetLock Arany (Class Gold) Főta...	NetLock Arany (Class Gold) Főtanú...	12/6/2028	Server Authenticatio...	NetLock Arany (Clas...
NO LIABILITY ACCEPTED, (c)97 Ve...	NO LIABILITY ACCEPTED, (c)97 VeriS...	1/7/2004	Time Stamping	VeriSign Time Stam...
QuoVadis Root CA 2	QuoVadis Root CA 2	11/24/2031	Server Authenticatio...	QuoVadis Root CA 2
QuoVadis Root CA 2 G3	QuoVadis Root CA 2 G3	1/12/2042	Server Authenticatio...	QuoVadis Root CA 2...
QuoVadis Root Certification Aut...	QuoVadis Root Certification Autho...	3/17/2021	Server Authenticatio...	QuoVadis Root Certi...
SecureTrust CA	SecureTrust CA	12/31/2029	Server Authenticatio...	Trustwave
Security Communication RootCA1	Security Communication RootCA1	9/29/2023	Server Authenticatio...	SECOM Trust Syste...
Starfield Class 2 Certification Aut...	Starfield Class 2 Certification Auth...	6/29/2034	Server Authenticatio...	Starfield Class 2 Cert...
Starfield Root Certificate Authori...	Starfield Root Certificate Authority...	12/31/2037	Server Authenticatio...	Starfield Root Certifi...
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root f...	3/14/2032	Code Signing	<None>
Thawte Premium Server CA	Thawte Premium Server CA	12/31/2020	Server Authenticatio...	thawte
thawte Primary Root CA	thawte Primary Root CA	7/16/2036	Server Authenticatio...	thawte
thawte Primary Root CA - G3	thawte Primary Root CA - G3	12/1/2037	Server Authenticatio...	thawte Primary Root...
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestampi...
T-TeleSec GlobalRoot Class 2	T-TeleSec GlobalRoot Class 2	10/1/2033	Server Authenticatio...	T-TeleSec GlobalRo...
USERTrust RSA Certification Auth...	USERTrust RSA Certification Author...	1/18/2038	Server Authenticatio...	Sectigo
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Encrypting File Syst...	Sectigo (UTN Object)
VeriSign Class 3 Public Primary C...	VeriSign Class 3 Public Primary Cert...	7/16/2036	Server Authenticatio...	VeriSign
VeriSign Universal Root Certifica...	VeriSign Universal Root Certificatio...	12/1/2037	<All>	<None>
VeriSign Universal Root Certifica...	VeriSign Universal Root Certificatio...	12/1/2037	Server Authenticatio...	VeriSign Universal R...

Examples of Browsers Rejecting Revoked Certificates

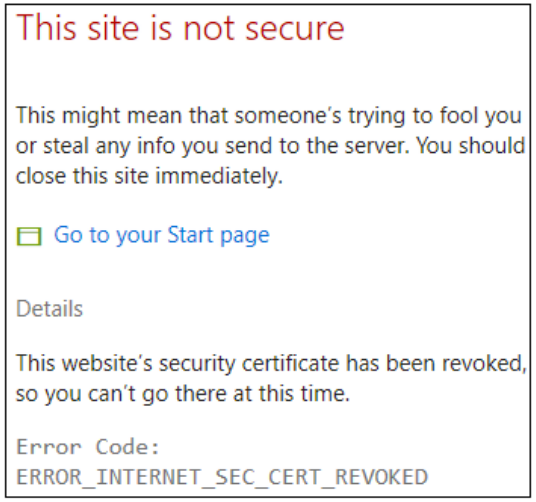
- **Chrome:** `NET::ERR_CERT_REVOKED`



- **Safari:** Generic `This Connection is Not Private` message. If you click the **Show Details** button and then the **view the certificate** link, you can confirm that the certificate is, in fact, revoked.



- **Edge:** `ERROR_INTERNET_SEC_CERT_REVOKED` (visible after clicking **Details** link on **This site is not secure** message).



Certificate Revocation List (CRL) – in practice

CRLs are problematic in many PKI implementations for many reasons

- Either user's browser must check a central CRL to find out if a certificate has been revoked
- …or the CA must continually push out CRL values to clients to ensure they have an updated CRL

By default, web browsers do not check a CRL to ensure that a certificate is not revoked

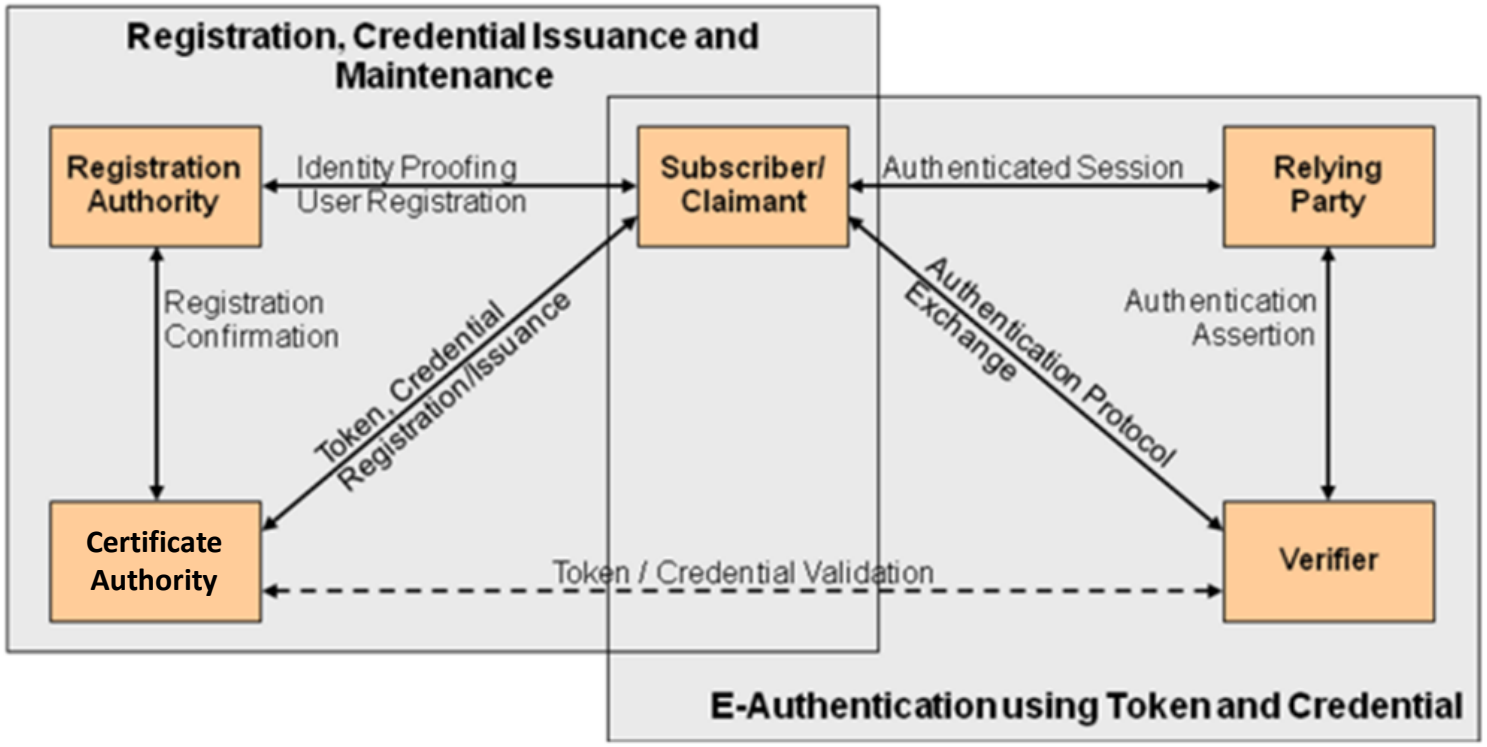
- So when you are setting up a SSL connection to do e-Commerce over the Internet, you may be relying on a revoked certificate and not know it

Online Certificate Status Protocol (OCSP) is increasingly being used…

- If OCSP is implemented, it works automatically
- OCSP does real-time certificate validation
  - Checks the CRL maintained by the CA
  - Notifies user if certificate is valid, invalid, or unknown
- Publicly trusted CAs (e.g. SSL.com) maintain HTTP servers called OCSP responders
  - OCSP responders sign their responses with the CA's private signing key so browsers can verify that the received revocation status was generated by the actual CA

Example of "invalid" certificate: https://www.iad.gov/nietp/caerequirements.cfm

PKI Roles and Workflows



Token, Credential = Public Key

Basic Online Certificate Status Protocol (OCSP)

1. Alice and Bob have public key certificates issued by Carol, the certificate authority (CA)
2. Alice wishes to perform a transaction with Bob and sends him her public key certificate
3. Bob, concerned that Alice's public key may have been compromised, creates an 'OCSP request' that contains Alice's certificate serial number and sends it to Carol
4. Carol's OCSP responder reads the certificate serial number from Bob's request. The OCSP responder uses the certificate serial number to look up the revocation status of Alice's certificate. The OCSP responder looks in a CA database that Carol maintains. In this scenario, Carol's CA database is the only trusted location where a compromise to Alice's certificate would be recorded
5. Carol's OCSP responder confirms that Alice's certificate is still OK, and returns a signed, successful 'OCSP response' to Bob
6. Bob cryptographically verifies Carol's signed response. Bob has stored Carol's public key sometime before this transaction. Bob uses Carol's public key to verify Carol's response
7. Bob completes the transaction with Alice

Online Certificate Status Protocol (OCSP) – In Practice

Contacting a responder and waiting for a response for every certificate encountered by a browser encounters adds perceptible network overhead, especially in pages containing third-party content stored in remote content-distribution servers

- *Amazon calculated that a delay of one second can cost them about $1.6 billion yearly*

This motivated browsers and other client software to implement OCSP checking in soft-fail mode

If an OCSP server cannot be reached or times out while giving its response, browsers consider the certificate valid and proceed with the HTTPS connection anyway

Man-in-the-middle (MITM) attackers can exploit this behavior by blocking all connections to OCSP responders, and then can use a stolen certificate and key pair for a malicious site, regardless of the certificate's revocation status

OCSP Stapling Solution

Servers include (or **staple**) the cached OCSP response in their HTTPS responses alongside the SSL certificate

- This enables browsers before the secure connection is established to verify the CAs signature on the OCSP response and be assured that the certificate has not been revoked
- OCSP stapling enables servers to retrieve cached OCSP responses in non-real-time and remove performance overhead imposed by CRLs and OCSP
- OCSP stapling does not completely solve OCSP's soft-fail security issue, since stapling is implemented in the server and browsers cannot know if a server actually supports Stapling or not

- OCSP Must-Staple (extension of SSL Certificates: RFC 7633)
  - Mandates OCSP stapling for the certificate
  - If a browser encounters a certificate with this extension that is used without OCSP Stapling, then it will be rejected
  - Enabling OCSP stapling on servers improves security and performance for your web site at the same time

https://www.ssl.com/article/page-load-optimization-ocsp-stapling/

Agenda

- ✓Public Key Infrastructure
- ✓Digital Certificate
- ✓Public key Certificates
- ✓Roles in PKI: Certificate Authority (CA)
- ✓Roles in PKI: Registration Authority (RA)
- ✓PKI Steps
- ✓Chain of Trust
- ✓Root Programs
- ✓Certificate Revocation List (CRL)
- ✓PKI Roles / Workflows…