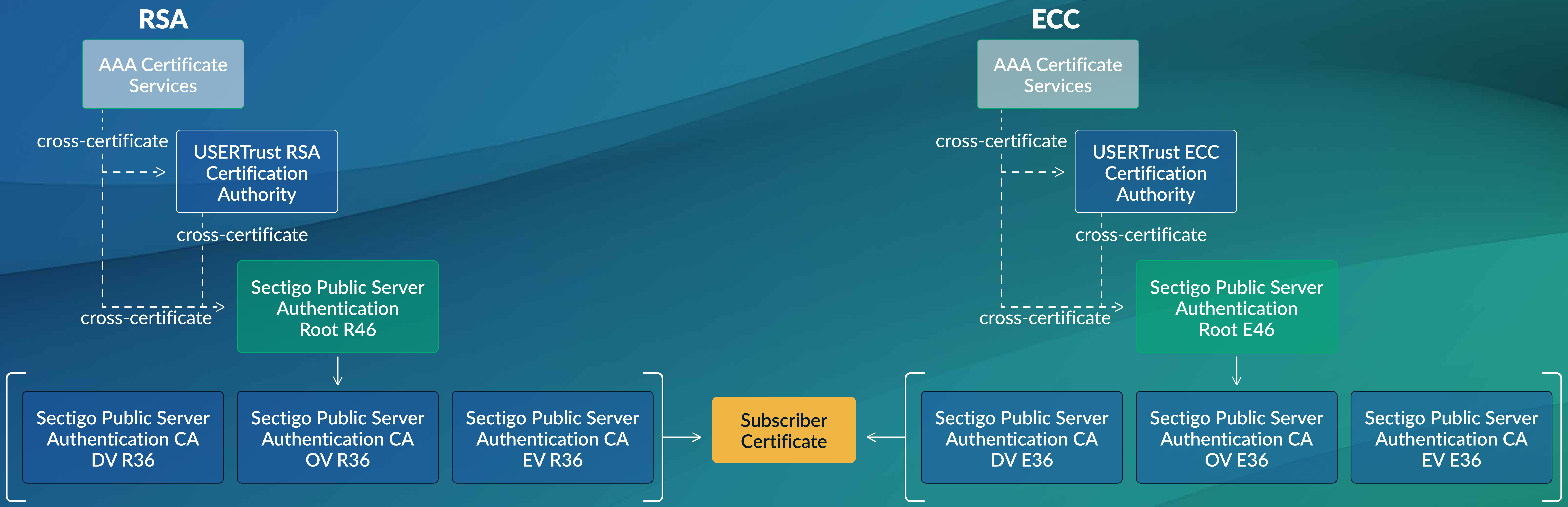
Sectigo Roots and Issuing CAs

This document shows the new (in-use in 2024/2025) Sectigo issuing CAs and hierarchies, including cross-certificates.
Information is provided on all of the self-signed ‘roots’ and cross-certificates, along with a table showing which versions of popular software the roots were initially included in.

Sectigo Roots and Issuing CAs



RSA

AAA Certificate Services

cross-certificate

USERTrust RSA Certification Authority

cross-certificate

cross-certificate

Sectigo Public Server Authentication Root R46

Sectigo Public Server Authentication CA DV R36

Sectigo Public Server Authentication CA OV R36

Sectigo Public Server Authentication CA EV R36

Subscriber Certificate

ECC

AAA Certificate Services

cross-certificate

USERTrust ECC Certification Authority

cross-certificate

cross-certificate

Sectigo Public Server Authentication Root E46

Sectigo Public Server Authentication CA DV E36

Sectigo Public Server Authentication CA OV E36

Sectigo Public Server Authentication CA EV E36

Cross certificates are provided to offer compatibility with older, legacy devices which may not have been updated to include the newer certificates in their trust-stores.
A TLS client, such as a browser, aims to build a valid path to a certificate in its trust-store. If a client does not have the ‘newer’ roots, it may trust a cross-certificate signed by an ‘older’ root.
The subscriber may need to install the additional certificates on the server side, so they are provided in the TLS handshake.

Note that TLS clients will build their own trusted certificate path based on what they trust, but also include caches, internal software logic, ‘AIA chasing’ and other techniques, the details of which are often known only to those software vendors. It may not be possible to force a TLS client to use a specific path – only to provide a trusted path for the client.

Certificate information

The below table shows all the certificates from the diagram above, with details of Subject and Issuer, validity dates and a link to crt.sh where you can view all the details of the certificate and download the certificate itself.

Certificate subject	Certificate issuer	notBefore	notAfter	crt.sh link	Key & signature	Notes
AAA Certificate Services	AAA Certificate Services	1-Jan-2024	31-Dec-2028	https://crt.sh/?id=331986	RSA2048, sha1withRSA*	Self-signed root
USERTrust RSA Certification Authority	USERTrust RSA Certification Authority	1-Feb-2010	18-Jan-2038	https://crt.sh/?id=1199354	RSA4096, sha384withRSA	Self-signed root
USERTrust ECC Certification Authority	USERTrust ECC Certification Authority	1-Feb-2010	18-Jan-2038	https://crt.sh/?id=2841410	P-384, ecdsa-with-SHA384	Self-signed root
USERTrust RSA Certification Authority	AAA Certificate Services	12-Mar-2019	31-Dec-2028	https://crt.sh/?id=1282303295	RSA4096, sha384withRSA	Cross-certificate
USERTrust ECC Certification Authority	AAA Certificate Services	12-Mar-2019	31-Dec-2028	https://crt.sh/?id=1282303296	P-384, sha384withRSA	Cross-certificate
Sectigo Public Server Authentication Root R46	Sectigo Public Server Authentication Root R46	22-Mar-2021	21-Mar-2046	https://crt.sh/?id=4256644734	RSA4096, sha384withRSA	Self-signed root
Sectigo Public Server Authentication Root E46	Sectigo Public Server Authentication Root E46	22-Mar-2021	21-Mar-2046	https://crt.sh/?id=4256644603	P-384, ecdsa-with-SHA384	Self-signed root
Sectigo Public Server Authentication Root R46	USERTrust RSA Certification Authority	22-Mar-2021	18-Jan-2038	https://crt.sh/?id=11405654893	RSA4096, sha384withRSA	Cross-certificate
Sectigo Public Server Authentication Root E46	USERTrust ECC Certification Authority	22-Mar-2021	18-Jan-2038	https://crt.sh/?id=11405664274	P-384, ecdsa-with-SHA384	Cross-certificate
Sectigo Public Server Authentication Root R46	AAA Certificate Services	22-Mar-2021	31-Dec-2028	https://crt.sh/?id=11405654892	RSA4096, sha384withRSA	Cross-certificate
Sectigo Public Server Authentication Root E46	AAA Certificate Services	22-Mar-2021	31-Dec-2028	https://crt.sh/?id=11405664273	P-384, sha384withRSA	Cross-certificate
Issuing CAs						
Sectigo Public Server Authentication CA DV R36	Sectigo Public Server Authentication Root R46	22-Mar-2021	21-Mar-2036	https://crt.sh/?id=4267304690	RSA3072, sha384withRSA	Leaf certificates issued from these CAs will use: sha384withRSA Or ecdsa-with-SHA384
Sectigo Public Server Authentication CA OV R36	Sectigo Public Server Authentication Root R46	22-Mar-2021	21-Mar-2036	https://crt.sh/?id=4267304698	RSA3072, sha384withRSA	
Sectigo Public Server Authentication CA EV R36	Sectigo Public Server Authentication Root R46	22-Mar-2021	21-Mar-2036	https://crt.sh/?id=4267304687	RSA3072, sha384withRSA	
Sectigo Public Server Authentication CA DV E36	Sectigo Public Server Authentication Root E46	22-Mar-2021	21-Mar-2036	https://crt.sh/?id=4267304693	P-256, ecdsa-with-SHA384	
Sectigo Public Server Authentication CA OV E36	Sectigo Public Server Authentication Root E46	22-Mar-2021	21-Mar-2036	https://crt.sh/?id=4267304689	P-256, ecdsa-with-SHA384	
Sectigo Public Server Authentication CA EV E36	Sectigo Public Server Authentication Root E46	22-Mar-2021	21-Mar-2036	https://crt.sh/?id=4267304692	P-256, ecdsa-with-SHA384	

**The AAA Certificate Services root uses SHA-1, as it is a ‘legacy’ root, used to provide compatibility with older devices. While SHA-1 has security vulnerabilities when used to create new signatures, a root using SHA-1 that is included in trust stores has no such security concerns. All signatures created by Sectigo use the SHA-2 family of hash algorithms.*

Removal timelines

Trust-store operators have begun to remove older roots from their stores. These roots will be removed from modern, updated browsers – where the newer roots are already embedded. Older platforms, software and devices that do not update automatically or frequently will still continue to trust these older roots.

AAA Certificate Services: **April 15th 2025 – removal of trust in Chrome and Mozilla.**
USERTrust RSA/ECC CAs: Likely to remove trust in Chrome **around June 15th 2026.** Mozilla will remove trust bits on **April 15th 2027.**

Note that for Chrome, unexpired certificates will continue to be valid until they expire. For Mozilla, unexpired certificates will immediately stop being trusted if no other paths are trusted. Root removal timelines and information is subject to change. Note also that the Mozilla root store is used by many other clients as a trust-store, including many major Linux distributions. These changes will impact those systems over time.

Root inclusion/ubiquity

Details of the minimum versions in which Sectigo roots were added to the most popular platforms and operating systems.
N/A means currently not yet included but still trusted through use of cross-certificates to the ‘older’ roots.

Root	Apple	Google	Microsoft	Mozilla	Oracle	Other
AAA Certificate Services	iOS 3 macOS 10.4	Android 2.3 Gingerbread	Windows XP and above	Firefox 1.0	JRE 1.5.0_08	
USERTrust ECC/RSA	iOS 10 macOS 10.12.1	Android 5.1 Chrome 38	Windows XP and above Windows Vista and above (ECC)	Firefox 36	JRE 8u51	Opera since 2012 360 Browser SE 10.1, Extreme Browser 11.0
Sectigo E/R46	iOS 17 macOS 14.4	Android 15 Chrome 121	Windows XP and above Windows Vista and above (ECC)	Firefox 117	N/A	