CA/BROWSER FORUM

CERTIFICATE VALIDITY UPDATES 2025

PKI SOLUTIONS

INTRODUCTION

Since the news about changes to certificate validity was released, we have received numerous questions and observed a significant amount of misinformation stemming from misunderstandings. In this white paper, our goal is to provide background information and guidance to support future planning. Specifically, we aim to clarify how the upcoming changes — shortening certificate validity periods — will impact public and private PKI-issued certificates differently.

Where The Guidelines and Updates Come From:

The Certification Authority Browser Forum (CA/Browser Forum) is a voluntary gathering of Certificate Issuers and suppliers of internet browser software and other applications that use certificates (Certificate Consumers).

TABLE OF CONTENTS

FAQs

QUESTION:

Will upcoming changes to certificate validity periods impact internal PKI issued certificates?

ANSWER:

No, the CAB Forum guidelines only impact certificates from publicly trusted certification authorities.

QUESTION:

Should organizations follow new certificate duration guidelines with their internal PKI?

ANSWER:

Most likely no. These new guidelines specifically target how browsers interact with publicly trusted certificates. PKI teams may want review their use cases, it is not necessary to apply the guidelines to all issued certificates.

IMPORTANT DATES FOR CHANGING CERTIFICATE VALIDITY PERIODS

Certificate operational periods and key pair usage periods:

- Subscriber Certificates issued before **March 15th, 2026** should not have a Validity Period greater than **397 days** and must not have a Validity Period greater than **398 days**.
- Subscriber Certificates issued on or after **March 15th, 2026** and before **March 15th, 2027** should not have a Validity Period greater than **199 days** and must not have a Validity Period greater than **200 days**.
- Subscriber Certificates issued on or after **March 15th, 2027** and before **March 15th, 2029** should not have a Validity Period greater than **99 days** and must not have a Validity Period greater than **100 days**.
- Subscriber Certificates issued on or after **March 15th, 2029** should not have a Validity Period greater than **46 days** and must not have a Validity Period greater than **47 days**.

REFERENCE FOR MAXIMUM VALIDITY PERIODS OF SUBSCRIBER CERTIFICATES*

Certificate issued on or after	Certificate issued before	Maximum Validity Period
Before March 15th, 2026	March 15th, 2026	398 days
March 15th, 2026	March 15th, 2027	200 days
March 15th, 2027	March 15th, 2029	100 days
March 15th, 2029		47 days

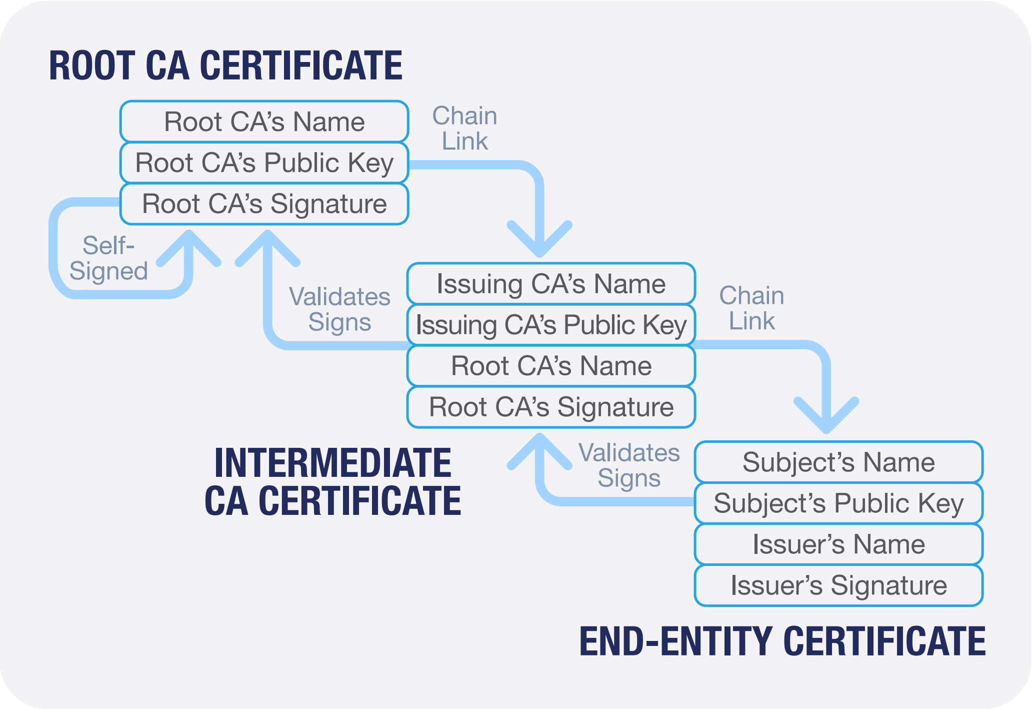
source: https://github.com/cabforum/servercert/releases/tag/BRs/v2.1.5

WHO MUST FOLLOW CAB FORUM RULES?

The simple answer is only public or third-party certificates must adhere to the CAB Forum rules and guidelines.

How do systems and browsers differentiate between Public and Internal CAs

Certificate chaining, or *chain building*, is the process by which systems or browsers validate who issued a certificate. To trust a certificate, each certificate in the “chain” is validated based on who signed or issued it. The process is considered successful when validation reaches a root certificate that is trusted. For a root certificate to be trusted, it must be present in a system or browser’s trusted root store.



ROOT CA CERTIFICATE

Root CA’s Name
Root CA’s Public Key
Root CA’s Signature

Chain Link

Self-Signed

Validates Signs

INTERMEDIATE CA CERTIFICATE

Issuing CA’s Name
Issuing CA’s Public Key
Root CA’s Name
Root CA’s Signature

Chain Link

Validates Signs

END-ENTITY CERTIFICATE

Subject’s Name
Subject’s Public Key
Issuer’s Name
Issuer’s Signature

Two Types of Root CA Trust Stores

Browsers and operating systems maintain two types of trusted root stores: the system-trusted root store and the updatable trusted root store. System-trusted root certificates follow strict guidelines to be included with the initial installation and are updated only by the operating system or browser vendor.

Organizations and end users can add private or internal PKI root certificates to the updatable trusted store; however, it is maintained independently from the system store. When a browser validates a certificate through the chaining process and the chain ends with a root certificate in the system-trusted root store, it must comply with the CAB Forum guidelines. Certificates that chain to a private or internal PKI root certificate added by an organization or end user are not subject to CAB Forum rules or guidelines.

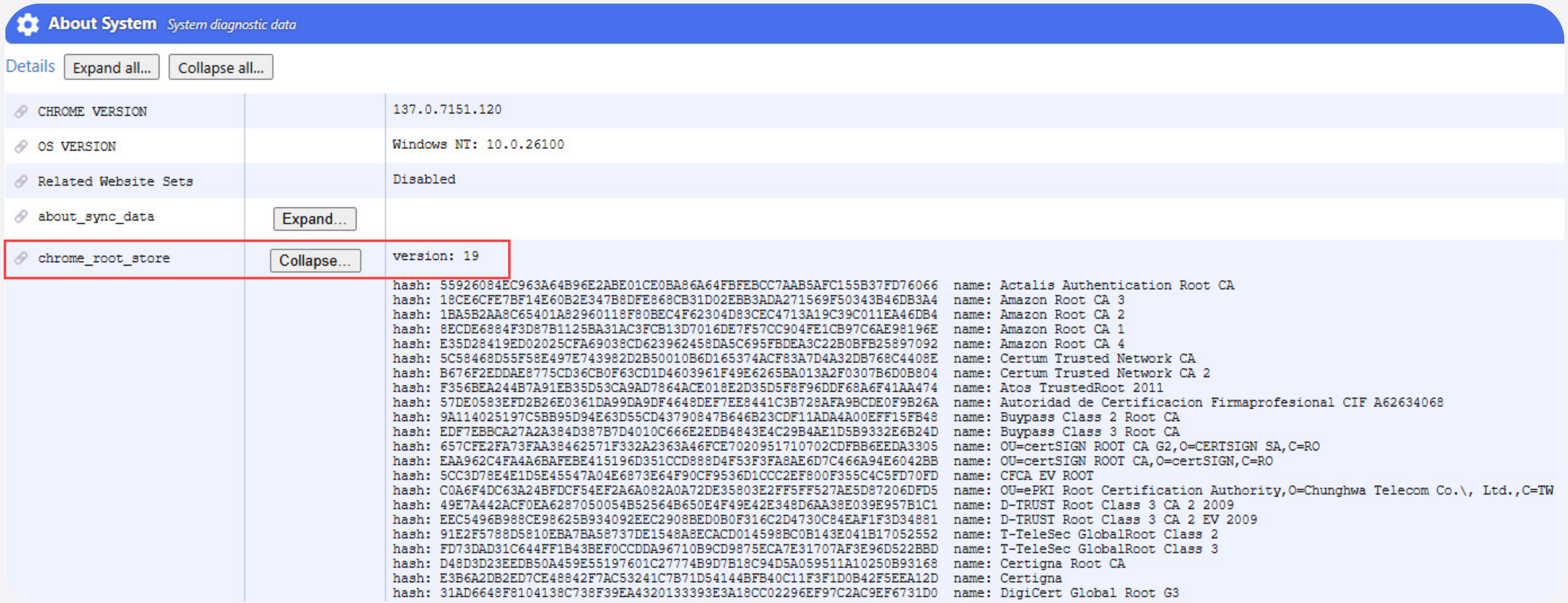
ROOT CA DETAILS AND PROGRAMS

In the past, Microsoft acted as a primary authority for vetting root certificates and was relied upon by many software vendors. More recently, companies and products have chosen to create their own root CA programs. This shift is significant because organizations may now need to track multiple lists of trusted root CA certificates.

Browsers

This isn't meant as an exhaustive list; however, it covers the majority of what our clients are using.

Chrome's list of trusted root CA certificates, currently **118** in the version **19** list can be found by entering: `chrome://system/#chrome_root_store` then `Expand`



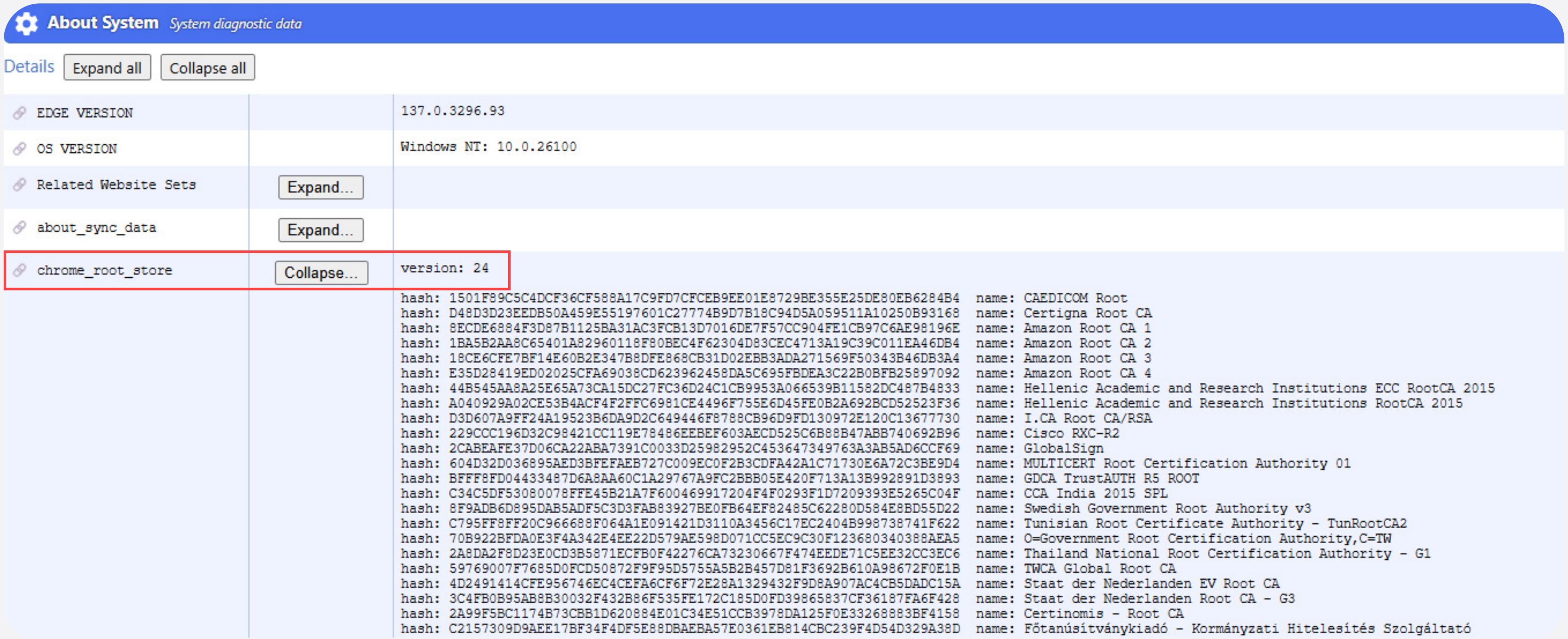
CHROME VERSION	137.0.7151.120
OS VERSION	Windows NT: 10.0.26100
Related Website Sets	Disabled
about_sync_data	
chrome_root_store	version: 19

```
hash: 55926084EC963A64B96E2ABE01CE0BA86A64FBFEBCC7AAB5AFC155B37FD76066  name: Actalis Authentication Root CA
hash: 18CE6CFE7BF14E60B2E347B8DFE868CB31D02EBB3ADA271569F50343B46DB3A4  name: Amazon Root CA 3
hash: 1BA5B2AA8C65401A82960118F80BEC4F62304D83CEC4713A19C39C011EA46DB4  name: Amazon Root CA 2
hash: 8ECDE6884F3D87B1125BA31AC3FCB13D7016DE7F57CC904FE1CB97C6AE98196E  name: Amazon Root CA 1
hash: E35D28419ED02025CFA69038CD623962458DA5C695FBDEA3C22B0BFB25897092  name: Amazon Root CA 4
hash: 5C58468D55F58E497E743982D2B50010B6D165374ACF83A7D4A32DB768C4408E  name: Certum Trusted Network CA
hash: B676F2EDDAE8775CD36CB0F63CD1D4603961F49E6265BA013A2F0307B6D0B804  name: Certum Trusted Network CA 2
hash: F356BEA244B7A91EB35D53CA9AD7864ACE018E2D35D5F8F96DDF68A6F41AA474  name: Atos TrustedRoot 2011
hash: 57DE0583EFD2B26E0361DA99DA9DF4648DEF7EE8441C3B728AFA9BCDE0F9B26A  name: Autoridad de Certificacion Firmaprofesional CIF A62634068
hash: 9A114025197C5BB95D94E63D55CD43790847B646B23CDF11ADA4A00EFF15FB48  name: Buypass Class 2 Root CA
hash: EDF7EBBCA27A2A384D387B7D4010C666E2EDB4843E4C29B4AE1D5B9332E6B24D  name: Buypass Class 3 Root CA
hash: 657CFE2FA73FAA38462571F332A2363A46FCE7020951710702CDFBB6EEDA3305  name: OU=certSIGN ROOT CA G2,O=CERTSIGN SA,C=RO
hash: EAA962C4FA4A6BAFEBE415196D351CCD888D4F53F3FA8AE6D7C466A94E6042BB  name: OU=certSIGN ROOT CA,O=certSIGN,C=RO
hash: 5CC3D78E4E1D5E45547A04E6873E64F90CF9536D1CCC2EF800F355C4C5FD70FD  name: CFCA EV ROOT
hash: C0A6F4DC63A24BFDCF54EF2A6A082A0A72DE35803E2FF5FF527AE5D87206DFD5  name: OU=ePKI Root Certification Authority,O=Chunghwa Telecom Co.\, Ltd.,C=TW
hash: 49E7A442ACF0EA6287050054B52564B650E4F49E42E348D6AA38E039E957B1C1  name: D-TRUST Root Class 3 CA 2 2009
hash: EEC5496B988CE98625B934092EEC2908BED0B0F316C2D4730C84EAF1F3D34881  name: D-TRUST Root Class 3 CA 2 EV 2009
hash: 91E2F5788D5810EBA7BA58737DE1548A8ECACD014598BC0B143E041B17052552  name: T-TeleSec GlobalRoot Class 2
hash: FD73DAD31C644FF1B43BEF0CCDDA96710B9CD9875ECA7E31707AF3E96D522BBD  name: T-TeleSec GlobalRoot Class 3
hash: D48D3D23EEDB50A459E55197601C27774B9D7B18C94D5A059511A10250B93168  name: Certigna Root CA
hash: E3B6A2DB2ED7CE48842F7AC53241C7B71D54144BFB40C11F3F1D0B42F5EEA12D  name: Certigna
hash: 31AD6648F8104138C738F39EA4320133393E3A18CC02296EF97C2AC9EF6731D0  name: DigiCert Global Root G3
```

**For educational purposes only. All trademarks used are the property of their respective owners, and their use here does not imply endorsement.*

ROOT CA DETAILS AND PROGRAMS cont.

Similarly, Edge trusted root list currently **249** in version **24** can be viewed here: `edge://system/#chrome_root_store` then `Expand`

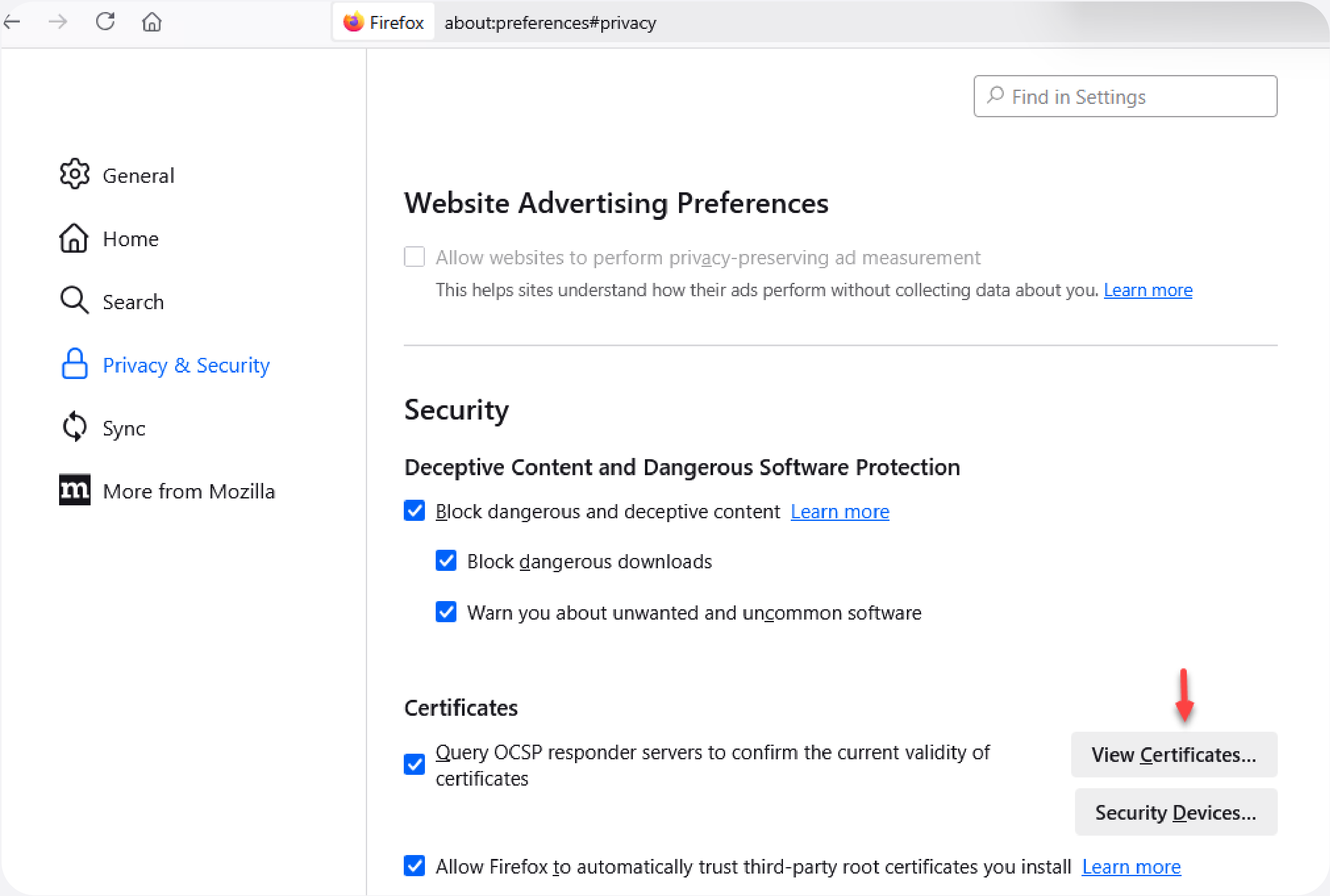


```
EDGE VERSION                    137.0.3296.93
OS VERSION                      Windows NT: 10.0.26100
Related Website Sets
about_sync_data
chrome_root_store               version: 24
hash: 1501F89C5C4DCF36CF588A17C9FD7CFCEB9EE01E8729BE355E25DE80EB6284B4  name: CAEDICOM Root
hash: D48D3D23EEDB50A459E55197601C27774B9D7B18C94D5A059511A10250B93168  name: Certigna Root CA
hash: 8ECDE6884F3D87B1125BA31AC3FCB13D7016DE7F57CC904FE1CB97C6AE98196E  name: Amazon Root CA 1
hash: 1BA5B2AA8C65401A82960118F80BEC4F62304D83CEC4713A19C39C011EA46DB4  name: Amazon Root CA 2
hash: 18CE6CFE7BF14E60B2E347B8DFE868CB31D02EBB3ADA271569F50343B46DB3A4  name: Amazon Root CA 3
hash: E35D28419ED02025CFA69038CD623962458DA5C695FBDEA3C22B0BFB25897092  name: Amazon Root CA 4
hash: 44B545AA8A25E65A73CA15DC27FC36D24C1CB9953A066539B11582DC487B4833  name: Hellenic Academic and Research Institutions ECC RootCA 2015
hash: A040929A02CE53B4ACF4F2FFC6981CE4496F755E6D45FE0B2A692BCD52523F36  name: Hellenic Academic and Research Institutions RootCA 2015
hash: D3D607A9FF24A19523B6DA9D2C649446F8788CB96D9FD130972E120C13677730  name: I.CA Root CA/RSA
hash: 229CCC196D32C98421CC119E78486EEBEF603AECD525C6B88B47ABB740692B96  name: Cisco RXC-R2
hash: 2CABEAFE37D06CA22ABA7391C0033D25982952C453647349763A3AB5AD6CCF69  name: GlobalSign
hash: 604D32D036895AED3BFEFAEB727C009EC0F2B3CDFA42A1C71730E6A72C3BE9D4  name: MULTICERT Root Certification Authority 01
hash: BFFF8FD04433487D6A8AA60C1A29767A9FC2BBB05E420F713A13B992891D3893  name: GDCA TrustAUTH R5 ROOT
hash: C34C5DF53080078FFE45B21A7F600469917204F4F0293F1D7209393E5265C04F  name: CCA India 2015 SPL
hash: 8F9ADB6D895DAB5ADF5C3D3FAB83927BE0FB64EF82485C62280D584E8BD55D22  name: Swedish Government Root Authority v3
hash: C795FF8FF20C966688F064A1E091421D3110A3456C17EC2404B998738741F622  name: Tunisian Root Certificate Authority - TunRootCA2
hash: 70B922BFDA0E3F4A342E4EE22D579AE598D071CC5EC9C30F123680340388AEA5  name: O=Government Root Certification Authority,C=TW
hash: 2A8DA2F8D23E0CD3B5871ECFB0F42276CA73230667F474EEDE71C5EE32CC3EC6  name: Thailand National Root Certification Authority - G1
hash: 59769007F7685D0FCD50872F9F95D5755A5B2B457D81F3692B610A98672F0E1B  name: TWCA Global Root CA
hash: 4D2491414CFE956746EC4CEFA6CF6F72E28A1329432F9D8A907AC4CB5DADC15A  name: Staat der Nederlanden EV Root CA
hash: 3C4FB0B95AB8B30032F432B86F535FE172C185D0FD39865837CF36187FA6F428  name: Staat der Nederlanden Root CA - G3
hash: 2A99F5BC1174B73CBB1D620884E01C34E51CCB3978DA125F0E33268883BF4158  name: Certinomis - Root CA
hash: C2157309D9AEE17BF34F4DF5E88DBAEBA57E0361EB814CBC239F4D54D329A38D  name: Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató
```

*For educational purposes only. All trademarks used are the property of their respective owners, and their use here does not imply endorsement.

ROOT CA DETAILS AND PROGRAMS cont.

Firefox certificates can be viewed by entering: `about:preferences#privacy` then select `View Certificates`



Website Advertising Preferences

□ Allow websites to perform privacy-preserving ad measurement
This helps sites understand how their ads perform without collecting data about you. Learn more

Security

Deceptive Content and Dangerous Software Protection

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon software

Certificates

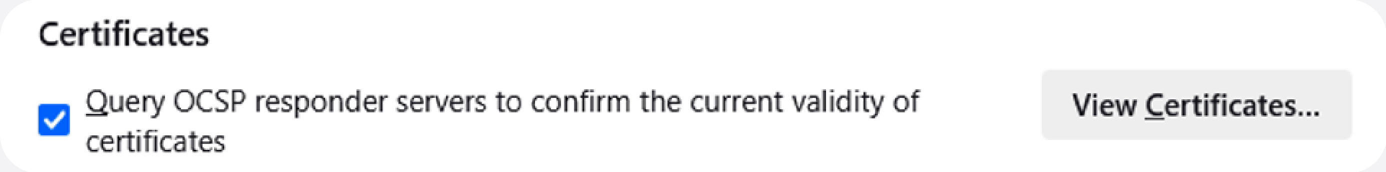
☑ Query OCSP responder servers to confirm the current validity of certificates

☑ Allow Firefox to automatically trust third-party root certificates you install Learn more

**For educational purposes only. All trademarks used are the property of their respective owners, and their use here does not imply endorsement.*

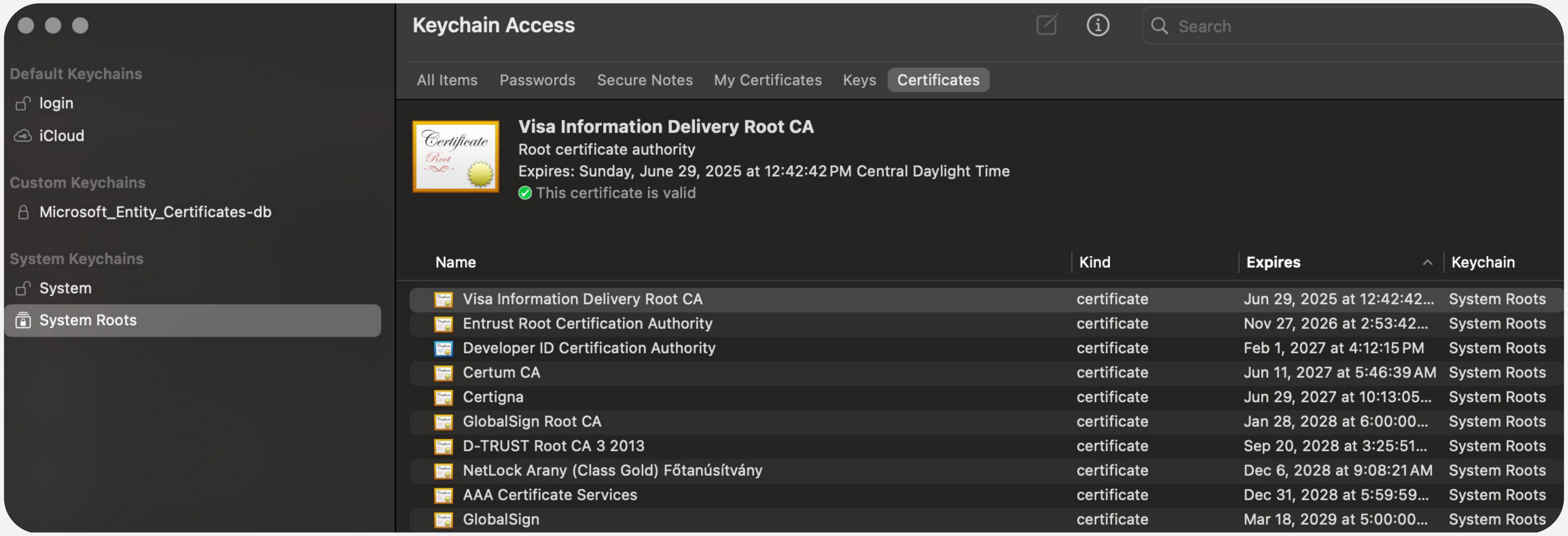
ROOT CA DETAILS AND PROGRAMS cont.

Unlike the other browsers, Safari relies on the root certificate store of the system it is running on. This can be viewed in the system Keychain on macOS, or in iOS under General > About > Certificate Trust Settings.



Certificates

☑ Query OCSP responder servers to confirm the current validity of certificates



Visa Information Delivery Root CA
Root certificate authority
Expires: Sunday, June 29, 2025 at 12:42:42 PM Central Daylight Time
✓ This certificate is valid

Name	Kind	Expires	Keychain
Visa Information Delivery Root CA	certificate	Jun 29, 2025 at 12:42:42...	System Roots
Entrust Root Certification Authority	certificate	Nov 27, 2026 at 2:53:42...	System Roots
Developer ID Certification Authority	certificate	Feb 1, 2027 at 4:12:15 PM	System Roots
Certum CA	certificate	Jun 11, 2027 at 5:46:39 AM	System Roots
Certigna	certificate	Jun 29, 2027 at 10:13:05...	System Roots
GlobalSign Root CA	certificate	Jan 28, 2028 at 6:00:00...	System Roots
D-TRUST Root CA 3 2013	certificate	Sep 20, 2028 at 3:25:51...	System Roots
NetLock Arany (Class Gold) Főtanúsítvány	certificate	Dec 6, 2028 at 9:08:21 AM	System Roots
AAA Certificate Services	certificate	Dec 31, 2028 at 5:59:59...	System Roots
GlobalSign	certificate	Mar 18, 2029 at 5:00:00...	System Roots

**For educational purposes only. All trademarks used are the property of their respective owners, and their use here does not imply endorsement.*

ROOT CA DETAILS AND PROGRAMS cont.

Operating Systems

Similarly to browsers, we are only covering the operating systems most of our clients use.

Windows

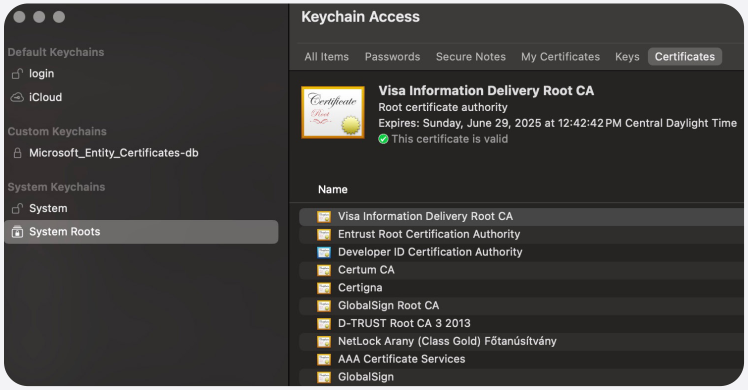
Microsoft Server & Clients

Windows operating systems and applications may or may not use the same root certificate store. However, when it comes to CAB Forum guidelines, the browser(s) are what matter. For example, a certificate issued by a public CA and used for secure LDAP would not be impacted by CAB Forum guidelines. In that case, the only consideration would be whether the certificate was issued by a trusted authority.

macOS / iOS

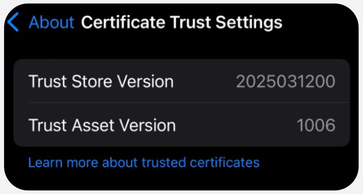
Apple macOS & iOS

Both macOS and iOS operate similarly when using the Safari browser. Safari utilizes the system's trust store, which contains Apple-managed trusted root certificates. When visiting a site with Safari, if the certificate does not chain to an existing root certificate in the Apple-managed trust store, CAB Forum guidelines will not be applied. Browsers other than Safari on macOS or iOS — such as Chrome, Edge, or Firefox — will use their own trusted root stores.



Visa Information Delivery Root CA
Root certificate authority
Expires: Sunday, June 29, 2025 at 12:42:42 PM Central Daylight Time
✓ This certificate is valid

Name
Visa Information Delivery Root CA
Entrust Root Certification Authority
Developer ID Certification Authority
Certum CA
Certigna
GlobalSign Root CA
D-TRUST Root CA 3 2013
NetLock Arany (Class Gold) Főtanúsítvány
AAA Certificate Services
GlobalSign



Trust Store Version	2025031200
Trust Asset Version	1006

Learn more about trusted certificates

**For educational purposes only. All trademarks used are the property of their respective owners, and their use here does not imply endorsement.*

SUMMARY

Hopefully, we have added clarity about which certificates the **CAB Forum** guidelines apply to, and when the changes can be expected. We also highlighted where the most common browsers and operating systems maintain their lists of trusted public root certificates.

This is an exciting time to be in the PKI space. Multiple changes are on the horizon, including Post-Quantum Cryptography (PQC), additional CAB Forum updates, operating system end-of-life events, and hardware security module upgrades, to name a few.

There's a smarter way forward — and we're here to show you how.

If you're looking to strengthen your PKI or certificate management strategy, let's connect and explore how our products and consulting services can support your goals.

✉ Let's Chat

PKI SOLUTIONS

Revolutionary Cybersecurity Monitoring

www.pkisolutions.com
(971) 231-5523
hello@pkisolutions.com