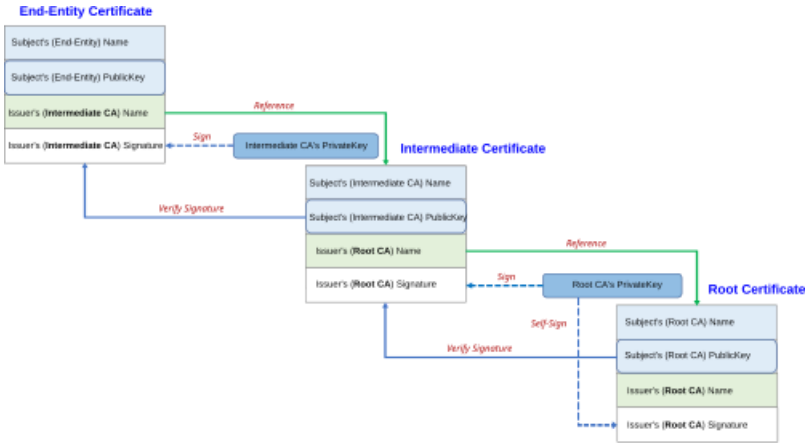
Root certificate

By Contributors to Wikimedia projects

Published: 2003-08-14 · Archived: 2026-04-05 17:25:50 UTC

From Wikipedia, the free encyclopedia



The role of root certificate as in the chain of trust.

In cryptography and computer security, a **root certificate** is a public key certificate that identifies a root certificate authority (CA).[1] Root certificates are self-signed (and it is possible for a certificate to have multiple trust paths, say if the certificate was issued by a root that was cross-signed) and form the basis of an X.509-based public key infrastructure (PKI). Either it has matched Authority Key Identifier with Subject Key Identifier, in some cases there is no Authority Key identifier, then Issuer string should match with Subject string (RFC 5280). For instance, the PKIs supporting HTTPS[2] for secure web browsing and electronic signature schemes depend on a set of root certificates.

A certificate authority can issue multiple certificates in the form of a tree structure. A root certificate is the top-most certificate of the tree, the private key which is used to "sign" other certificates. All certificates signed by the root certificate, with the "CA" field set to true, inherit the trustworthiness of the root certificate—a signature by a root certificate is somewhat analogous to "notarizing" identity in the physical world. Such a certificate is called an intermediate certificate or subordinate CA certificate. Certificates further down the tree also depend on the trustworthiness of the intermediates.

The root certificate is usually made trustworthy by some mechanism other than a certificate, such as by secure physical distribution. For example, some of the best-known root certificates are distributed in operating systems by their manufacturers. Microsoft distributes root certificates belonging to members of the Microsoft Root Certificate Program to Windows desktops and Windows Phone 8.[2] Apple distributes root certificates belonging to members of its own root program.

Incidents of root certificate misuse

[edit]

DigiNotar hack of 2011

[edit]

In 2011, the Dutch certificate authority DigiNotar suffered a security breach. This led to the issuing of various fraudulent certificates, which was among others abused to target Iranian Gmail users. The trust in DigiNotar certificates was retracted and the operational management of the company was taken over by the Dutch government.

China Internet Network Information Center (CNNIC) issuance of fake certificates

[edit]

Example of a DigiCert root certificate

In 2009, an employee of the China Internet Network Information Center (CNNIC) applied to Mozilla to add CNNIC to Mozilla's root certificate list[3] and was approved. Later, Microsoft also added CNNIC to the root certificate list of Windows.

In 2015, many users chose not to trust the digital certificates issued by CNNIC because an intermediate CA issued by CNNIC was found to have issued fake certificates for Google domain names[4] and raised concerns about CNNIC's abuse of certificate issuing power.[5]

On April 2, 2015, Google announced that it no longer recognized the electronic certificate issued by CNNIC.[6][7][8] On April 4, following Google, Mozilla also announced that it no longer recognized the electronic certificate issued by CNNIC.[9][10]

WoSign and StartCom: Issuing fake and backdated certificates

[edit]

In 2016, WoSign, China's largest CA certificate issuer owned by Qihoo 360[11] and its Israeli subsidiary StartCom, were denied recognition of their certificates by Google. Microsoft removed the relevant certificates in 2017.[12]

WoSign and StartCom issued hundreds of certificates with the same serial number in just five days, as well as issuing backdated certificates.[13] In 2016, a system administrator in Florida was able to get WoSign and StartCom to issue fake certificates for multiple GitHub domains.[14]

- Online Certificate Status Protocol (OCSP)
- Superfish
- SHA-1
- Timestamp
- Verisign
- Google and Symantec clash on website security checks

1. ^ *"What Are CA Certificates?"*. *Microsoft TechNet*. *2003-03-28.*
2. ^ Jump up to: *a b* *"Windows and Windows Phone 8 SSL Root Certificate Program (Member CAs)"*. *Microsoft TechNet*. *October 2014.*
3. ^ *"476766 - Add China Internet Network Information Center (CNNIC) CA Root Certificate"*. *bugzilla.mozilla.org. Archived from the original on 2020-02-22. Retrieved 2020-01-03.*
4. ^ *"CNNIC发行的中级CA发行了Google的假证书"*. *solidot. 2015-03-24. Archived from the original on 2015-03-26. Retrieved 2015-03-24.*
5. ^ *"最危险的互联网漏洞正在逼近"*. *Archived from the original on 2015-11-21. Retrieved 2015-03-26.*
6. ^ *"Google Bans China's Website Certificate Authority After Security Breach"*. *No. April 2, 2015. Extra Crunch.*
7. ^ *"谷歌不再承認中國CNNIC頒發的信任證書"*. *華爾街日報. 2015-04-03. Retrieved 2015-04-03.*
8. ^ *"谷歌不再信任中国CNNIC 的网站信任证书"*. *美國之音. 2015-04-03. Retrieved 2015-04-03.*
9. ^ *"Google and Mozilla decide to ban Chinese certificate authority CNNIC from Chrome and Firefox"*. *VentureBeat. April 2, 2015.*
10. ^ *"Mozilla紧随谷歌 拒绝承认中国安全证书"*. *美國之音. 2015-04-04. Retrieved 2015-04-04.*
11. ^ *"谷歌宣布开始全面封杀使用沃通CA证书网站，信誉破产的恶果 - 超能网"*. *www.expreview.com. Retrieved 2020-01-03.*
12. ^ *Microsoft Defender Security Research Team (2017-08-08). "Microsoft to remove WoSign and StartCom certificates in Windows 10". Microsoft.*
13. ^ *"CA:WoSign Issues - MozillaWiki"*. *wiki.mozilla.org. Retrieved 2020-01-03.*
14. ^ *Stephen Schrauger. "The story of how WoSign gave me an SSL certificate for GitHub.com". Schrauger.com.*
