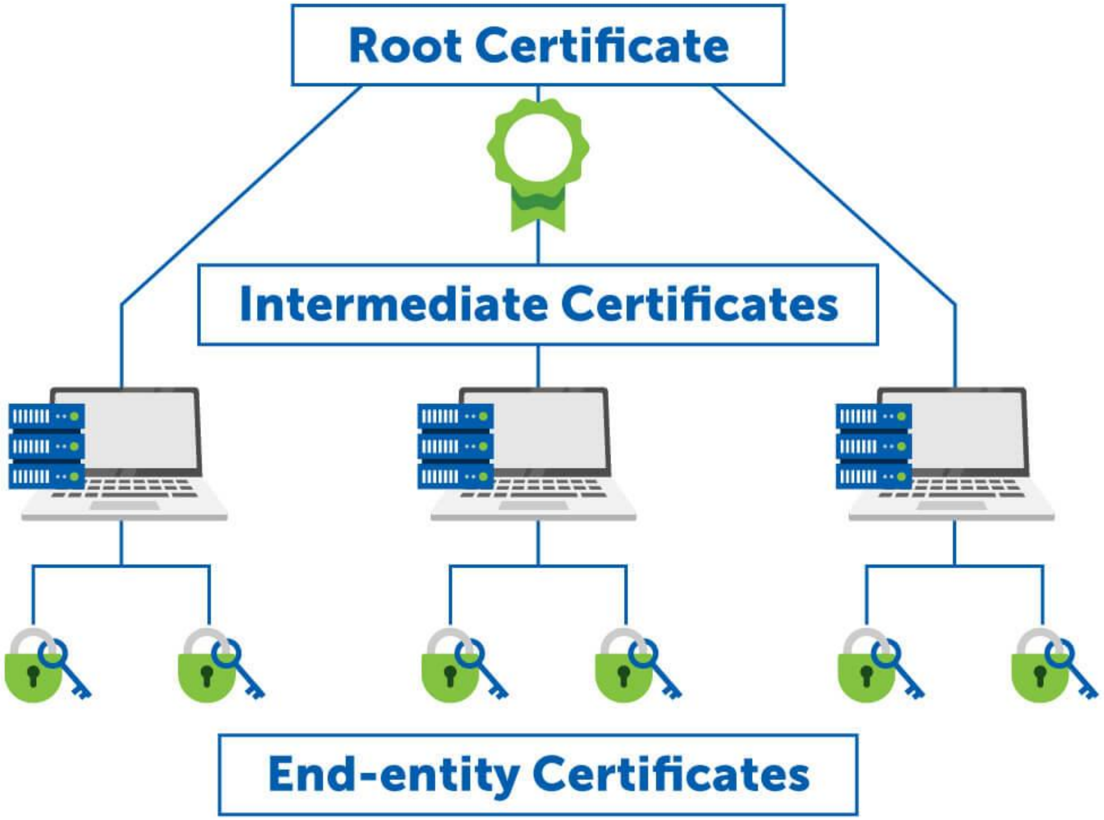
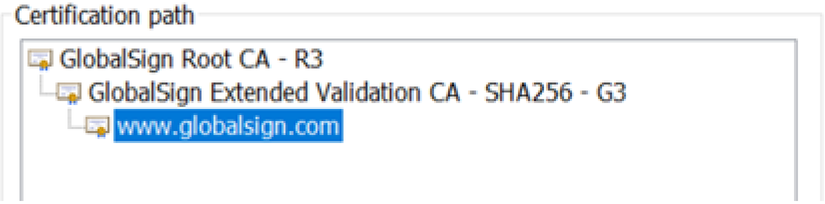
อัพเดทความรู้เรื่อง TLS (SSL) CERTIFICATE กัน

อัพเดทความรู้เรื่อง TLS (SSL) CERTIFICATE กัน

- เล่ากรณีศึกษาเกี่ยวกับการออก TLS Certificate แบบ EV (Extended Validation) ที่ทำให้เข้าใจผิด
- เมื่อต้นปีกูเกิลเสนอจำกัดอายุ TLS Certificate เหลือ 90 วัน จะเตรียมตัวรับมืออย่างไร
- ทำความรู้จัก ACME Protocol เพื่อทำการขอ TLS Certificate แบบอัตโนมัติ

ROOT CA CERTIFICATE

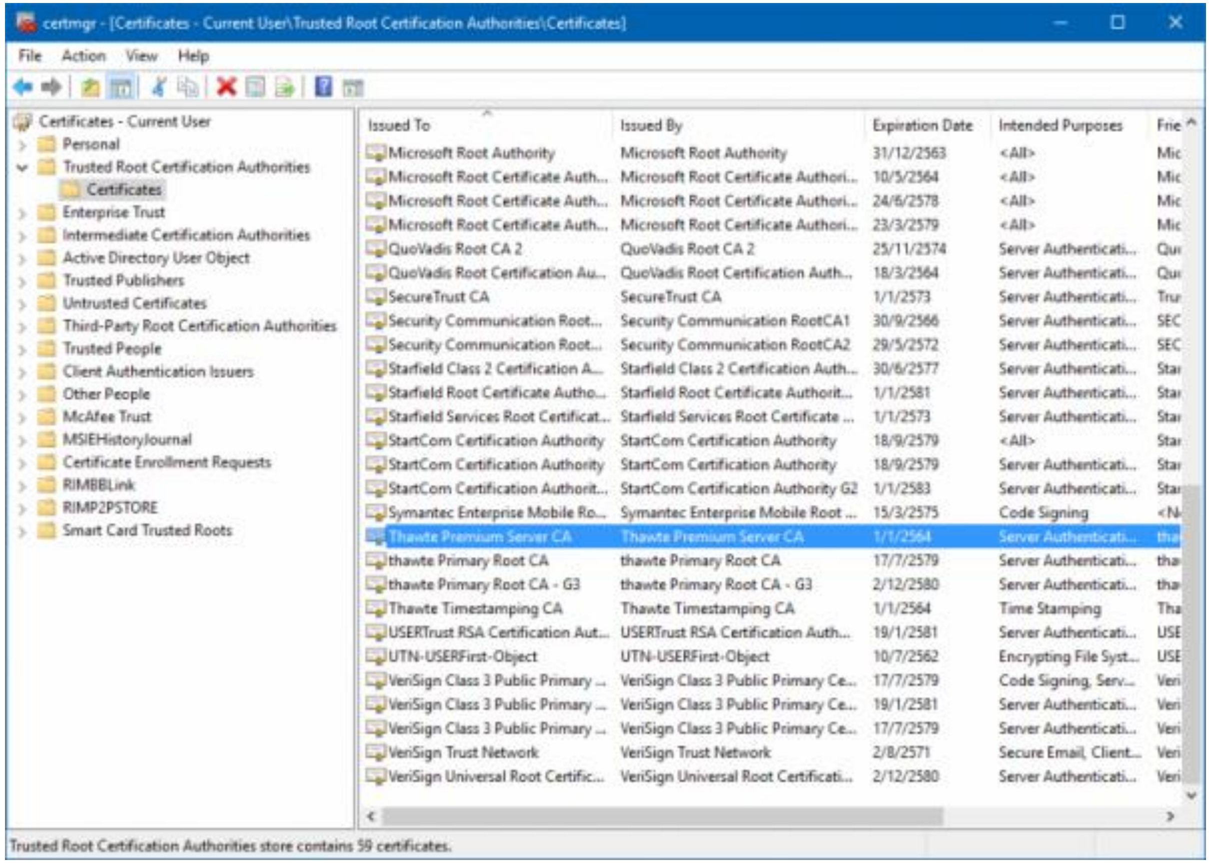




GlobalSign Root CA - R3
GlobalSign Extended Validation CA - SHA256 - G3
www.globalsign.com

https://www.globalsign.com/en-sg/blog/what-should-i-do-if-my-cas-root-certificate-has-expired-experts-advice

TRUSTED ROOT CERTIFICATION AUTHORITIES IN WINDOWS



certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]

- Certificates - Current User
  - Personal
  - Trusted Root Certification Authorities
    - Certificates
  - Enterprise Trust
  - Intermediate Certification Authorities
  - Active Directory User Object
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification Authorities
  - Trusted People
  - Client Authentication Issuers
  - Other People
  - McAfee Trust
  - MSIEHistoryJournal
  - Certificate Enrollment Requests
  - RIMBBLink
  - RIMP2PSTORE
  - Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Frie
Microsoft Root Authority	Microsoft Root Authority	31/12/2563	<All>	Mic
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	10/5/2564	<All>	Mic
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	24/6/2578	<All>	Mic
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	23/3/2579	<All>	Mic
QuoVadis Root CA 2	QuoVadis Root CA 2	25/11/2574	Server Authenticati...	Qu
QuoVadis Root Certification Au...	QuoVadis Root Certification Auth...	18/3/2564	Server Authenticati...	Qu
SecureTrust CA	SecureTrust CA	1/1/2573	Server Authenticati...	Tru
Security Communication Root...	Security Communication RootCA1	30/9/2566	Server Authenticati...	SEC
Security Communication Root...	Security Communication RootCA2	29/5/2572	Server Authenticati...	SEC
Starfield Class 2 Certification A...	Starfield Class 2 Certification Auth...	30/6/2577	Server Authenticati...	Star
Starfield Root Certificate Autho...	Starfield Root Certificate Authorit...	1/1/2581	Server Authenticati...	Star
Starfield Services Root Certificat...	Starfield Services Root Certificate ...	1/1/2573	Server Authenticati...	Star
StartCom Certification Authority	StartCom Certification Authority	18/9/2579	<All>	Star
StartCom Certification Authority	StartCom Certification Authority	18/9/2579	Server Authenticati...	Star
StartCom Certification Authorit...	StartCom Certification Authority G2	1/1/2583	Server Authenticati...	Star
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	15/3/2575	Code Signing	<N
Thawte Premium Server CA	Thawte Premium Server CA	1/1/2564	Server Authenticati...	tha
thawte Primary Root CA	thawte Primary Root CA	17/7/2579	Server Authenticati...	tha
thawte Primary Root CA - G3	thawte Primary Root CA - G3	2/12/2580	Server Authenticati...	tha
Thawte Timestamping CA	Thawte Timestamping CA	1/1/2564	Time Stamping	Tha
USERTrust RSA Certification Aut...	USERTrust RSA Certification Auth...	19/1/2581	Server Authenticati...	USE
UTN-USERFirst-Object	UTN-USERFirst-Object	10/7/2562	Encrypting File Syst...	USE
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	17/7/2579	Code Signing, Serv...	Veri
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	19/1/2581	Server Authenticati...	Veri
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	17/7/2579	Server Authenticati...	Veri
VeriSign Trust Network	VeriSign Trust Network	2/8/2571	Secure Email, Client...	Veri
VeriSign Universal Root Certific...	VeriSign Universal Root Certificati...	2/12/2580	Server Authenticati...	Veri

Trusted Root Certification Authorities store contains 59 certificates.

DIFFERENCE DV, OV AND EV CERTIFICATES

1. Validation Levels
2. Warranty
3. Trust Site Seal

DIFFERENCE DV, OV AND EV CERTIFICATES

Domain Validation Certificates (DV)

- **Domain Verification**
  1. E-mail
  2. DNS
  3. HTTP

Organization Validated Certificates (OV)

provide business identity confirmation

- **Verification Organization**
  - Legal existence checked via public government database using company name or unique identification number (registration number) OR via verified public 3rd party databases
  - Company verification with LEI code
  - Company can be verified using one of the documents like Articles of Incorporation, Government Issued Business License, copy of a recent company bank statement, copy of a recent company phone bill, copy of a recent major utility bill of the company (i.e., power bill, water bill, etc.).
- **Domain Verification**
- **Verification Call**

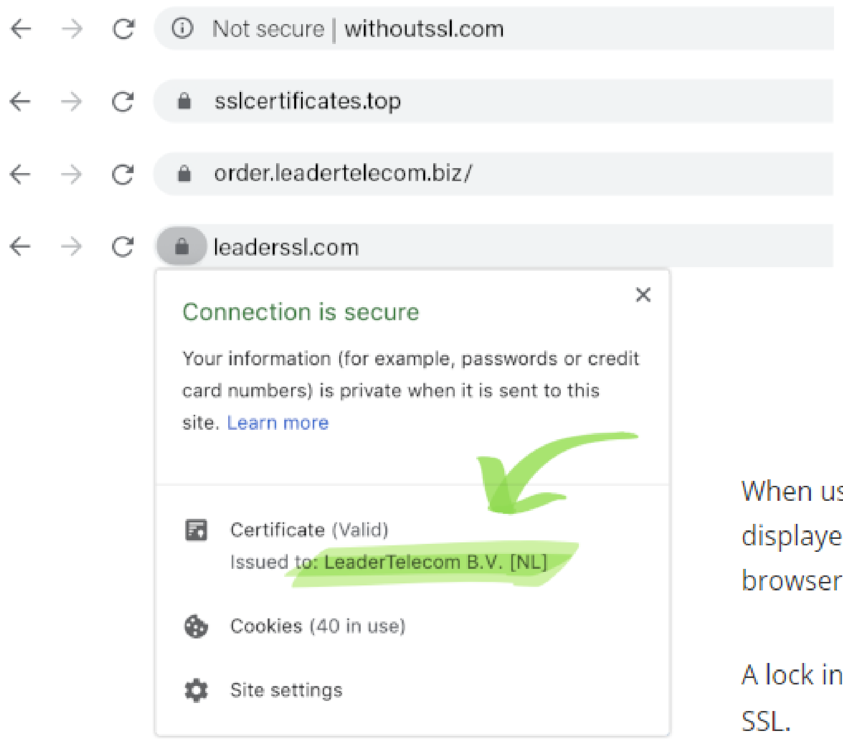
Extended Validation Certificate (EV)

provide **more** business identity confirmation

- Agreement signing and Lawyer's letter
  1. EV Certificate Request
  2. EV SSL Subscriber Agreement
- **Verification Organization**
- **Domain Verification**
- **Verification Call**
- EV SSL CA Approver's Authentication
- Other Documents

DIFFERENCE BETWEEN DV, OV AND EV CERTIFICATES

Display in the browser address bar



Not secure | withoutssl.com

sslcertificates.top

order.leadertelecom.biz/

leaderssl.com

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: LeaderTelecom B.V. [NL]

Cookies (40 in use)

Site settings

without SSL certificate

DV SSL (Domain Validation)

OV SSL (Organisation Validation)

EV SSL (Extended Validation)

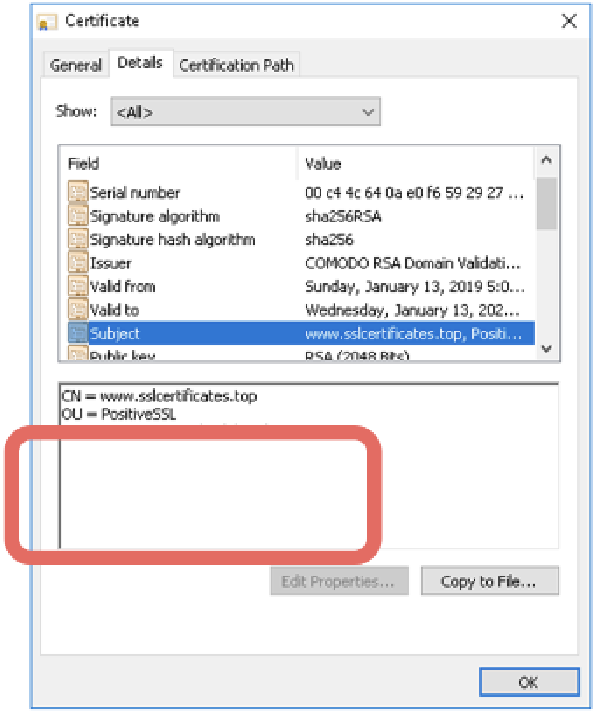
When using EV certificates, the name of your organisation is displayed in the address bar of the browser. In addition, in some browsers, the address bar is colored green.

A lock in the browser bar is displayed when using all three types of SSL.

https://www.leaderssl.com/certificate_type_dv_ov_ev

DIFFERENCE BETWEEN DV, OV AND EV CERTIFICATES

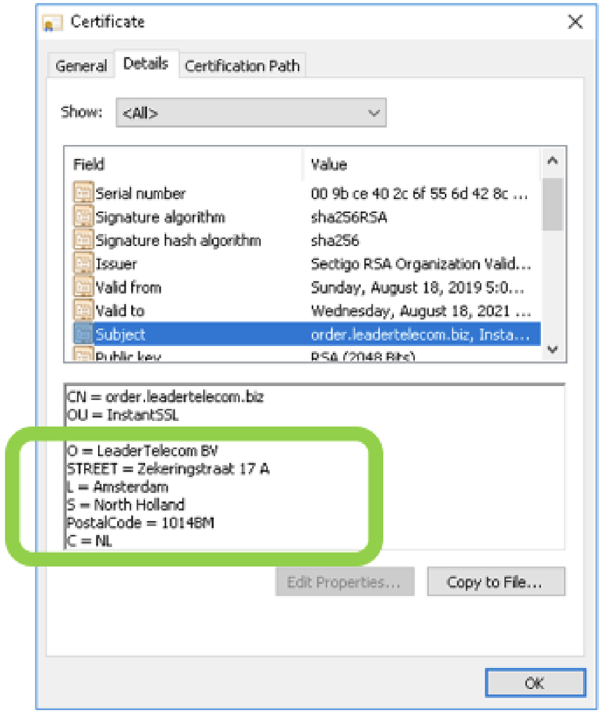
DV SSL
(Domain Validation)



Field	Value
Serial number	00 c4 4c 64 0a e0 f6 59 29 27 ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	COMODO RSA Domain Validati...
Valid from	Sunday, January 13, 2019 5:0...
Valid to	Wednesday, January 13, 202...
Subject	www.sslcertificates.top, Positi...
Public key	RSA (2048 Bits)

CN = www.sslcertificates.top
OU = PositiveSSL

OV SSL
(Organisation Validation)

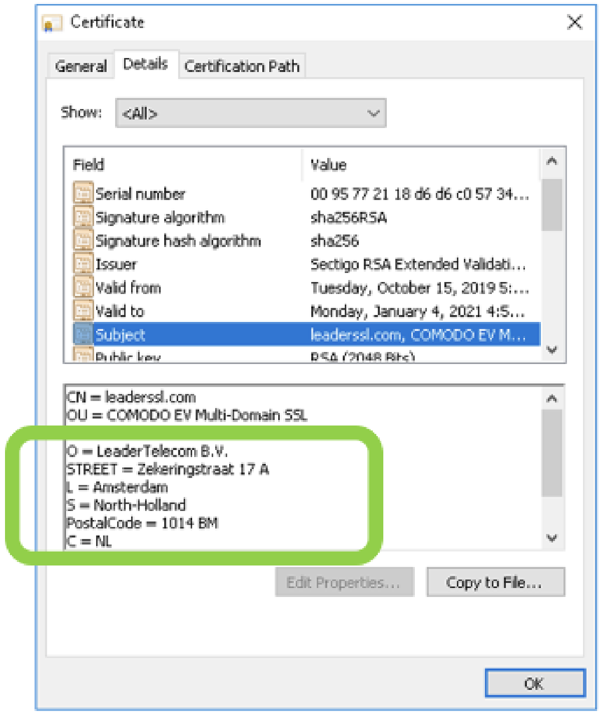


Field	Value
Serial number	00 9b ce 40 2c 6f 55 6d 42 8c ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Sectigo RSA Organization Valid...
Valid from	Sunday, August 18, 2019 5:0...
Valid to	Wednesday, August 18, 2021 ...
Subject	order.leadertelecom.biz, Insta...
Public key	RSA (2048 Bits)

CN = order.leadertelecom.biz
OU = InstantSSL

O = LeaderTelecom BV
STREET = Zekeringstraat 17 A
L = Amsterdam
S = North Holland
PostalCode = 1014BM
C = NL

EV SSL
(Extended Validation)



Field	Value
Serial number	00 95 77 21 18 d6 d6 c0 57 34...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Sectigo RSA Extended Validati...
Valid from	Tuesday, October 15, 2019 5:...
Valid to	Monday, January 4, 2021 4:5...
Subject	leaderssl.com, COMODO EV M...
Public key	RSA (2048 Bits)

CN = leaderssl.com
OU = COMODO EV Multi-Domain SSL

O = LeaderTelecom B.V.
STREET = Zekeringstraat 17 A
L = Amsterdam
S = North-Holland
PostalCode = 1014 BM
C = NL

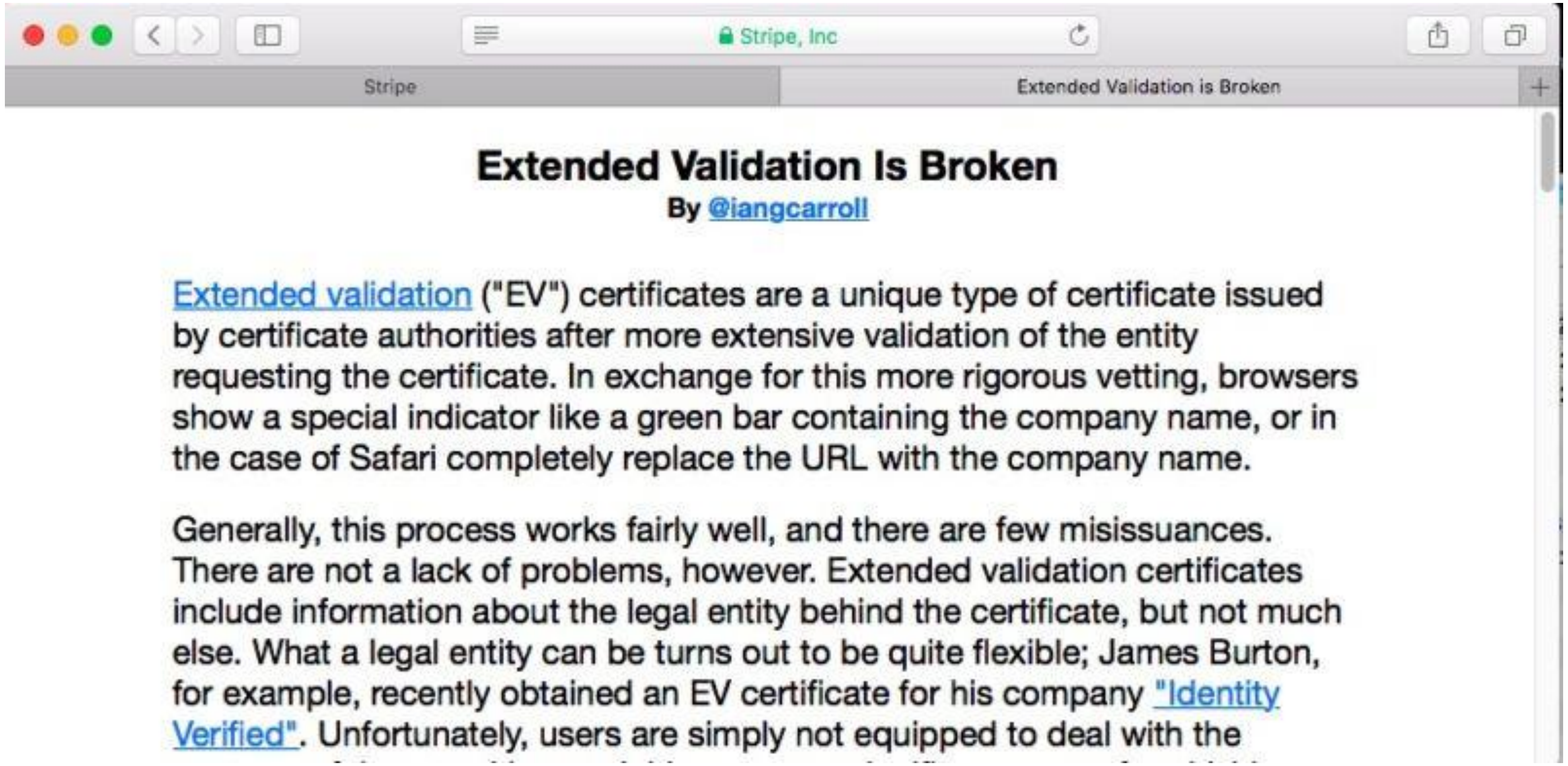
https://www.leaderssl.com/certificate_type_dv_ov_ev

เล่ากรณีศึกษาเกี่ยวกับการออก TLS CERTIFICATE แบบ EV (EXTENDED VALIDATION) ที่ทำให้เข้าใจผิด

Researcher Ian Carroll filed the necessary paperwork to incorporate a business called Stripe Inc. He then used the legal entity to apply for an EV certificate to authenticate the Web page https://stripe.ian.sh/. When viewed in the address bar, the page looks eerily similar to https://stripe.com/, the online payments service that also authenticates itself using an EV certificate issued to Stripe Inc.

https://arstechnica.com/information-technology/2017/12/nope-this-isnt-the-https-validated-stripe-website-you-think-it-is/

https://stripe.ian.sh



Extended Validation Is Broken

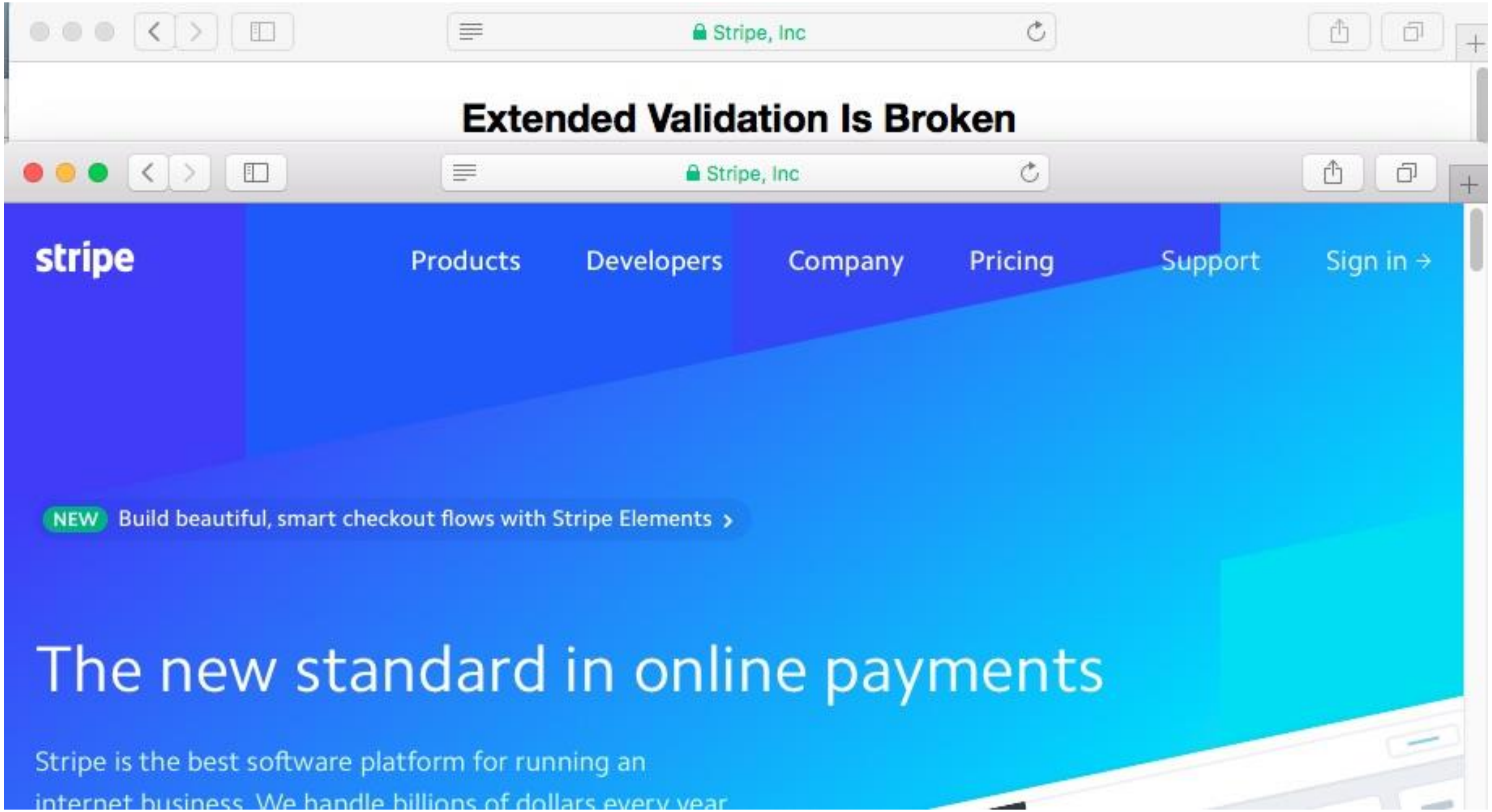
By @iangcarroll

Extended validation ("EV") certificates are a unique type of certificate issued by certificate authorities after more extensive validation of the entity requesting the certificate. In exchange for this more rigorous vetting, browsers show a special indicator like a green bar containing the company name, or in the case of Safari completely replace the URL with the company name.

Generally, this process works fairly well, and there are few misissuances. There are not a lack of problems, however. Extended validation certificates include information about the legal entity behind the certificate, but not much else. What a legal entity can be turns out to be quite flexible; James Burton, for example, recently obtained an EV certificate for his company "Identity Verified". Unfortunately, users are simply not equipped to deal with the

https://arstechnica.com/information-technology/2017/12/nope-this-isnt-the-https-validated-stripe-website-you-think-it-is/

stripe.com vs stripe.ian.sh



Extended Validation Is Broken

Build beautiful, smart checkout flows with Stripe Elements ›

The new standard in online payments

Stripe is the best software platform for running an internet business. We handle billions of dollars every year

https://arstechnica.com/information-technology/2017/12/nope-this-isnt-the-https-validated-stripe-website-you-think-it-is/

เมื่อต้นปีกูเกิลเสนอจำกัดอายุ TLS CERTIFICATE เหลือ 90 วัน จะเตรียมตัวรับมืออย่างไร

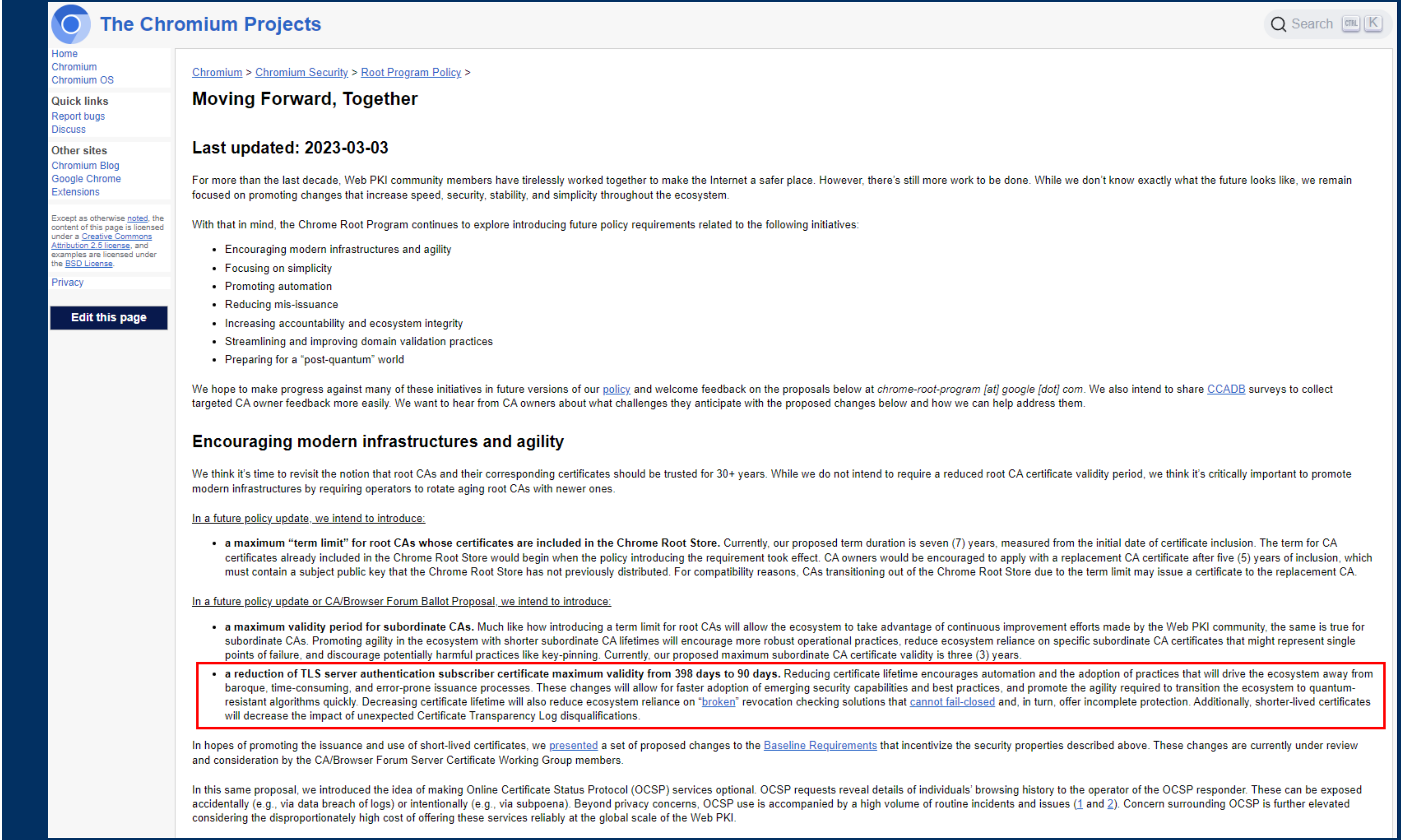
ที่มาที่ไป

ก่อนปี 2017 อายุใบรับรองดิจิตอลมีอายุได้มากถึง 5 ปี

13/02/2017 - กูเกิลเสนอจำกัดอายุใบรับรองดิจิตอลเหลือ 398 วัน แม้โหวตไม่ผ่านก็จะบังคับใน Chrome

31/08/2020 - วันสุดท้ายของการออกใบรับรองเข้ารหัสเว็บอายุ 2 ปี จากนี้ไปใบรับรองอายุไม่เกิน 397 วัน

03/03/2023 - กูเกิลเสนอจำกัดอายุใบรับรองดิจิตอลเหลือ 90 วัน และคาดว่าจะมีผลภายในปี 2025



Chromium > Chromium Security > Root Program Policy >

Moving Forward, Together

Last updated: 2023-03-03

For more than the last decade, Web PKI community members have tirelessly worked together to make the Internet a safer place. However, there's still more work to be done. While we don't know exactly what the future looks like, we remain focused on promoting changes that increase speed, security, stability, and simplicity throughout the ecosystem.

With that in mind, the Chrome Root Program continues to explore introducing future policy requirements related to the following initiatives:

- Encouraging modern infrastructures and agility
- Focusing on simplicity
- Promoting automation
- Reducing mis-issuance
- Increasing accountability and ecosystem integrity
- Streamlining and improving domain validation practices
- Preparing for a "post-quantum" world

We hope to make progress against many of these initiatives in future versions of our policy and welcome feedback on the proposals below at *chrome-root-program [at] google [dot] com*. We also intend to share CCADB surveys to collect targeted CA owner feedback more easily. We want to hear from CA owners about what challenges they anticipate with the proposed changes below and how we can help address them.

Encouraging modern infrastructures and agility

We think it's time to revisit the notion that root CAs and their corresponding certificates should be trusted for 30+ years. While we do not intend to require a reduced root CA certificate validity period, we think it's critically important to promote modern infrastructures by requiring operators to rotate aging root CAs with newer ones.

In a future policy update, we intend to introduce:

- **a maximum "term limit" for root CAs whose certificates are included in the Chrome Root Store.** Currently, our proposed term duration is seven (7) years, measured from the initial date of certificate inclusion. The term for CA certificates already included in the Chrome Root Store would begin when the policy introducing the requirement took effect. CA owners would be encouraged to apply with a replacement CA certificate after five (5) years of inclusion, which must contain a subject public key that the Chrome Root Store has not previously distributed. For compatibility reasons, CAs transitioning out of the Chrome Root Store due to the term limit may issue a certificate to the replacement CA.

In a future policy update or CA/Browser Forum Ballot Proposal, we intend to introduce:

- **a maximum validity period for subordinate CAs.** Much like how introducing a term limit for root CAs will allow the ecosystem to take advantage of continuous improvement efforts made by the Web PKI community, the same is true for subordinate CAs. Promoting agility in the ecosystem with shorter subordinate CA lifetimes will encourage more robust operational practices, reduce ecosystem reliance on specific subordinate CA certificates that might represent single points of failure, and discourage potentially harmful practices like key-pinning. Currently, our proposed maximum subordinate CA certificate validity is three (3) years.
- **a reduction of TLS server authentication subscriber certificate maximum validity from 398 days to 90 days.** Reducing certificate lifetime encourages automation and the adoption of practices that will drive the ecosystem away from baroque, time-consuming, and error-prone issuance processes. These changes will allow for faster adoption of emerging security capabilities and best practices, and promote the agility required to transition the ecosystem to quantum-resistant algorithms quickly. Decreasing certificate lifetime will also reduce ecosystem reliance on "broken" revocation checking solutions that cannot fail-closed and, in turn, offer incomplete protection. Additionally, shorter-lived certificates will decrease the impact of unexpected Certificate Transparency Log disqualifications.

In hopes of promoting the issuance and use of short-lived certificates, we presented a set of proposed changes to the Baseline Requirements that incentivize the security properties described above. These changes are currently under review and consideration by the CA/Browser Forum Server Certificate Working Group members.

In this same proposal, we introduced the idea of making Online Certificate Status Protocol (OCSP) services optional. OCSP requests reveal details of individuals' browsing history to the operator of the OCSP responder. These can be exposed accidentally (e.g., via data breach of logs) or intentionally (e.g., via subpoena). Beyond privacy concerns, OCSP use is accompanied by a high volume of routine incidents and issues (1 and 2). Concern surrounding OCSP is further elevated considering the disproportionately high cost of offering these services reliably at the global scale of the Web PKI.

https://www.chromium.org/Home/chromium-security/root-ca-policy/moving-forward-together/

A REDUCTION OF TLS SERVER AUTHENTICATION SUBSCRIBER CERTIFICATE MAXIMUM VALIDITY FROM 398 DAYS TO 90 DAYS.

Reducing certificate lifetime encourages automation and the adoption of practices that will drive the ecosystem away from baroque, time-consuming, and error-prone issuance processes. These changes will allow for faster adoption of emerging security capabilities and best practices, and promote the agility required to transition the ecosystem to quantum-resistant algorithms quickly. Decreasing certificate lifetime will also reduce ecosystem reliance on “broken” revocation checking solutions that cannot fail-closed and, in turn, offer incomplete protection. Additionally, shorter-lived certificates will decrease the impact of unexpected Certificate Transparency Log disqualifications.

https://www.chromium.org/Home/chromium-security/root-ca-policy/moving-forward-together/

Google’s Moving Forward Together Proposals for Root CA Policy: Rotating ICAs More Frequently | DigiCert

https://www.digicert.com/blog/googles-moving-forward-together-proposals-for-root-ca-policy

Chrome’s Proposed 90-Day Certificate Validity Period: What You Need to Know | DigiCert

https://www.digicert.com/blog/chromes-proposed-90-day-certificate-validity-period

Google's 90 Day SSL Certificate Validity Requires Automation - GlobalSign

https://www.globalsign.com/en/blog/google-90-day-certificate-validity-requires-automation

Google Announces Intentions to Limit TLS Certificates to 90 Days: Why Automated CLM is Crucial

https://www.sectigo.com/resource-library/google-announces-intentions-to-limit-tls-certificates-to-90-days-why-automated-clm-is-crucial

AUTOMATED CERTIFICATE MANAGEMENT ENVIRONMENT

ทำความรู้จัก ACME PROTOCOL เพื่อทำการขอ TLS CERTIFICATE แบบอัตโนมัติ

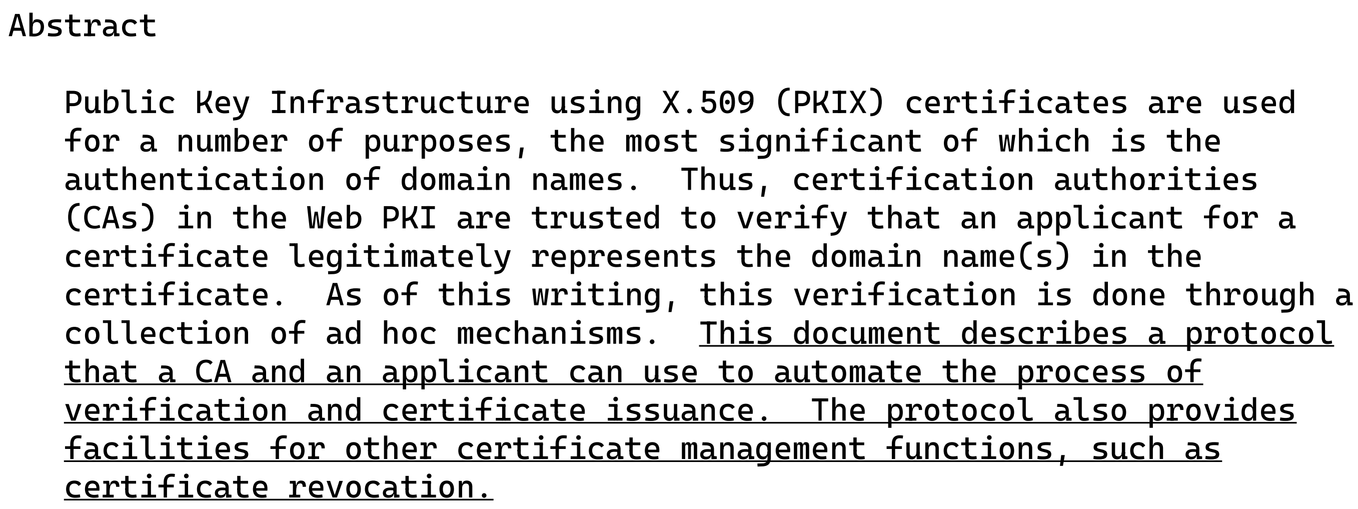
AUTOMATIC CERTIFICATE MANAGEMENT ENVIRONMENT (ACME)

RFC8555 - The protocol was originally designed by the Internet Security Research Group (ISRG)

https://datatracker.ietf.org/doc/html/rfc8555

ACME v1 was released on April 12, 2016 (deprecated)

ACME v2 was released on March 13, 2018.



Abstract

Public Key Infrastructure using X.509 (PKIX) certificates are used for a number of purposes, the most significant of which is the authentication of domain names. Thus, certification authorities (CAs) in the Web PKI are trusted to verify that an applicant for a certificate legitimately represents the domain name(s) in the certificate. As of this writing, this verification is done through a collection of ad hoc mechanisms. This document describes a protocol that a CA and an applicant can use to automate the process of verification and certificate issuance. The protocol also provides facilities for other certificate management functions, such as certificate revocation.

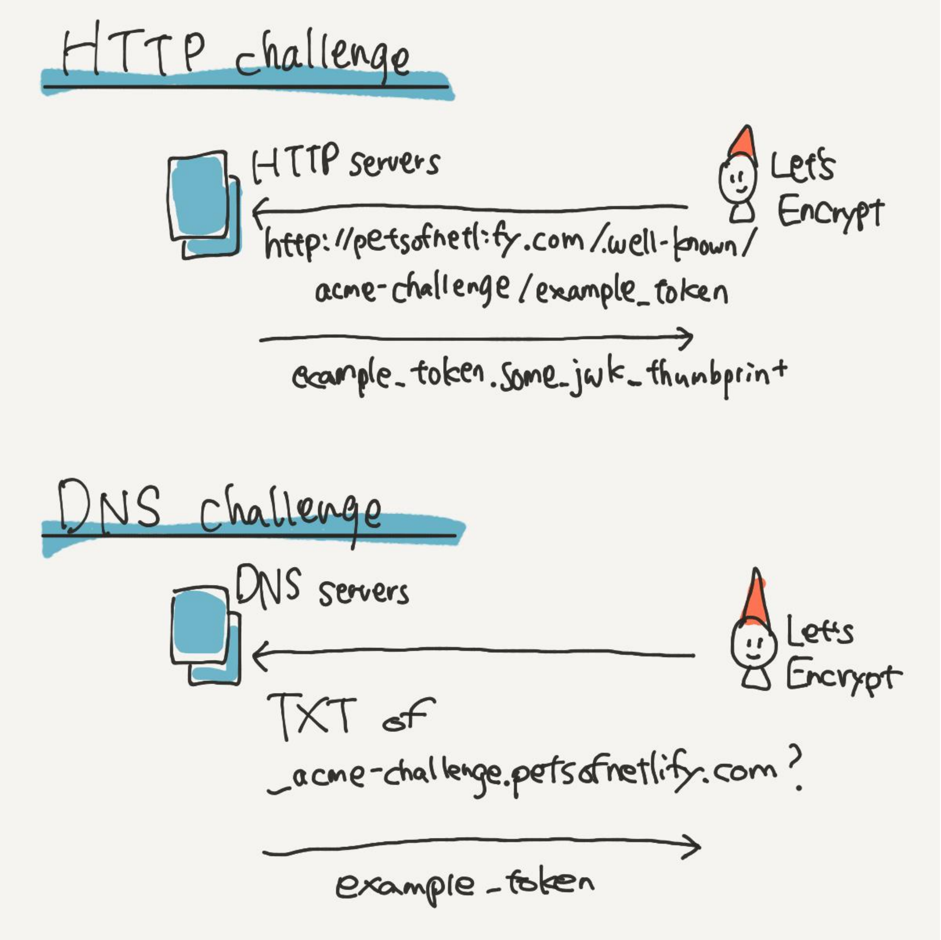
DOMAIN VALIDATION / CHALLENGES

- **HTTP challenge**

  create an HTTP resource on http://petsofnetlify.com/.well-known/acme-challenge/example_token with the content example_token.some_jwk_thumbprint.

- **DNS challenge**

  create a TXT DNS record with domain _acme-challenge.petsofnetlify.com with example_token a value.


HTTP challenge
HTTP servers
Let's Encrypt
http://petsofnetlify.com/.well-known/acme-challenge/example_token
example_token.some_jwk_thumbprint
DNS challenge
DNS servers
Let's Encrypt
TXT of _acme-challenge.petsofnetlify.com?
example_token

https://www.netlify.com/blog/2018/08/20/enabling-free-wildcard-domain-certificates-with-lets-encrypt/

DOMAIN VALIDATION / CHALLENGES

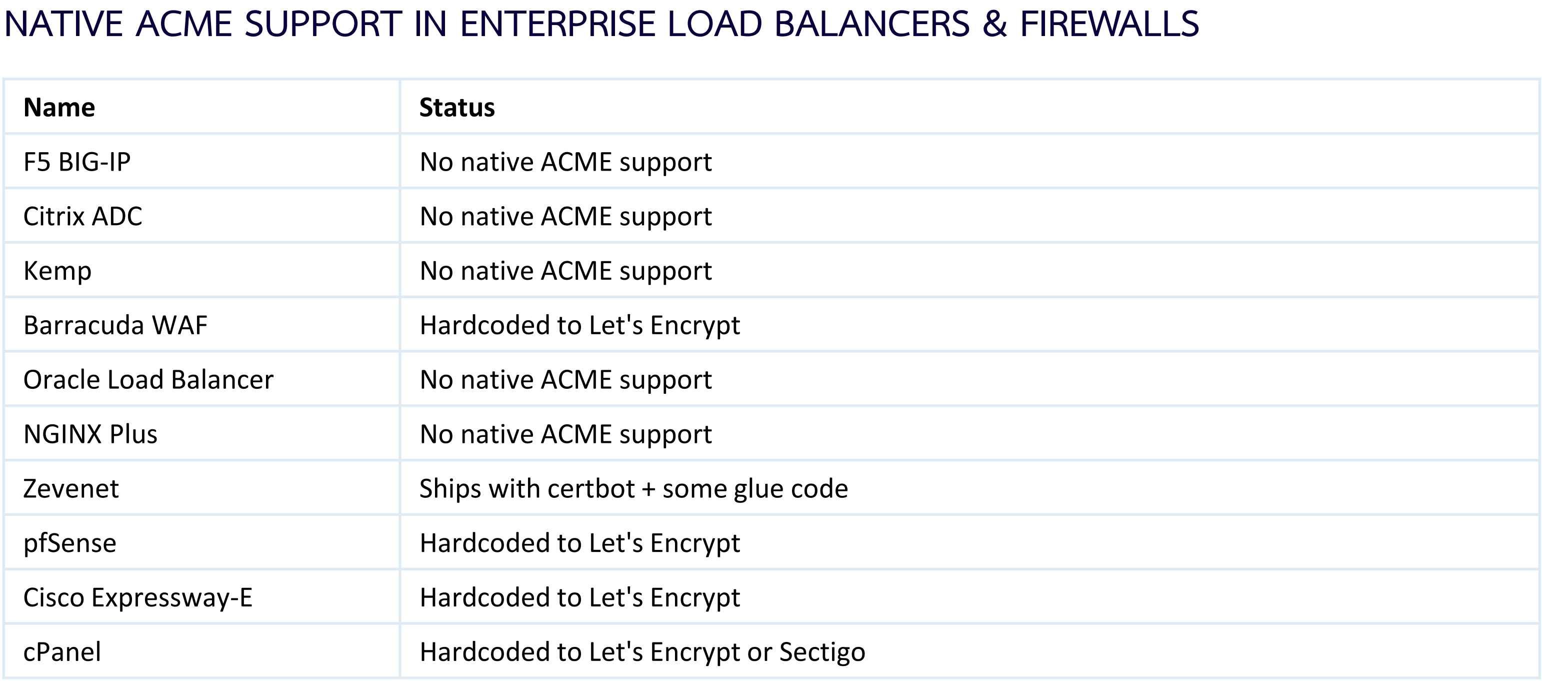
http-01 — the client places the challenge value at a well-known URL on an HTTP server at a domain named in the certificate request.

dns-01 — the client creates a DNS TXT record that matches the challenge value, confirming that the client has control over DNS for a domain named in the certificate request.

tls-alpn-01— the client adds the challenge value to the initial TLS handshake (using the Application-Layer Protocol Negotiation (ALPN) TLS extension) of a server answering at a domain named in the certificate request.

CLIENTS

https://letsencrypt.org/docs/client-options/
- certbot
- acme.sh



NATIVE ACME SUPPORT IN ENTERPRISE LOAD BALANCERS & FIREWALLS

Name	**Status**
F5 BIG-IP	No native ACME support
Citrix ADC	No native ACME support
Kemp	No native ACME support
Barracuda WAF	Hardcoded to Let's Encrypt
Oracle Load Balancer	No native ACME support
NGINX Plus	No native ACME support
Zevenet	Ships with certbot + some glue code
pfSense	Hardcoded to Let's Encrypt
Cisco Expressway-E	Hardcoded to Let's Encrypt
cPanel	Hardcoded to Let's Encrypt or Sectigo

https://smallstep.com/blog/the-embarrassing-state-of-enterprise-acme/

CERTIFICATE LIFECYCLE MANAGEMENT (CLM) SOFTWARE

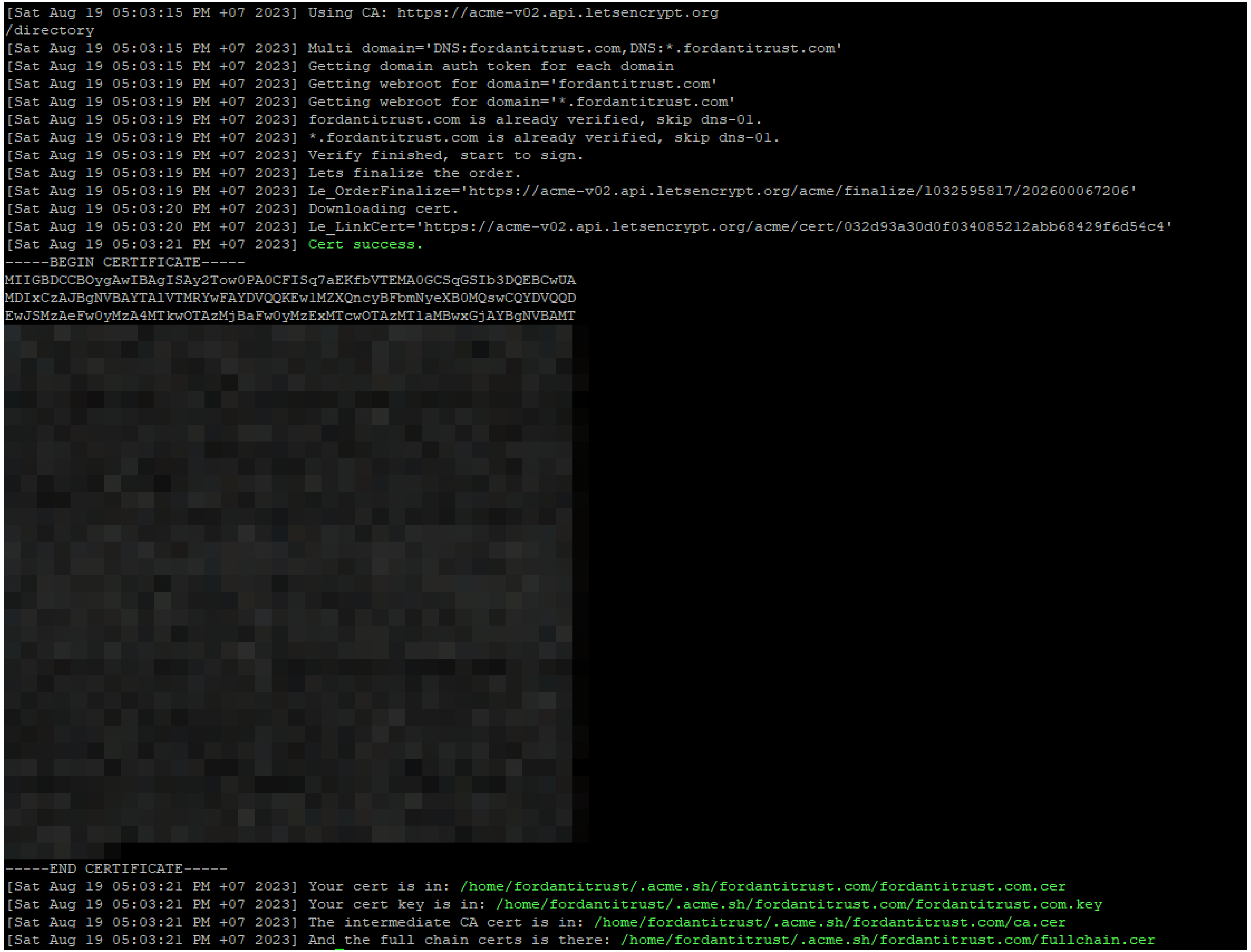
- Sectigo Certificate Manager
- DigiCert CertCentral
- GlobalSign's cloud-based certificate management
- Entrust Datacard Certificate Manager
- AWS Certificate Manager
- Google Cloud Certificate Authority Service

Free Wildcard SSL on a Local Server by acme.sh + Cloudflare
https://letswp.justifiedgrid.com/free-wildcard-ssl-local-server-acme-sh-cloudflare/

```
curl https://get.acme.sh | sh

export CF_Zone_ID="put_your_zone_ID_here"

export CF_Token="put_the_API_token_here"

acme.sh --issue -d example.dev --dns dns_cf -d *.example.dev --server letsencrypt
```

```
https://github.com/acmesh-official/acme.sh
```

https://github.com/acmesh-official/acme.sh/wiki/dnsapi#dns_cf



```
[Sat Aug 19 05:03:15 PM +07 2023] Using CA: https://acme-v02.api.letsencrypt.org
/directory
[Sat Aug 19 05:03:15 PM +07 2023] Multi domain='DNS:fordantitrust.com,DNS:*.fordantitrust.com'
[Sat Aug 19 05:03:15 PM +07 2023] Getting domain auth token for each domain
[Sat Aug 19 05:03:19 PM +07 2023] Getting webroot for domain='fordantitrust.com'
[Sat Aug 19 05:03:19 PM +07 2023] Getting webroot for domain='*.fordantitrust.com'
[Sat Aug 19 05:03:19 PM +07 2023] fordantitrust.com is already verified, skip dns-01.
[Sat Aug 19 05:03:19 PM +07 2023] *.fordantitrust.com is already verified, skip dns-01.
[Sat Aug 19 05:03:19 PM +07 2023] Verify finished, start to sign.
[Sat Aug 19 05:03:19 PM +07 2023] Lets finalize the order.
[Sat Aug 19 05:03:19 PM +07 2023] Le_OrderFinalize='https://acme-v02.api.letsencrypt.org/acme/finalize/1032595817/202600067206'
[Sat Aug 19 05:03:20 PM +07 2023] Downloading cert.
[Sat Aug 19 05:03:20 PM +07 2023] Le_LinkCert='https://acme-v02.api.letsencrypt.org/acme/cert/032d93a30d0f034085212abb68429f6d54c4'
[Sat Aug 19 05:03:21 PM +07 2023] Cert success.
-----BEGIN CERTIFICATE-----
MIIGBDCCBOygAwIBAgISAy2Tow0PA0CFISq7aEKfbVTEMA0GCSqGSIb3DQEBCwUA
MDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQD
EwJSMzAeFw0yMzA4MTkwOTAzMjBaFw0yMzExMTcwOTAzMTlaMBwxGjAYBgNVBAMT
[redacted]
-----END CERTIFICATE-----
[Sat Aug 19 05:03:21 PM +07 2023] Your cert is in: /home/fordantitrust/.acme.sh/fordantitrust.com/fordantitrust.com.cer
[Sat Aug 19 05:03:21 PM +07 2023] Your cert key is in: /home/fordantitrust/.acme.sh/fordantitrust.com/fordantitrust.com.key
[Sat Aug 19 05:03:21 PM +07 2023] The intermediate CA cert is in: /home/fordantitrust/.acme.sh/fordantitrust.com/ca.cer
[Sat Aug 19 05:03:21 PM +07 2023] And the full chain certs is there: /home/fordantitrust/.acme.sh/fordantitrust.com/fullchain.cer
```

ACME OV/EV ?

Digicert

Automation examples with third-party ACME clients

https://docs.digicert.com/en/certcentral/certificate-tools/certificate-lifecycle-automation-guides/use-a-third-party-acme-client-for-host-automations/automation-examples-with-third-party-acme-clients.html

Enabled automatic certificate request approvals

https://docs.digicert.com/en/certcentral/manage-certificates/manage-certificate-request-approvals/enable-automatic-certificate-request-approvals.html

Submit an organization for pre-validation

https://docs.digicert.com/en/certcentral/manage-certificates/organization-and-domain-management/manage-organizations/submit-an-organization-for-pre-validation.html

GlobalSign

GlobalSign Announces ACME OV Certificate Support

https://www.globalsign.com/en/company/news-events/news/acme-ov-certificate-support