



OWASP 2025
GLOBAL
AppSec[®]

USA

NOV 3-7 | 2025



OWASP 2025
GLOBAL
AppSec

USA

**IVAN
RISTIĆ**

How to Defend Your PKI Estate

**The last 15 years
have been great for
transport layer
security...**

**...but public PKI
remains as insecure
as it's ever been.**

**In 2011, the
DigiNotar CA was
struck. Full
compromise.**



More than 500 fraudulent certificates issued.

Table 5.1. Common names used in rogue certificates issued by the DigiNotar attacker

..com	*.*.org	*.10million.org (2)
*.android.com	*.aol.com	*.azadegi.com (2)
*.balatarin.com (3)	*.comodo.com (3)	*.digicert.com (2)
*.globalsign.com (7)	*.google.com (26)	*.JanamFadayeRahbar.com
*.logmein.com	*.microsoft.com (3)	*.mossad.gov.il (2)
*.mozilla.org	*.RamzShekaneBozorg.com	*.SahebeDonyayeDigital.com
*.skype.com (22)	*.startssl.com	*.thawte.com (6)
*.torproject.org (14)	*.walla.co.il (2)	*.windowsupdate.com (3)
*.wordpress.com (14)	addons.mozilla.org (17)	azadegi.com (16)
Comodo Root CA (20)	CyberTrust Root CA (20)	DigiCert Root CA (21)
Equifax Root CA (40)	friends.walla.co.il (8)	GlobalSign Root CA (20)
login.live.com (17)	login.yahoo.com (19)	my.screenname.aol.com
secure.logmein.com (17)	Thawte Root CA (45)	twitter.com (18)

Source: Bulletproof TLS and PKI, 2nd edition



Estimated **300,000** **users** attacked.

Figure 5.2. DigiNotar OCSP activity in August 2011 [Source: Fox-IT]



Source: Bulletproof TLS and PKI, 2nd edition

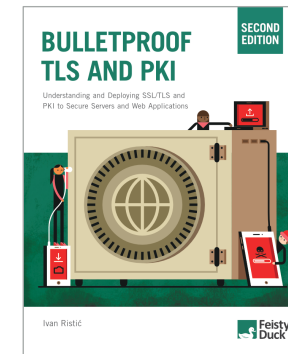
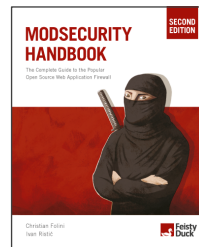
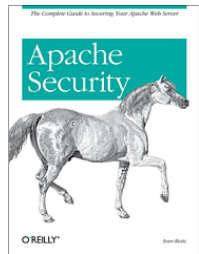
The same thing could happen today.

We'd only be better at detecting it,
but the core problem remains.

Agenda: State of The Art Public PKI Security

- 1** Can someone else get a certificate for my domain?
- 2** Can we detect them?
- 3** Can we prevent them?
- 4** How will we recover?

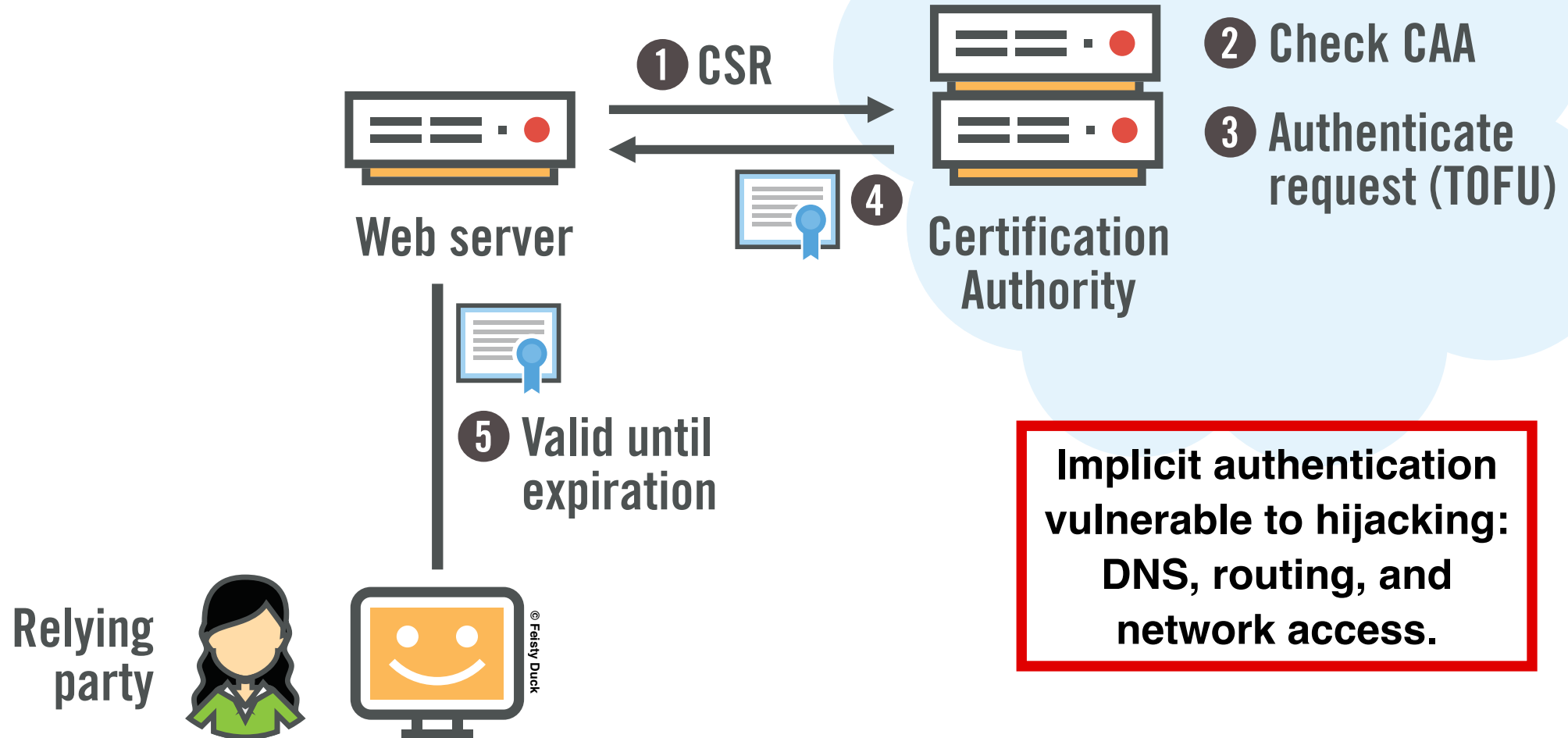
Who am I?



How Public PKI Works

Certificate issuance TOFU

TOFU stands for Trust On First Use



**Any CA can issue
certificates for
your domains...
without your
consent.**



Common CA Database

CCADB is the system Apple, Chrome, Microsoft, and Mozilla use to track CAs and their certificates.

94

Organizations

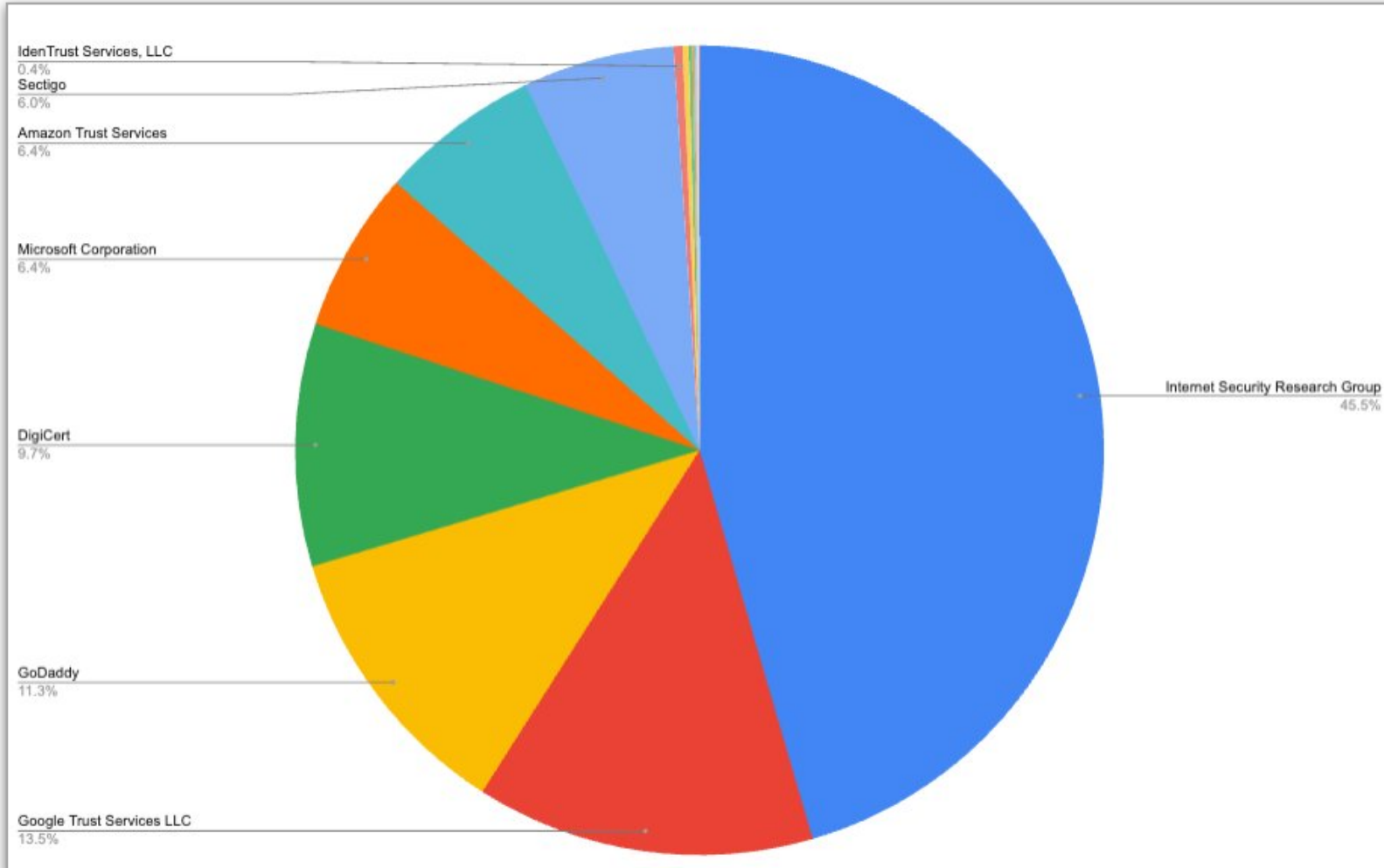
39 with roots trusted by all 4 vendors

42

Countries

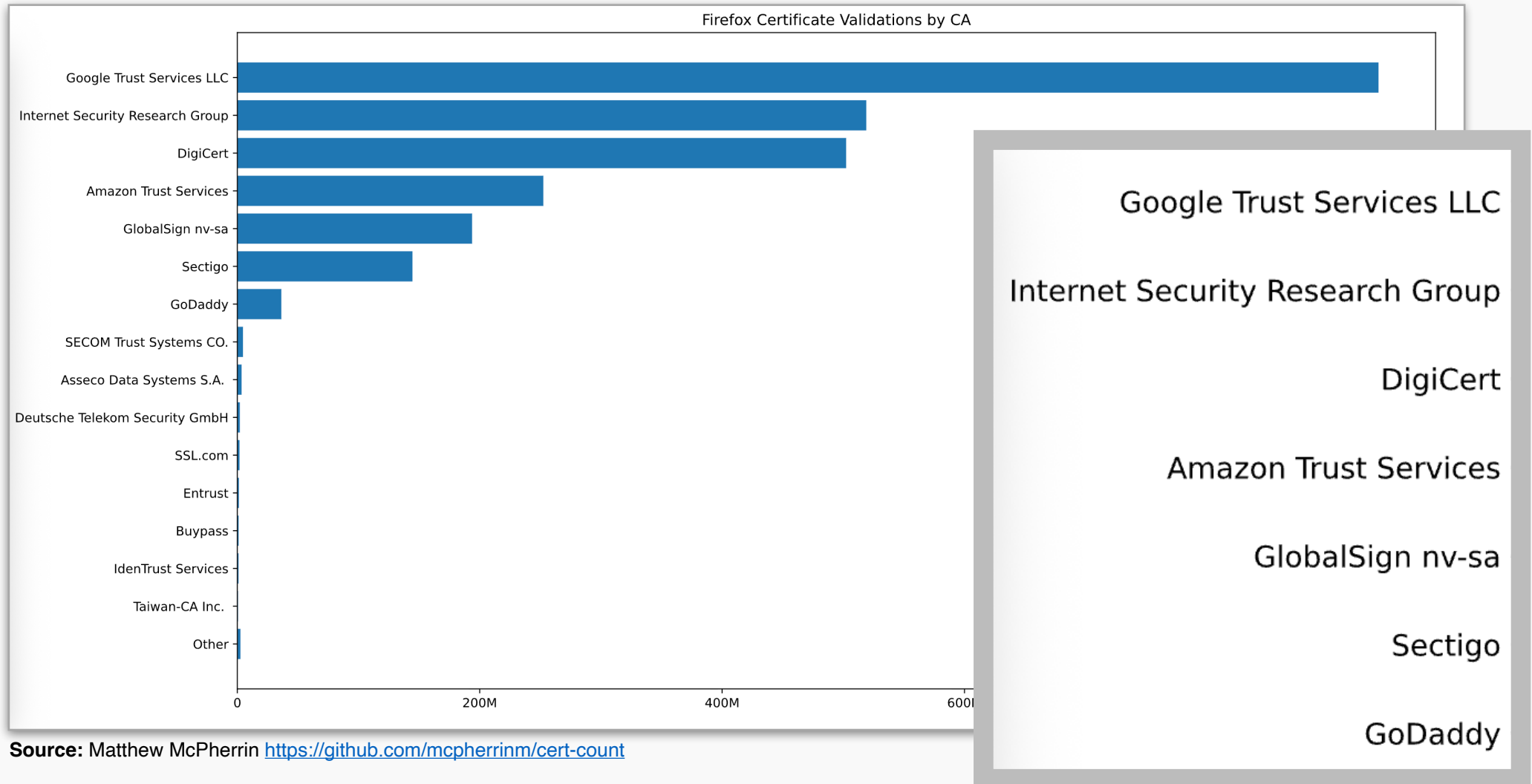
22 with CAs trusted by all 4 vendors

Top CAs: By Issuance



Source: Ryan Hurst <https://x.com/rmhrisk/status/1868740608275497364/photo/1>

Top CAs: Firefox



Attack Vectors

What are some of the more likely exploitation vectors?

- **Active Network Attacks**

Against DNS and servers, and routing

- **Direct Infrastructure Attacks**

Your validation infrastructure, incl. DNS

- **Misconfiguration**

Predominantly dangling DNS

- **CA Compromise**

Lack of security; **governments
and law agencies**



Historical Attacks Against Public PKI

Showing that these attacks are
practical, not only theoretical

.cd dangling nameserver

WRITEUPS

Hijacking the top-level domain of a sovereign state



Fredrik Nordberg Almroth Jan 15, 2021



Imagine what could happen if the country-code top-level domain (ccTLD) of a sovereign state fell into the wrong hands. Here's how I ([@Almroot](#)) bought the domain name used in the NS delegations for the ccTLD of the Democratic Republic of Congo (.cd) and temporarily took over 50% of all DNS traffic for the TLD that could have been exploited for MITM or other abuse.

Source: <https://labs.detectify.com/writeups/show-i-hijacked-the-top-level-domain-of-a-sovereign-state/>



KLAYswap BGP hijack

Mitigated, as of recently, via multi-perspective validation (MPIC).

Attackers exploit fundamental flaw in the web's security to steal \$2 million in cryptocurrency

March 9, 2022 – by [Henry Birge-Lee](#)

[Comments](#)

■ Uncategorized

By Henry Birge-Lee, Liang Wang, Grace Cimaszewski, Jennifer Rexford and Prateek Mittal

On Thursday, Feb. 3, 2022, attackers stole approximately \$2 million worth of

Source: <https://blog.cis.princeton.edu/2022/03/09/attackers-exploit-fundamental-flaw-in-the-webs-security-to-steal-2-million-in-cryptocurrency>



MITM against jabber.ru

Hijacked the network connection to get a certificate and MITM traffic.

Encrypted traffic interception on Hetzner and Linode targeting the largest Russian XMPP (Jabber) messaging service

ValdikSS 3rd November 2023 at 5:17pm

TL;DR: we have discovered XMPP (Jabber) the-Middle attack) of jabber.ru (aka xmpp.ru)

The attacker has issued several new TLS certificates

STARTTLS connections on port 5222 using transparent MiTM proxy. The attack was discovered due to expiration of one of the MiTM certificates, which haven't been reissued.

There are no indications of the server breach or spoofing attacks on the network segment, quite the contrary: the traffic redirection has been configured on the hosting provider network.

The wiretapping may have lasted for up to 6 months overall (90 days confirmed). We believe this is lawful interception. Hetzner and Linode were forced to setup.

Last update: [03 Nov 2023](#)

[REDACTED] The attack was discovered due to expiration of one of the MiTM certificates, which haven't been reissued. [REDACTED]

The network is not secure

Motivated attackers will attack your DNS and network traffic.



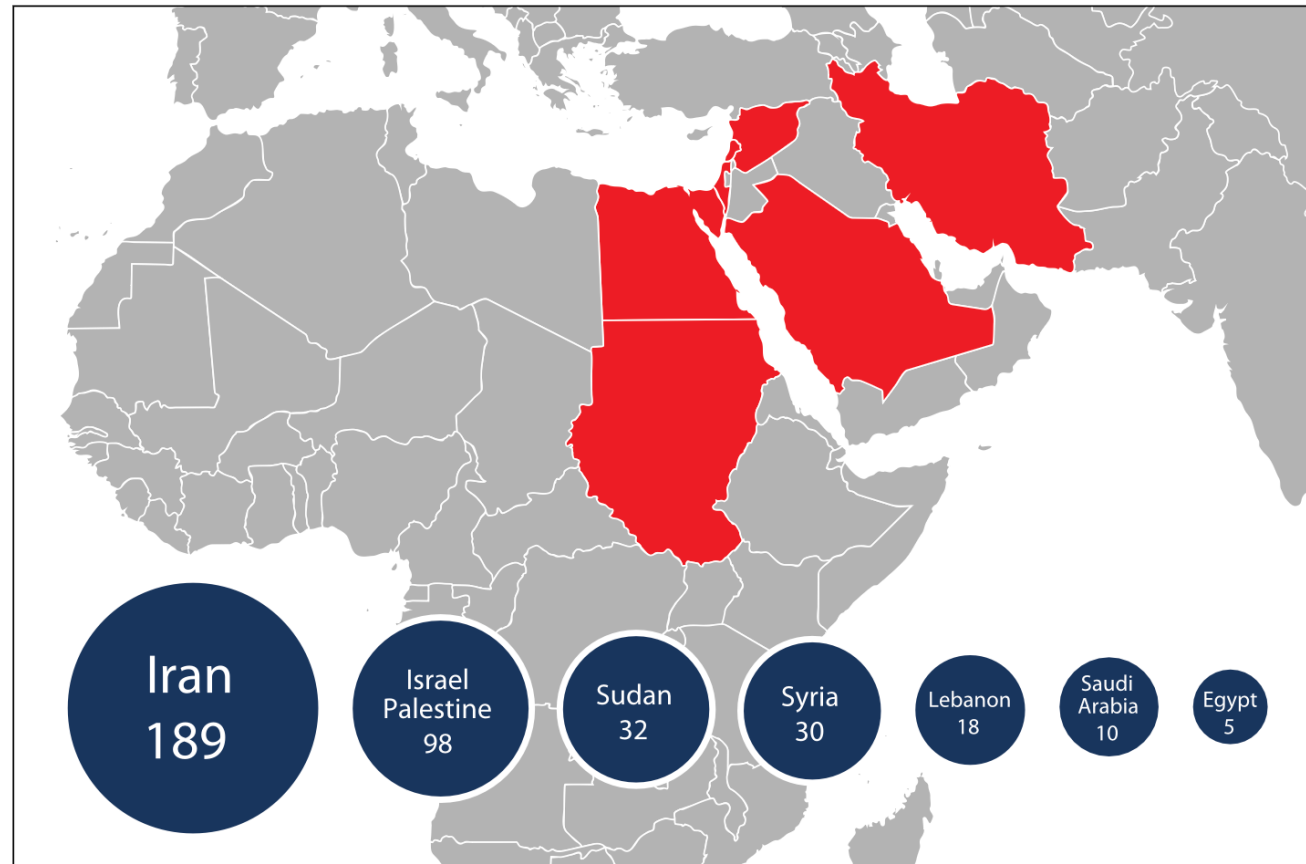
The screenshot shows the ITPro website interface. At the top is a dark blue header with the ITPro logo, a US flag, and navigation icons for email and search. Below the header is a navigation bar with links: Home, Business, Cloud, Hardware, Infrastructure, Security, Content Hubs, Advertise, More, and CHANNELPro. A 'TRENDING' section highlights articles like 'Subscribe to the ITPro newsletter', 'Pure Accelerate 2025', and 'Automating cybersecurity without disruptir'. The main content area shows a breadcrumb trail: Home > Security > Cyber Attacks. The headline reads: 'All US forces must now assume their networks are compromised' after Salt Typhoon breach. Below the headline is a sub-headline: 'The announcement marks the second major Salt Typhoon incident in the space of two years'. At the bottom are social media sharing icons for Facebook, YouTube, LinkedIn, Twitter, and Email.

Source: <https://www.itpro.com/security/cyber-attacks/all-us-forces-must-now-assume-their-networks-are-compromised-2>

Flame breaks MD5

It's a question of motivation. Flame was extraordinary.

Figure 5.3. Flame activity [Source: Kaspersky Lab]



Source: Bulletproof TLS and PKI, 2nd edition

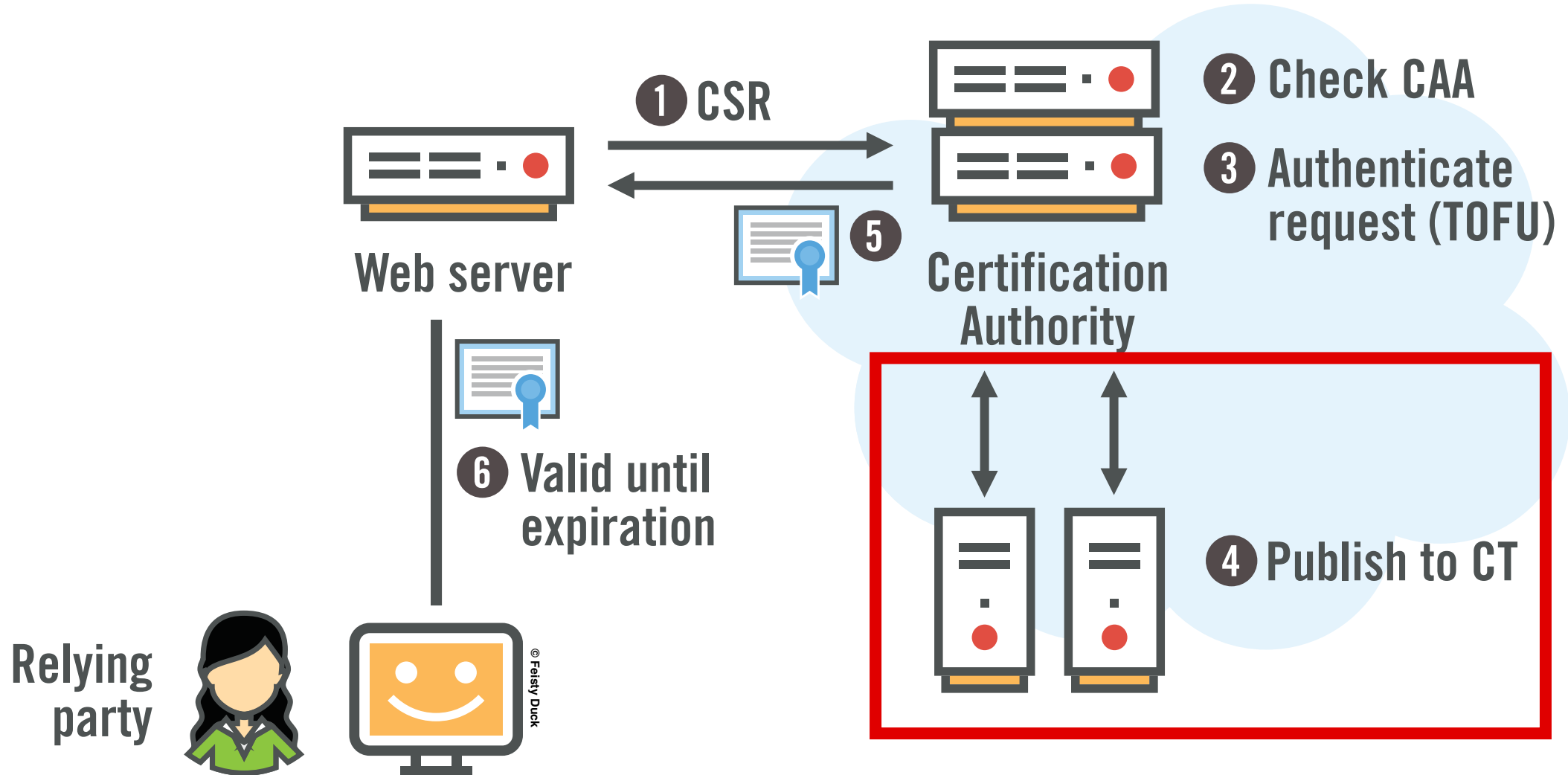
Certificate Transparency

A global system for certificate
issuance monitoring in Web PKI



Certificate Transparency

Before issuance, CAs publish to multiple Certificate Transparency logs.

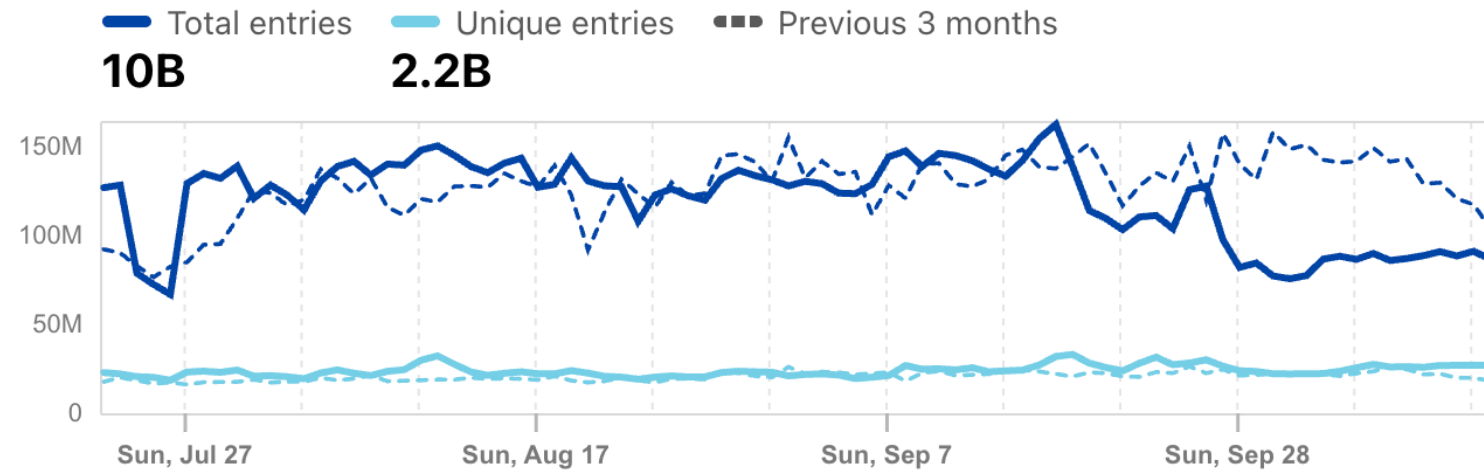


2.4 billion valid certificates

In October 2025, about 1 billion issued in the past three months

Certificate issuance volume

Total number of certificates issued over the selected time period ? 🔍



Entry type

Unique ☒

● Certificates
882M



● Pre-certificates
1B

Source: <https://radar.cloudflare.com/certificate-transparency>

3 billion entries in a single log



FEISTYDUCKDOMAINSHOSTSCERTIFICATESISSUESSEARCHREPORTSWORKBENCHDOCSSETTINGSACCOUNT

Certificate Transparency

CERTIFICATE INVENTORY

Dashboard

Expiring Endpoints

Issuance History

Revocation History

CERTIFICATE TRANSPARENCY

Active Discoveries

Archived Discoveries

CT Log List

The table below shows all Certificate Transparency logs currently monitored by Hardenize. If your hostnames appear in any of the log entries that appear in these logs, we will add the corresponding certificates to your inventory. The statistics in the last two columns are updated every 10 minutes.

Name	Network Endpoint	MMD ?	Total Entries	Last Update
Cloudflare 'Nimbus2025'	ct.cloudflare.com/logs/nimbus2025	86,400	3,030,489,112	13 Oct 2025 08:20 UTC
Cloudflare 'Nimbus2026'	ct.cloudflare.com/logs/nimbus2026	86,400	622,317,345	13 Oct 2025 08:20 UTC

Cloudflare 'Nimbus2025'	ct.cloudflare.com/logs/nimbus2025	86,400	3,030,489,112	13 Oct 2025 08:20 UTC
Cloudflare 'Nimbus2026'	ct.cloudflare.com/logs/nimbus2026	86,400	622,317,345	13 Oct 2025 08:20 UTC
Cloudflare 'Nimbus2027'	ct.cloudflare.com/logs/nimbus2027	86,400	7,036	13 Oct 2025 08:34 UTC

DigiCert 'Wyvern2026h1'	wyvern.ct.digicert.com/2026h1	86,400	260,002,660	13 Oct 2025 08:58 UTC
DigiCert 'Wyvern2026h2'	wyvern.ct.digicert.com/2026h2	86,400	123,210,561	13 Oct 2025 08:58 UTC
DigiCert 'Wyvern2027h1'	wyvern.ct.digicert.com/2027h1	86,400	1,166	13 Oct 2025 08:34 UTC



MANY CT ADVANTAGES

**Issuance monitoring.
Discovery. Availability.
Cryptoagility.**

A global system for certificate issuance
monitoring in **Web PKI and mobile apps.**



CT Monitoring

CT is noisy and can turn into a waste of time.
Consider these two strategies.

1

Easy: Alert on observing unexpected CAs.

2

High Assurance: Track what you issue, compare with what you observe.

Certification Authority Authorization (CAA)

Tools for domain name owners to
control certificate issuance.

DNS CAA Resource Record

Mandatory for all CAs from September 2017. RFCs 6844, 8659, 9495, BIML VMC.

Internet Engineering Task Force (IETF)
Request for Comments: [8659](#)
Obsoletes: [6844](#)
Category: Standards Track
Published: November 2019
ISSN: 2070-1721

P. Hallam-Baker
Venture Cryptography
R. Stradling
Sectigo
J. Hoffman-Andrews
Let's Encrypt

DNS Certification Authority Authorization (CAA) Resource Record

Abstract

The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue. This document defines the syntax of the CAA record and rules for processing CAA records by CAs.

This document obsoletes RFC 6844.





feistyduck.com

14 Oct 2025 07:36 UTC

Tweet

Domain Name System

- ✓ DNS Zone
- ✓ DNS Records
- ✗ DNSSEC
- ✓ CAA

Email

- ✓ Mail servers
- SECURE TRANSPORT (SMTP)
- ✓ TLS
- ✓ Certificates
- ✗ MTA-STX
- ✗ TLS-RPT
- ✗ DANE
- AUTHENTICATION AND POLICY
- ✓ SPF
- ✓ DMARC

Certification Authority Authorization

CAA (RFC 8659) is a new standard that allows domain name owners to restrict which CAs are allowed to issue certificates for their domains. This can help to reduce the chance of misissuance, either accidentally or maliciously. In September 2017, CAA became mandatory for CAs to implement.



Test passed

Everything seems to be well configured. Well done.

CAA Policy Information

Policy host	feistyduck.com
issue	letsencrypt.org flags: 0
iodef	mailto:pki@feistyduck.com flags: 0

Analysis



Issuance of S/MIME certificates not restricted

This policy doesn't restrict the issuance of S/MIME certificates. Consider using the `issuemail` directive to restrict which CAs, if any, can issue.



Issuance of BIMl not restricted

This policy doesn't restrict issuance of BIMl certificates. Consider using the `issuevmc` directive to restrict which CAs, if any, can issue.



CAA policy restricts issuance

Great. This domain name uses CAA to restrict which CAs are allowed to issue certificates for it.



Policy uses reporting

Good. This policy uses reporting, which means that your contact information is available should someone need to contact you about a CAA violation. Do note that you're not guaranteed to be notified, given that CAs generally don't support notifications yet.

Template CAA Configuration

Control of issuance, wildcards, email, and BIMl certificates.

```
example.com.  CAA      0 issue "letsencrypt.org"
example.com.  CAA      0 issuewild "digicert.com"
example.com.  CAA      0 issuewild "sectigo.com"
example.com.  CAA      0 issuemail ";"
example.com.  CAA      0 issuevmc ";"
example.com.  CAA      0 iodef "pki@example.com"
```

CAA ACME Extensions

RFC 8657 (November 2019). Limited support at the moment.

Internet Engineering Task Force (IETF)

H. Landau

Request for Comments: [8657](#)

Category: Standards Track

Published: November 2019

ISSN: 2070-1721

Certification Authority Authorization (CAA) Record Extensions for Account URI and Automatic Certificate Management Environment (ACME) Method Binding

Abstract

The Certification Authority Authorization (CAA) DNS record allows a domain to communicate an issuance policy to Certification Authorities (CAs) but only allows a domain to define a policy with CA-level granularity. However, the CAA specification (RFC 8659) also provides facilities for an extension to admit a more granular, CA-specific policy. This specification defines two such parameters: one allowing specific accounts of a CA to be identified by URIs and one allowing specific methods of domain control validation as defined by the Automatic Certificate Management Environment (ACME) protocol to be required.



CAA ACME Extensions

Restrict ACME validation methods and enforce issuance from specific CA customer accounts.

```
example.com.    CAA    0    issue "letsencrypt.org; accounturi=  
https://acme-v02.api.letsencrypt.org  
/acme/acct/1726001367"
```

```
example.com.    CAA    0    issue "letsencrypt.org; validationmethods=  
dns-01"
```

DigiCert's Proprietary Account Locking

Configure CAA with a random number provided
in the CertCentral product.

```
example.com.    CAA    0    issue "digicert.com; account=  
fce9431ca2df7ae0d25a6de09587fdc1  
ff1616e7187655a18eb72723a0b85c86"
```

PKI Posture Management Blueprint

Step 1: Threat Modelling

Understand your attack surface against attacker resources and motivation

- **Websites**

CT for detection and deterrence

- **Mobile apps**

CT supported on iOS and Android 16

- **Public APIs**

No CT

- **Other network traffic**

No CT. DANE may help with SMTP

Step 2: CT Monitoring

Make use of CT and additional monitoring to build an inventory of assets and configuration.

- 1** Build an inventory of your top-level domain names.
- 2** Use CT to build an inventory of your certificates.
- 3** Mine certificates for subdomains.

Step 3: Network Monitoring

Deploy monitoring of some or all aspects of security configuration.

**TLS / PKI / HSTS / CSP /
HTTP / CAA / Automation
/ Expiration / Post-
quantum cryptography**

Step 4: Easy CAA

Start with easy improvements that will improve security of your entire inventory.

- 1 Restrict issuance to CAs already in use**
- 2 Restrict S/MIME and BIMl because you can**
- 3 Monitor for certificates from unknown CAs**

Step 5: Robust CAA

Maybe difficult to do for everything, but feasible for selected **high-value properties**.

- 1** Resolve to use certificates from only two or three CAs
- 2** **Centralize issuance** so that you can build an inventory of "known good" certificates
- 3** Monitor for certificates that are not on your list

Step 6: DNSSEC

DNSSEC prevents DNS spoofing. Mandatory for CAs to check from March 2026. **Alternatively, distribute your DNS servers to take advantage of multi-perspective validation (MPIC).**

 CA/BROWSER FORUM

[Home](#) [About](#) [Server Cert WG](#) [Code Signing Cert WG](#) [NetSec WG](#) [S/MIME Cert WG](#) [Definitions WG](#) [Proceedings](#) [Resources](#)

[Home](#) » [All CA/Browser Forum Posts](#) » Ballot SC-085v2: Require Validation of DNSSEC (when present) for CAA and DCV Lookups

BALLOT SC-085V2: REQUIRE VALIDATION OF DNSSEC (WHEN PRESENT) FOR CAA AND DCV LOOKUPS

[Voting Results](#)

[Certificate Issuers](#)

LATEST RELEASES

Server Certificate Requirements
[SC-089: Mass Revocation Planning](#) - Aug 26, 2025

Source: <https://cabforum.org/2025/06/18/ballot-sc-085v2-require-validation-of-dnssec-when-present-for-caa-and-dcv-lookups/>



Step 7: Short-Lived Certificates

No one is seriously checking for revocation. Short-lived certificates offer better security for high-value properties.

Cryptography & Security Newsletter



Short-Lived Certificates Are Coming in 2025

31 December 2024

Judging from recent events, the focus in the next couple of years will be on adopting significantly reduced certificate lifetimes. We've known for a while that Google wants to reduce certificate lifetimes to ninety days, but earlier this year, **Apple surprised everyone** by pushing for as little as forty-five days (forty-seven in the latest proposal). Unlike Apple and Google, which are forcing everyone to follow their direction, Let's Encrypt is approaching the problem from the other end by offering us a choice.



Step 8: Use a Private PKI

Extra security for private ecosystems, such as mobile APIs.



Advantages

Insulates you from the weaknesses in public PKIs.



Disadvantages

More work to build and maintain, easier to mess up.

Step 9: Monitor For Attacks

From multiple perspectives, check that you're seeing the certificates you know. Reuse DANE if you have it. NEL may help.



Step 10: Static Public Key Pinning

In Chrome since 2011, later added to Firefox. Now used only by Google and Mozilla.

The screenshot shows the Chrome net-internals/#hsts page. The left sidebar contains links to Events, Proxy, DNS, Sockets, Domain Security Policy, and Shared Dictionaries. The main content area is titled 'HSTS/Static Public Key Pinning' and includes sections for adding and querying HSTS domains. A blue box highlights the configuration for google.co.uk, showing the static_public_key_pin_domain, static_public_key_pin_include_subdomains, static_public_key_pin_observed, and static_public_key_pin_hashes.

HSTS/Static Public Key Pinning

HSTS is HTTP Strict Transport Security: a way for sites to tell browsers that they only want to be accessed over HTTPS.

Add HSTS domain

Input a domain name to add it to the HSTS set:

Domain: Include subdomains: ☐

Query HSTS/Static Public Key Pinning domain

Input a domain name to query the current HSTS/Static Public Key Pinning configuration:

Domain:

Found:

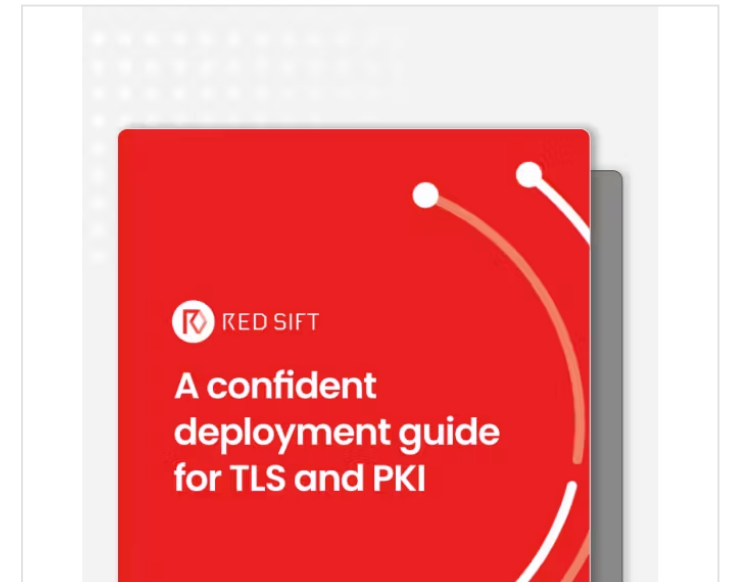
```
static_public_key_pin_domain: google.co.uk
static_public_key_pin_include_subdomains: true
static_public_key_pin_observed: 1759323180
static_public_key_pin_hashes:
  sha256/dABIANkDRIX3bqM85I6We7wBUh0DPycNFBMvYkXGX2Q=, sha256/IGnQeIPjbxIR+JteR7
  AkUXl7pV+19BT4x3o15saZBNE=, sha256/0dSImQD9NWJh4Ebc0HBxkhygPwNSwA9Q91eounfbcOE
  =, sha256/CL0mM1/0XvSPjw5U0YbAf9GK0xImEp9hhku9W90fHMk=, sha256/YPtHaftLw6/0vnc2
  BnNKGf54xiCA28WFcccjKA4ypCM=, sha256/Vfd95BwDeSQo+NUYxVEEIlvk0lWY2SaLKK1lPhz0x
  78=, sha256/IPmBDajLVSGntG03WP53X/zilCVndez5YJ2+vJvhJsA=, sha256/hZe10erqJ1Pnq6
  F4N0gVjjpHqm037Ndf4aLLVpZZdAE=, sha256/kIdp6NNEd8wsugYyyIYFs1yLMCED3hZbSR8ZF
  s/a/A4=, sha256/05TQDB/wa4SkRjBrQL2Aq9CG317H9MDDgpTVcrpJDa4=, sha256/vh78KSg1Ry4N
  aqGDV10w/cTb9VH3BQUZoCWNa93W/EY=, sha256/mEfLZT5enoR1FuXLgYYGqnVEoZvmf9c2bVBpi
  0jYQ0c=, sha256//RoweMyX8j8/fAaaeAIwzhWxigZDrh/J2BBJaHrjX90=, sha256/yDu9og255N
  N5GEf+Bwa9rTrqFQ0EydZ0r1FCh9TdAW4=, sha256/QXnt2YHvdHR3tJYmQIr0Paosp6t/nggsEGD
  4QJZ3Q0g=, sha256/8yZxLgpr8Eb08ANRRwKAzIzz9XdlSUgtYPkXKYULGSY=, sha256/hxqRLPTu
  1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc=
```

Resources

We've just scratched the surface.
Here are some of our free resources
for you to continue with.



In-depth TLS, PKI, and PQC guides



<https://redsift.com/resource-center>
(registration not required)

Hardenize

<https://www.hardenize.com>

**hardenize.com**
10 Jul 2018 13:30 UTC

Domain

- ✓ Name servers
- ✗ DNSSEC
- ✗ CAA

Email

- ✓ Mail servers
- SECURE TRANSPORT (SMTP)
 - ✓ TLS
 - ✓ Certificates
 - ✓ MTA-STS
 - ✗ DANE
- AUTHENTICATION AND POLICY
 - ✓ SPF
 - ✗ DMARC

WWW

- PROTOCOLS
 - ✓ HTTP (80)
 - ✓ HTTPS (443)

WEB SECURITY OVERVIEW

✓ **HTTPS**

Web sites need to use encryption to help their visitors know they're in the right place, as well as provide confidentiality and content integrity. Sites that don't support HTTPS may expose sensitive data and have their pages modified and subverted.

For all sites

- VERY IMPORTANT
- MEDIUM EFFORT

✓ **HTTPS Redirection**

To deploy HTTPS properly, web sites must redirect all unsafe (plaintext) traffic to the encrypted variant. This approach ensures that no sensitive data is exposed and that further security technologies can be activated.

For all sites

- VERY IMPORTANT
- LOW EFFORT

✓ **HTTP Strict Transport Security**

HTTP Strict Transport Security (HSTS) is an HTTPS extension that instructs browsers to remember sites that use encryption and enforce strict security requirements. Without HSTS, active network attacks are easy to carry out.

For important sites

- VERY IMPORTANT
- MEDIUM EFFORT

✓ **HSTS Preloaded**

HSTS Preloading is informing browsers in advance about a site's use of HSTS, which means that strict security can be enforced even on the first visit. This approach provides best HTTPS security available today.

For important sites

- VERY IMPORTANT
- MEDIUM EFFORT

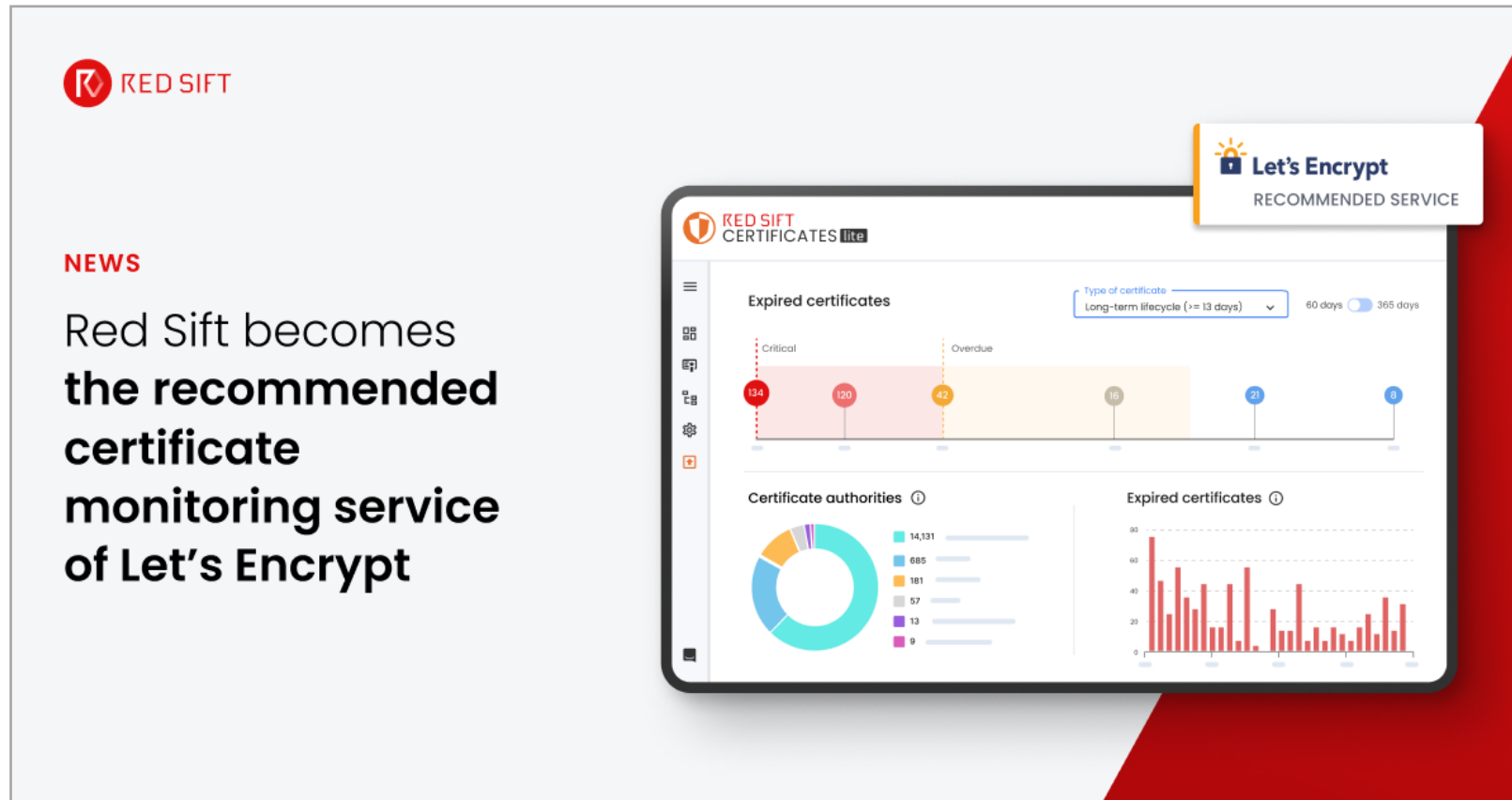
✓ **Content Security Policy**

Content Security Policy (CSP) is an additional security layer that enables web sites to control browser behavior, creating a safety net that can counter attacks such as cross-site scripting.

For important sites

- IMPORTANT
- HIGH EFFORT

Free PKI monitoring, in collaboration with Let's Encrypt



<https://redsift.com/pulse-platform/certificates-lite>





OWASP 2025
GLOBAL
AppSec

| **USA**

**THANK
YOU!**

Alternatives and Possible Future Improvements

Roads less travelled, which may be
useful for your use cases.

DANE binds PKI to DNSSEC

Browsers don't support it. SMTP servers might. See also RFC 9102 as a way to avoid DNSSEC lookups.

Internet Engineering Task Force (IETF)
Request for Comments: 6698
Category: Standards Track
ISSN: 2070-1721

P. Hoffman
VPN Consortium
J. Schlyter
Kirei AB
August 2012

The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA

Abstract

Encrypted communication on the Internet often uses Transport Layer Security (TLS), which depends on third parties to certify the keys used. This document improves on that situation by enabling the administrators of domain names to specify the keys used in that domain's TLS servers. This requires matching improvements in TLS client software, but no change in TLS server software.

Status of This Memo

This is an Internet Standards Track document.



CAA extensions for strong authentication?

Cryptographically-Secured Domain Validation

Henry Birge-Lee *
Princeton University

Grace H. Cimaszewski *
Princeton University

Cyrill Krähenbühl
Princeton University

Liang Wang
Princeton University

Aaron Gable
Let's Encrypt

Prateek Mittal
Princeton University

Abstract

Certificate Authorities (CAs) bootstrap HTTPS-based trust on the Internet by authenticating the identity of domain names via a process known as domain control validation (DV). Because of their reliance on unauthenticated web protocols (including DNS and HTTP), currently used DV protocols have been shown to be vulnerable to a range of network attacks. To remedy this situation, we propose a framework for cryptographic DV, which fundamentally mitigates network-layer attacks. Our framework offers secure DV protocol mechanisms that are coupled with a secure policy specified by the

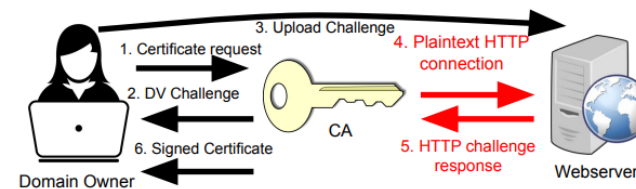


Figure 1: Domain Control Validation via HTTP.

Authority (CA) through the domain control validation (DV) challenge response mechanism. This typically involves mak

CAA “False Positives”

Watch for delegated domains and services that provide managed certificate issuance.

- When you delegate your DNS via a CNAME, **you're delegating CAA as well.**
- Your suppliers will override CAA and may have their own preferred CAs.
- Their CAA may be ephemeral.

Revocation

What do we do when we discover a
misissued certificate?

There is **no revocation checking** in Web PKI

Cryptography & Security Newsletter

121

The Slow Death of OCSP

30 January 2025

Everybody is talking about OCSP now because, just last month, at the end of 2024, **Let's Encrypt announced** it was going to stop supporting online certificate revocation checking. Beginning in early May 2025, there will no longer be any OCSP revocation information in Let's Encrypt's certificates. Once all its earlier certificates expire, Let's Encrypt will shut down its OCSP servers.

Let's Encrypt's reasoning is sound. As it stands today, OCSP is not making anyone more secure. Browsers are either not checking it or are implementing it in a way that provides no



Mozilla's CRLite... too little too late?

Cryptography & Security Newsletter



Mozilla Fixes Certificate Revocation Checking

31 March 2025

You may recall from our January 2025 newsletter, which was dedicated to the demise of OCSP revocation checking (*The Slow Death of OCSP*), that Let's Encrypt is planning to stop supporting OCSP in early May—only one month from now. Let's Encrypt is the leading CA in terms of issued certificates, so its withdrawal from OCSP creates a problem for user agents that still rely on this method of revocation checking. This impending deadline may have

spurred one such agent—Mozilla—to complete the outstanding work required to replace OCSP

