Ten Years as a Free, Open, and Automated Certificate Authority

Real World Crypto 2025

Very Quick Web PKI Overview

Certificate Authorities (CAs) issue digital certificates based on demonstrated control of a domain.

Certificates provide a binding for relying parties between domains and public keys.

TLS needs encryption and authentication.
Certificates provide authentication.

The Web PKI Before 2015

- Mostly complex manual processes
- Often expensive $$$
- People weren't convinced of the necessity of enabling HTTPS

Result:

- 39% of page loads used HTTPS
  - Smaller percentage of sites

An Undermining Problem

Browser network security before Let’s Encrypt.

It wasn’t totally pointless, but it sure felt like it!

What are we going to do?

Wanted a solution that would get the Web close to 100% HTTPS within about five years.

Basically the fastest amount of time that seemed within the realm of possibility.

(avoid IPv6/DNSSEC timelines!)

Certificates seemed to be the roadblock.

Start a new CA!

The only feasible solution was to start a new CA that’s easy to use and gives certificates away for free.

Getting To Work

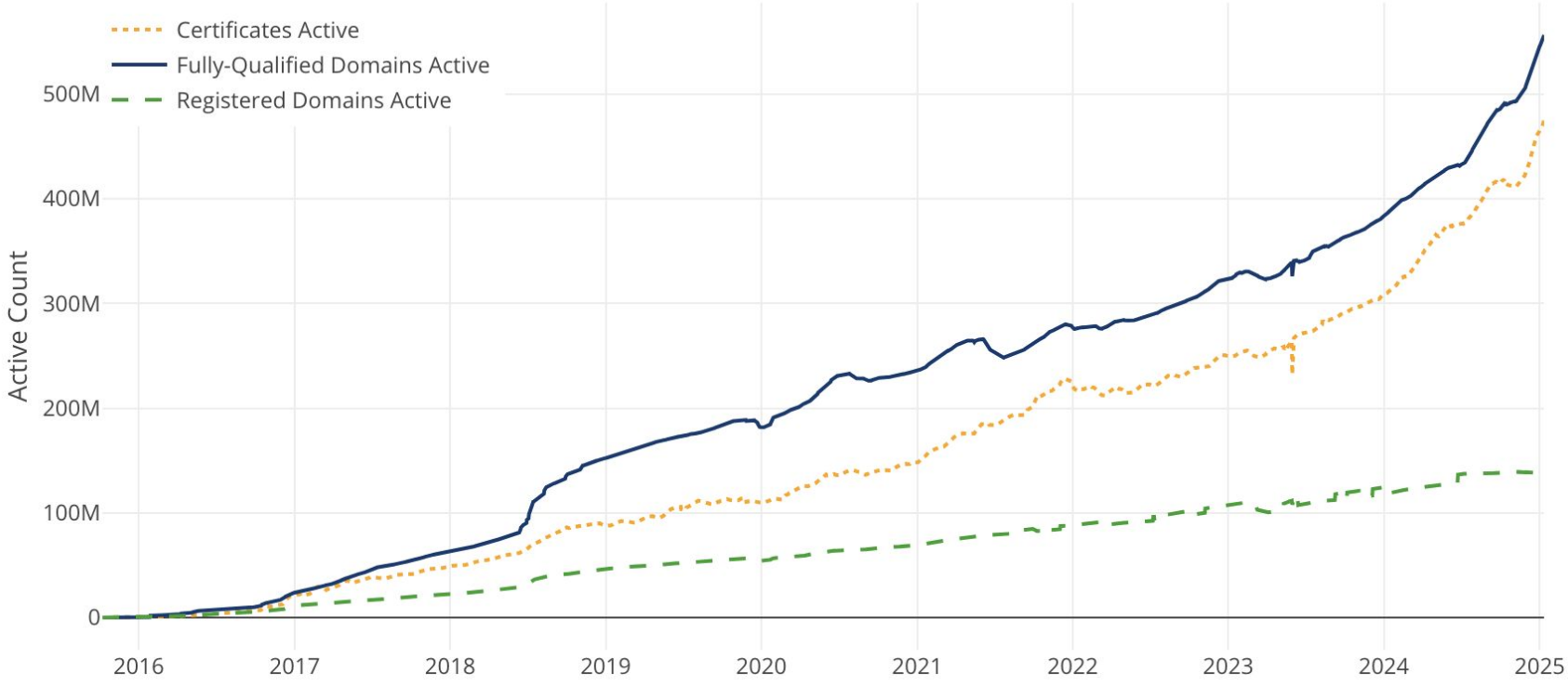
2013: Started planning

2014: Incorporated nonprofit ISRG

- Initial sponsors: Cisco, Mozilla, EFF, IdenTrust, University of Michigan, Akamai
- Started technical development
- Announced Let’s Encrypt

2015: Issued first Let’s Encrypt certificate

Fast Forward To Today



Organizational Infrastructure

Internet Security Research Group

ISRG is the nonprofit that runs Let's Encrypt.

- 25 staff total, including engineers, fundraising, comms, finance, management
- 3 projects: Let's Encrypt, Divvi Up, Prossimo
- Total annual budget of $6.7M
  - Funding from corporate sponsorship, individual donations, and grants

CA Infrastructure

Let’s Encrypt Staff

- Operated by 12 engineers
  - 3-4 writing CA software
  - 8-9 SREs operating infrastructure
- Supported by additional staff including fundraising, finance, legal, comms, HR, management

Physical Infrastructure

- 3 racks of hardware across 2 locations
  - HSMs, compute, db, networking
- Physical security more intense than a typical data center setup
- Cloud for some ancillary systems
- CDN for OCSP and CRLs
- Accommodations for performing key ceremonies

Software Stack

Linux, Proxmox, Nomad, OpenZFS, SaltStack, Ansible, MariaDB, Redis

Open source CA software, Boulder (Golang)

Moving more components to memory safe software: NTP (ntpd-rs), DNS (Hickory DNS), TLS (Rustls), Reverse Proxy (River)

Output and Cost

- Issuing 6 million certs/day on average
- Supporting > 585,000,000 websites
- OCSP: 15,000 RPS @ origin, 139,000 RPS @ edge
- CT log handling issuance for Let’s Encrypt and other CAs

Let’s Encrypt will cost about $4.5M in 2025.

What’s Coming

Short Lived Certificates

Currently: 90 day certificate lifetimes

Soon: Optional 6 day certificate lifetimes

Shorter lifetimes are better for security.

If your renewals are automated as they should be, this will have no impact.

IP Address Support

Right now you can only get certificates from Let's Encrypt for domain names.

Later this year you will be able to get certificates for IP addresses.

Will allow making authenticated TLS connections to IP addresses.

Ending OCSP Support

Turning it off in August of 2025. Use CRLs.

Serving 84 billion OCSP responses per week. 15,000/second at origin.

- Privacy problems
- Expensive to operate
- Takes up most of our HSM capacity

More ACME Renewal Info (ARI)

ARI is an API that can tell you when to get a new certificate.

If your client implements ARI, we will have it get a new certificate prior to any revocation.

Going to be pushing hard on clients to implement in 2025.

If you're an ACME client maintainer, let's chat after this talk.

Evolution of Transparency Logs

Certificate Transparency (CT) logs are moving from RFC 6962 to static-ct-api (“tiled logs”).

Goal is to make running logs easier and cheaper, and to make them more reliable.

Let’s Encrypt is already running tiled logs and is planning to shut down RFC 6962 logs ASAP.

Problems with RFC 6962 Logs

- Essentially requires a large and expensive cloud-managed SQL database.
- Database can be relatively easily overwhelmed by dynamic queries.
- Maximum Merge Delay violations can lead to distrust.
- Generally complex to run, expensive in terms of staff time.

Evolution of Transparency Logs

- Logs simply return easily cache-able “tiles” of responses rather than performing dynamic queries.
- Moves storage burden to S3 and serving to a CDN, don’t need a big managed database.
- No more Maximum Merge Delay (MMD) deadline to be violated - certs added to the tree before SCTs are returned.

Not Working on PQ Yet

Things we need to see before we could really do anything with PQ in the Web PKI:

- Web PKI community agreement on a plan
- Root Programs and CABF rules allowing for PQ signatures
- HSMs that support PQ algorithms
  - Probably at least 10,000 signatures per second per HSM (i.e. hardware support)

Principles

Principle: Simplicity

Web PKI requirements and technologies are complex, not easy to implement.

We try to encapsulate that complexity and expose it as simply as possible.

- Good for ease of use and adoption
- Good for security
- Good for financial sustainability

Always looking for ways to cut down on things!

Example: One API

Let’s Encrypt has one automated API for issuing certificates.

There is no other way to do it, no exceptions, not even internally.

If we want a certificate, we get it the same way you do.

Example: Database Architecture

2015-2025: Single instance without sharding or clustering (replicas for redundancy though).

Required powerful hardware but simplified infra, software, management for many years.

Maybe nearing the end of this strategy.

Principle: Efficiency

We have to be efficient, it’s our financial reality.

It’s also the right thing to to: we should do the most good we can with the public benefit dollars entrusted to us.

Example: Scaling

	2015	2018	2025
Engineers	4	8-9	12
Budget	$1M	$2.6M	$4.5M
Domains Served	300k	63M	500M

Example: Staff Scaling

We can’t keep adding staff at the rate our issuance increases. That’s not financially realistic.

We have to become more efficient every year to keep up with demand while staying on budget.

Make decisions that optimize for staff time and spend staff time reducing toil.

Principle: Transparency

Example: Incident Reports

Early on we started filing detailed public incident reports, before it was common to do so.

Wondered if it would lead to more or less trust.

Showed that we understood and responded well.

Led to more trust.

Example: Open Source CA Software

Our CA software, Boulder, is open source.

Others can see exactly how Let's Encrypt works if they want.

Lots of good mutual benefits for us and our dependencies, including Golang itself!

Helps ACME client developers.

Lessons

Lesson: Stay Out Of The Hot Path

Mercifully, Let's Encrypt is not involved in every TLS connection.

Except for OCSP, sort of, which is a problem we will rectify shortly by turning it off.

Not being on the hot path greatly reduces the amount of work involved.

Think about this when designing other services.

Lesson: Open Standards Can Help

Building an open standard API (ACME) helped our community build a client ecosystem more vibrant that we could ever have built ourselves.

Also helped move the whole Web PKI ecosystem forward. ACME is an industry standard now.

Lesson: Focus On What's Important

You can't do it all and you can't make everyone happy, especially if you want to be efficient.

Need to stay focused on what's most important, be willing to say no.

Example: No OV, EV, OCSP EOL, limited support

Example: We spend a lot of effort writing our own CA software because that's very important!

Lesson: Hardware is Cheap

(compared to staff)

Expensive hardware is often cheaper than paying for staff to manage more complex systems.

20 TB data, 10,000 reads/sec, 1600 writes/sec

Fits, with room for growth, on:

2x EPYC 7542, 2TB RAM, 24x 6.4TB NVMe (OpenZFS)

So far it has always been cheaper and more reliable to buy bigger hardware than shard/cluster (we do have replicas).

Lesson: Intimidation & Uncertainty

At times before we started, building Let's Encrypt seemed insurmountably hard. We needed to...

Create a legal entity. Hire staff.

Figure out how CAs actually work then build one.

Get trusted by all major browsers.

Figure out how to raise enough money every year.

It was a lot of work!

But it was not an insurmountable amount of work.

And it was totally worth it!

Billions of people experience a significantly more secure and privacy-respecting Internet every day.

Help us celebrate 10 years!

How to help:

- Help convince remaining non-HTTPS websites to make the switch.
- Donate to Let’s Encrypt.
- Get your company to sponsor us.
- Contribute to an ACME client.
- Help people on our community forum.
- Help make the next piece of public benefit infrastructure the Web needs happen!