Let's Encrypt

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

FOSDEM 2025

What We’ll Talk About Today

- Quick overview of Web PKI
- Let’s Encrypt History
- Our Infrastructure
- What’s Coming
- Principles & Lessons Learned
- How You Can Help

Quick Overview of Web PKI

Ideally you connect to websites using the TLS protocol. (TLS + HTTP = HTTPS)

TLS offers both:

Encryption: scrambles data in transit

Authentication: provides confidence regarding who you are communicating with

One without the other is a lot less secure.

Quick Overview of Web PKI

Digital TLS certificates are the mechanism for authentication in TLS. A server needs a certificate to enable TLS.

Certificate is a small file with:

1) domain(s)

2) public key for domain(s)

3) some other stuff

4) signature from the CA that

Quick Overview of Web PKI

Servers get these certificates from Certificate Authorities (CAs), like Let’s Encrypt.

This whole certificate ecosystem is called:

“Web Public Key Infrastructure” or “Web PKI”

Many more details, but this should get you through this talk.

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

What’s wrong with plain HTTP?

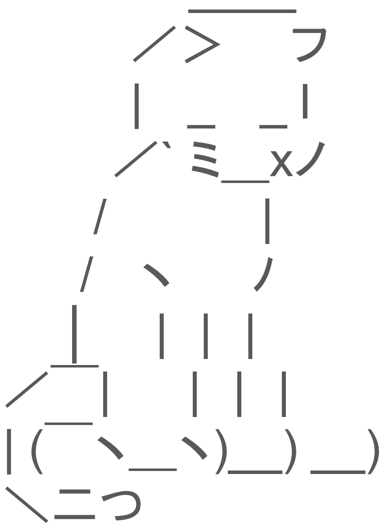
Everyone knows the data is **visible** on the network.

Obviously bad for some things, but not obvious to everyone that it’s bad for everything?

¯_(ツ)_/¯

Plain HTTP is bad for everything.

What many people don’t consider is that it’s also **modifiable**, so if you connect to a server with plain HTTP you can’t be confident the data you get back is what was sent!



An Undermining Problem

I worked on 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.

(please no 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 gave certificates away for free.

Let’s Encrypt

Getting To Work

2013: Started planning

2014: Incorporated nonprofit ISRG

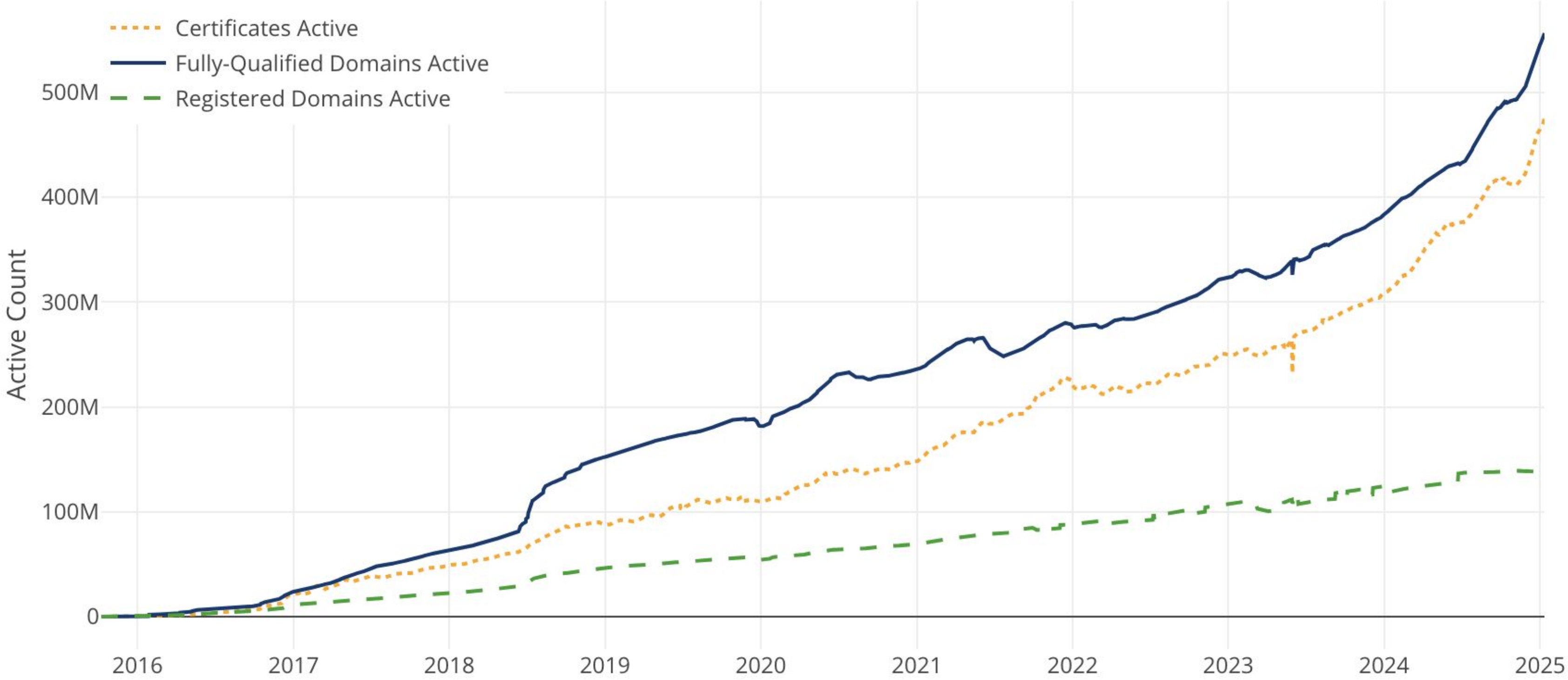
Initial sponsors: Cisco, Mozilla, EFF, IdenTrust, University of Michigan, Akamai

Started technical development

Announced Let's Encrypt

2015: Issued first Let's Encrypt certificate

Fast Forward To Today



Organizational Infrastructure

ISRG Today

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 (moving to MySQL)
- Redis
- Our open source CA software, Boulder

Pursuing Memory Safety

Our core CA software is memory safe (written in Go). Our infrastructure is not.

We are working on it.

- Already moved NTP to ntpd-rs
- Memory safe DNS coming soon
- Memory safe TLS coming soon
- Memory safe reverse proxy coming soon

Output and Cost

- Issuing more than 6 million certs/day
- Supporting > 500,000,000 websites
- OCSP: 15,000rps origin, 139,000rps 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 (Part 1)

Online **C**ertificate **S**tatus **P**rotocol (OCSP)

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

Signing OCSP responses takes up the largest percentage of our HSM capacity, far more than signing certificates.

Ending OCSP Support (Part 2)

OCSP is problematic for privacy.

Also expensive for us to run.

We’re turning it off later this year.

Use CRLs instead.

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.

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.

Nearing the end of this strategy. Will use Vitess.

Example: Static Websites

Our websites are static (Hugo on Netlify).

Easy to maintain.

Fast to load.

Good for security.

Has been this way since day one.

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.

Example: Simplicity → Efficiency

We already talked about simplicity.

It’s very related to, and good for, efficiency.

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, 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)

Even expensive hardware is often cheaper than deploying more complex systems and optimizations.

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: Hardware is Cheap

In other words:

Buying more expensive but simpler hardware is cheaper than paying engineers to manage cheaper but more complex hardware (e.g. a cluster).

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!

Thank you to our funders

Diamond Level Funders

Google

aws

Sovereign Tech Fund

Open Technology Fund

Alpha-Omega

Platinum Level Funders

moz://a

cisco

EFF

OVHcloud

Internet Society Foundation

Gold Level Funders

IdenTrust part of HID Global

Ford Foundation

shopify

IBM

SAP

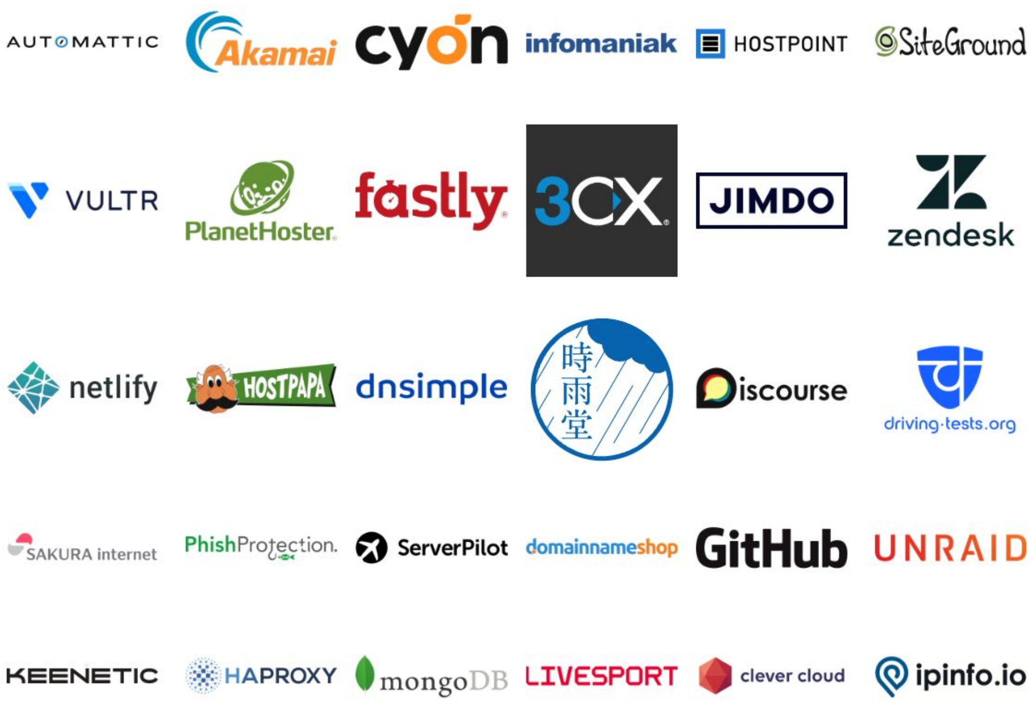
Squarespace

acton family giving

craig newmark philanthropies

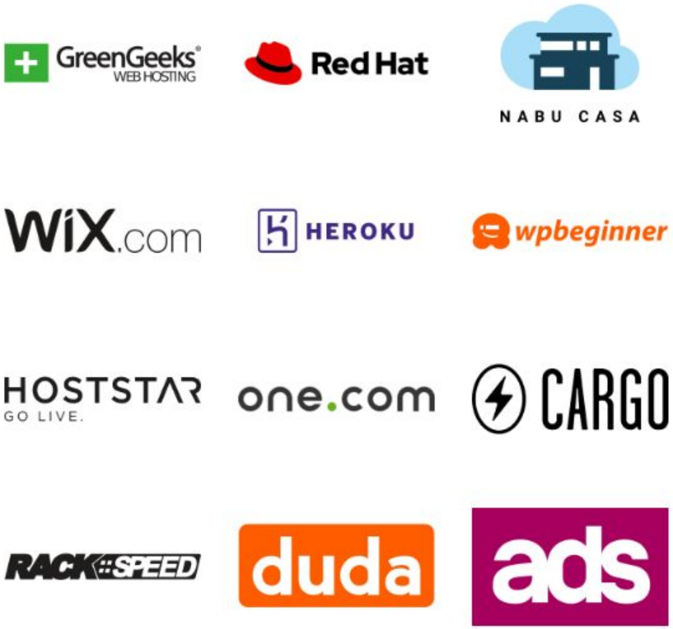
Thank you to our funders

Silver Level Funders



Thank you to our funders

Silver Level Funders



Thank you to our funders

Silver Level Funders

cdmon Teleport NGINX Part of F5 tailscale BitLaunch IBAN

4K Video Downloader entri CONFLUENT ngrok secure W2 20i®

Chainguard SerpApi IPv6.rs Self host, because trust is not security. icuk interServer.net DigitalOcean

CDN77 SNIPE-IT OPEN SOURCE ASSET MANAGEMENT SHOWIT ClouDNS SMTP2GO