Let’s Encrypt

Eric Rescorla
Mozilla
ekr@rtfm.com

What problem are we trying to solve?

- Not enough TLS on the Internet
- Current estimates:
  - ~32% of page loads*
  - ~56% of HTTP transactions*
- We’d like these numbers to be 100%

* Data from Firefox Telemetry

Getting a certificate is no fun

“I can’t f’ing figure out how to get a cert from [redacted] - kid you not

...

god help people that don’t know what a CSR is

...

I am like 45 minutes in ”

--- Cullen Jennings, PhD
Cisco Fellow
Former IETF Area Director

A new certificate authority

- Free
- Automatic
- Secure
- Transparent
- Open
- Cooperative

Founding Sponsors

- Mozilla
- Akamai
- Cisco
- EFF
- IdenTrust

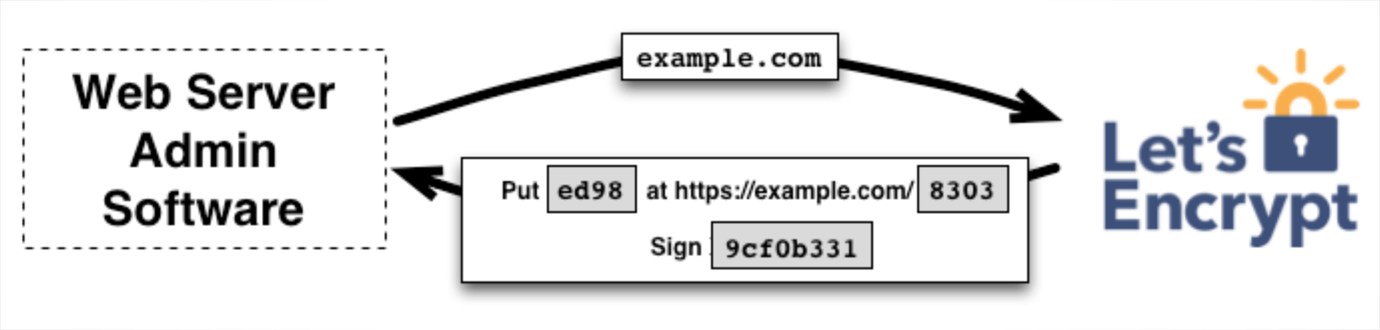
Board of Directors

- **Josh Aas** (Mozilla) — *ISRG Executive Director*
- **Stephen Ludin** (Akamai)
- **Dave Ward** (Cisco)
- **J. Alex Halderman** (University of Michigan)
- **Andreas Gal** (Mozilla)
- **Jennifer Granick** (Stanford Law School)
- **Alex Polvi** (CoreOS)
- **Peter Eckersley** (EFF) — *Observer*

Initial offering

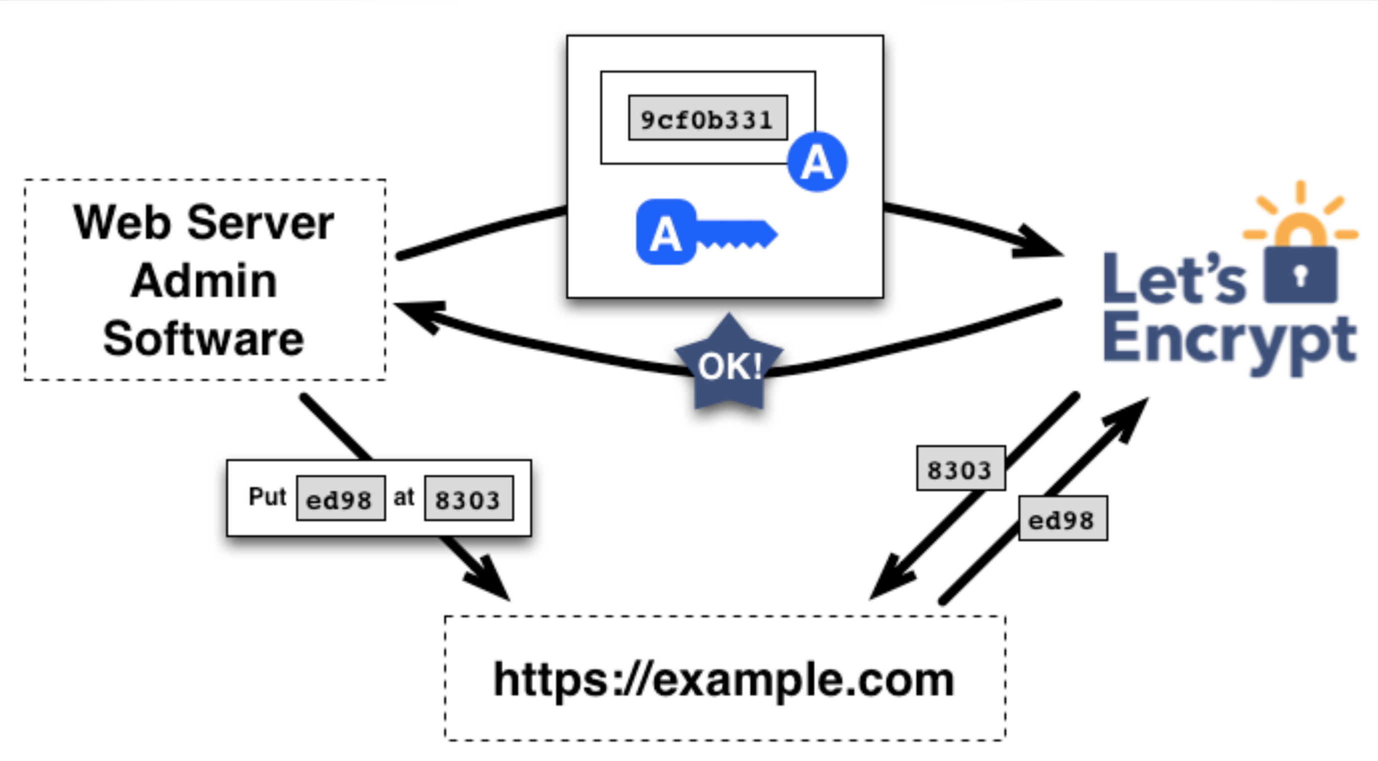
- Domain Validated certificates only
- Automated issuance
- Published APIs/protocols
- Expect to issue first certificate Q2 2015

Domain Registration


Web Server Admin Software
example.com
Let's Encrypt
Put ed98 at https://example.com/ 8303
Sign 9cf0b331

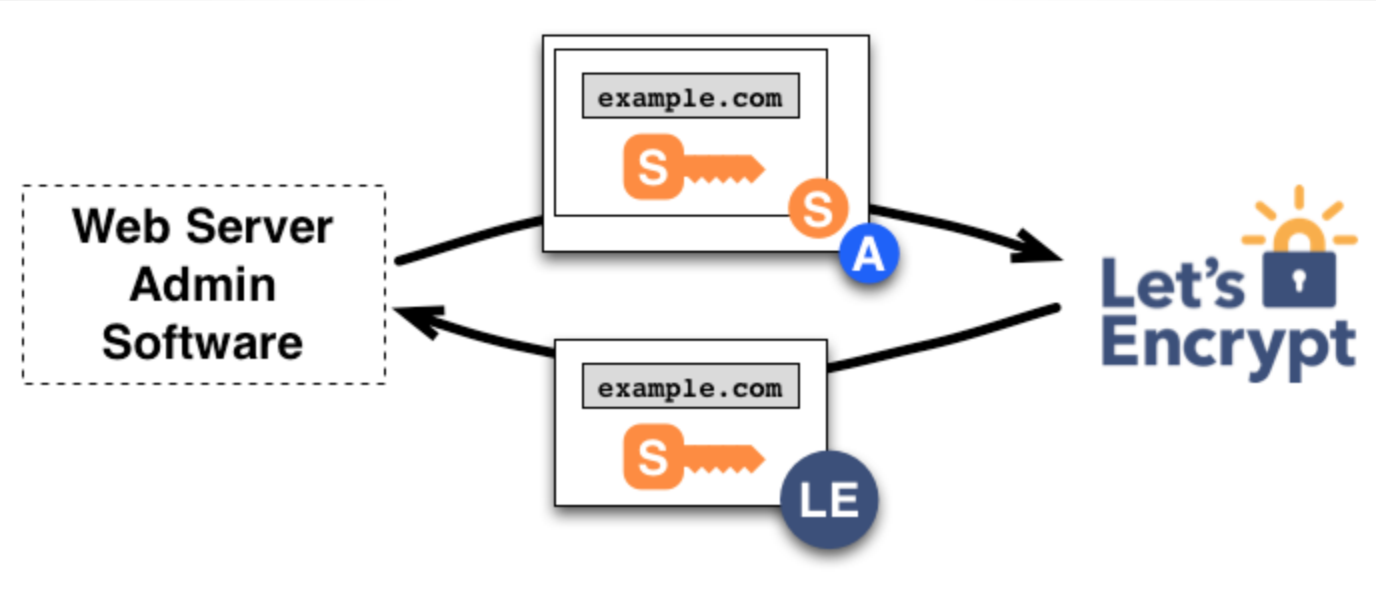
From: https://letsencrypt.org/howitworks/technology/

Domain Validation



From: https://letsencrypt.org/howitworks/technology/

Certificate Issuance



From: https://letsencrypt.org/howitworks/technology/

FAQs

- Will these certificates be globally verifiable?
- Are you applying for root program membership?
- What about EV/OV?
- What about non-Web?
- How does this interact with DANE?
- Will you do OCSP stapling/short-lived certs?
- Are you standardizing this?
- Who is doing the client software?
- How can I help?

Learn more

Main site: https://letsencrypt.org

Specs & Code: https://github.com/letsencrypt/

IETF Mailing List: https://www.ietf.org/mailman/listinfo/acme