



Richard Barnes

Mozilla

rlb@ipv.sx

What problem are we trying to solve?

- Not enough encryption on the Internet
- Current estimates for HTTPS:
 - ~32% of page loads*
 - ~65% of HTTP transactions**
- These numbers should be 100%
- OBTW: <https://https.cio.gov>

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

Sponsors

mozilla



AUTOMATTIC

THIS SPACE
FOR SALE

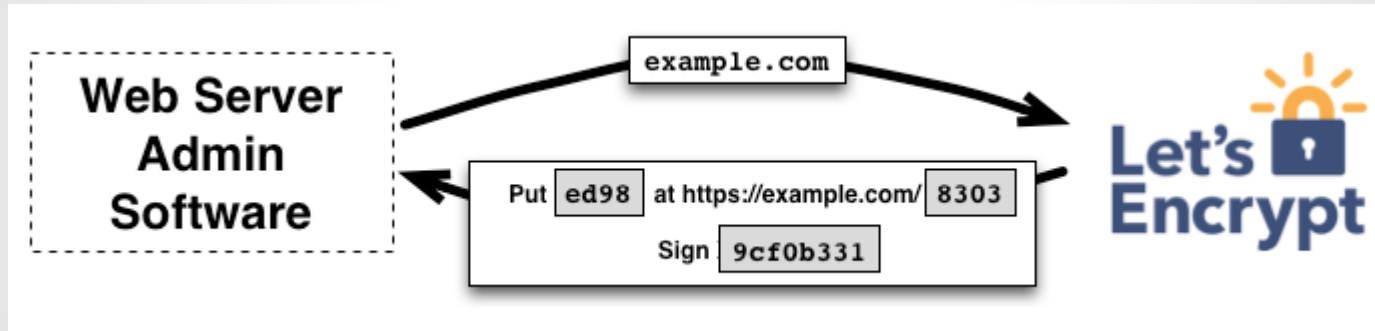
Board of Directors

- **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

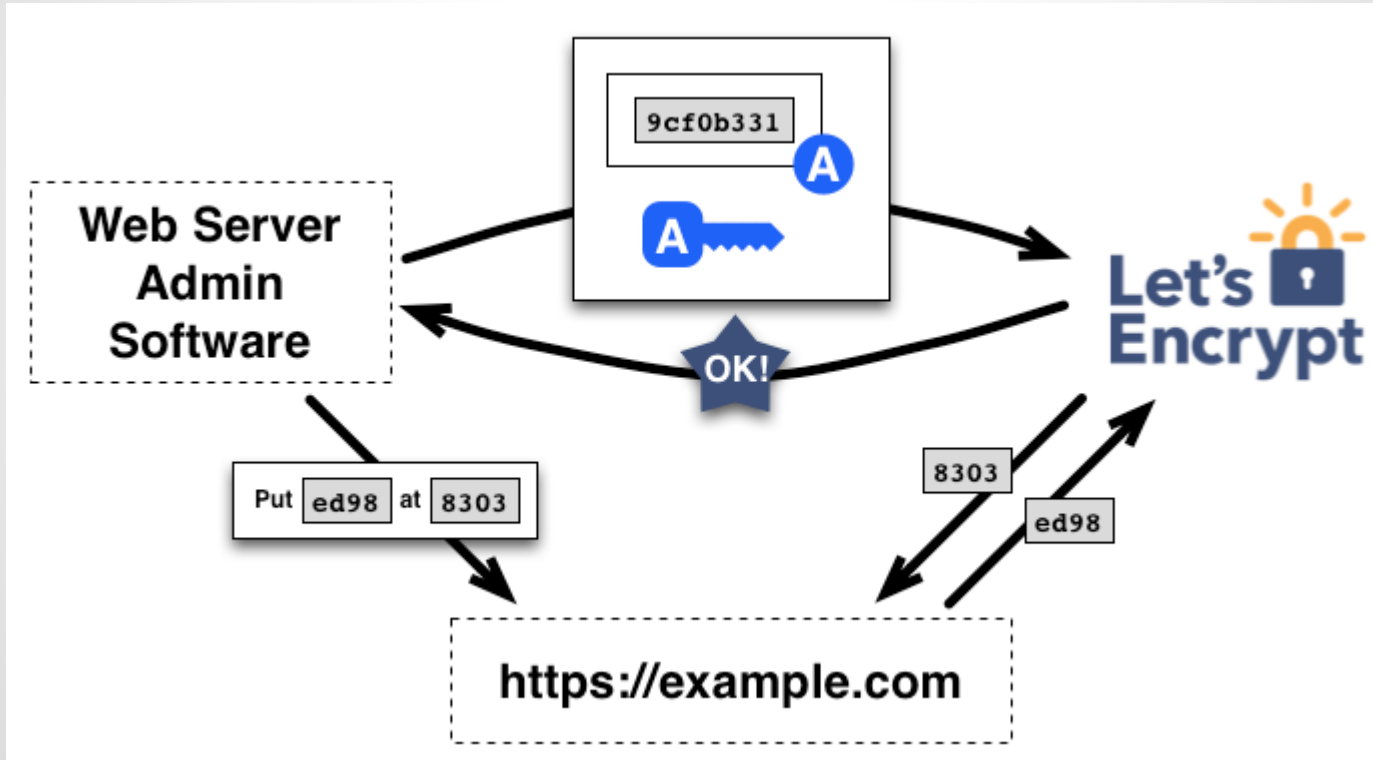
- Domain Validated certificates only
- Automated issuance
- Published APIs/protocols
- Expect to issue first certificate Q2 2015

Domain Registration

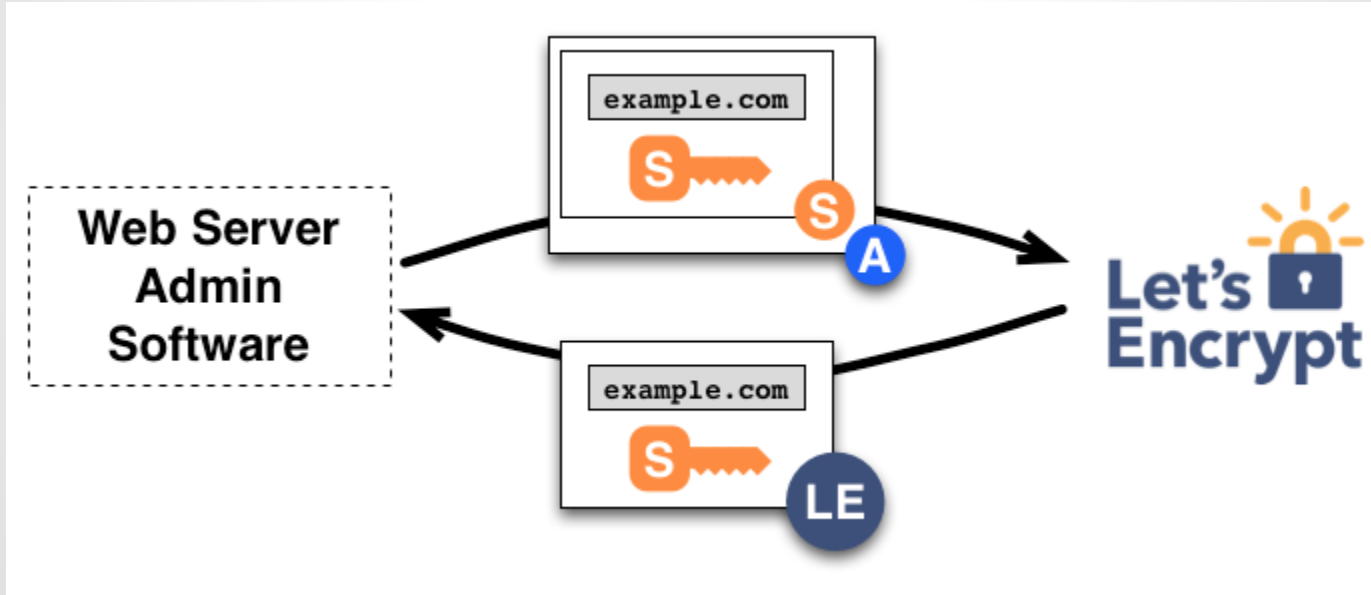


From: <https://letsencrypt.org/howitworks/technology/>

Domain Validation



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?

FAQs

- Will these certificates be globally verifiable? **Yes**
- Are you applying for root program membership? **Yes**
- What about EV/OV? **No**
- What about non-Web? **Probably**
- How does this interact with DANE? **Well, we hope**
- Will you do OCSP stapling/short-lived certs? **Probably**
- Are you standardizing this? **See ACME BoF**
- Who is doing the client software? **[your name here]**
- How can I help? **<https://github.com/letsencrypt/>**

Learn more

Main site: <https://letsencrypt.org>

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

IETF Mailing List:

<https://www.ietf.org/mailman/listinfo/acme>