ACME Objectives

Eric Rescorla
Mozilla
ekr@rtfm.com

What problem are we trying to solve?

- Not enough TLS on the Internet
- Current estimates for HTTPS:
  - ~32% of page loads*
  - ~65% of HTTP transactions**
- These numbers should be 100%

Data from Firefox telemetry. * http://mzl.la/1wUbvWo ** http://mzl.la/1xgEh49

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

Background: Let’s Encrypt

- A new certification authority
- Free
- Automatic
- Secure
- Transparent
- Open
- Cooperative

What do we want?

- Automatic (=> reduced operational cost)
    - Registration
    - Verification of domain control
    - Reissuance / renewal
- Seamless
    - Requires minimal operator intervention
    - Single time setup, permanent operation
- Flexible
    - Adapts to different CA policies and practices

Example: Certificate lifetimes

- Currently certificates have long lifetimes
  - OCSP for revocation
  - Potentially OCSP must-staple for hard-fail
- Lots of talk about short-lived certificates
  - As an alternative to OCSP + must-staple
- Natural fit for automatic renewal
  - CA tells you lifetime
  - Server automatically retrieves new cert
- Result: CA can dial up and down lifetime

Example: New algorithms

- Right now servers support RSA (+ maybe ECDSA)
- What about new algorithms
  - New curves
  - EdDSA
- This can be done automatically
  - Client gets new software
  - Discovers CA supports new algorithm
  - Mission accomplished

Example: Delegated Issuance

- Datacenter with a lot of servers
  - Multiple servers for the same domain
  - Multiple domains for the same server
  - Mix-and-match
- Authenticate domain once
  - Establish an authentication credential
  - Use that key to issue new certificates
- Authentication key K tied to set of domains D
  - Server can get a cert for any subset of domains in D

Questions?