Let's Encrypt

A FREE CERTIFICATE AUTHORITY TO ENCRYPT THE ENTIRE WEB

J.C. Jones <jcjones@letsencrypt.org>

ACRONYMS

- SSL (Secure Sockets Layer) – the old name for the main security layer for TCP
- TLS (Transport Layer Security) – the modern name for SSL
- HTTPS (HTTP Secure) – HTTP plus TLS X.509 – the format used by TLS certs
- PKI (Public Key Infrastructure) – an infrastructure for distributing crypto keys

IMPORTANCE OF TLS

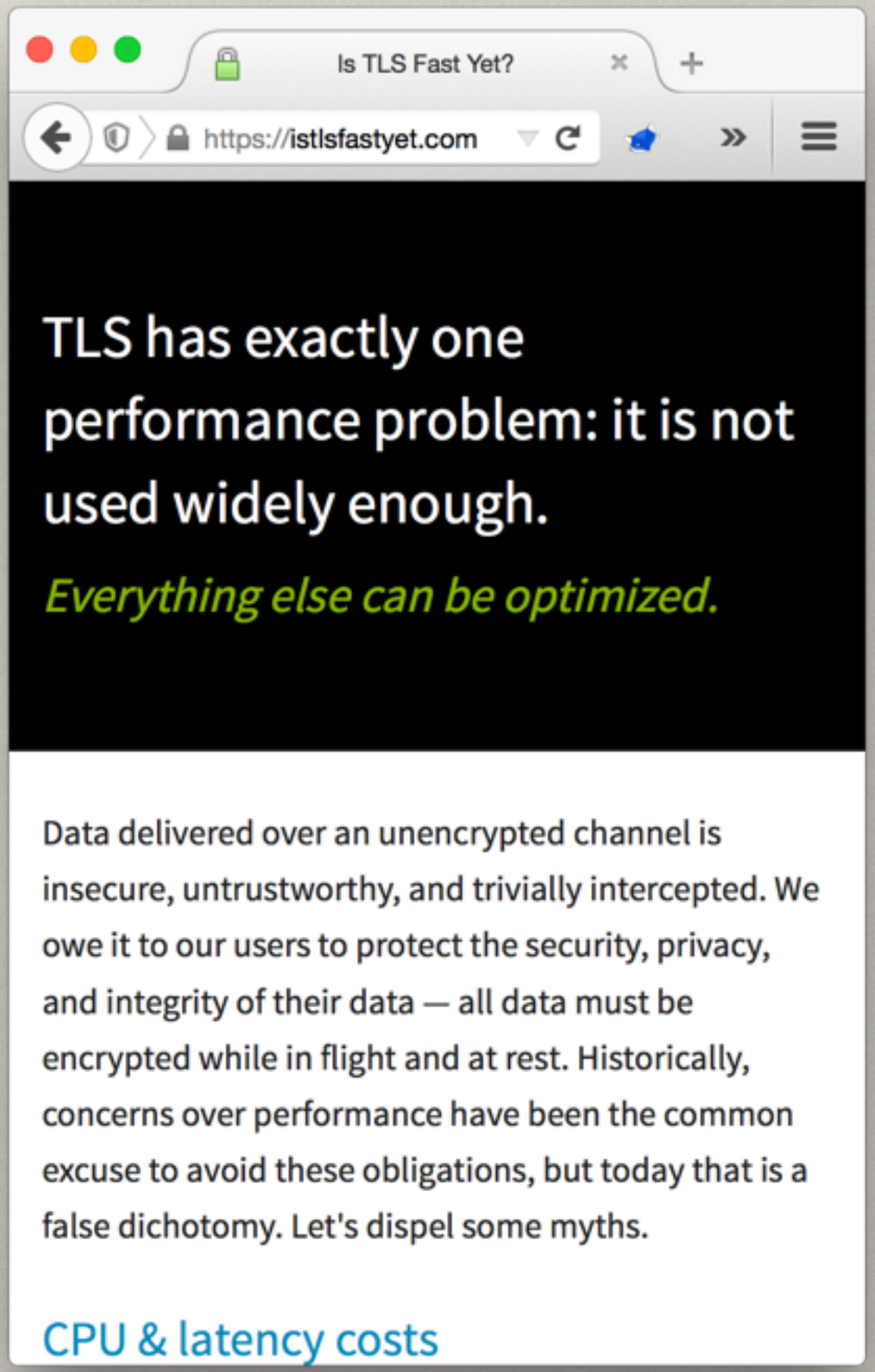
- Not just for financial data or website logins
- Wide area networks are inherently untrustworthy
- **Plain HTTP offers no defense**

IMPORTANCE OF TLS

- Not just for financial data or website logins
- Wide area networks are inherently untrustworthy
- **Plain HTTP offers no defense**
- Sidejacking
- Location tracking
- Reader privacy
- Content-based censorship
- ISP header or advertisement injection

HANGUPS

- Lower performance
- Inhibiting load balancing
- Certificates cost money
- It is time consuming, error-prone and complex to install certificates correctly

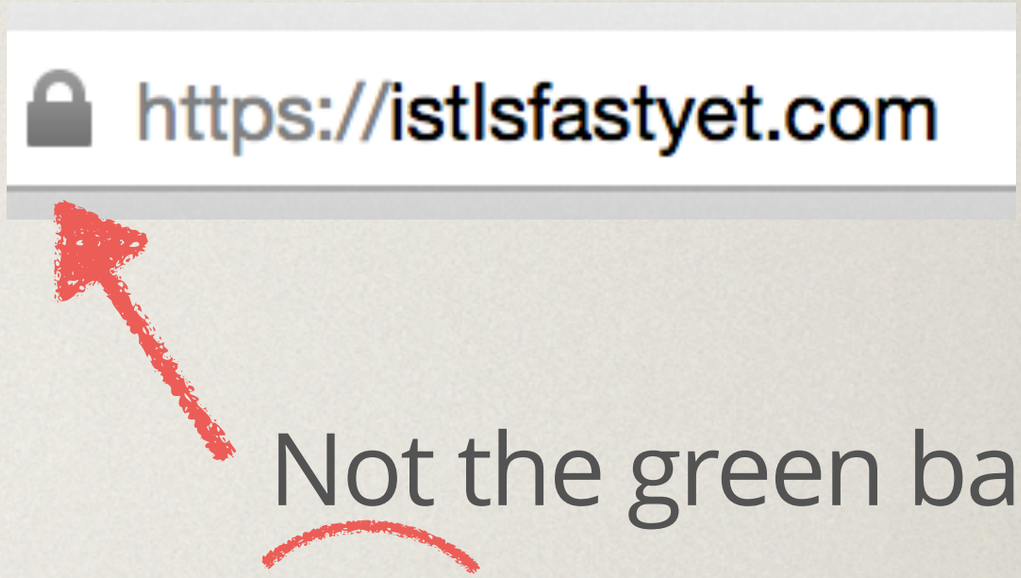


LET'S ENCRYPT

- Initially, a collaboration among EFF, University of Michigan, and Mozilla
- Fully-automated Certificate Authority
- Publicly trusted in all major web browsers

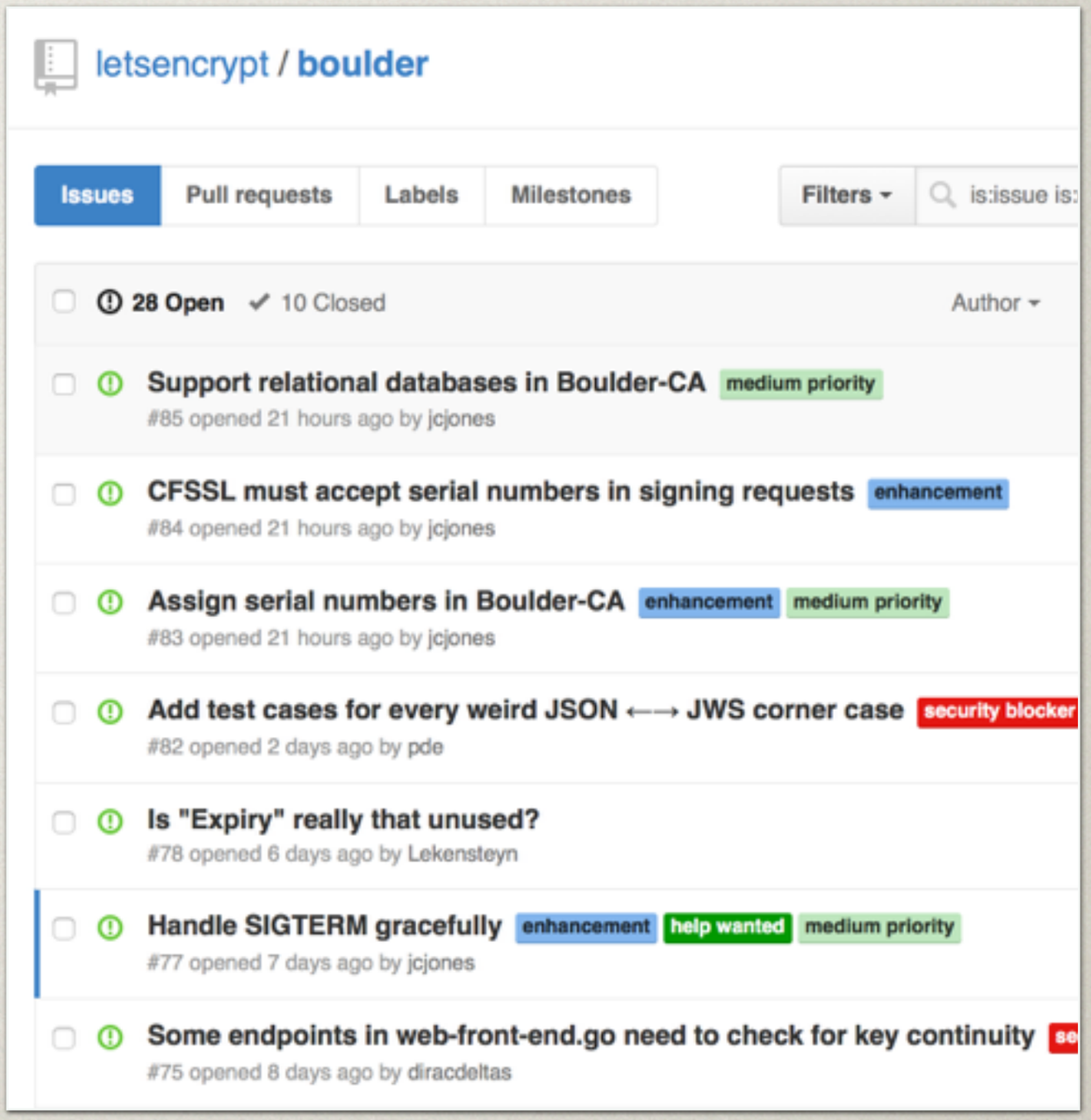
DOMAIN VALIDATION

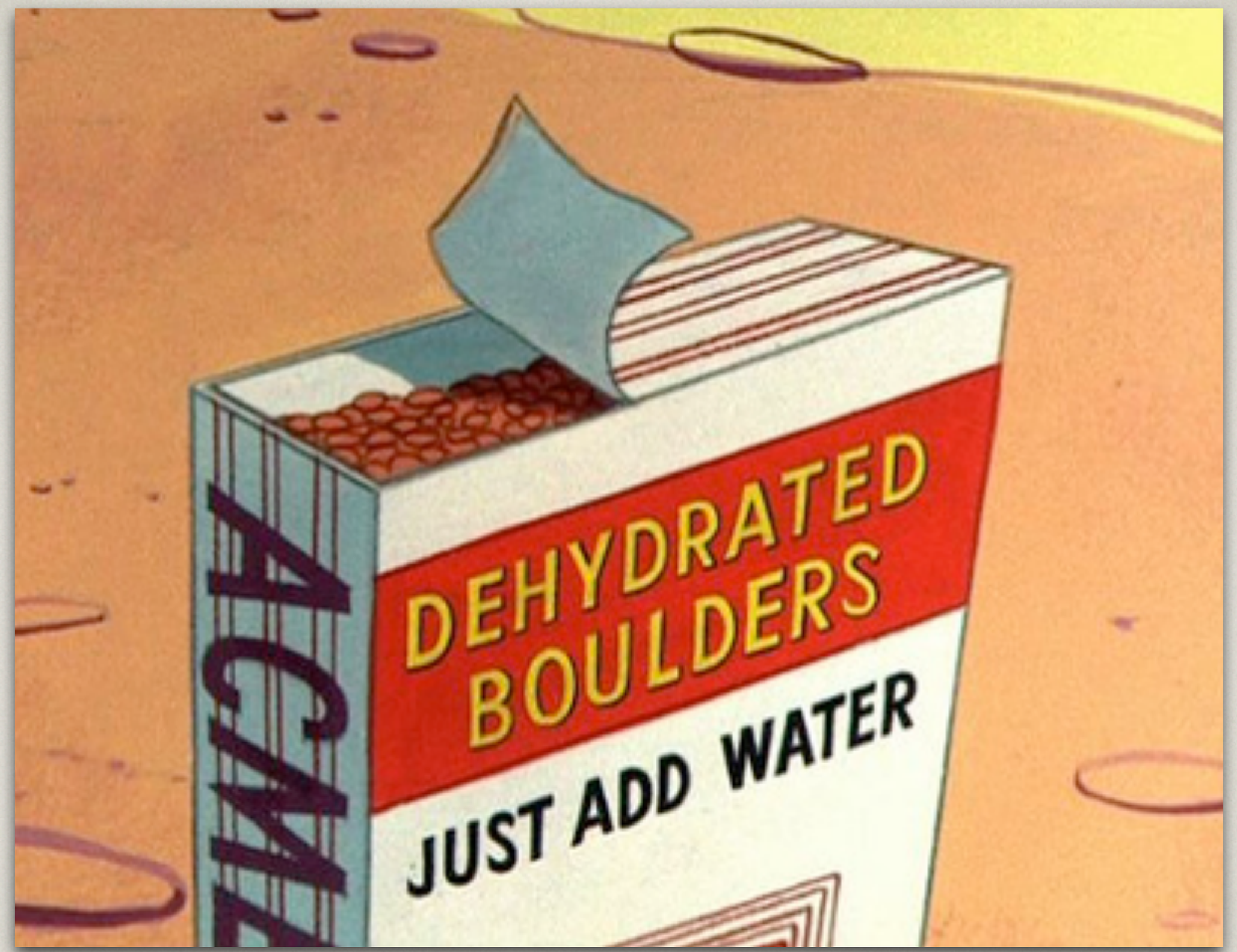
- The free certificates attest that the applicant controls the domain
  - OV and EV are out of scope for now
- Attesting domain control is ripe for automation



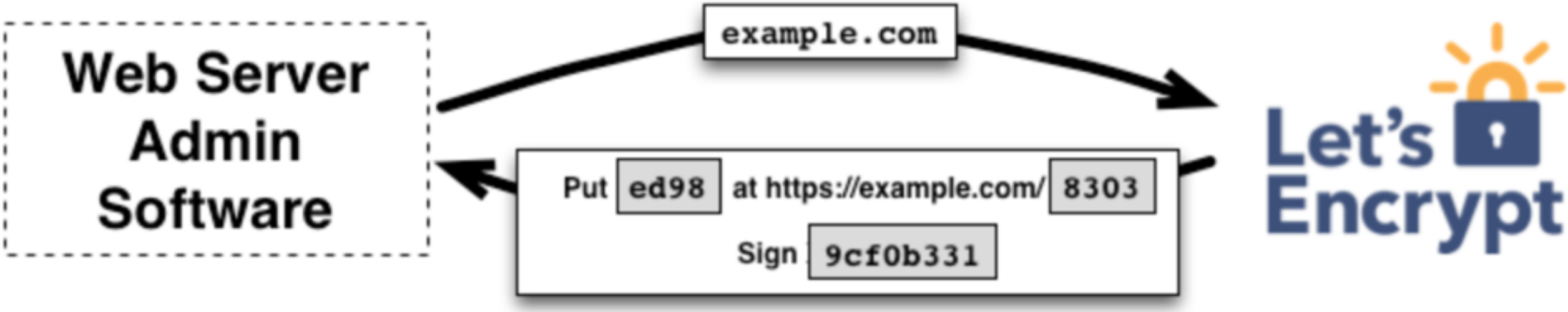
PUBLICLY TRUSTED

- Comply with all WebTrust audit requirements
- Open source software and specs
- Open Audits / Publication
- Browser root programs
- Cross-signatures from IdenTrust

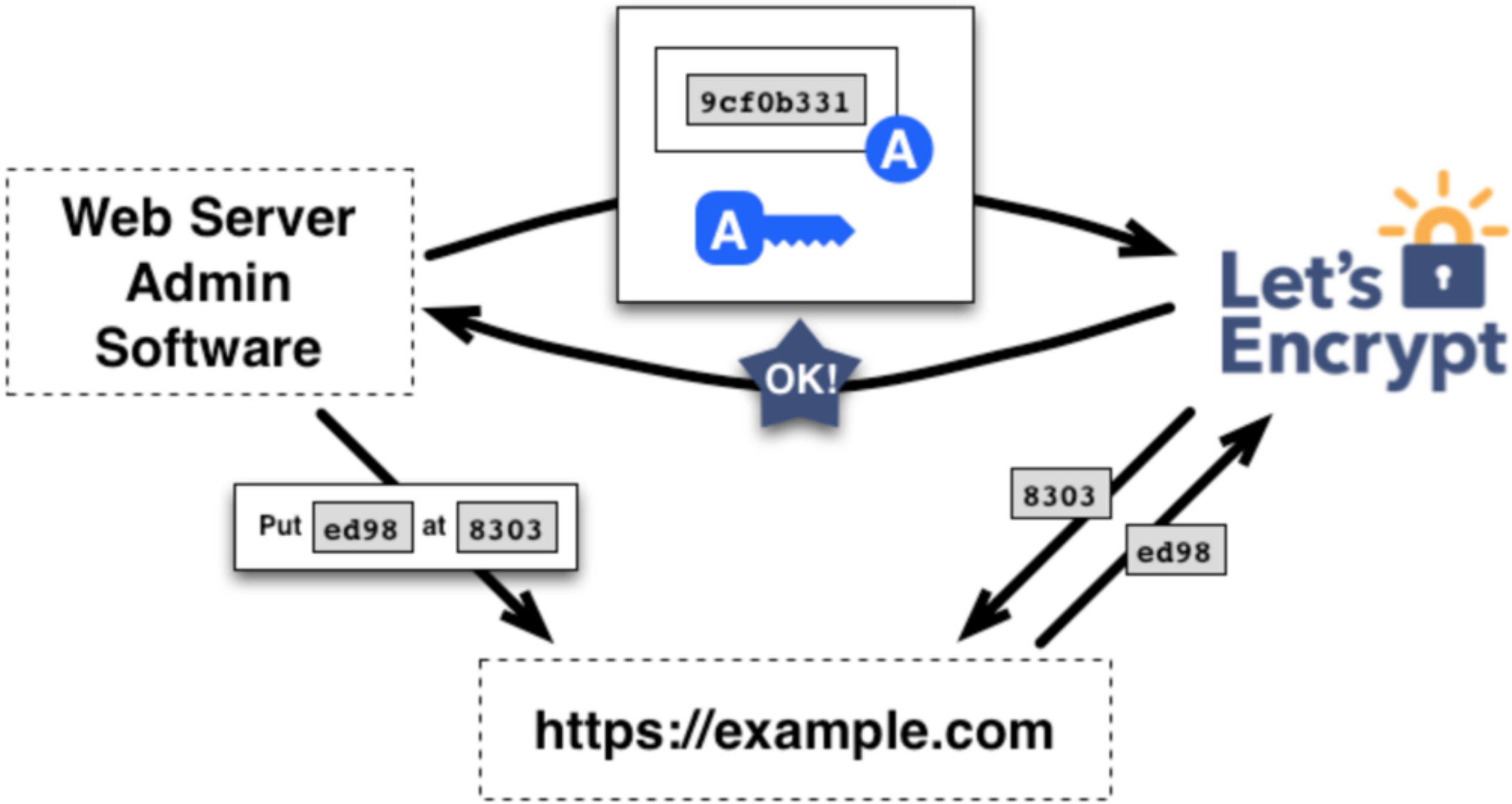




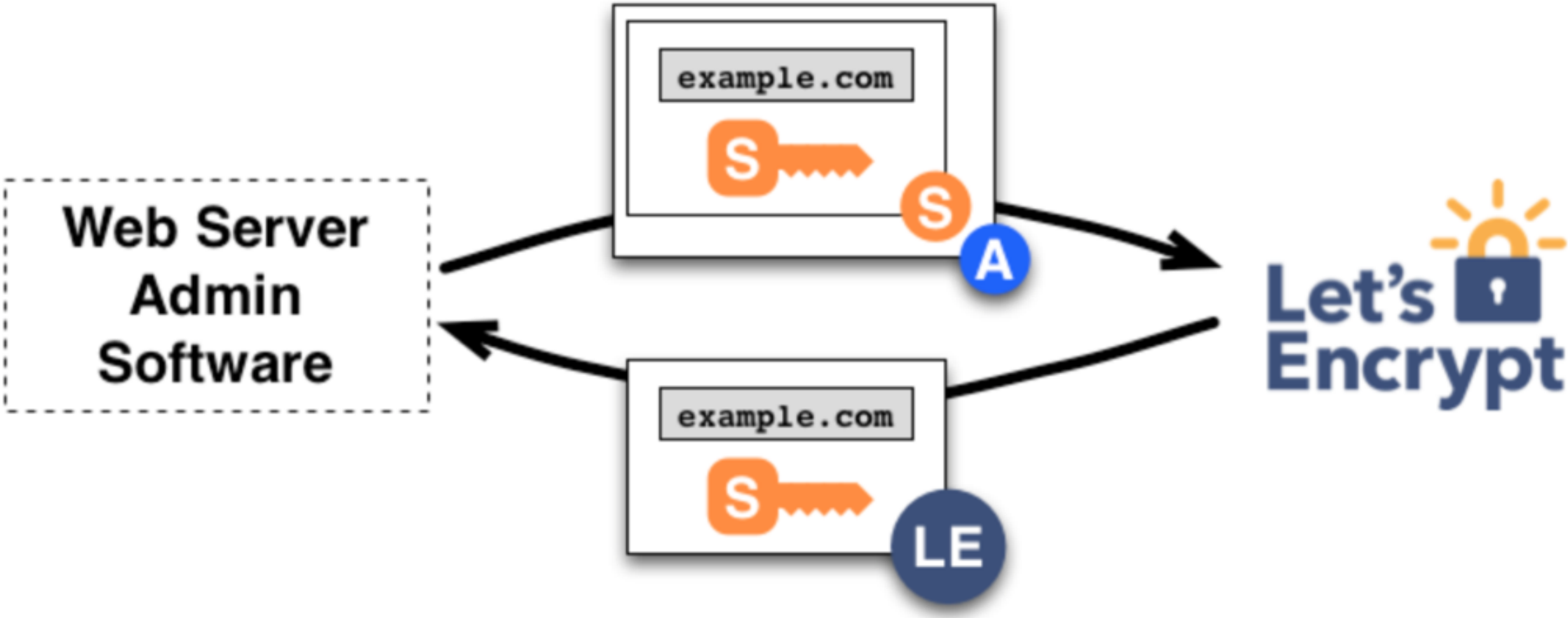
ACME



DOMAIN REGISTRATION



DOMAIN VALIDATION



CERTIFICATE ISSUANCE

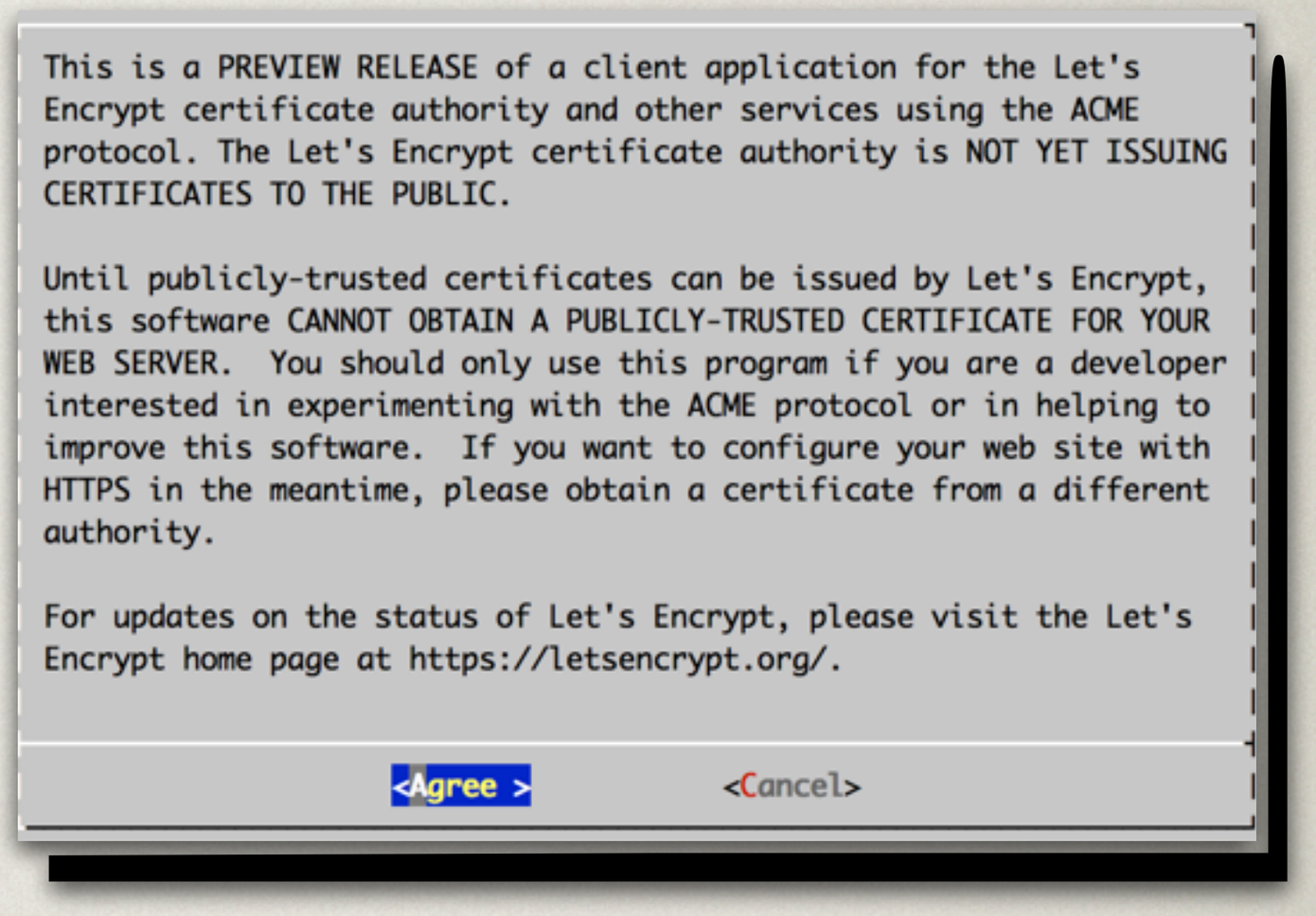
ACME CONVENIENCE

- We anticipate people who administer their own web servers will run something like
  - `sudo apt-get install lets-encrypt`
  - `sudo lets-encrypt`

  and the lets-encrypt client will not only obtain, but also deploy, the new cert in less than one minute

FUTURE

- ACME is on the path to being an RFC
- Foresee integration into all web servers and application hosting platforms
- Free and open



THANKS, GATORLUG!

Contact: jcjones@letsencrypt.org
BD4E B26B 978D F884

Thanks to my colleagues with whom I'm developing Let's Encrypt and ACME, including Josh Aas (Mozilla), Richard Barnes (Mozilla), Peter Eckersley (EFF), Alex Halderman (UMich), James Kasten (UMich), Eric Rescorla (Mozilla), and Seth Shoen (EFF)

CHALLENGES AND RESPONSES

- Source code: https://github.com/letsencrypt
- ACME spec: https://letsencrypt.github.io/acme-spec/