



# Let's Encrypt

A FREE CERTIFICATE AUTHORITY  
TO ENCRYPT THE ENTIRE WEB

J.C. Jones <[jcjones@letsencrypt.org](mailto: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

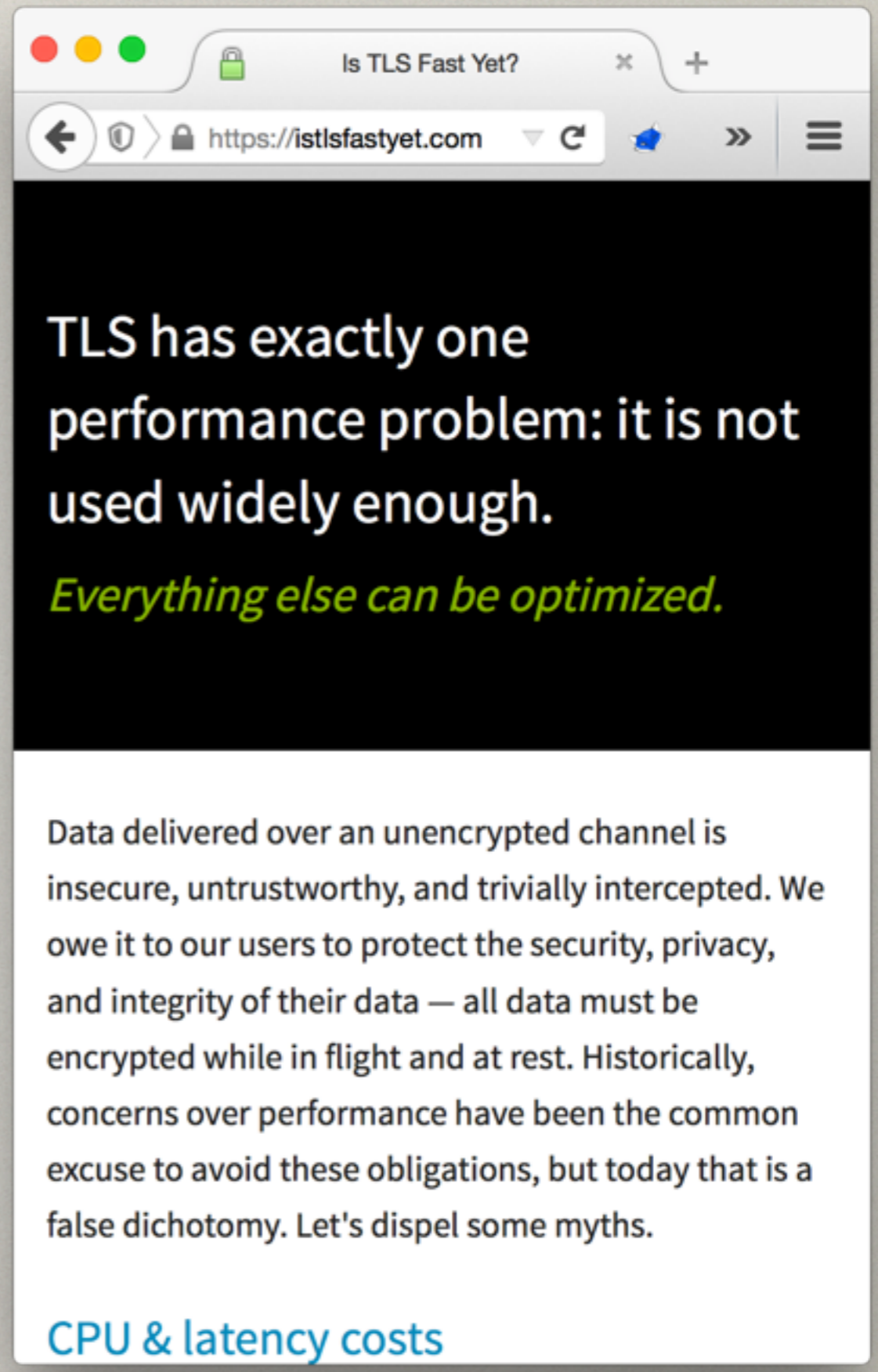
- Not just for financial data or website logins
- Wide area networks are inherently untrustworthy
- **Plain HTTP offers no defense**

# 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

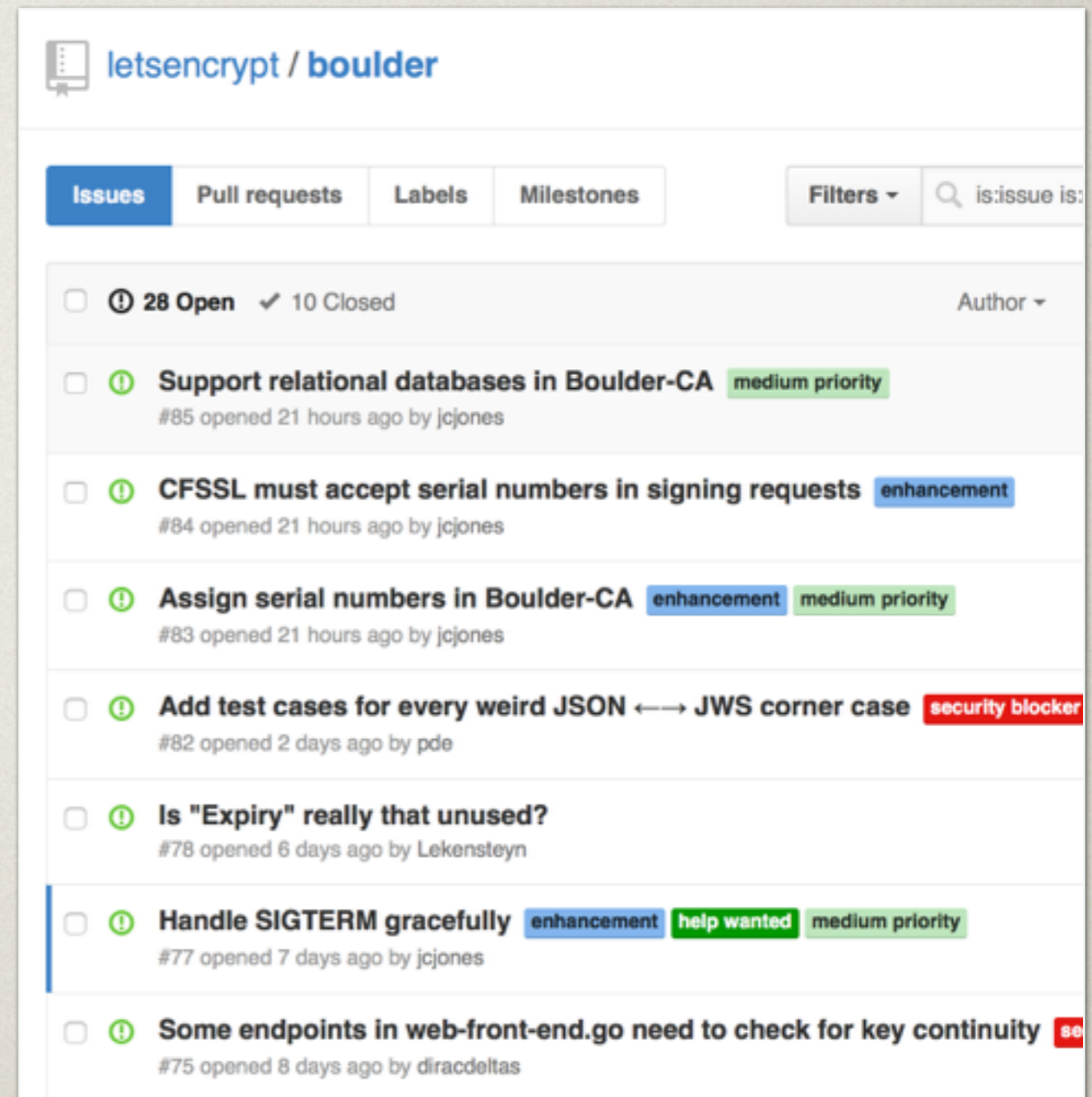
- The free certificates attest that the applicant controls the domain
  - OV and EV are out of scope for now
- Attesting domain control is ripe for automation



  Not the green bar

# PUBLICLY TRUSTED

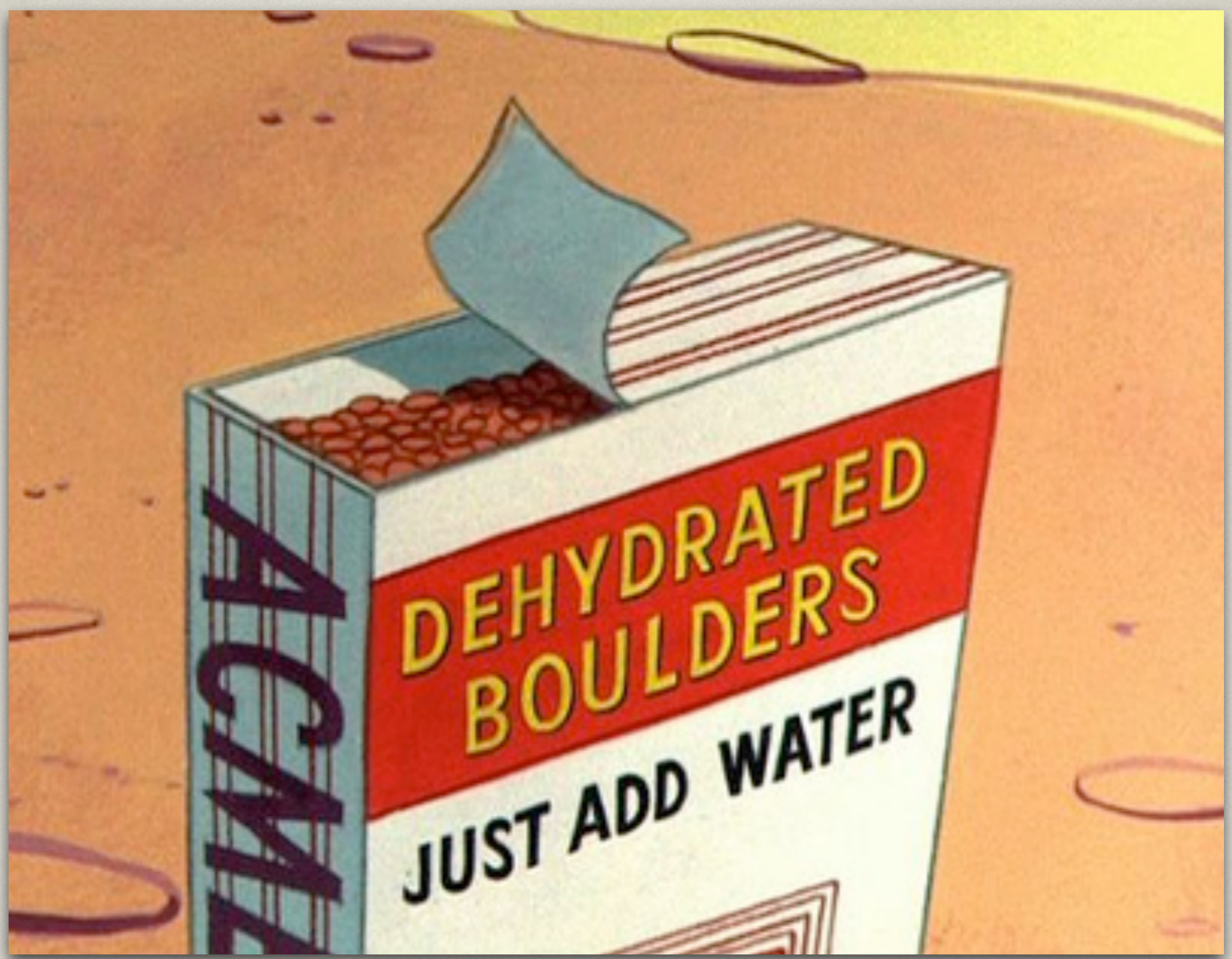
- Comply with all WebTrust audit requirements
- Open source software and specs
- Open Audits / Publication
- Browser root programs
- Cross-signatures from IdenTrust



The screenshot displays the GitHub interface for the repository 'letsencrypt / boulder'. The 'Issues' tab is selected, showing a list of 28 open issues and 10 closed issues. The issues are listed with their titles, priority labels, and the user who opened them. The issues are:

- Support relational databases in Boulder-CA** medium priority  
#85 opened 21 hours ago by jcjones
- CFSSL must accept serial numbers in signing requests** enhancement  
#84 opened 21 hours ago by jcjones
- Assign serial numbers in Boulder-CA** enhancement medium priority  
#83 opened 21 hours ago by jcjones
- Add test cases for every weird JSON  $\longleftrightarrow$  JWS corner case** security blocker  
#82 opened 2 days ago by pde
- Is "Expiry" really that unused?**  
#78 opened 6 days ago by Lekensteyn
- Handle SIGTERM gracefully** enhancement help wanted medium priority  
#77 opened 7 days ago by jcjones
- Some endpoints in web-front-end.go need to check for key continuity** security blocker  
#75 opened 8 days ago by diracdeltas

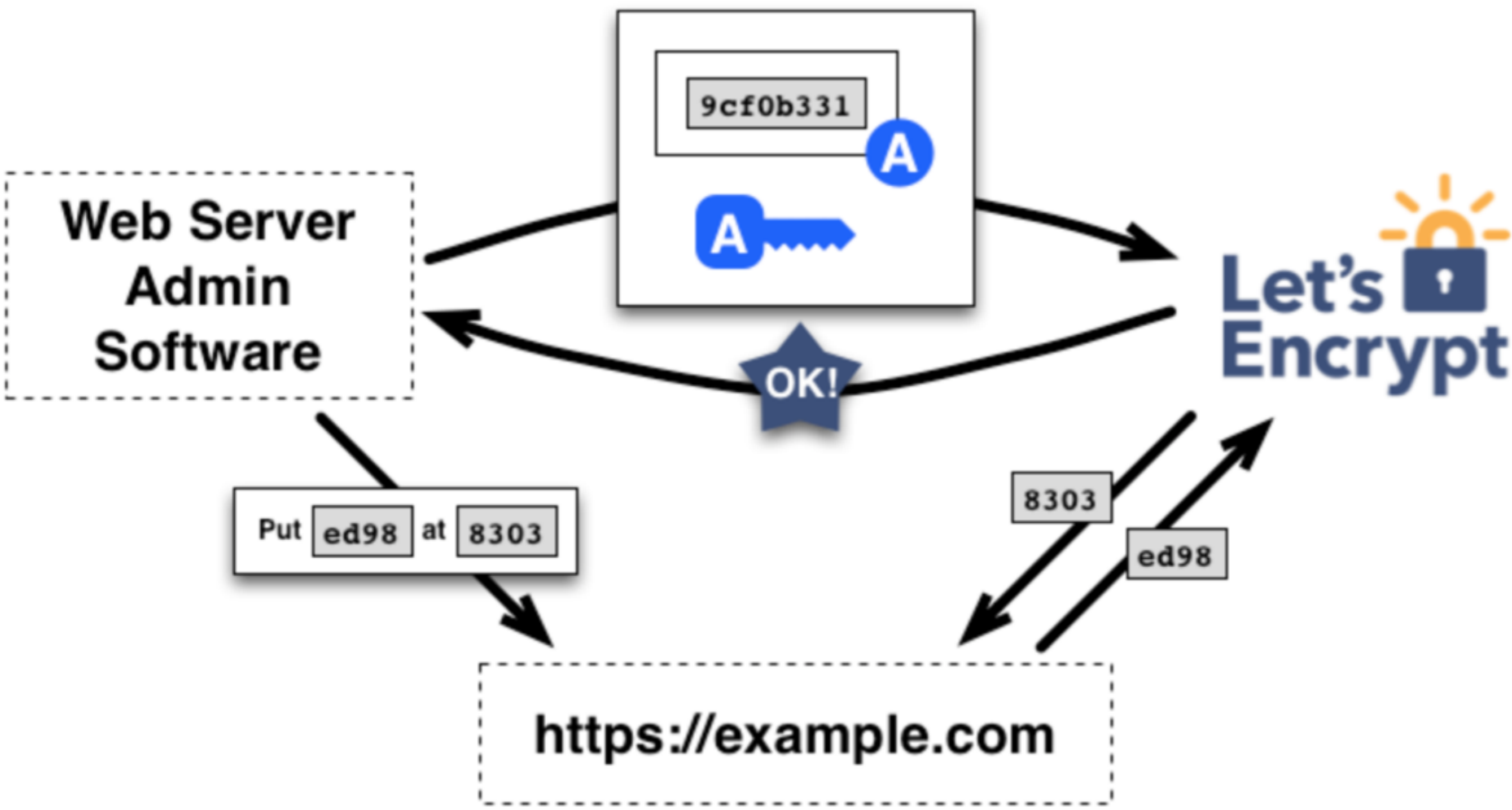




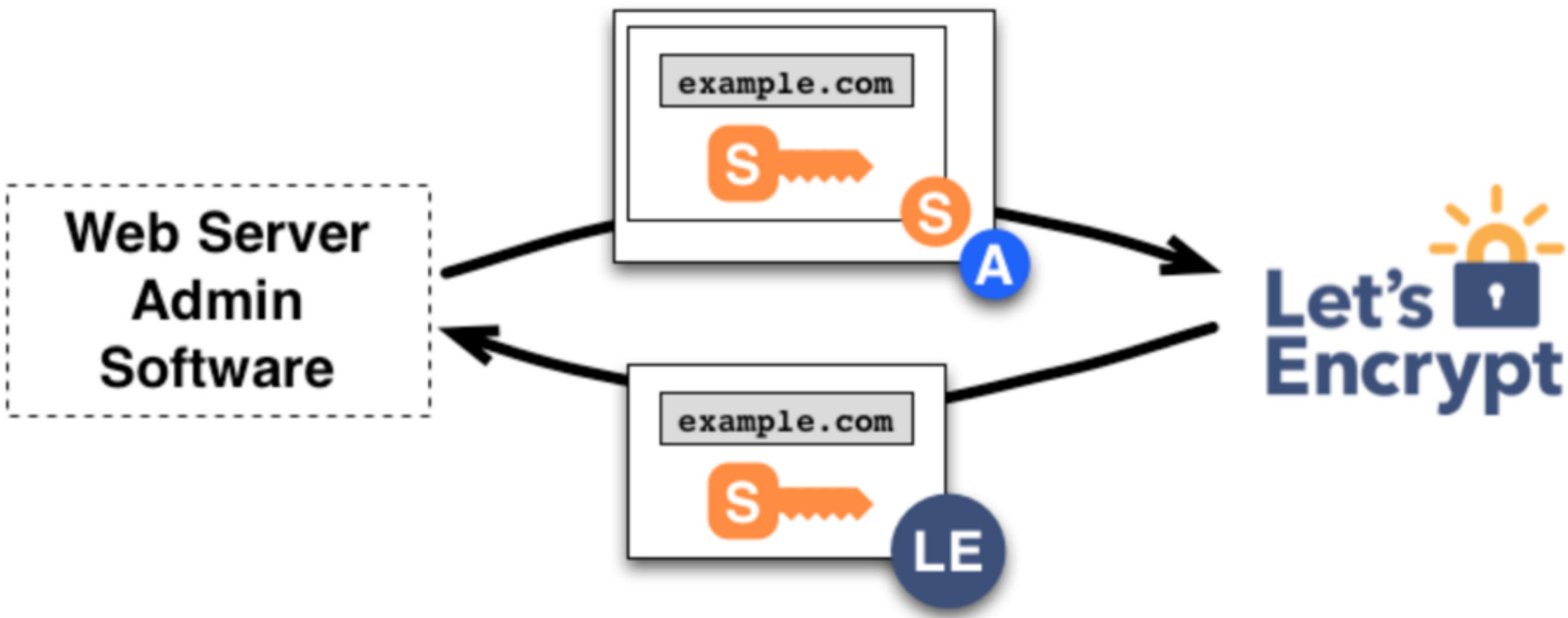
**ACME**



# 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

This is a PREVIEW RELEASE of a client application for the Let's Encrypt certificate authority and other services using the ACME protocol. The Let's Encrypt certificate authority is NOT YET ISSUING CERTIFICATES TO THE PUBLIC.

Until publicly-trusted certificates can be issued by Let's Encrypt, this software CANNOT OBTAIN A PUBLICLY-TRUSTED CERTIFICATE FOR YOUR WEB SERVER. You should only use this program if you are a developer interested in experimenting with the ACME protocol or in helping to improve this software. If you want to configure your web site with HTTPS in the meantime, please obtain a certificate from a different authority.

For updates on the status of Let's Encrypt, please visit the Let's Encrypt home page at <https://letsencrypt.org/>.

<Agree >

<Cancel>

# THANKS, GATORLUG!

Contact: [jcjones@letsencrypt.org](mailto: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/>