Let's Encrypt Everything

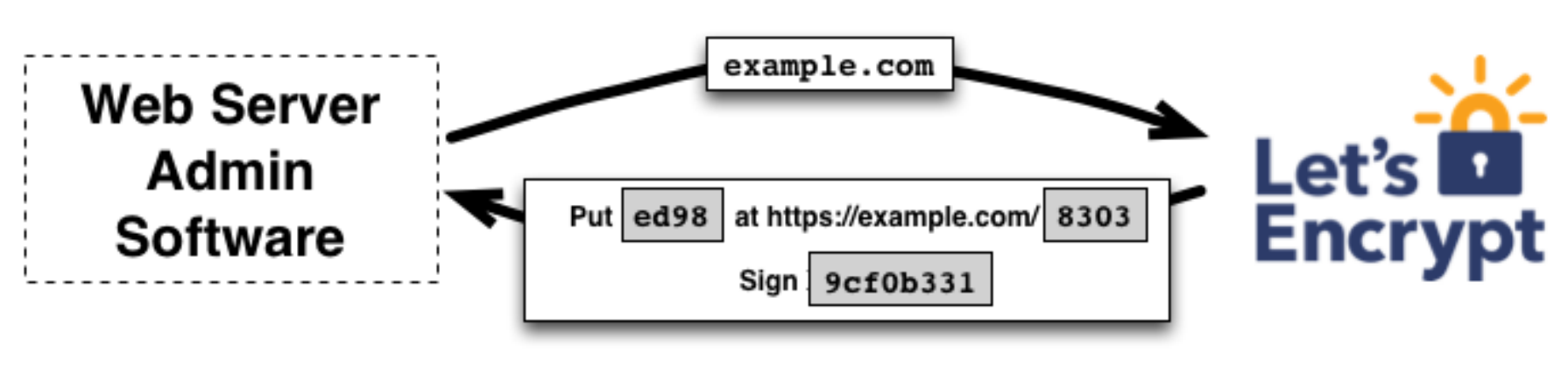
A journey into the vulnerabilities of *Let's Encrypt*

What is Let's Encrypt?

- Automated Certificate Authority
  - Client
  - Certificate Authority
- Free
- Open Source
- Automatic Certificate Management Environment (ACME)

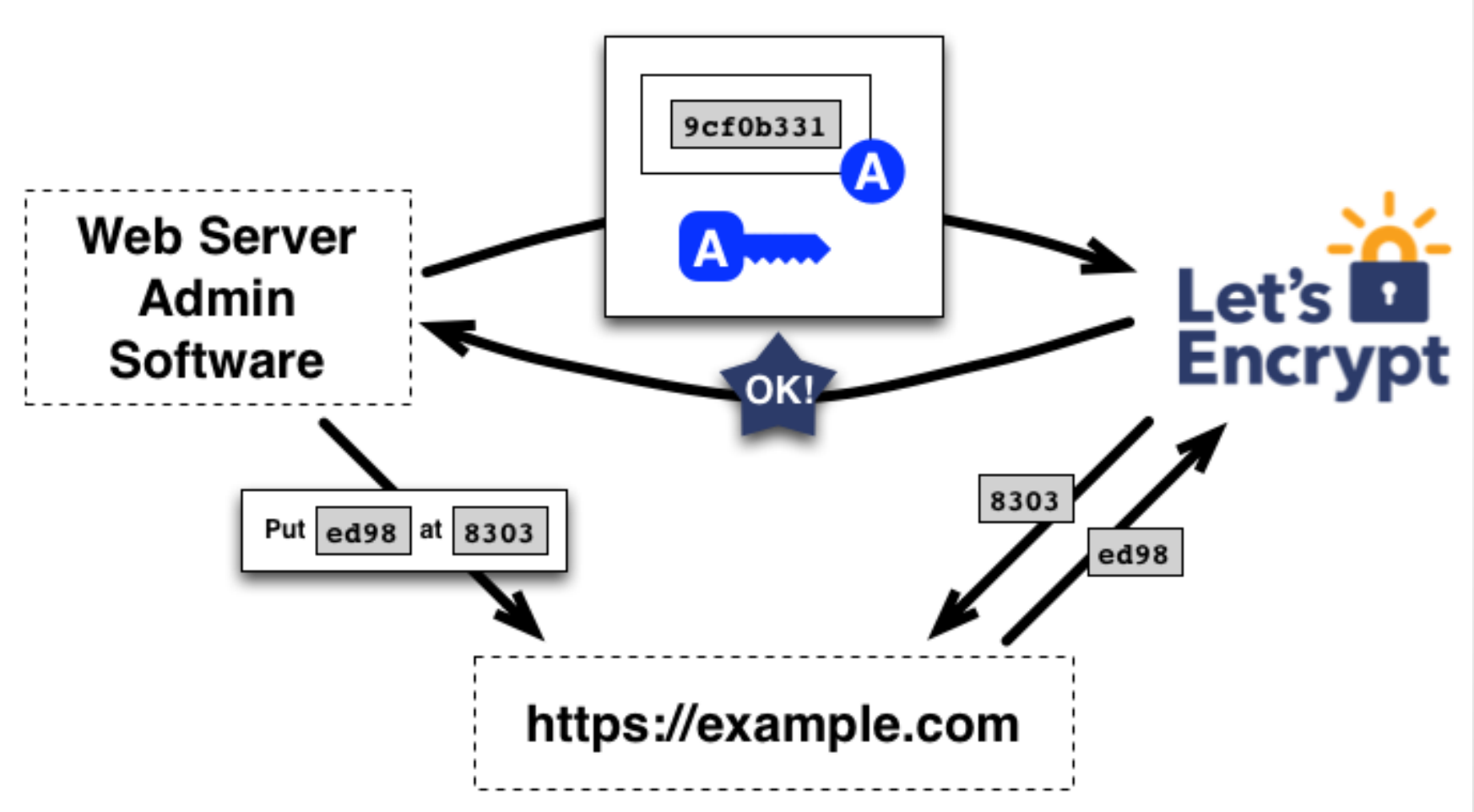
How does it work?

- ACME protocol



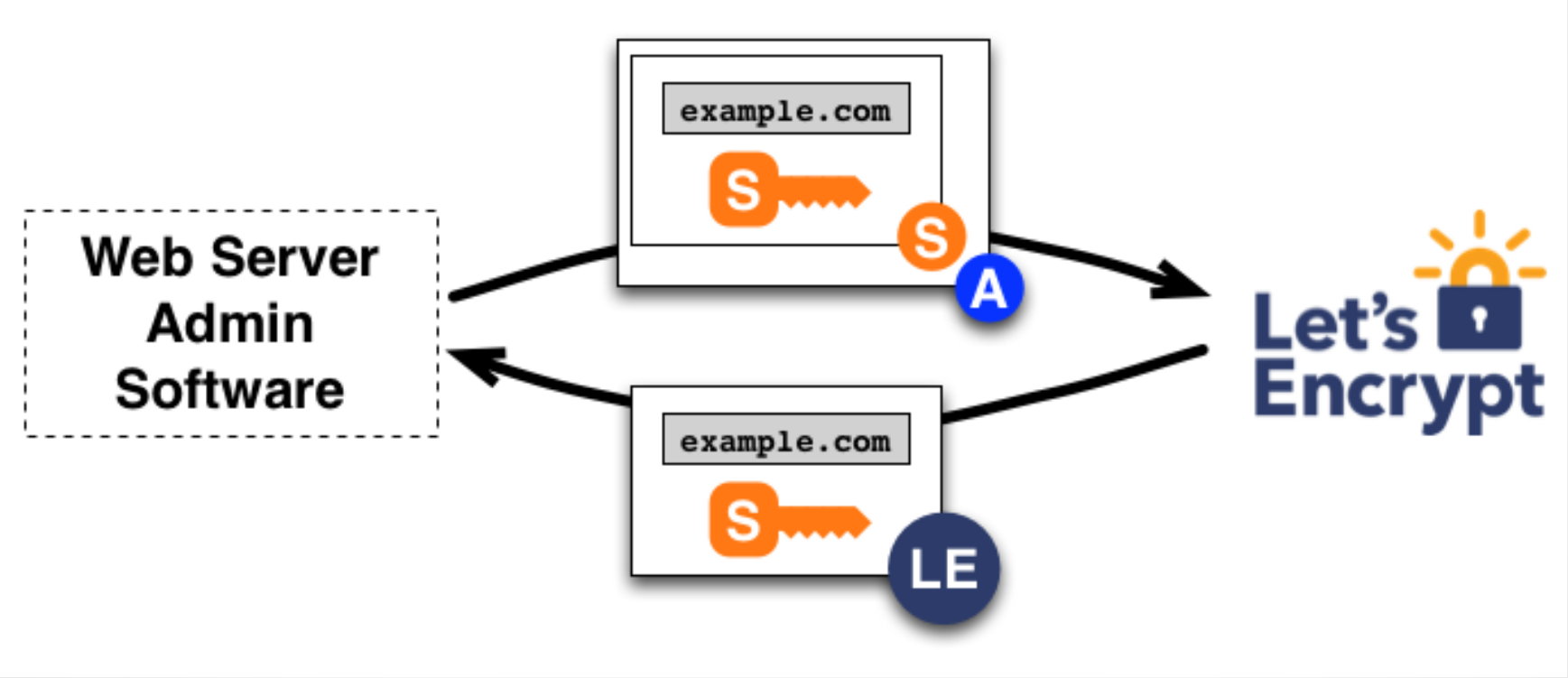
How does it work?

- ACME protocol



How does it work?

- ACME protocol



Why *Let's Encrypt*?

- The internet is spooky skeletons.
- Valid certificates cost all this money.
  - Maintaining big-boy certificates is cost-prohibitive for low-cost or no-cost sites.
- I mean... why not?

What are we doing?

- Testing it
- Breaking it (or trying to)
  - Fake CA's
  - Man in the middle sabotage of ACME protocol
- Trolling for vulnerabilities
  - CA software (theoretically isolated on *LE's* system)
  - Client Software

More fun at...

Main Site:
https://letsencrypt.org

Client Source:
https://github.com/letsencrypt/letsencrypt

CA Source:
https://github.com/letsencrypt/boulder/

ACME Spec:
https://letsencrypt.github.io/acme-spec/