

Mari Mengenkripsi dengan



saputroyulianto@gmail.com

#MaIMingGLiB

:~\$ whoami



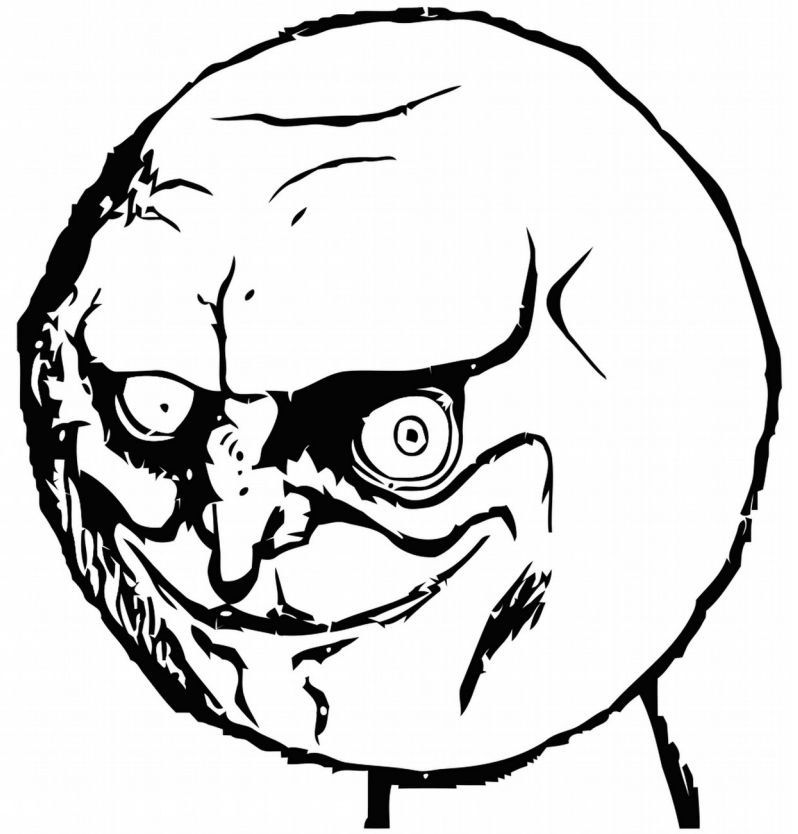
@aryulianto

Reference

- <https://letsencrypt.org>
- <https://community.letsencrypt.org/c/docs/>
- <http://www.slideshare.net/JoergHenning/lets-encrypt-59295465>
- <https://getcarina.com/docs/tutorials/nginx-with-lets-encrypt/>
- <http://www.slideshare.net/apnic/lets-encrypt-better-security-through-automation>

SSL certificate orders/renewals so far

- Generate Key
- Fill out certificate order form
- Pay a lot of money
- Verify domain
- Receive certificate
- Install certificate



Let's Encrypt !

is a new Certificate Authority:

It's free, automated, and open

Major Sponsor

Platinum

mozilla



Gold



facebook



Silver

AUTOMATTIC



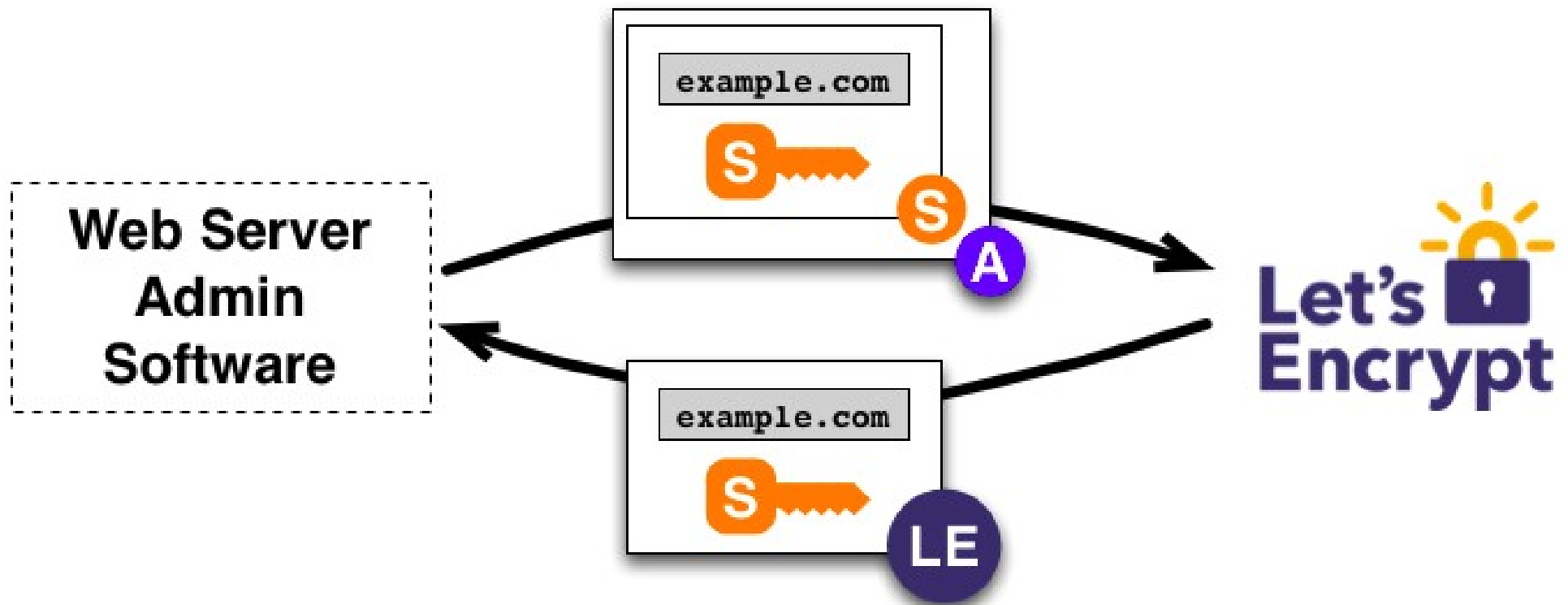
Proving domain Ownership

- Applicant asks to be authorized for example.com
- CA challenges the applicant to do something that only the real owner of example.com can do:
 1. Provision a DNS record at `_acme-challenge.example.com`
 2. Provision a file at `http://example.com/.well-known/acme-challenge/`

Cont ...

- Applicant chooses a challenge and does what was asked
- CA verifies that the applicant has complete the challenge
 1. Look for DNS record at `_acme-challenge.example.com`
 2. Download the file a `http://example.com/.well-know/acme-challenge/`

How It Works



Limitations

- No love for Windows XP
- No wildcards
- 3 Month expired

Let's Hekkk !

Thanks !

