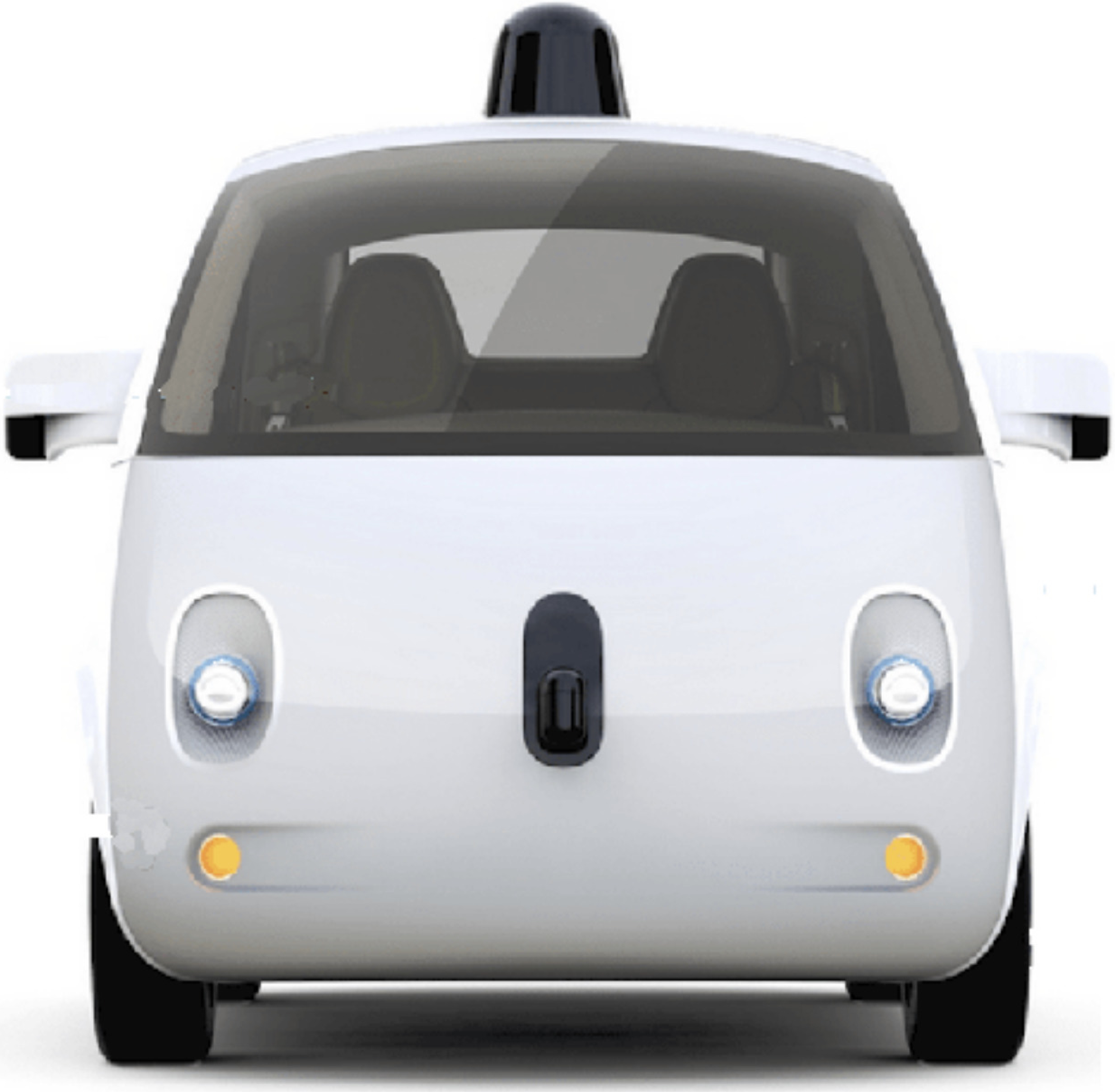
Security and Self-Driving Computers



Computer

Designed specifically for self-driving

Let's Encrypt

Apache httpd

mod_md

...oh, my!

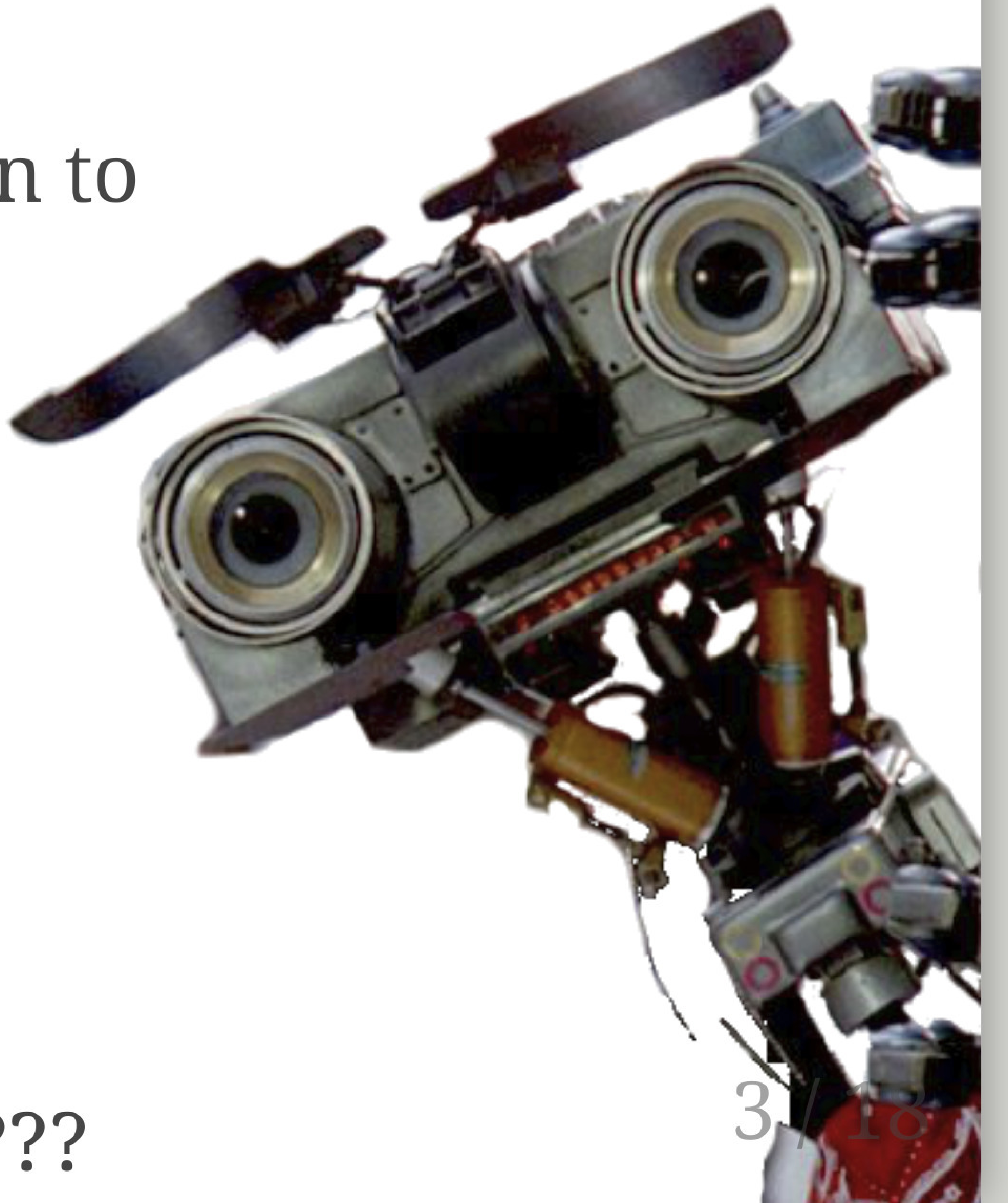
Who am I?

- Stefan Eissing
- @icing on twitter/github
- co-founder greenbytes
- ASF Member, Apache httpd

`...wrote Apache HTTP/2 in 2015.`

Self...what?

- updating software
- updating credentials
- secured communication to
  - servers
  - router
  - printer
  - tv
  - headphones?
  - fridge??
  - tooth brush???
  - intimate devices??????



Is it really neccessary?

- manually unmaintainable
- search: certificate+has+expired
- about 33.900.000 hits (google)

Who's not done it?

¯_(ツ)_/¯

Let's Encrypt(LE): Mini Recap (1)

- a Certificate Authority (CA)
- with a Web API (instead of forms)
- proof (cryptographic) of domain ownership

```
...no humans involved
   in the issuing...
```

Let's Encrypt(LE): Mini Recap (2)

- ACME, a HTTP-based protocol
- using JWS messages
- ACMEv1, standardized into ACMEv2
- Other CAs are adopting it

Let's Encrypt(LE): Mini Recap (3)

- ACME's 3 ways to prove:
  - "http-01" (port 80)
  - "tls-sni-01" (port 443)
  - "dns-01" (DNS TXT)

```
"tls-sni-01" out of grace...
"tls-alpn-01" coming up...
```

Apache httpd + LE

- certbot (https://certbot.eff.org)
  - apache plugin
  - careful config parsing/rewrite
- Mozilla grant via MOSS
- mod_md, alpha summer 2017
- shipped in Apache 2.4.33

mod_md: goals

- Integrated, easy to configure
- Robust, failure recovery
- Defensive, restricted privileges

`And a short name.`

mod_md: restrictions

- ACMEv1, as v2 was not ready then
- "http-01" + "tls-sni-01"
- RSA certificates

```
Secure ECDSA key parameters
...any suggestions?
```

mod_md: integrated

- works closely with mod_ssl
- enabled in one line
- "MDomain mydomain.net"

```
Plus some Terms of
Service Agreement, of course.
```

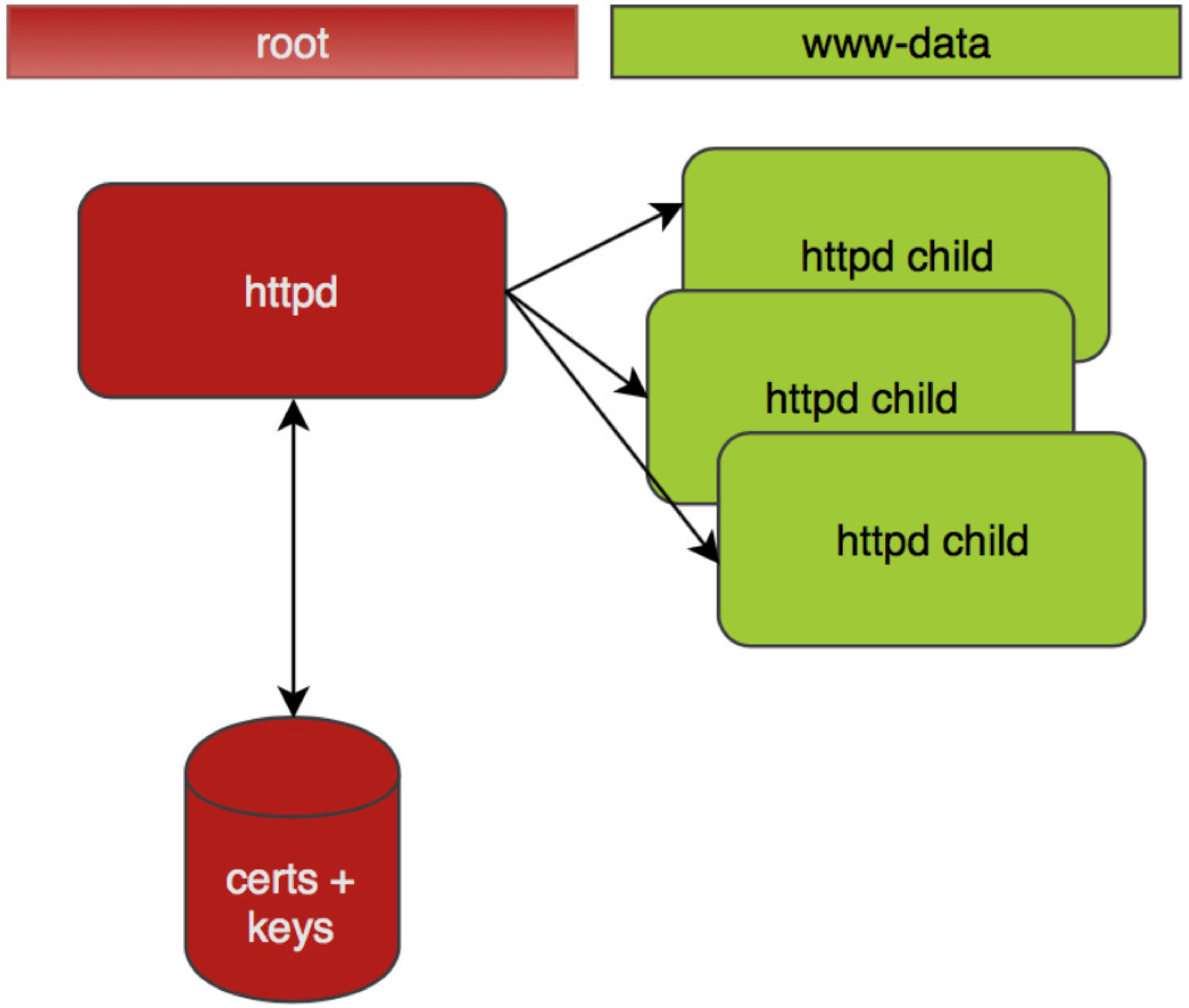
mod_md: use

- configure once
  - add notify command
  - or reload regularly
- checks twice a day

```
Changes to server names tracked.
Renews at 33% of time left.
```

Apache: basic security

privileged start, unprivileged op:



mod_md: robustness

- all progress saved
- restarts happen all the time
- pick up, carry on

`Private keys need saving too, though...`

mod_md: defense

- private keys need protection
- access for parent process
- access for other children, too!
- child files unsafe

```
Some IPC maybe?
Too heavy lifting.
```

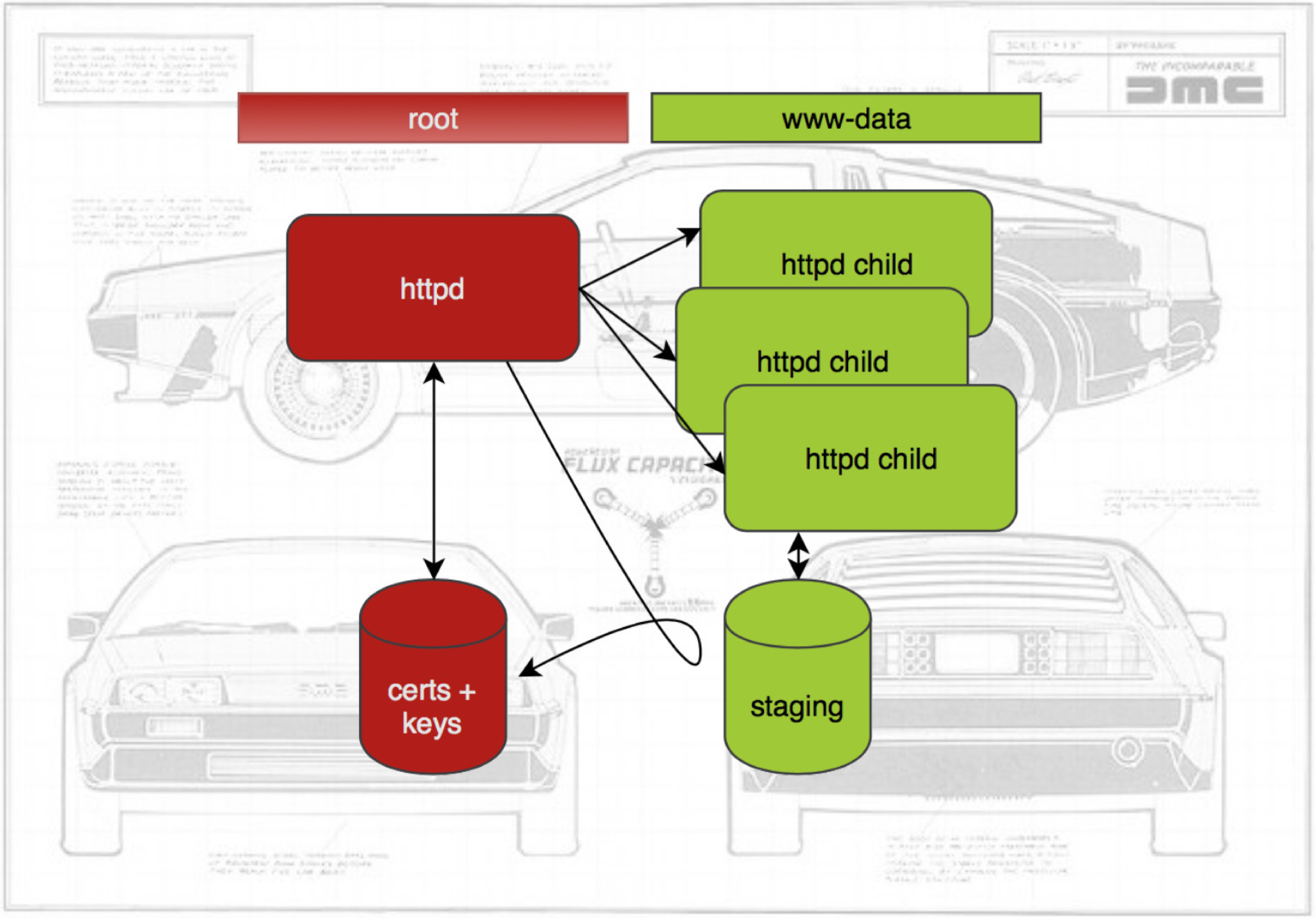
mod_md: a shared secret

- generate pass phrase
- save, pass on memory copy
- use to en-/decrypt keys

`48 RAND_bytes(), only once though.`

mod_md: basic arch

- stage changes, encrypt key
- transfer on start/reload



mod_md: good enough?

- Maybe.
- Security is never certain.

```
"A ship in harbor is safe,
 but that is not what ships are built for."
```