Prudent TLS for fun and profit

Jakob Schlyter

kirei

The state of WebPKI 2018

kirei

CA/Browser Forum

sets the policy

kirei

Mozilla & Google
decides who you trust

kirei

Clue- and reckless

CAs are distrusted

kirei

Symantec

GeoTrust – RapidSSL – Thawte – VeriSign

kirei

StartCom & WoSign

kirei

Accountability

kirei

Certificate Transparency is the new black

kirei

Revocation still doesn't work

kirei

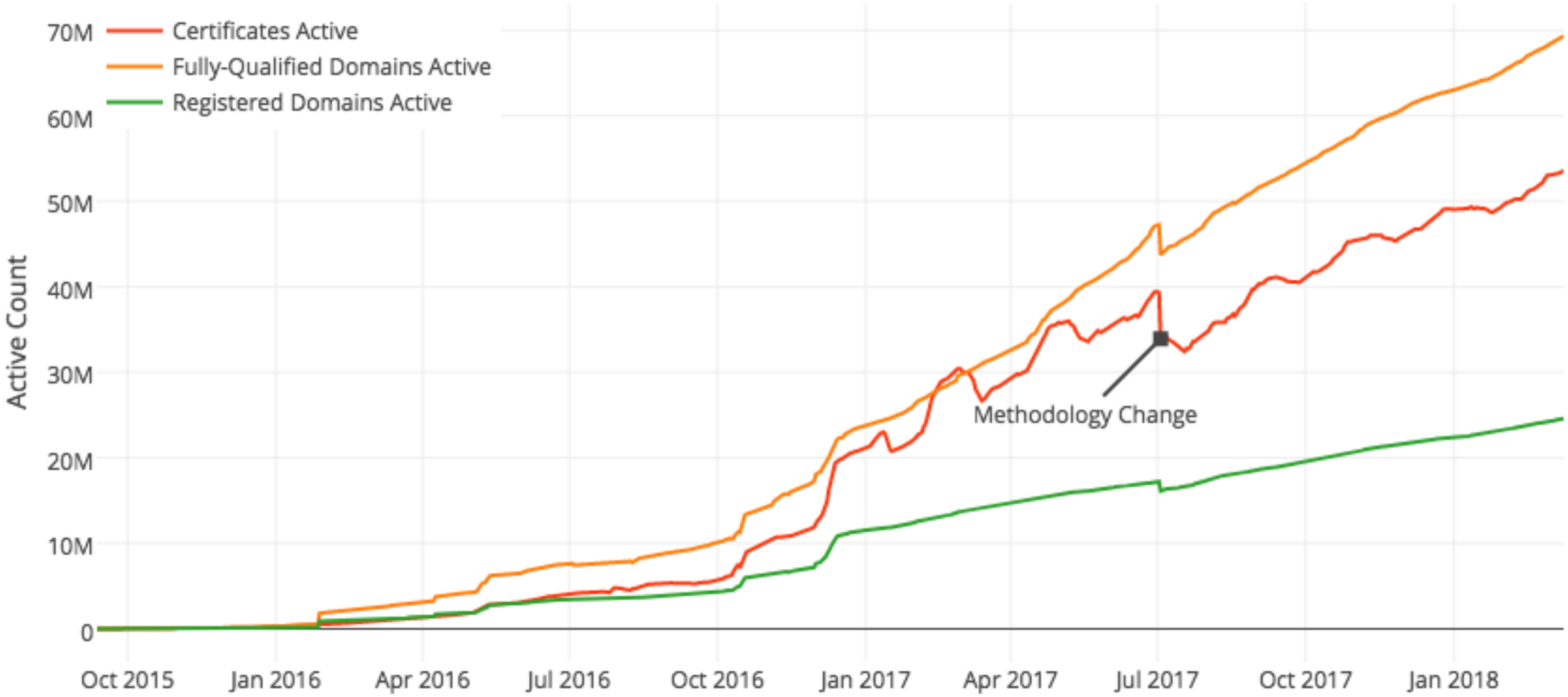
Everyone wants

Let's Encrypt

kirei

Automate or die

kirei


Certificates Active
Fully-Qualified Domains Active
Registered Domains Active
70M
60M
50M
40M
30M
20M
10M
0
Active Count
Methodology Change
Oct 2015
Jan 2016
Apr 2016
Jul 2016
Oct 2016
Jan 2017
Apr 2017
Jul 2017
Oct 2017
Jan 2018

kirei

All other CAs struggling

kirei

Prudent configuration

kirei

DNS

kirei

All your certs are belong to DNS

CAA

Who may issue certs for your domain?

kirei

```
kirei.se. CAA 128 issue "letsencrypt.org"
```

kirei

TLSA

Keeping PKI on a leash

kirei

SMTP only so far

kirei

_25._tcp.spg.kirei.se. TLSA 3 1 1 DEAD…BEEF

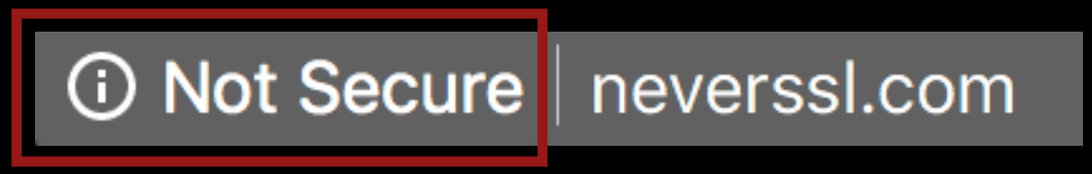
kirei

HTTP

kirei

HTTPS for everything

kirei


Not Secure
neverssl.com


Secure
https://www.netnod.se


SWEDBANK AB [SE]
https://www.swedbank.se

kirei

Anyone still trying to do captive portals for wifi?

Force HTTPS

kirei

HSTS

HTTP Strict Transport Security

kirei

Strict-Transport-Security
max-age=63072000;includeSubdomains;preload

kirei

HPKP

HTTP Public Key Pinning

kirei

```
Public-Key-Pins
max-age=3600;
pin-sha256="HiMk…zt8=";
pin-sha256="3Rst…cjM="
```

kirei

HPKP pining for the fjords :-(

kirei

TLS today

TLS 1.2
only?

Perfect Forward Secrecy

ECDHE or DHE

kirei

AES-GCM / SHA-2

kirei

ChaCha20 / Poly1035

kirei

OCSP Stapling

kirei

No fancy pants

kirei

TLS tomorrow

kirei

TLS 1.3

kirei

Faster, less cruft, less pervasive monitoring

kirei

Prudent operations

kirei

Analyze & Benchmark

kirei

https://hardenize.com

kirei

https://www.ssllabs.com

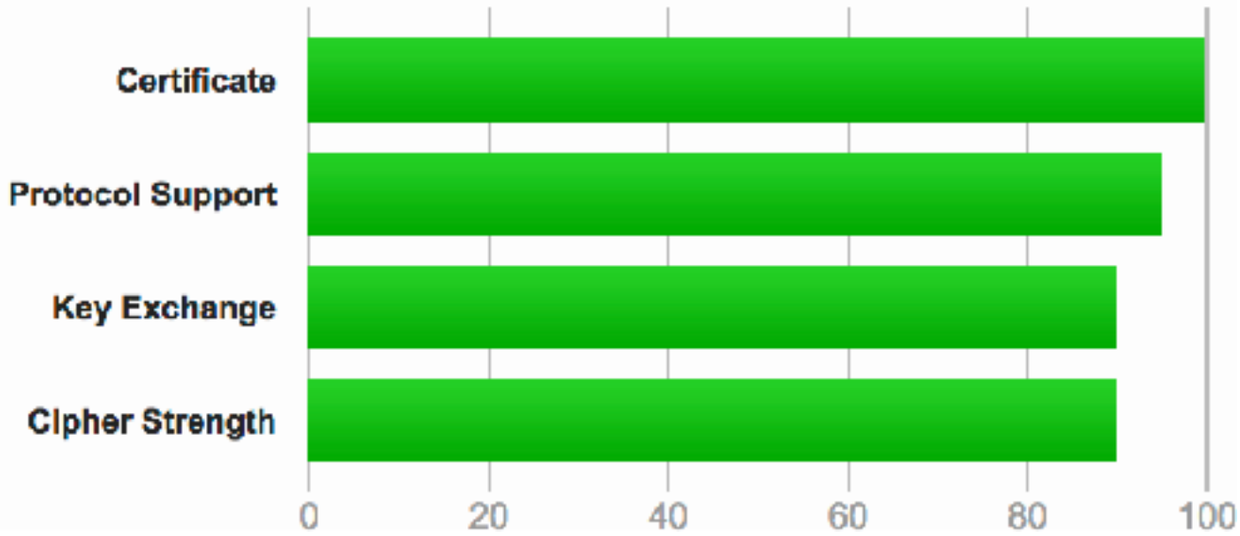
kirei

Game on!

kirei

Overall Rating

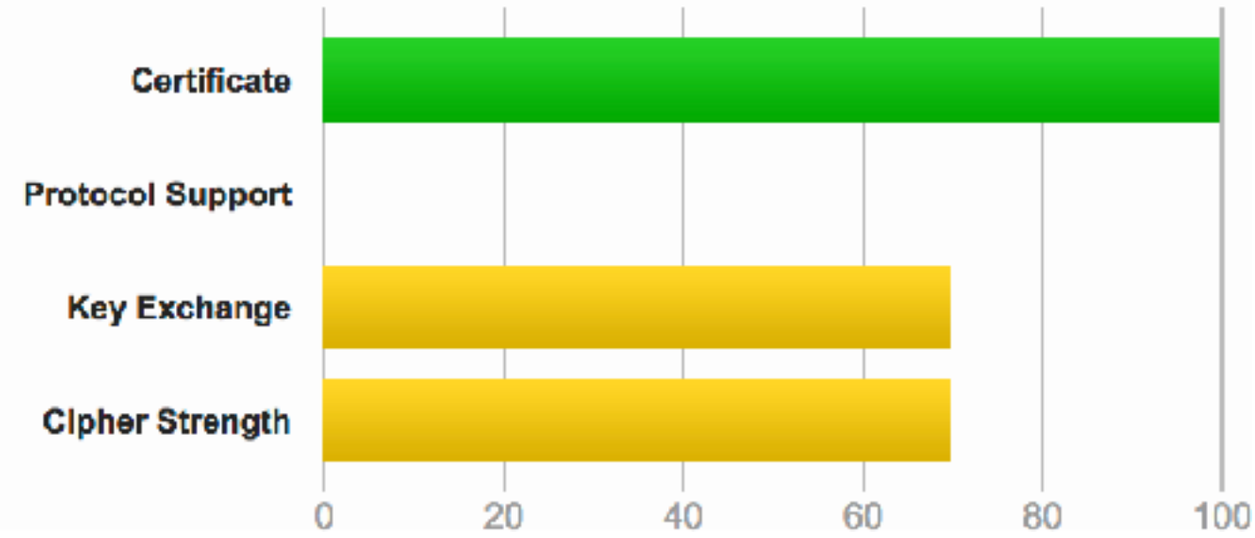
A+



kirei

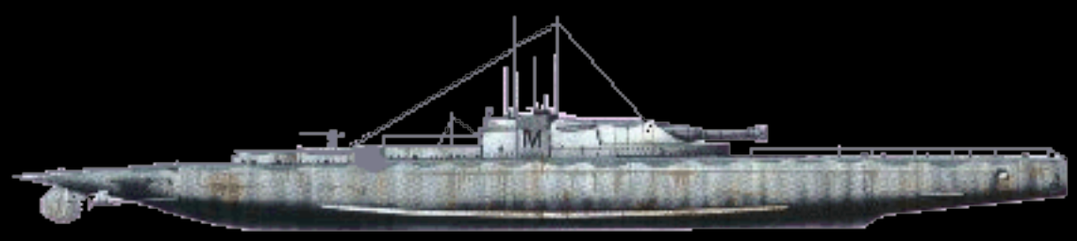
Overall Rating

F

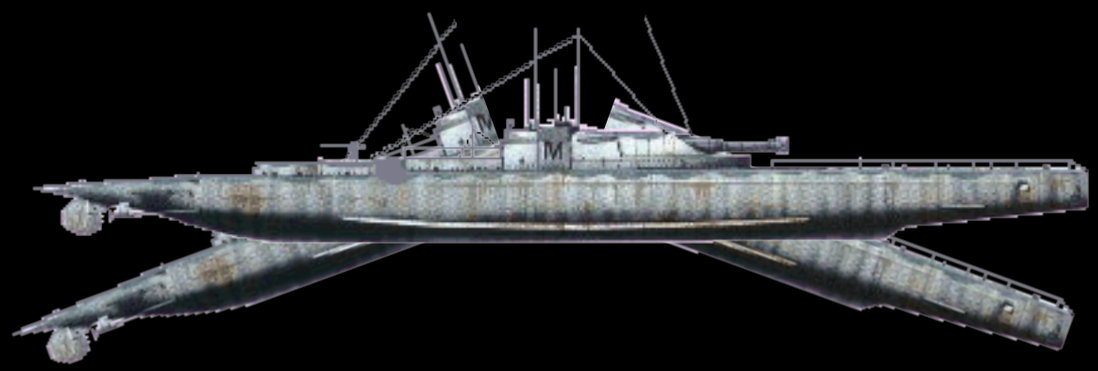


kirei

Monitor



kirei



Detect breakage

kirei

Watch certificate expiration

kirei

Note certificate issuing

kirei

https://crt.sh

https://sslmate.com/certspotter

kirei

https://keychest.net

kirei

kirei

jakob@kirei.se

kirei