SSL/TLS Automatisierung

@cmitasch
Christoph Mitasch, Thomas-Krenn.AG

Webinar, 28. Oktober 2020

THOMAS KRENN®

Über mich

- Christoph Mitasch
- seit 2005 bei der Thomas-Krenn.AG Niederlassung Österreich
- Diplomstudium Computer- und Mediensicherheit
- Erfahrung in Web Operations, Linux und HA
- Cyber-Security-Practitioner (v1)

Status Quo TLS-Zertifikate

CA/BROWSER FORUM

- CA/Browser Forum (https://cabforum.org/)
  - Zusammenschluss von Browser-Herstellern und CAs
  - CA-Browser Forum Baseline Requirements 1.7.0

2018-03-01	4.2.1 and 6.3.2	Certificates issued MUST have a Validity Period no greater than 825 days and re-use of validation information limited to 825 days
2020-09-01	6.3.2	Certificates issued SHOULD NOT have a Validity Period greater than 397 days and MUST NOT have a Validity Period greater than 398 days.

  - seit März 2018: max. 2 statt 3 Jahre
  - seit September 2020: **max. 397 Tage**
    → 1 Jahr Gültigkeit, Renewal frühestens 30 Tage davor
  - betrifft nur in Browser vorinstallierte Root-CAs
    → **interne CAs nicht betroffen**

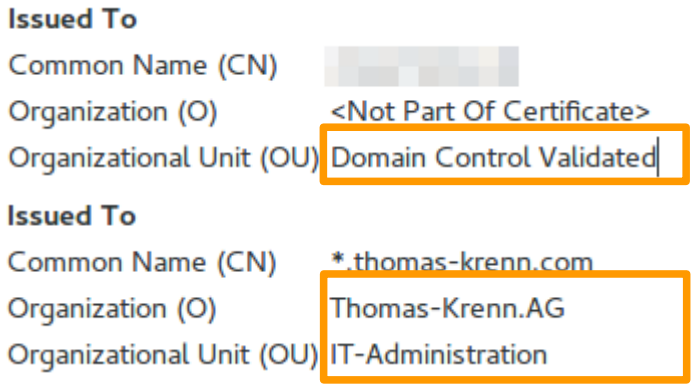
Auswirkungen 1 Jahr Laufzeit

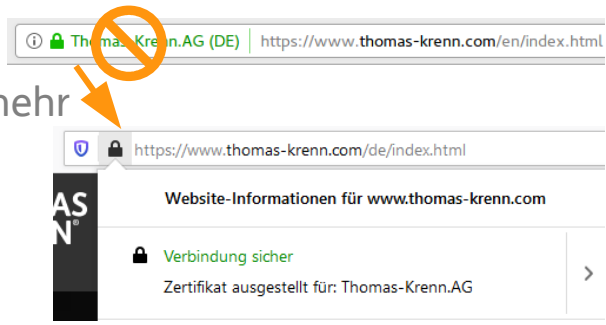
- doppelter Aufwand
- je kürzer desto sicherer
  - Entschlüsselung wird schwieriger durch kürzere Laufzeit
  - Technologie-Wechsel schneller möglich (z.B.: SHA1 → SHA2)
- Automatisierung macht Sinn
  - erlaubt zukünftig auch kürzere Laufzeiten

Quelle: https://www.flickr.com/photos/labormikro/2809055850

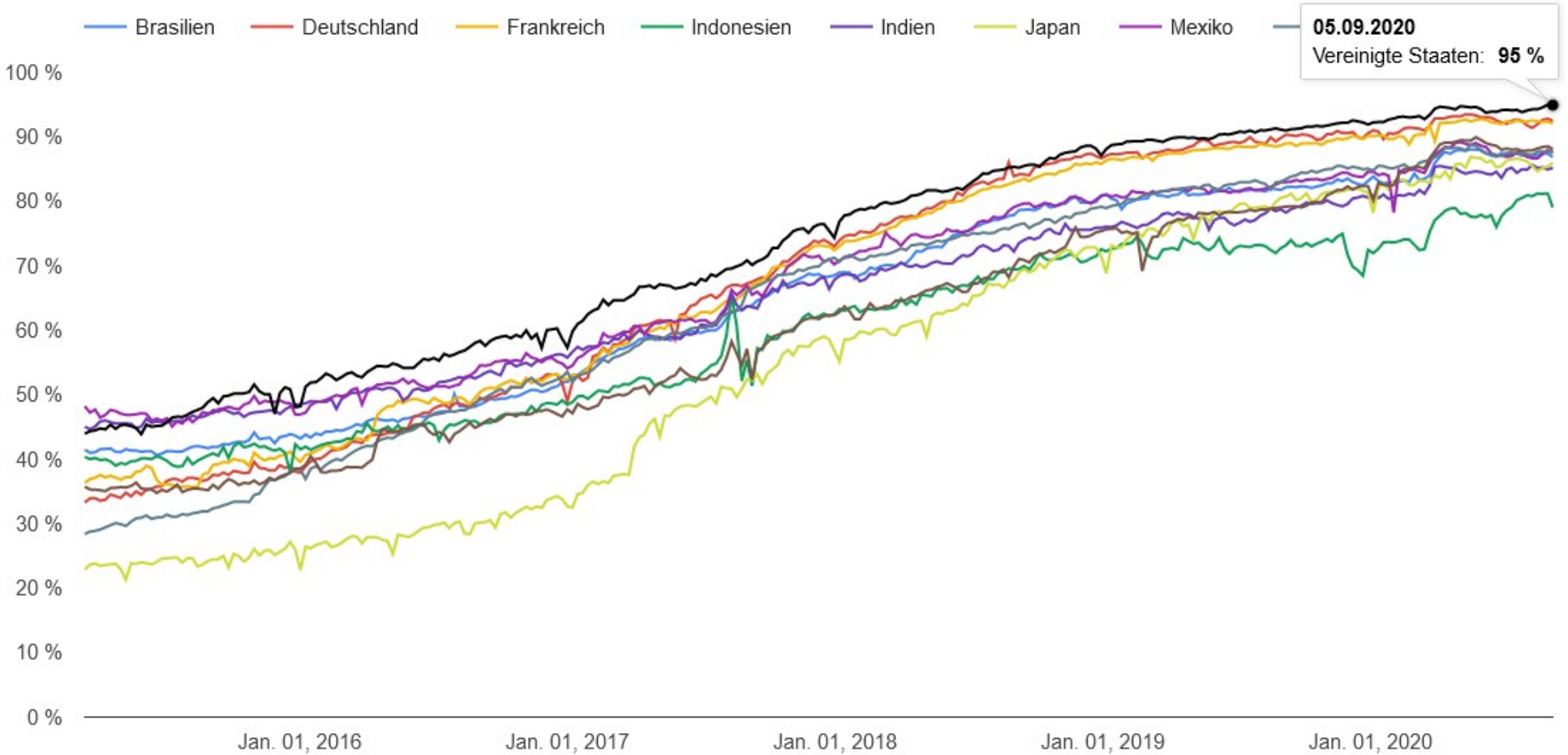
Zertifikatstypen

- DV … Domain Validated
- OV … Organization Validated
- EV … Extended Validation
  - Validierung ident wie OV, kein Wildcard möglich
  - seit Chrome 70 und Firefox 77 keine spezielle Browser-Sichtbarkeit mehr
- Multidomain/SAN (Subject Alternative Name)
- Wildcard
  - nur für 1 Subdomain-Level → *.example.com & *.test.example.com unterschiedl. Certs
  - aus Sicherheitsgründen wird in RFC 6125 und auch vom BSI von Wildcard abgeraten
- Self-Signed
  - Intern OK, wenn root-CA an Clients verteilt wird





Prozentsatz der in Chrome über HTTPS geladenen Seiten nach Land/Region



Quelle: https://transparencyreport.google.com/https/overview

Agenda

- Let’s Encrypt
- Kommerzielle CAs
- Ablöse TLS 1.0/1.1
- Demo tls-check.de

Agenda

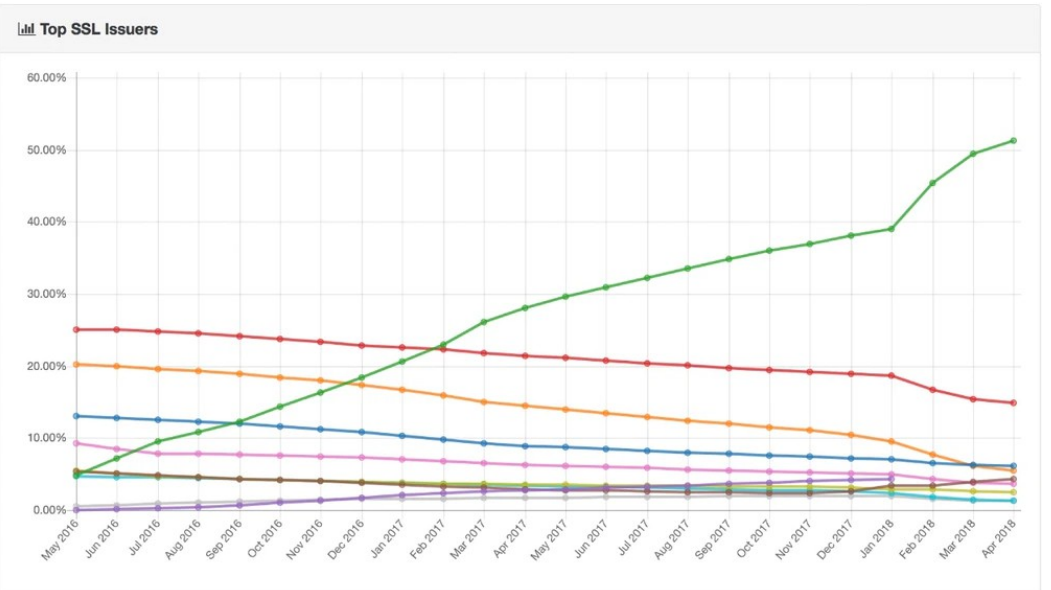
- Let’s Encrypt
- Kommerzielle CAs
- Ablöse TLS 1.0/1.1
- Demo tls-check.de

Umfrage

Verwenden Sie Let‘s Encrypt Zertifikate
in Ihrem Unternehmen?

Let's Encrypt

- Februar 2020 einmilliardstes Zertifikat ausgestellt (4,5 Jahre)
- im April 2018 > 50% Anteil an ausgestellten Zertifikaten
- aktuell ~ 1,5 Mio pro Tag
- gemeinnützige Organisation Internet Security Research Group (ISRG) + Sponsoren
- Gültigkeit: 90 Tage
- DV-only
- Ziel: 100% Verschlüsselung



#	SSL Issuer	Percentage
1	Let's Encrypt	51.21%
2	COMODO CA Limited	14.82%
3	GoDaddy.com	6.14%

Quelle: https://t3n.de/news/lets-encrypt-erfolg-1067009/

ACME Protokoll

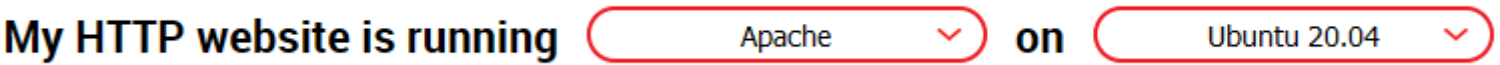
- Automated Certificate Management Environment
- im März 2019 als RFC 8555 standardisiert
- JSON über HTTPS
- ACME v1: EOL im Juni 2021
- ACME v2:
  - RFC, IETF Standard
  - Wildcard Zertifikate
  - besser für andere CAs einsetzbar

Challenges

- HTTP-01
  - http://<YOUR_DOMAIN>/.well-known/acme-challenge/<TOKEN>
  - Port 80
- DNS-01
  - TXT Record im DNS _acme-challenge.<YOUR_DOMAIN>
  - für Wildcard notwendig
  - DNS Provider-Unterstützung notwendig oder API
  - DNS selbt betreiben als Alternative
- TLS-ALPN-01
  - Port 443, Application-Layer Protocol Negotiation, wenig Client-Support bis jetzt
    Apache mit mod_md (experimental), Nginx mit dehydrated
- TLS-SNI-01 → deaktiviert

certbot

- offizieller Client
- seit Ende 2019 als Beta-Version für Windows
- https://certbot.eff.org/instructions



- Ubuntu/Debian: Snapd, Repo oder PPA
- eigene Staging-Umgebung für Tests
  https://letsencrypt.org/docs/staging-environment/

certbot

```
root@test:~# certbot --apache
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache

Which names would you like to activate HTTPS for?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: www.example.com
2: example.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate numbers separated by commas and/or spaces, or
leave input
blank to select all options shown (Enter 'c' to cancel): 1
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for www.example.com
Waiting for verification...
Cleaning up challenges
```

certbot

- „Single Step“ mit Apache/Nginx
  - $ sudo certbot --apache/--nginx
- nur das Zertifikat ohne Konfiguration
  - $ sudo certbot certonly --apache/--nginx
- „Dry-run“ Erneuerung
  - $ sudo certbot renew --dry-run
- Revoke
  - $ certbot revoke --cert-path /etc/letsencrypt/live/CERTNAME/cert.pem
  - ggf. noch „delete“ machen, wenn es nicht mehr erneuert werden soll

certbot

- Pre/Post-Hooks
  - --manual-auth-hook, --manual-cleanup-hook
- Automatischer Renewal via cron oder systemd
- /etc/letsencrypt
  - Account-Daten, Zertifikate, Private Keys
  - in Backup aufnehmen

certbot: DNS-01

- Eigener DNS-Server, z.B. BIND

Generate a new SHA512 TSIG key

```
dnssec-keygen -a HMAC-SHA512 -b 512 -n HOST keyname.
```

Sample BIND configuration

```
key "keyname." {
  algorithm hmac-sha512;
  secret "4q4wM/2I180UXoMyN4INVhJNi8V9BCV+jMw2mXgZw/CSuxUT8C7NKKFs AmKd7ak51vWKgSl12ib86oQRPkpDjg==";
};

zone "example.com." IN {
  type master;
  file "named.example.com";
  update-policy {
    grant keyname. name _acme-challenge.example.com. txt;
  };
};
```


Quelle: https://certbot-dns-rfc2136.readthedocs.io/en/stable/

certbot: DNS-01

- Eigener DNS-Server, z.B. BIND

To acquire a certificate for `example.com`, waiting 30 seconds for DNS propagation

```
certbot certonly \
  --dns-rfc2136 \
  --dns-rfc2136-credentials ~/.secrets/certbot/rfc2136.ini \
  --dns-rfc2136-propagation-seconds 30 \
  -d example.com
```

- DNS-Plugins certbot

- certbot-dns-cloudflare
- certbot-dns-cloudxns
- certbot-dns-digitalocean
- certbot-dns-dnsimple
- certbot-dns-dnsmadeeasy
- certbot-dns-google
- certbot-dns-linode
- certbot-dns-luadns
- certbot-dns-nsone
- certbot-dns-ovh
- certbot-dns-rfc2136
- certbot-dns-route53

Quelle: https://certbot-dns-rfc2136.readthedocs.io/en/stable/

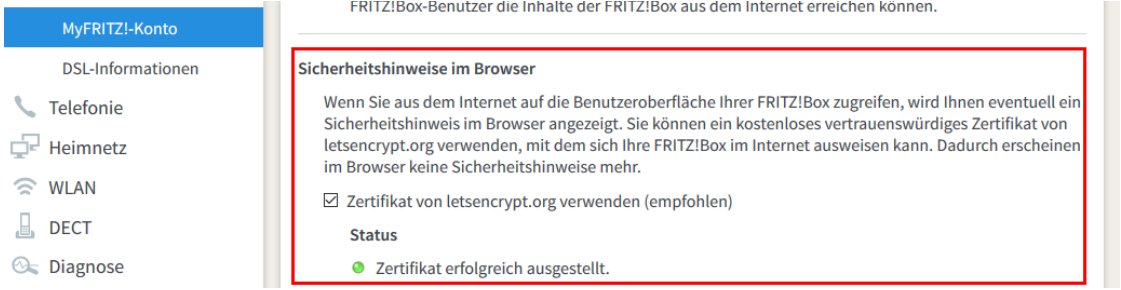
DNS-01

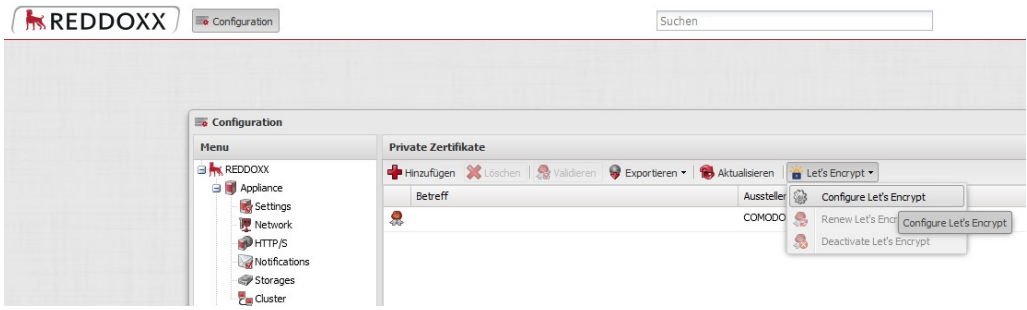
- DNS-Provider Liste mit Let's Encrypt Clients
  - https://community.letsencrypt.org/t/dns-providers-who-easily-integrate-with-lets-encrypt-dns-validation/86438

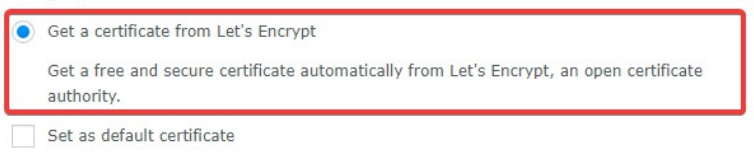
DNS Hosting Provider	ACME Client Support	Cost
Akamai Edge DNS 43	Certbot 20, lego 710, Posh-ACME 525	Contract Specific
Aliyun (CN) 74 & Alibaba Cloud DNS (EN) 60	acme.sh 4.9k, lego 710, Posh-ACME 525	Bundled with domain registration or Cloud DNS pricing 46
Amazon Route53 685	Certbot 587, acme.sh 4.9k, others 276	~$0.50/mo per domain
Azure DNS 466	acme.sh 4.9k, lego 710, Posh-ACME 525	~$0.50/mo per domain
Cloudflare 2.3k	Certbot 838, acme.sh 4.9k, others 276	Free (except for Freenom domains) 251
ClouDNS 200	acme.sh 4.9k, lego 710, Posh-ACME 525, others 276	>= $1.95/mo (with API-support)
CloudXNS 33	Certbot 22, acme.sh 4.9k, lego 710	Free, Chinese only
deSEC 222	Certbot 34, acme.sh 4.9k, others 276	Free
DigitalOcean 997	Certbot 281, acme.sh 4.9k, others 276	Free
DNS Made Easy 155	Certbot 93, acme.sh 4.9k, others 276	$29.95/yr per 10 domains

Appliances

- AVM Fritzbox
- Reddoxx
- Synology
- VMware
  - seit 3/2020 Sponsor von Let's Encrypt
  - derzeit aber (noch) keine offizielle Unterstützung
  - mit Powershell für UAG/Horizon
    https://digitalworkspace.blog/2020/01/03/automating-lets-encrypt-cerificates-lifecycle-for-horizon-and-unified-access-gateway/
  - mit Ansible für ESXi (/etc/vmware/ssl/rui.crt)
    https://graspingtech.com/ansible-lets-encrypt-esxi/





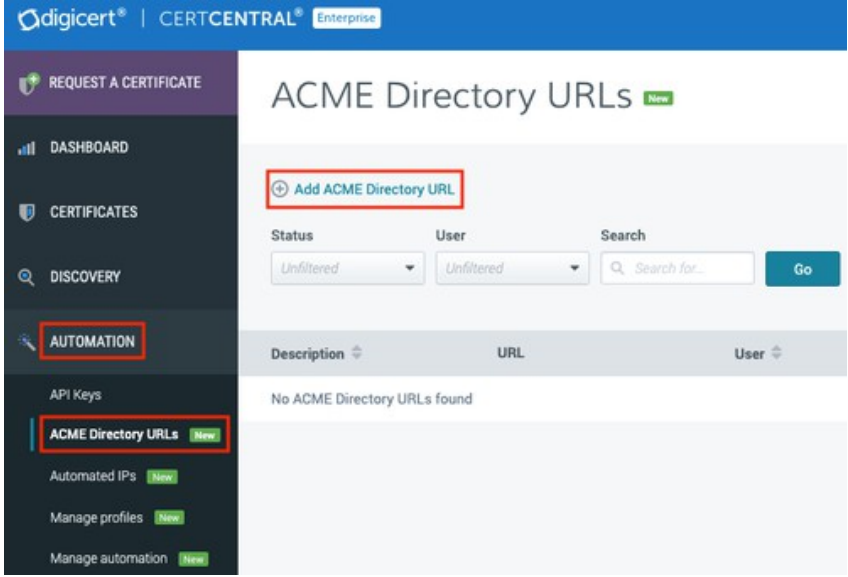


Agenda

- Let’s Encrypt
- Kommerzielle CAs
- Ablöse TLS 1.0/1.1
- Demo tls-check.de

Kommerzielle CAs

- nicht nur DV, auch OV, EV, … möglich
- Eigene APIs und Clients von CAs
- Eigene APIs von Resellern
- ACME-Support von CAs
  - unabhängig von proprietären APIs, CA kann leichter gewechselt werden
  - z.B. Digicert mit CertCentral Management
    https://docs.digicert.com/certificate-tools/Certificate-lifecycle-automation-index/acme-user-guide/
    Pre-Validation von Domains, Organizationen für sofortige Ausstellung
    $ sudo certbot --apache --register-unsafely-without-email --eab-kid "xxxxxx" --eab-hmac-key "xxxxxx" --server “https://acme.digicert.com/v2/acme/directory/” -d www.example.com
  - Entrust mit Certificate Services
  - Sectigo (früher Comodo) mit Sectigo Certificate Manager
  - keine öffentlichen Preislisten dafür gefunden → ist aktuell Enterprise Feature
    **CertCentral® is available for Enterprise & Reseller clients only right now. For Retail customers, it will be available soon.*



Quelle: https://docs.digicert.com/

Kommerzielle CAs

- seit 9/2020 neue Zertifikate max. 1 Jahr gültig
- Renewal frühestens 30 Tage vorher (bisher 90 Tage)
- Kauf von Multi-Year trotzdem möglich
  - Expiration vs. Order Expiration

Expires On :	11/21/2021
Order Expiry Date :	10/26/2022

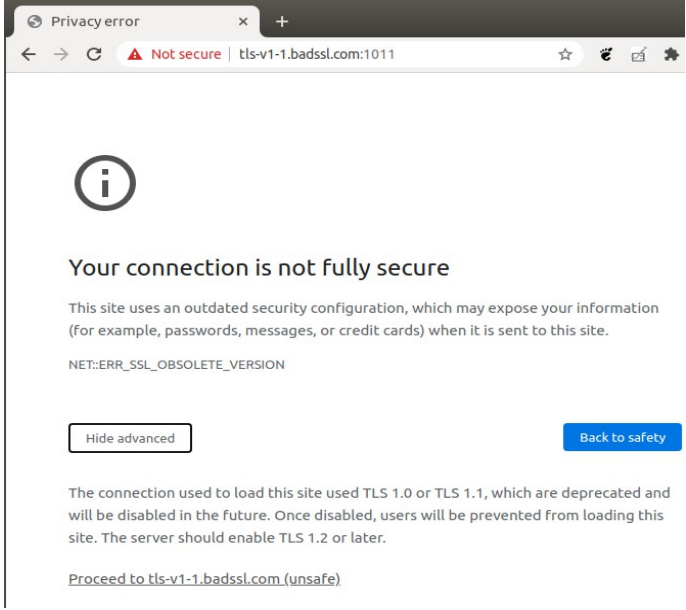
  - Regenerate nach 1 Jahr
    - mit identem CSR möglich (nicht empfohlen!)
    - mit neuem private Key und CSR

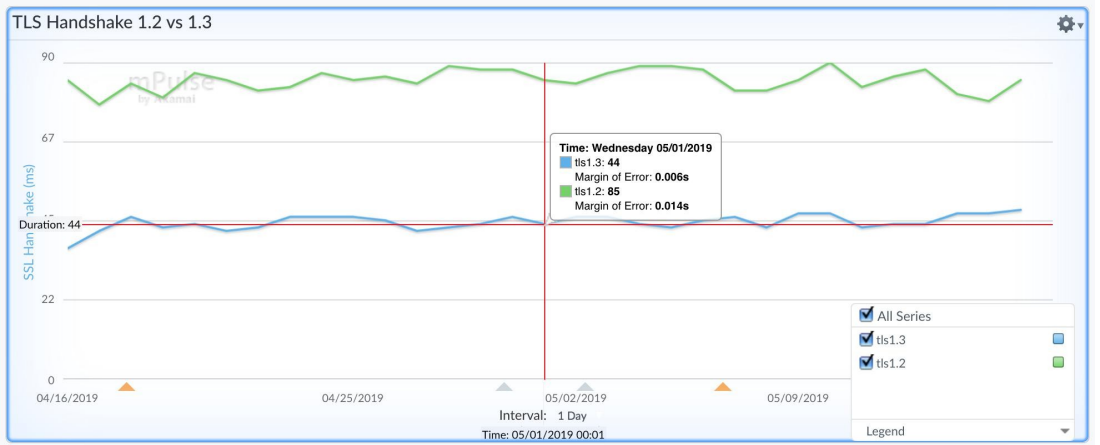
Agenda

- Let’s Encrypt
- Kommerzielle CAs
- Ablöse TLS 1.0/1.1
- Demo tls-check.de

Ablöse TLS 1.0/1.1

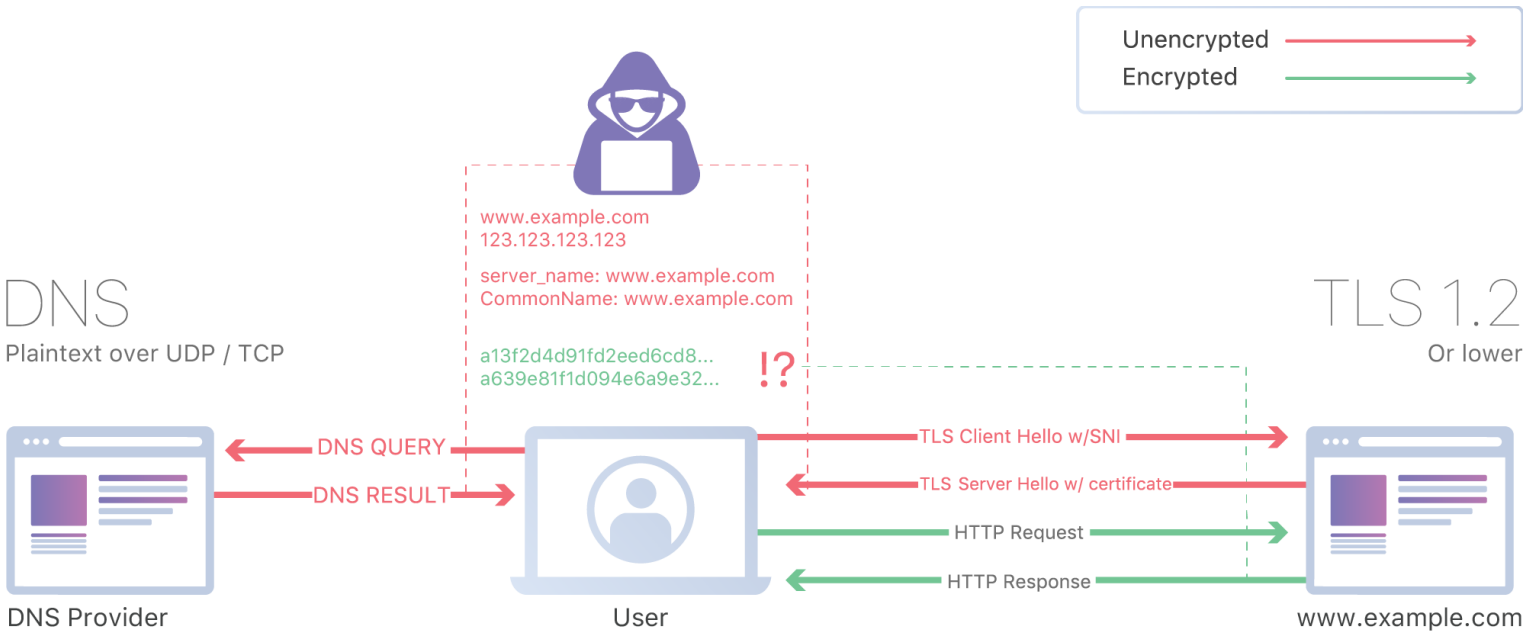
- Firefox
  - mit Version 74 erstmals im März 2020 deaktiviert
    kurz danach wegen Pandemie wieder zurückgenommen
  - mit Version 78 Ende Juni erneut deaktiviert
- Chrome
  - mit Version 84 im Mai deaktiviert
- TLS 1.3
  - schneller und sicherer
  - RFC 8446 im August 2018 finalisiert
  - seit OpenSSL 1.1.1, Apache 2.4.36, Nginx 1.13.0
  - ESNI derzeit noch ein Draft





Quelle: https://kinsta.com/blog/tls-1-3/

Ablöse TLS 1.0/1.1



CLOUDFLARE

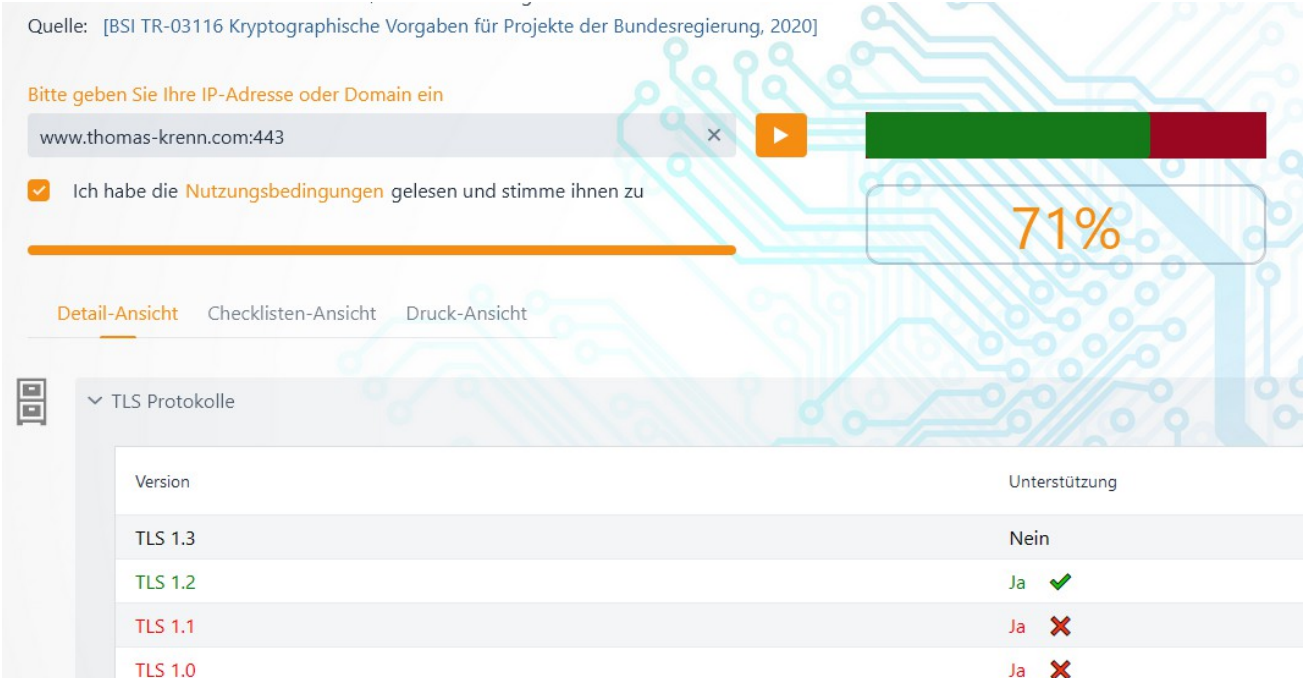
Quelle: https://blog.cloudflare.com/esni/

Agenda

- Let’s Encrypt
- Kommerzielle CAs
- Ablöse TLS 1.0/1.1
- Demo tls-check.de

tls-check.de

- BSI TR-03116-4
  - Checklisten-Ansicht
  - Alternative zu https://www.ssllabs.com



tls-check.de

TLS Protokolldetails

Name	Unterstützung
Sichere Neuverhandlung	Ja ✔
Sichere Client-initiierte Neuverhandlung	Nein ✔
Alte Client-initiierte Neuverhandlung	Nein ✔
TLS Komprimierung	Nein ✔
Heartbeat-Unterstützung	Ja ✘
Truncated HMAC-Unterstützung	Nein ✔
Encrypt then MAC-Unterstützung	Nein ⚠
Unterstützung von Sitzungstickets	Ja
OCSP-Stapling	Nein ⚠
Erweiterte Master Secret-Unterstützung	Nein ⚠

Vielen Dank für Ihre Aufmerksamkeit!

THOMAS KRENN®