IT-Sicherheit
SSL/TLS in der Praxis

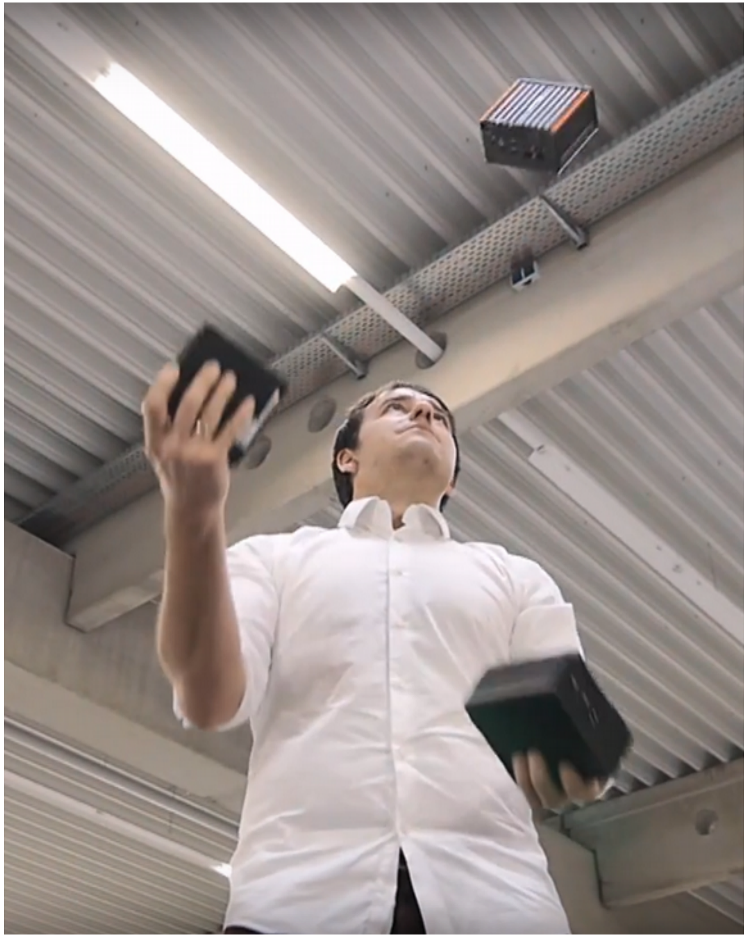
@cmitasch
Christoph Mitasch

Webinar, 24. Oktober 2018

THOMAS KRENN®

Über mich

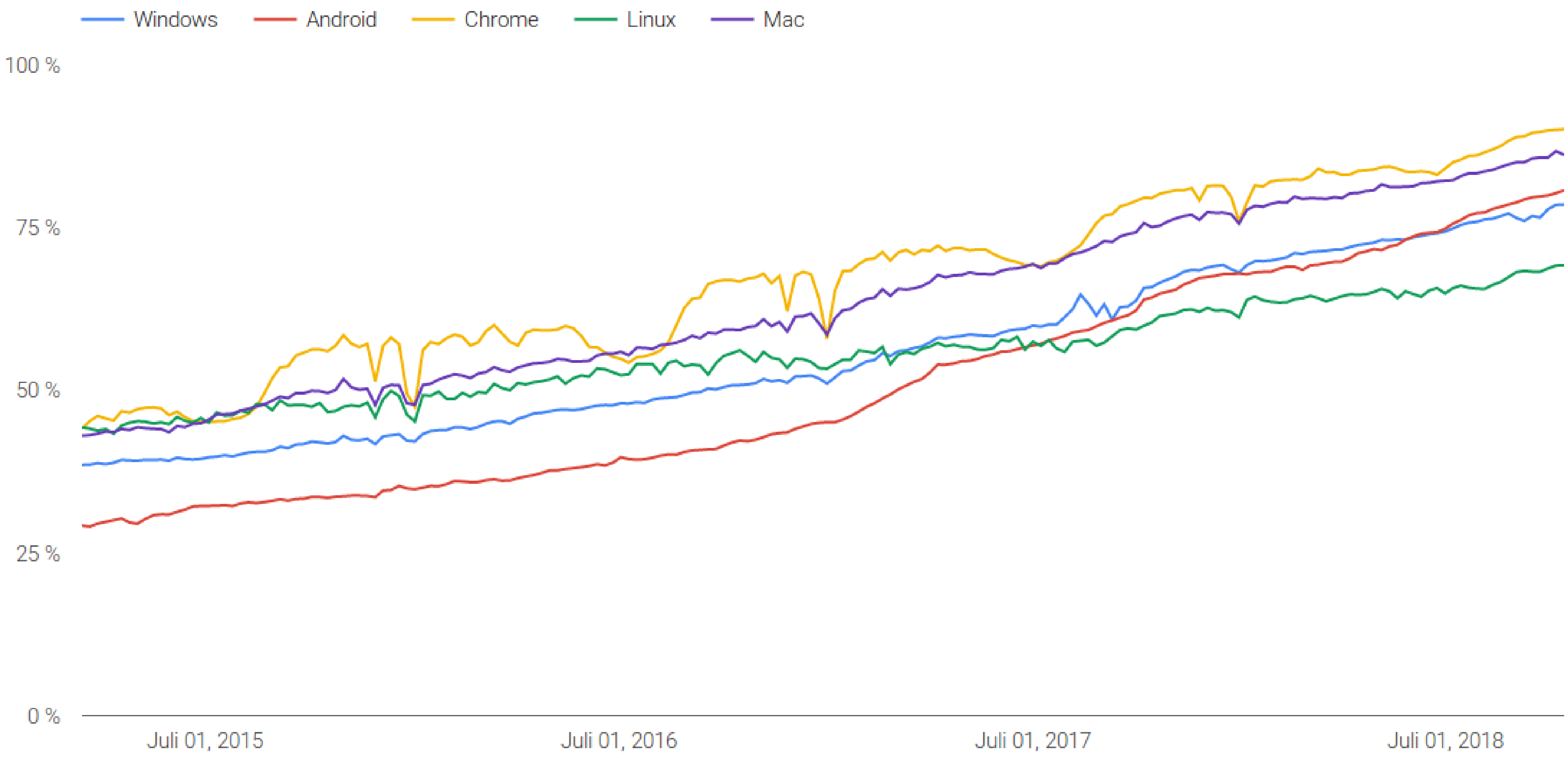
- Christoph Mitasch
- seit 2005 bei der Thomas-Krenn.AG Niederlassung Österreich
- Diplomstudium Computer- und Mediensicherheit
- Erfahrung in Web Operations, Linux und HA
- Cyber-Security-Practitioner



Agenda

- Aktuelle Entwicklungen
- Zertifikats-Typen
- Traditionell vs. Let‘s Encrypt
- Zertifikats-Management
- Konfiguration
- Tools

Prozentsatz der in Chrome über HTTPS geladenen Seiten nach Plattform

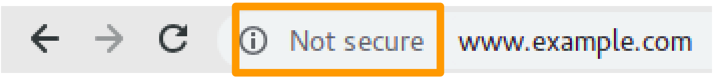


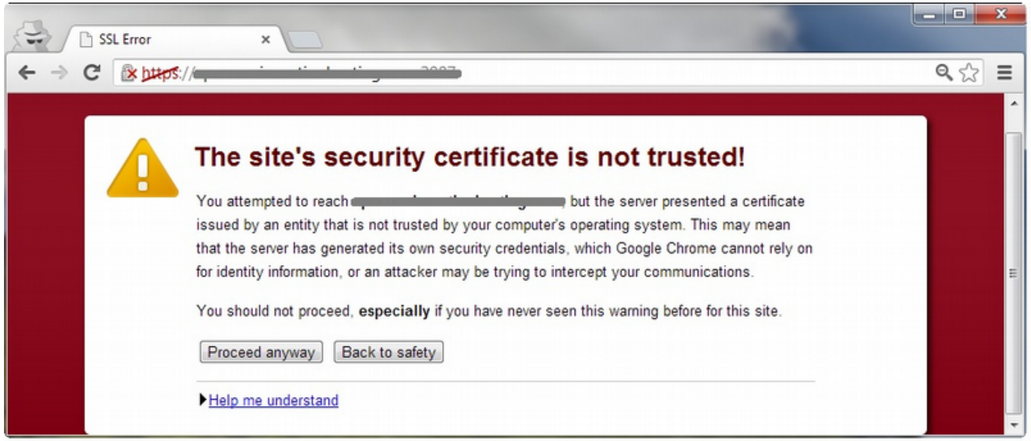
Quelle: https://transparencyreport.google.com/https/overview

Aktuelle Entwicklungen

- 7/2018: HTTP seit Chrome 68 als „Not secure“ markiert
  → HTTPS ist jetzt Standard

- 12/2018: Symantec-Root-CAs wird Vertrauen entzogen
  → Zertifikate von neuer DigiCert-Root-CA notwendig





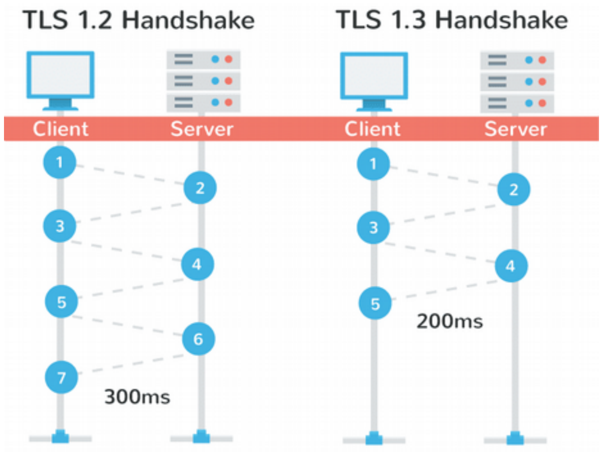
The site's security certificate is not trusted!

You attempted to reach [redacted], but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

Aktuelle Entwicklungen

- KTLS – Kernel TLS, nur symmetrische Verschlüsselung
  - 4.13 – nur Verschlüsselung
  - 4.17 – auch Entschlüsselung
  - Userspace kann in Zukunft an KTLS delegieren
- TLS 1.3
  - RFC 8446 im August veröffentlicht
  - Forward Secrecy verpflichtend
  - Verbindungsaufbau weitgehend verschlüsselt
  - schnellerer Verbindungsaufbau (0-RTT)
  - viele unsichere Altlasten entfernt
  - seit OpenSSL 1.1.1 und Apache 2.4.36
  - Browser wollen TLS 1.0/1.1 ab 2020 nicht mehr unterstützen
  - Seit 7/2018 TLS 1.0 nicht mehr für PCI DSS Compliance erlaubt

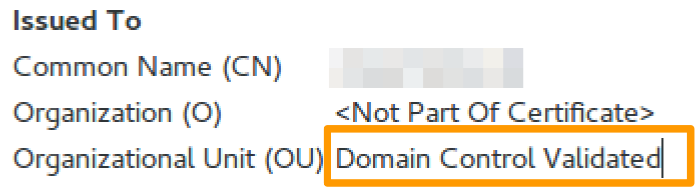


Quelle: https://kinsta.com/blog/tls-1-3/

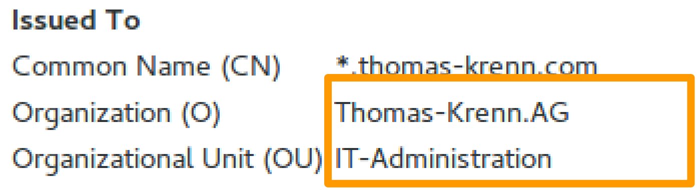
Agenda

- Aktuelle Entwicklungen
- Zertifikats-Typen
- Traditionell vs. Let‘s Encrypt
- Zertifikats-Management
- Konfiguration
- Tools

Zertifikatstypen

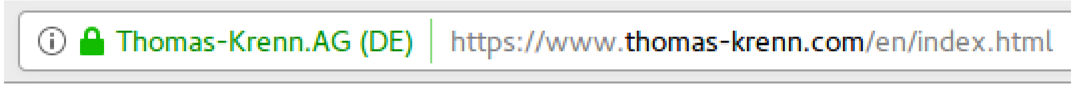


Issued To	
Common Name (CN)	[redacted]
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	Domain Control Validated



Issued To	
Common Name (CN)	*.thomas-krenn.com
Organization (O)	Thomas-Krenn.AG
Organizational Unit (OU)	IT-Administration

- DV … Domain Validated
- OV … Organization Validated
  - Validierungs-Prozess kann einige Tage dauern
- EV … Extended Validation
  - Validierung ident wie OV
  - Wildcard nicht möglich
  - in Browser vertrauensvollere Anzeige



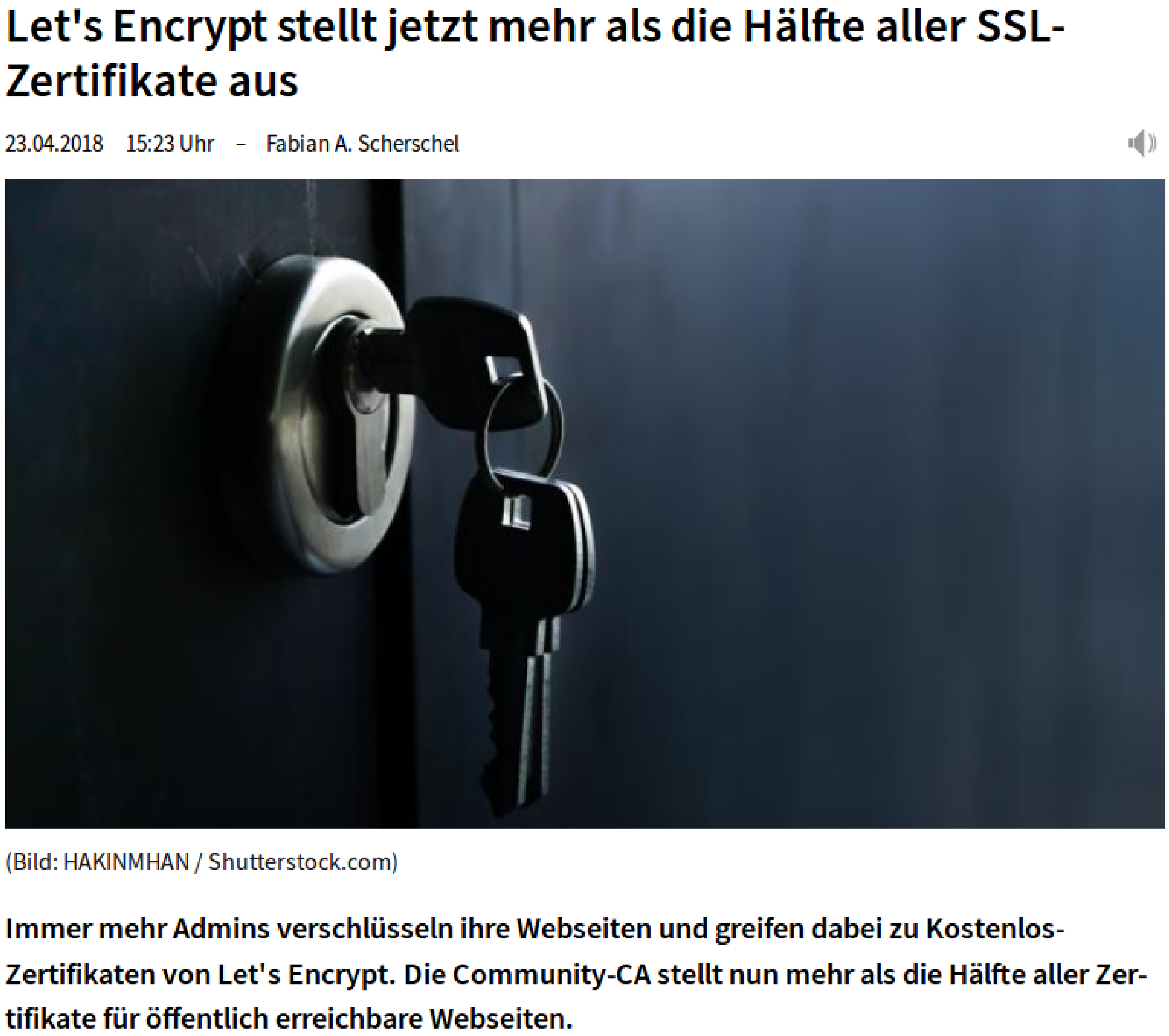
- Multidomain/SAN (Subject Alternative Name)
- Wildcard
  - nur für 1 Subdomain-Level → *.example.com und *.test.example.com unterschiedliche Zertifikate
- Self-Signed
  - Intern OK, wenn root-CA an Clients verteilt wird

Agenda

- Aktuelle Entwicklungen
- Zertifikats-Typen
- Traditionell vs. Let‘s Encrypt
- Zertifikats-Management
- Konfiguration
- Tools

Umfrage

Verwenden Sie Let‘s Encrypt Zertifikate
in Ihrem Unternehmen?



Let's Encrypt stellt jetzt mehr als die Hälfte aller SSL-Zertifikate aus

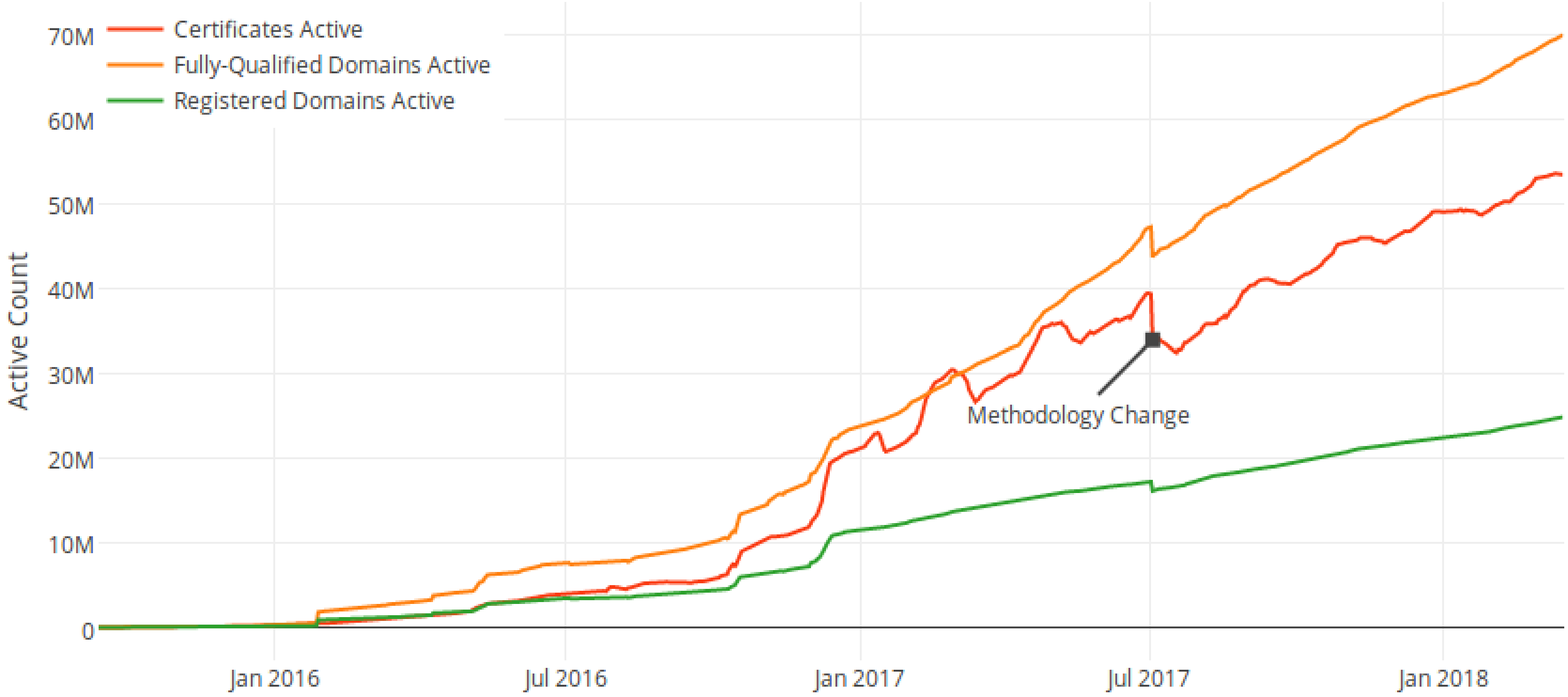
23.04.2018 15:23 Uhr – Fabian A. Scherschel

(Bild: HAKINMHAN / Shutterstock.com)

Immer mehr Admins verschlüsseln ihre Webseiten und greifen dabei zu Kostenlos-Zertifikaten von Let's Encrypt. Die Community-CA stellt nun mehr als die Hälfte aller Zertifikate für öffentlich erreichbare Webseiten.

Quelle: heise.de

Let‘s Encrypt Wachstum

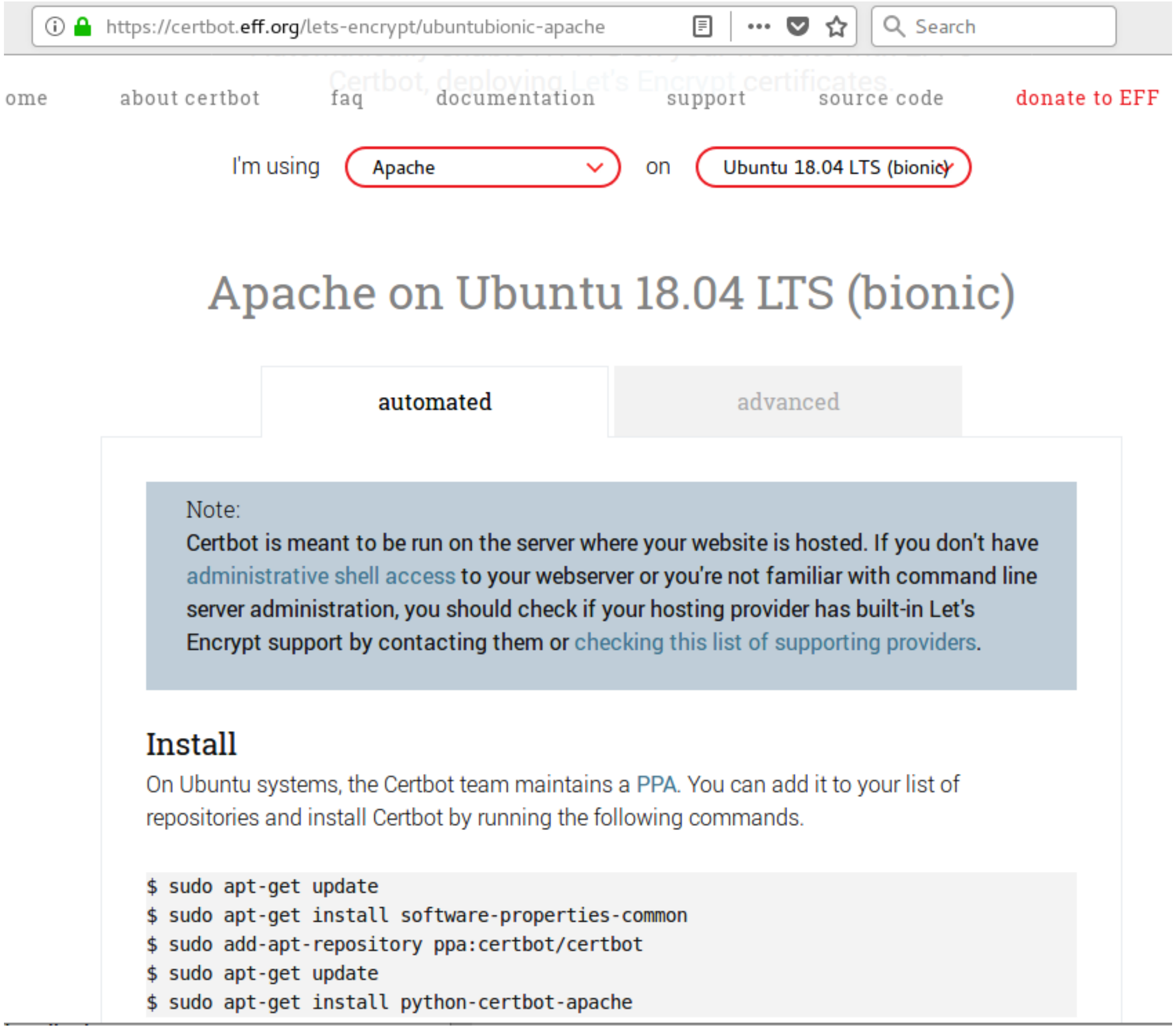


Vergleich

Let’s Encrypt	Traditionelle CA
kostenlos	kostenpflichtig
nur Domain-Validated	DV, OV, EV, ...
90 Tage gültig	max 2 Jahre (27 Monate)
Automatisierung via ACME (Automatic Certificate Management Environment)	Automatisierung teilweise kostenpflichtig bzw. propritär
Community Support	Professioneller Support
Software für Cert-Management erforderlich	Keine Software erforderlich
Automatischer Renewal	Manueller Renewal oder API
Keine Versicherung	Versicherungssumme von CA
Shell-Zugriff oder Support von Hoster notwendig	Kein Shell-Zugriff erforderlich

Let‘s Encrypt Clients

- sehr viele Clients für viele Programmier-Sprachen
- auch für Windows (z.B. win-acme)
- Empfehlung von Let‘s Encrypt: certbot
  - UNIX-only, Python
  - Ubuntu seit 18.04 (0.23.0-1) in universe, sowie PPA
  - Debian: 0.10 in jessie-backports und stretch (stable), 0.25 in stretch-backports
  - CentOS/RHEL 7: in EPEL (0.27)
  - Für Wildcard ACMEv2, certbot >= 0.22 und DNS-Challenge notwendig
  - Passende Anleitungen für Webserver und OS unter https://certbot.eff.org/



I'm using Apache on Ubuntu 18.04 LTS (bionic)

Apache on Ubuntu 18.04 LTS (bionic)

Note:
Certbot is meant to be run on the server where your website is hosted. If you don't have administrative shell access to your webserver or you're not familiar with command line server administration, you should check if your hosting provider has built-in Let's Encrypt support by contacting them or checking this list of supporting providers.

Install

On Ubuntu systems, the Certbot team maintains a PPA. You can add it to your list of repositories and install Certbot by running the following commands.

```
$ sudo apt-get update
$ sudo apt-get install software-properties-common
$ sudo add-apt-repository ppa:certbot/certbot
$ sudo apt-get update
$ sudo apt-get install python-certbot-apache
```

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

```
Created an SSL vhost at /etc/apache2/sites-enabled/www.example.com-
le-ssl.conf
Deploying Certificate to VirtualHost /etc/apache2/sites-
enabled/www.example.com-le-ssl.conf

Please choose whether or not to redirect HTTP traffic to HTTPS,
removing HTTP access.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: No redirect - Make no further changes to the webserver
configuration.
2: Redirect - Make all requests redirect to secure HTTPS access.
Choose this for
new sites, or if you're confident your site works on HTTPS. You can
undo this
change by editing your web server's configuration.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-2] then [enter] (press 'c' to
cancel): 1
```

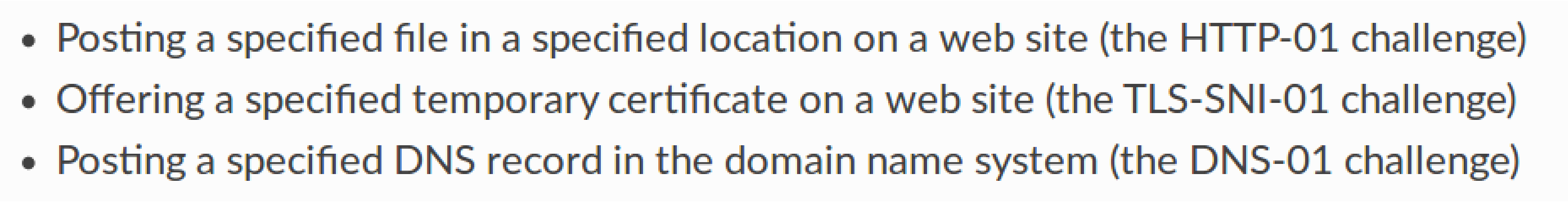
certbot

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Congratulations! You have successfully enabled
https://www.example.com

You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=www.example.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -


IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/www.example.com/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/www.example.com/privkey.pem
   Your cert will expire on 2019-01-17. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
again
   with the "certonly" option. To non-interactively renew *all* of
   your certificates, run "certbot renew"
```

certbot

- Nur Zertifikat ohne automatischer Apache-Konfiguration: **certbot --apache certonly**
- Renewal passiert automatisch über Cron-Job
- Konfiguration in /etc/letsencrypt
- certbot delete/revoke -d www.example.com

Let‘s Encrypt Challenges



- Posting a specified file in a specified location on a web site (the HTTP-01 challenge)
- Offering a specified temporary certificate on a web site (the TLS-SNI-01 challenge)
- Posting a specified DNS record in the domain name system (the DNS-01 challenge)

- HTTP-Challenge läuft nur via Port 80 /var/www/.well-known/acme-challenge/
- TLS-SNI-01 Anfang des Jahres teilweise deaktiviert, wegen Sicherheitslücke im Shared Hosting Umfeld
- für Wildcard ist DNS-01 Challenge erforderlich

Let‘s Encrypt Wildcard

- TXT Record muss von certbot erstellt werden können
- DNS-Privilegien auf _acme-challenge Record limitieren
- Dynamisches DNS Update mit Bind:

```
key "letsencrypt." {
  algorithm hmac-sha512;
  secret "abcdefghijklmnopqrstuvwxyz==";
};

zone "example.com" {
      type master;
       ...
      update-policy {
        grant letsencrypt. name _acme-challenge.example.com. txt;
  };
};
```

Let‘s Encrypt Wildcard

- Credentials müssen für Certbot zugänglich sein

```
certbot certonly --dns-rfc2136 --dns-rfc2136-credentials
~/.secrets/certbot/rfc2136.ini -d *.example.com --dns-rfc2136-
propagation-seconds 10
```

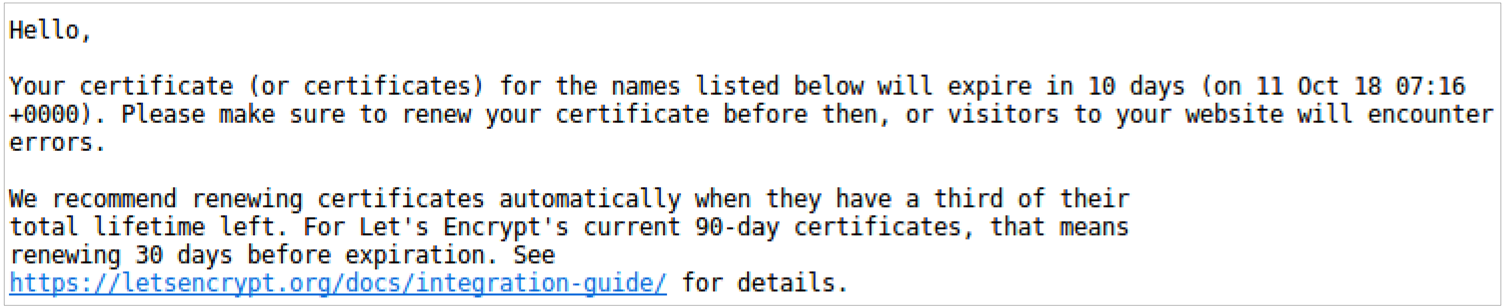
- Kontrolle über DNS Zone erforderlich

Agenda

- Aktuelle Entwicklungen
- Zertifikats-Typen
- Traditionell vs. Let‘s Encrypt
- Zertifikats-Management
- Konfiguration
- Tools

Zertifikats-Managment

- Renewal
  - passiert bei Let‘s Encrypt automatisch, Reminder E-Mail 20 Tage vor Ablauf



Hello,

Your certificate (or certificates) for the names listed below will expire in 10 days (on 11 Oct 18 07:16 +0000). Please make sure to renew your certificate before then, or visitors to your website will encounter errors.

We recommend renewing certificates automatically when they have a third of their total lifetime left. For Let's Encrypt's current 90-day certificates, that means renewing 30 days before expiration. See https://letsencrypt.org/docs/integration-guide/ for details.

  - Traditionelle CAs
    - schicken normalerweise 90 Tage vorher Reminder aus
    - Restzeit wird auf neues Zertifikat normalerweise gutgeschrieben
    - bei OV/EV rechtzeitig mit Renewal starten
  - Eigenständige Überwachung der Gültigkeit sinnvoll

Zertifikats-Managment

- Revoke
  - bei Let‘s Encrypt via Command-Line:
    `certbot --cert-path /etc/letsencrypt/archive/${YOUR_DOMAIN}/cert1.pem`
  - Bei traditionellen CAs via Webinterface oder API
  - auf OCSP Server eingetragen
- Monitoring
  - via Icinga Check
    - `check_http --sni -C 30` (Anzahl Tage Gültigkeit Zertifikat)
    - https://github.com/ssllabs/ssllabs-scan
  - Hosted Check
    - keychest.net, certificatemonitor.org, letsmonitor.org
    - Oder via healthchecks.io - https://medium.com/@healthchecks/diy-ssl-certificate-expiry-monitoring-a584ccd403bb
      ```
      ssl-cert-check -s example.com -p 443 -x 30 -n -q && curl -fsS --retry 3
      https://hchk.io/your-uuid-here > /dev/null
      ```

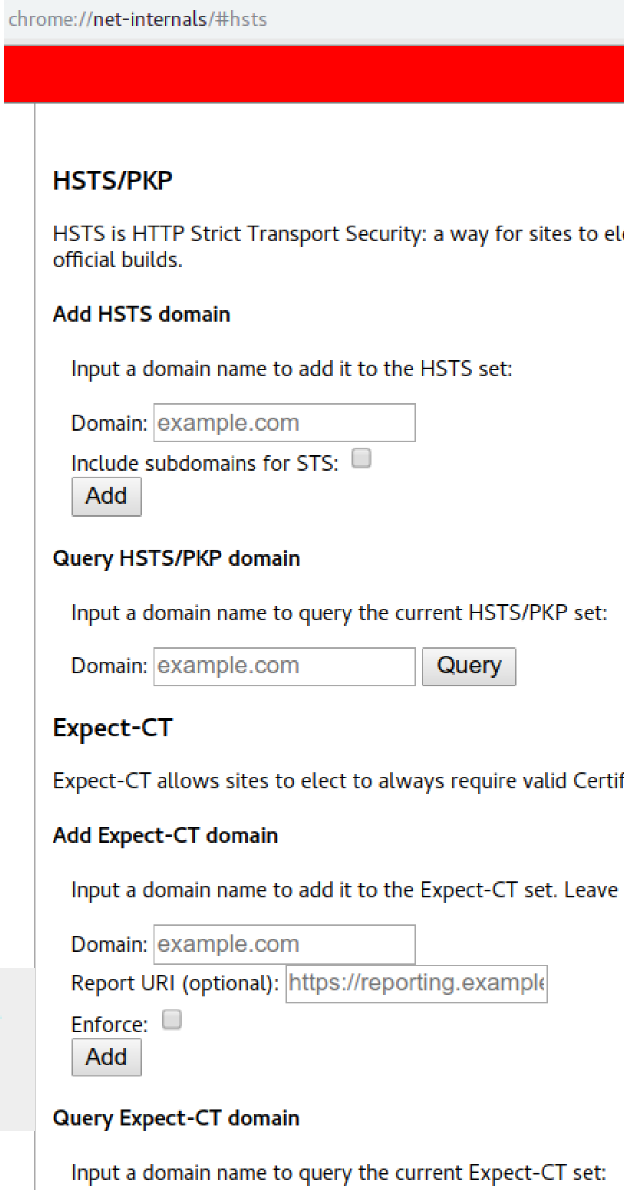
Agenda

- Aktuelle Entwicklungen
- Zertifikats-Typen
- Traditionell vs. Let‘s Encrypt
- Zertifikats-Management
- Konfiguration
- Tools

Konfiguration

- HSTS - HTTP Strict Transport Security
  - Wenn beim ersten Besuch HTTP Header „Strict-Transport-Security“ gesetzt ist, kann bis zu „max-age“ die Seite nur mehr per HTTPS aufgerufen werden
  - HSTS preload list löst das Problem von „trust on first use“
- HPKP - HTTP Public Key Pinning
  - Liste gültiger Zertifikate mit HTTP Header „Public-Key-Pins“ gesetzt und vom Browser des Nutzers gespeichert
  - Komplex, fehleranfällig, RansomPKP
  - In Chrome soll es von Expect-CT abgelöst werden
- Expect-CT (Certificate Transparency)
  - Zertifikat muss in öffentlichem CT Log aufscheinen

```
Expect-CT: report-uri="<uri>",
           enforce,
           max-age=<age>
```



chrome://net-internals/#hsts

HSTS/PKP

HSTS is HTTP Strict Transport Security: a way for sites to el
official builds.

Add HSTS domain

Input a domain name to add it to the HSTS set:

Domain: example.com

Include subdomains for STS: □

Add

Query HSTS/PKP domain

Input a domain name to query the current HSTS/PKP set:

Domain: example.com Query

Expect-CT

Expect-CT allows sites to elect to always require valid Certif

Add Expect-CT domain

Input a domain name to add it to the Expect-CT set. Leave

Domain: example.com

Report URI (optional): https://reporting.example

Enforce: □

Add

Query Expect-CT domain

Input a domain name to query the current Expect-CT set:

Konfiguration

- CAA
  - In DNS-Zone werden nur bestimmte CAs erlaubt

    ```
    $ dig www.thomas-krenn.com caa
    ...
    ;; ANSWER SECTION:
    www.thomas-krenn.com.900 IN  CAA 0 issue "digicert.com"
    ```

  - mehrere CAA Einträge für verschiedene CAs
  - „issuewild“ für Wildcard Certs
  - seit 9/2017 ist Prüfung durch CAs verpflichtend
- HTTP/2
  - Browser unterstüzen nur mehr „HTTP/2 over TLS“ - Protokoll „h2“

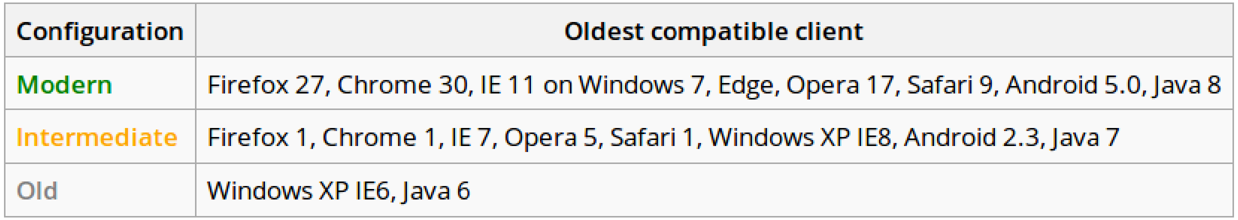
Konfiguration

- Let‘s Encrypt liefert Apache TLS-Config mit: /etc/letsencrypt/options-ssl-apache.conf

```
# This file contains important security parameters. If you modify this file
# manually, Certbot will be unable to automatically provide future security
# updates. Instead, Certbot will print and log an error message with a path to
# the up-to-date file that you will need to refer to when manually updating
# this file.

SSLEngine on

# Intermediate configuration, tweak to your needs
SSLProtocol             all -SSLv2 -SSLv3
SSLCipherSuite          ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-
GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-
SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-
SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-
SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA:!DSS
SSLHonorCipherOrder     on
SSLCompression          off

SSLOptions +StrictRequire

# Add vhost name to log entries:
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\"" vhost_combined
LogFormat "%v %h %l %u %t \"%r\" %>s %b" vhost_common

#CustomLog /var/log/apache2/access.log vhost_combined
#LogLevel warn
#ErrorLog /var/log/apache2/error.log

# Always ensure Cookies have "Secure" set (JAH 2012/1)
#Header edit Set-Cookie (?i)^(.*)(;\s*secure)??((\s*;)?(.*)) "$1; Secure$3$4"
```

Konfiguration

- Höhere Sicherheit → weniger Client-Support
- Umfassende TLS-Empfehlungen bei Mozilla: https://wiki.mozilla.org/Security/Server_Side_TLS

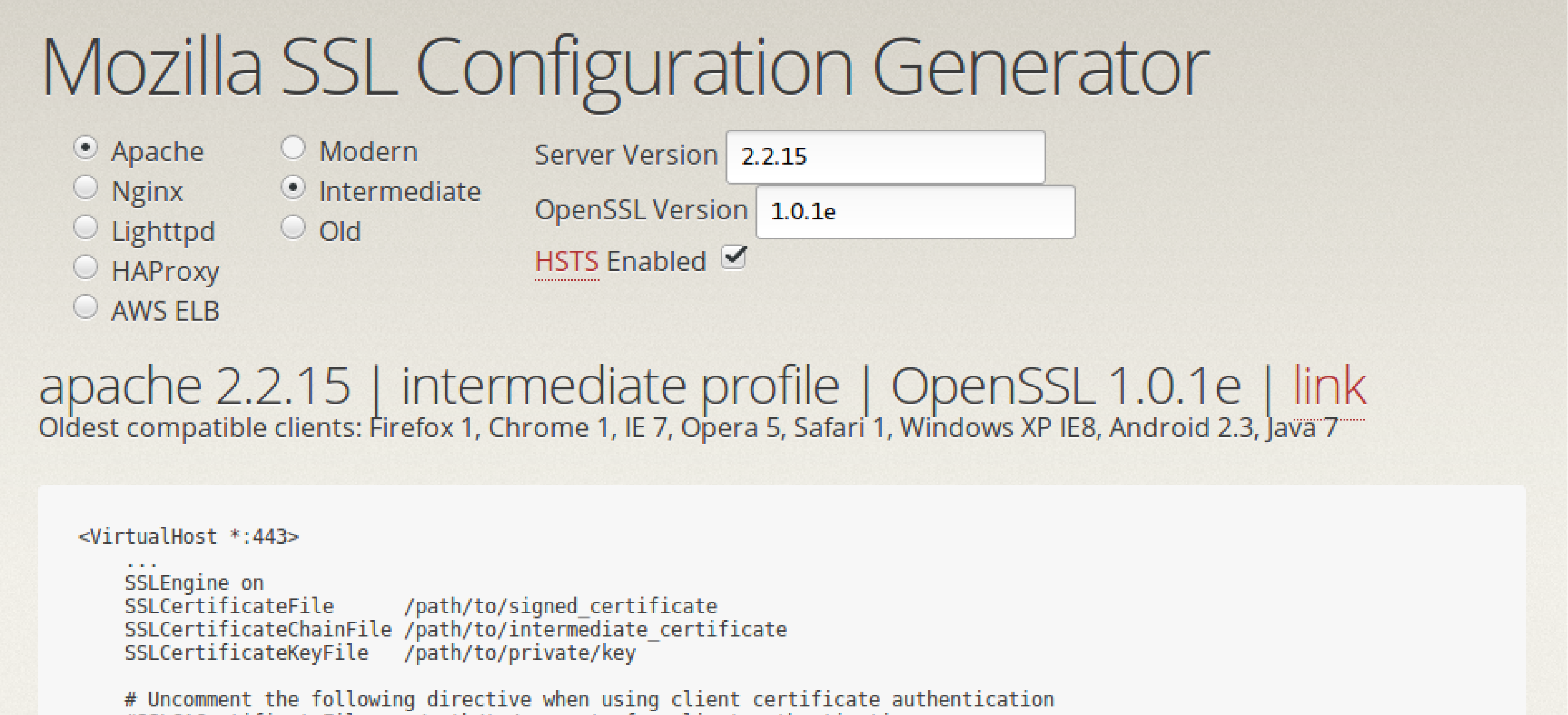


Configuration	Oldest compatible client
Modern	Firefox 27, Chrome 30, IE 11 on Windows 7, Edge, Opera 17, Safari 9, Android 5.0, Java 8
Intermediate	Firefox 1, Chrome 1, IE 7, Opera 5, Safari 1, Windows XP IE8, Android 2.3, Java 7
Old	Windows XP IE6, Java 6

- Weitere Empfehlungen:
  - OWASP: https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
  - Scott Helme: https://scotthelme.co.uk/https-cheat-sheet/ und https://securityheaders.com/
  - BSI Technische Richtlinie "Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)" Version: 2018-01 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html
- TLS-Konfiguration **nicht nur bei HTTPS** relevant
  → SMTP, IMAP, FTPS, XMMP, ...

Konfiguration

- Mozilla SSL Configuration Generator https://mozilla.github.io/server-side-tls/ssl-config-generator/



Mozilla SSL Configuration Generator

● Apache
○ Nginx
○ Lighttpd
○ HAProxy
○ AWS ELB

○ Modern
● Intermediate
○ Old

Server Version: 2.2.15
OpenSSL Version: 1.0.1e
HSTS Enabled ☑

apache 2.2.15 | intermediate profile | OpenSSL 1.0.1e | link
Oldest compatible clients: Firefox 1, Chrome 1, IE 7, Opera 5, Safari 1, Windows XP IE8, Android 2.3, Java 7

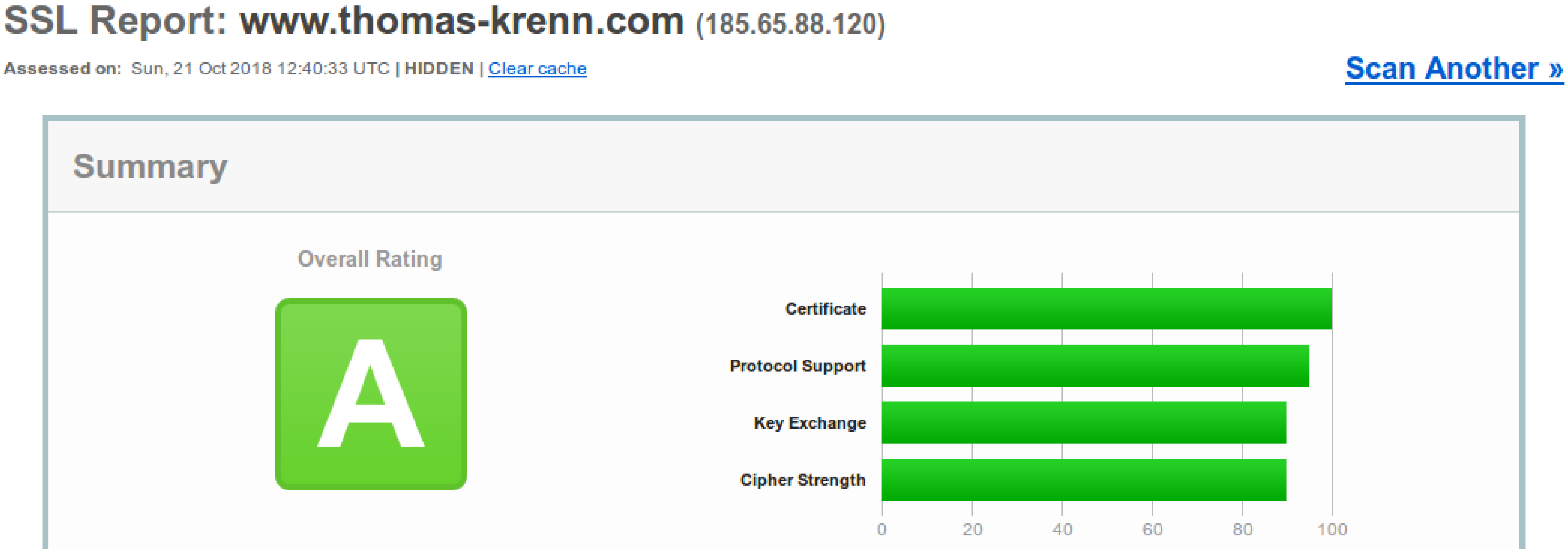
```
<VirtualHost *:443>
    ...
    SSLEngine on
    SSLCertificateFile      /path/to/signed_certificate
    SSLCertificateChainFile /path/to/intermediate_certificate
    SSLCertificateKeyFile   /path/to/private/key

    # Uncomment the following directive when using client certificate authentication
```

Agenda

- Aktuelle Entwicklungen
- Zertifikats-Typen
- Traditionell vs. Let‘s Encrypt
- Zertifikats-Management
- Konfiguration
- Tools

Tools

- Qualys. SSL Labs – SSL Server Test
  - https://www.ssllabs.com/ssltest/
  - Via CLI für automatisches Monitoring https://github.com/ssllabs/ssllabs-scan

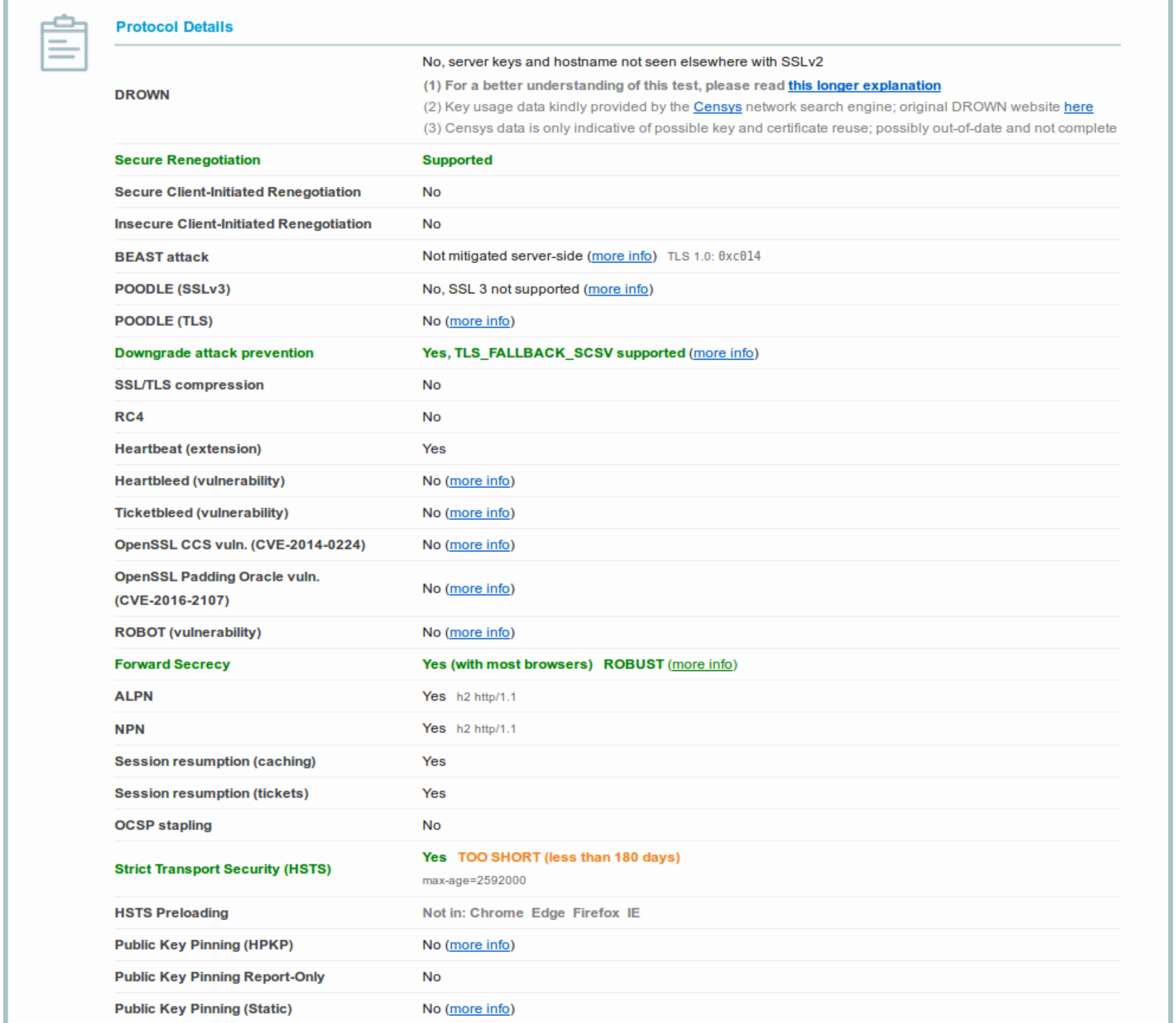


SSL Report: www.thomas-krenn.com (185.65.88.120)

Assessed on: Sun, 21 Oct 2018 12:40:33 UTC | **HIDDEN** | Clear cache

Scan Another »

Summary

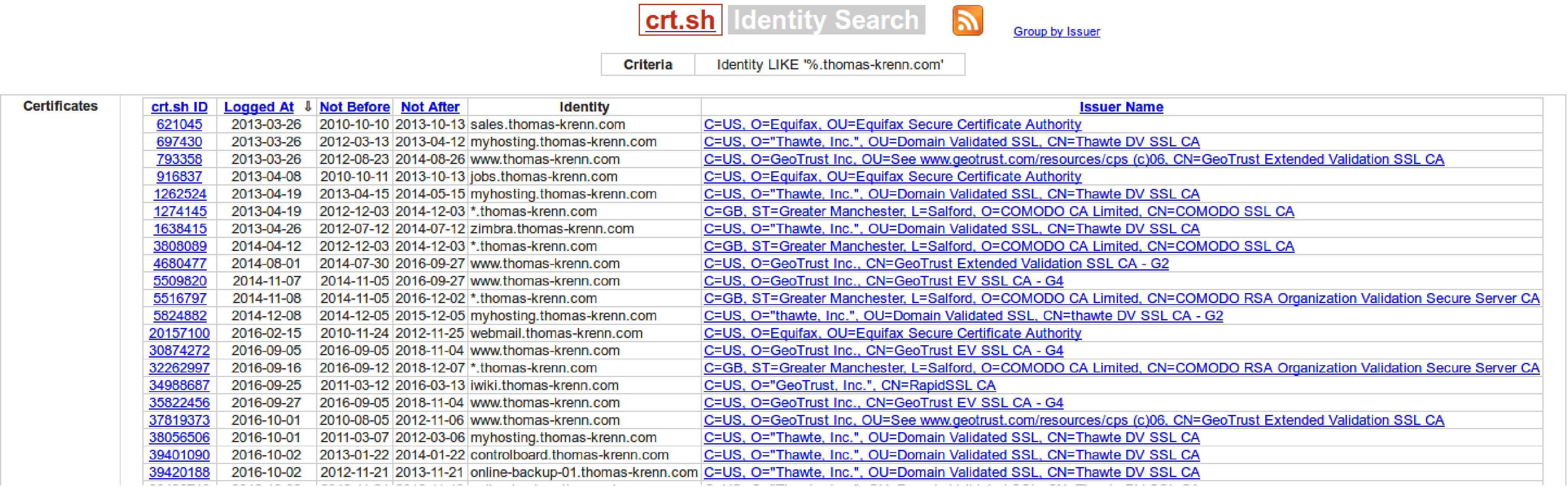


Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
ALPN	Yes h2 http/1.1
NPN	Yes h2 http/1.1
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	Yes TOO SHORT (less than 180 days) max-age=2592000
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)

Tools

- Certificate Transparency Logs abfragen
  - https://crt.sh/
  - Inhalte sollte für interne Dienste bedacht werden



Criteria	Identity LIKE '%.thomas-krenn.com'

Certificates

crt.sh ID	Logged At ⇩	Not Before	Not After	Identity	Issuer Name
621045	2013-03-26	2010-10-10	2013-10-13	sales.thomas-krenn.com	C=US, O=Equifax, OU=Equifax Secure Certificate Authority
697430	2013-03-26	2012-03-13	2013-04-12	myhosting.thomas-krenn.com	C=US, O="Thawte, Inc.", OU=Domain Validated SSL, CN=Thawte DV SSL CA
793358	2013-03-26	2012-08-23	2014-08-26	www.thomas-krenn.com	C=US, O=GeoTrust Inc, OU=See www.geotrust.com/resources/cps (c)06, CN=GeoTrust Extended Validation SSL CA
916837	2013-04-08	2010-10-11	2013-10-13	jobs.thomas-krenn.com	C=US, O=Equifax, OU=Equifax Secure Certificate Authority
1262524	2013-04-19	2013-04-15	2014-05-15	myhosting.thomas-krenn.com	C=US, O="Thawte, Inc.", OU=Domain Validated SSL, CN=Thawte DV SSL CA
1274145	2013-04-19	2012-12-03	2014-12-03	*.thomas-krenn.com	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO SSL CA
1638415	2013-04-26	2012-07-12	2014-07-12	zimbra.thomas-krenn.com	C=US, O="Thawte, Inc.", OU=Domain Validated SSL, CN=Thawte DV SSL CA
3808089	2014-04-12	2012-12-03	2014-12-03	*.thomas-krenn.com	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO SSL CA
4680477	2014-08-01	2014-07-30	2016-09-27	www.thomas-krenn.com	C=US, O=GeoTrust Inc., CN=GeoTrust Extended Validation SSL CA - G2
5509820	2014-11-07	2014-11-05	2016-09-27	www.thomas-krenn.com	C=US, O=GeoTrust Inc., CN=GeoTrust EV SSL CA - G4
5516797	2014-11-08	2014-11-05	2016-12-02	*.thomas-krenn.com	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Organization Validation Secure Server CA
5824882	2014-12-08	2014-12-05	2015-12-05	myhosting.thomas-krenn.com	C=US, O="thawte, Inc.", OU=Domain Validated SSL, CN=thawte DV SSL CA - G2
20157100	2016-02-15	2010-11-24	2012-11-25	webmail.thomas-krenn.com	C=US, O=Equifax, OU=Equifax Secure Certificate Authority
30874272	2016-09-05	2016-09-05	2018-11-04	www.thomas-krenn.com	C=US, O=GeoTrust Inc., CN=GeoTrust EV SSL CA - G4
32262997	2016-09-16	2016-09-12	2018-12-07	*.thomas-krenn.com	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Organization Validation Secure Server CA
34988687	2016-09-25	2011-03-12	2016-03-13	iwiki.thomas-krenn.com	C=US, O="GeoTrust, Inc.", CN=RapidSSL CA
35822456	2016-09-27	2016-09-05	2018-11-04	www.thomas-krenn.com	C=US, O=GeoTrust Inc., CN=GeoTrust EV SSL CA - G4
37819373	2016-10-01	2010-08-05	2012-11-06	www.thomas-krenn.com	C=US, O=GeoTrust Inc, OU=See www.geotrust.com/resources/cps (c)06, CN=GeoTrust Extended Validation SSL CA
38056506	2016-10-01	2011-03-07	2012-03-06	myhosting.thomas-krenn.com	C=US, O="Thawte, Inc.", OU=Domain Validated SSL, CN=Thawte DV SSL CA
39401090	2016-10-02	2013-01-22	2014-01-22	controlboard.thomas-krenn.com	C=US, O="Thawte, Inc.", OU=Domain Validated SSL, CN=Thawte DV SSL CA
39420188	2016-10-02	2012-11-21	2013-11-21	online-backup-01.thomas-krenn.com	C=US, O="Thawte, Inc.", OU=Domain Validated SSL, CN=Thawte DV SSL CA

Tools

- openssl s_client CLI
  - **`openssl s_client -connect www.thomas-krenn.com:443 -servername www.thomas-krenn.com`**
    … -servername → für SNI relevant
  - mit STARTTLS testen und Datum extrahieren

```
openssl s_client -connect mail.thomas-krenn.com:25 -starttls smtp | openssl x509 -noout -dates
depth=2 C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA
Certification Authority
verify return:1
depth=1 C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA
Organization Validation Secure Server CA
verify return:1
depth=0 C = DE, postalCode = 94078, ST = Bavaria, L = Freyung, street = Steinaecker 1,
postOfficeBox = 94078, O = Thomas-Krenn.AG, OU = IT-Administration, OU = PremiumSSL Wildcard, CN
= *.thomas-krenn.com
verify return:1
notBefore=Sep 12 00:00:00 2016 GMT
notAfter=Dec  7 23:59:59 2018 GMT
250 SIZE 104857600
```

Fazit

- HTTPS löst HTTP großteils ab
- Komplexes und sehr agiles Thema
- Automatisierung und Monitoring der Zertifikate
- TLS-Konfiguration regelmäßig prüfen
- TLS-relevante Software aktuell halten

Vielen Dank für Ihre Aufmerksamkeit!

THOMAS KRENN®