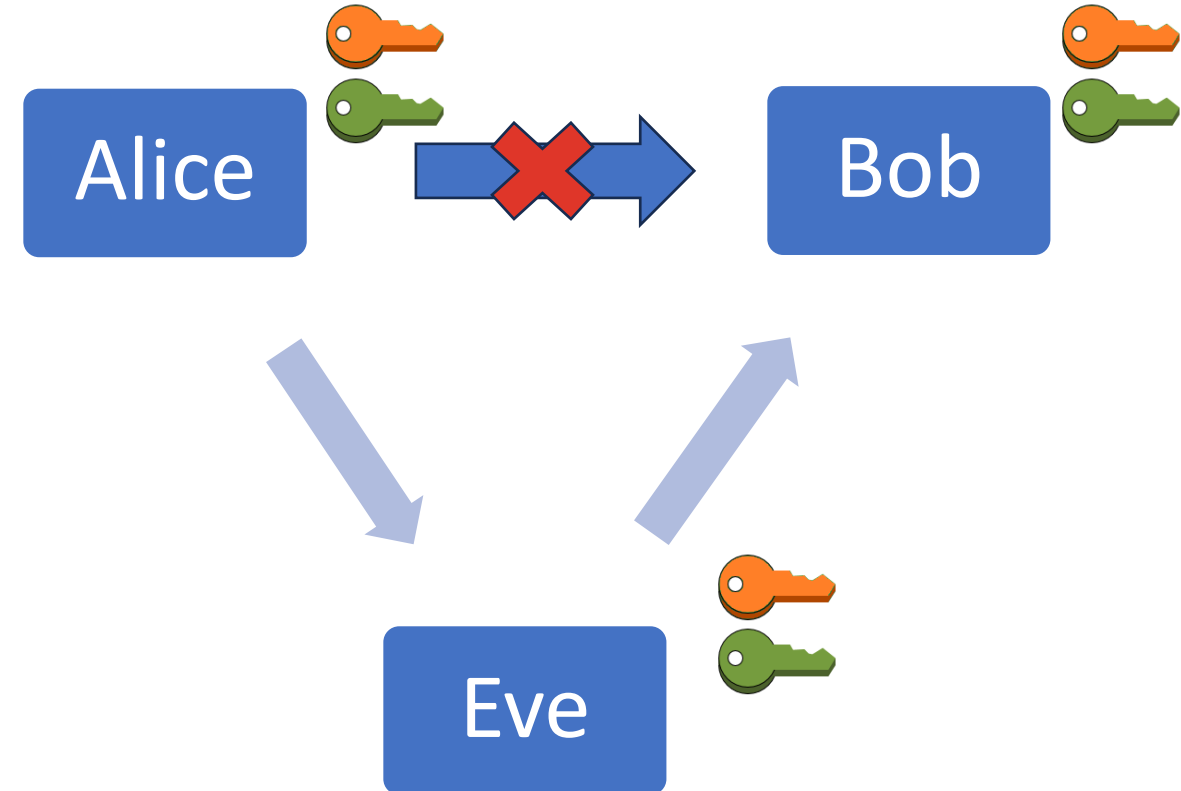


IT Sicherheit

01 PKI – Public Key Infrastructure

Einführung / Probleme mit asymmetrischer Verschlüsselung

- Asymmetrische Verschlüsselung:
Public Key / Private Key
- Problem: Wie bekommt Kommunikationspartner B den Public Key des Kommunikationspartners A?



Einführung / Probleme mit asymmetrischer Verschlüsselung



- Lösung: Zertifikate
- Zertifikat: Digitaler Datensatz, mit dessen Hilfe bestimmte Eigenschaften bzw. Identitäten nachgewiesen werden können

Certificate Viewer: *.orf.at

General Details

Issued To

| | |
|--------------------------|----------------------------|
| Common Name (CN) | *.orf.at |
| Organization (O) | Oesterreichischer Rundfunk |
| Organizational Unit (OU) | <Not Part Of Certificate> |

Issued By

| | |
|--------------------------|--|
| Common Name (CN) | Entrust Certification Authority - L1K |
| Organization (O) | Entrust, Inc. |
| Organizational Unit (OU) | See www.entrust.net/legal-terms |

Validity Period

| | |
|------------|--|
| Issued On | Wednesday, March 22, 2023 at 12:37:38 PM |
| Expires On | Sunday, April 21, 2024 at 1:37:38 PM |

Fingerprints

| | |
|---------------------|--|
| SHA-256 Fingerprint | C5 26 6E 7A 7A AF BE 73 07 C1 55 F9 A6 31 9D 25 2F 27 9A 7B 34 06 F7 D3 89 01 9B D9 E8 FE DF 14 |
| SHA-1 Fingerprint | 19 D5 46 1E 28 9B FF 06 20 EA 0C FB 6F AF 85 EE 8E 96 F5 5D |

Einführung / Probleme mit asymmetrischer Verschlüsselung



- PKI (Public-Key Infrastructure): Struktur zur Ausstellung, Verteilung und Prüfung von digitalen Zertifikaten
- Zwei gängige Varianten:
 - OpenPGP – Web of Trust
 - X.509 – Hierarchische Zertifizierungsstellen

OpenPGP – Web Of Trust

- Netz an Teilnehmern
- Teilnehmer erstellen Zertifikate selbst
- Teilnehmer teilen Zertifikate mit anderen Teilnehmern (z.B. Keyserver, Email, USB Stick, Messenger, ...)
- Zertifikate werden von anderen Teilnehmern signiert
- Teilnehmer können selbst entscheiden, welchen Zertifikaten Sie vertrauen:
 - Mindestens X andere haben das Zertifikat signiert
 - Bestimmte andere Personen haben das Zertifikat signiert

OpenPGP – Web Of Trust

- Übung

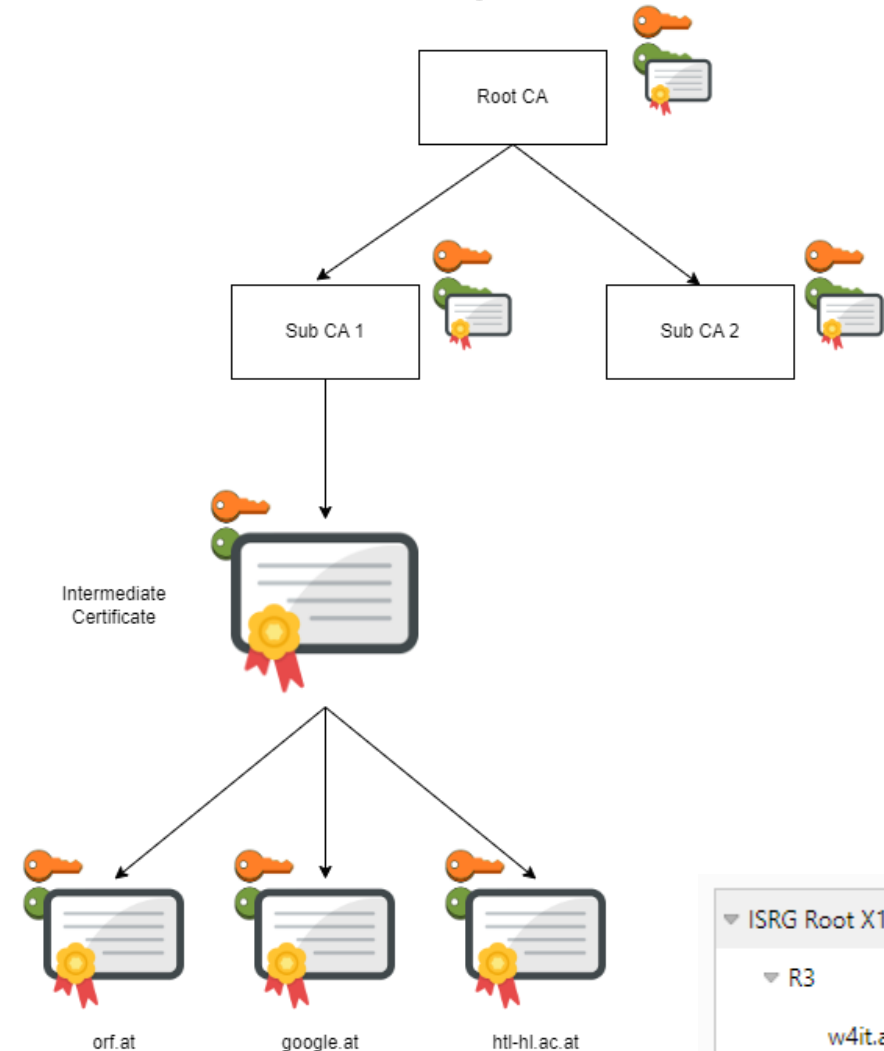
X.509 – Hierarchische Zertifizierungsstellen



- Streng hierarchisch aufgebaut – an der Spitze steht die Root-CA
- Unterschied zu “Web of Trust”: Nur eine CA signiert Zertifikate – nicht jeder
- Root-CA kann auch Sub-CAs ermöglichen – diese können dann auch Zertifikate signieren, welchen jeder vertraut der der Root-CA vertraut

X.509 – Hierarchische Zertifizierungsstellen

- Root CA
 - Private Key (stark geschützt – offline only)
 - Public Key und Zertifikat (wird von gängigen OS/Browsern vertraut)
- Sub CA 1/2
 - Private Key (stark geschützt – offline only)
 - Public Key und Zertifikat (Optional: wird von gängigen OS/Browsern vertraut, wird von Root CA signiert)
- Intermediate Certificate
 - Private Key: wird für Signierung von Zertifikaten genutzt
 - Public Key und Zertifikat
- Zertifikat
 - Private Key: Sollte von Administrator erzeugt werden (nicht von der CA)
 - Public Key und Zertifikat (wird von Intermediate Public Key signiert)
 - Damit Client dem Zertifikat vertraut, muss mit Zertifikat auch das Intermediate (und optional das Sub CA) Certificate ausgeliefert werden



| | |
|----------------|--------------|
| ▼ ISRG Root X1 | Root CA |
| ▼ R3 | Intermediate |
| w4it.at | Certificate |

X.509 – Hierarchische Zertifizierungsstellen



- Einmal signierte Zertifikate können nicht zurückgenommen werden – Lösung: CRL
- CRL gibt Auskunft über gesperrte Zertifikate – Sollte vor dem akzeptieren eines Zertifikats überprüft werden
- Weiterentwicklung: OCSP
- Online Service, welcher über den Status eines Zertifikats Auskunft gibt
- Weiterentwicklung: OCSP Stapling
- Zertifikatstatus wird vom Server in regelmäßigen Abständen bei der CA angefragt und dann bei Bedarf an den TLS Handshake angehängt

X.509 – Hierarchische Zertifizierungsstellen

▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 508

Version: TLS 1.2 (0x0303)

Random: 281c6121e5f595e919fb24c7780bfefb86c6321c010da6fe16b4f481510d29878

Session ID Length: 32

Session ID: 91b87b4e713b234d02e35e8d9eefb2f234de97b623cc99512614fa9e24332a12

Cipher Suites Length: 32

> Cipher Suites (16 suites)

Compression Methods Length: 1

> Compression Methods (1 method)

Extensions Length: 403

> Extension: Reserved (GREASE) (len=0)

> Extension: renegotiation_info (len=1)

> Extension: key_share (len=43)

> Extension: psk_key_exchange_modes (len=2)

▼ Extension: status_request (len=5)

Type: status_request (5)

Length: 5

Certificate Status Type: OCSP (1)

Responder ID list Length: 0

Request Extensions Length: 0

▼ OCSP Response

responseStatus: successful (0)

▼ responseBytes

ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)

▼ BasicOCSPResponse

▼ tbsResponseData

> responderID: byKey (2)

producedAt: 2023-09-19 15:29:52 (UTC)

> responses: 1 item

▼ SingleResponse

> certID

> certStatus: good (0)

thisUpdate: 2023-09-19 13:11:22 (UTC)

nextUpdate: 2023-09-27 13:31:22 (UTC)

> singleExtensions: 1 item

X.509 – Hierarchische Zertifizierungsstellen



- Typische Bestandteile eines Zertifikats
 - Subject / Common Name: Domain/Email – mittlerweile eher unwichtig
 - Subject Alternative Name: Domains – sehr wichtig
 - Validity: Not Before, Not After – sehr wichtig
 - Issuer – informativ
 - Serial Number – wichtig zur Überprüfung, ob Zertifikat gefälscht wurde

X.509 – Hierarchische Zertifizierungsstellen

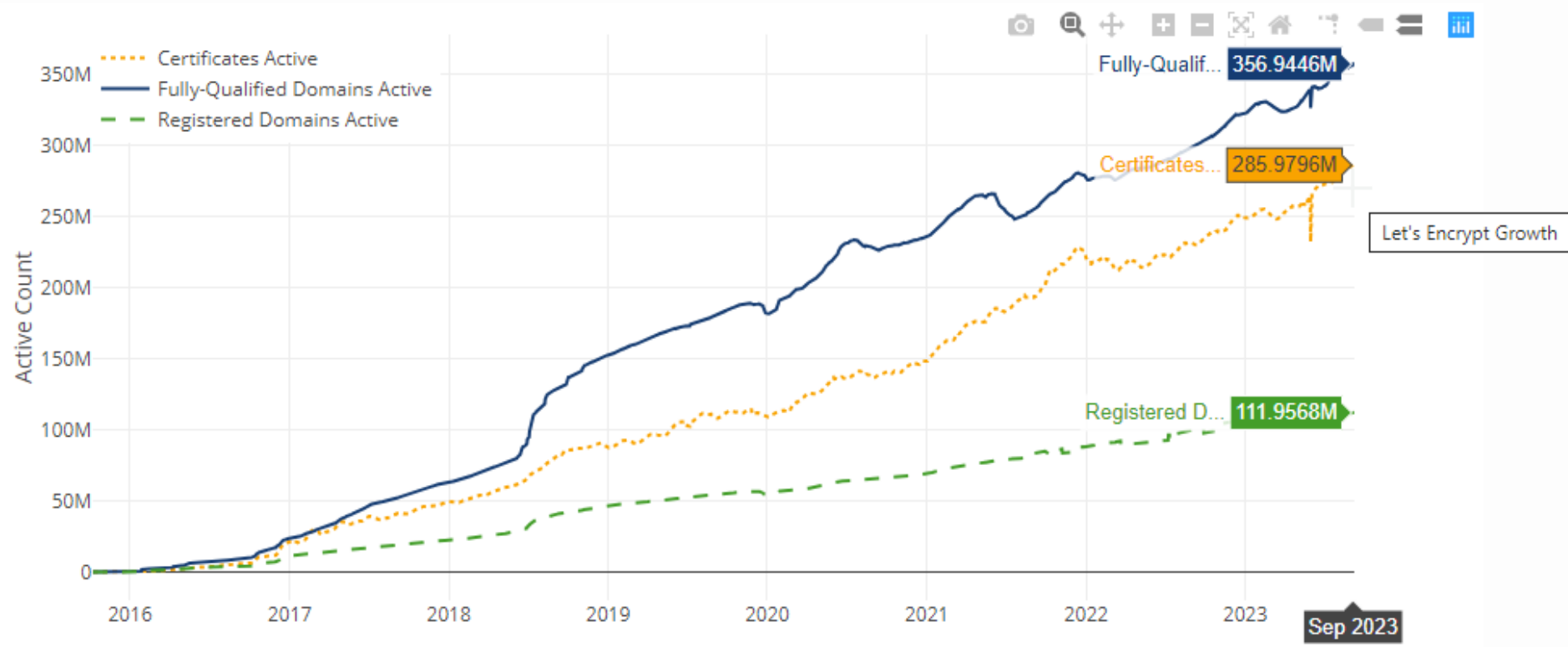
- Übung

Freie CA - Let's Encrypt

- Freie / Gemeinnützige CA aus den USA
- Aktiv seit 2014
- Ziel: HTTPS Verbindungen zum Standard machen
- Gültigkeit der Zertifikate: 90 Tage
 - Reduziert den Schaden bei Kompromittierung des Zertifikats / Keypairs
 - Motiviert Anwender den Prozess der Zertifikatsausstellung zu automatisieren
- Größte CA nach Anzahl Domains / ausgestellten Zertifikaten

Freie CA - Let's Encrypt

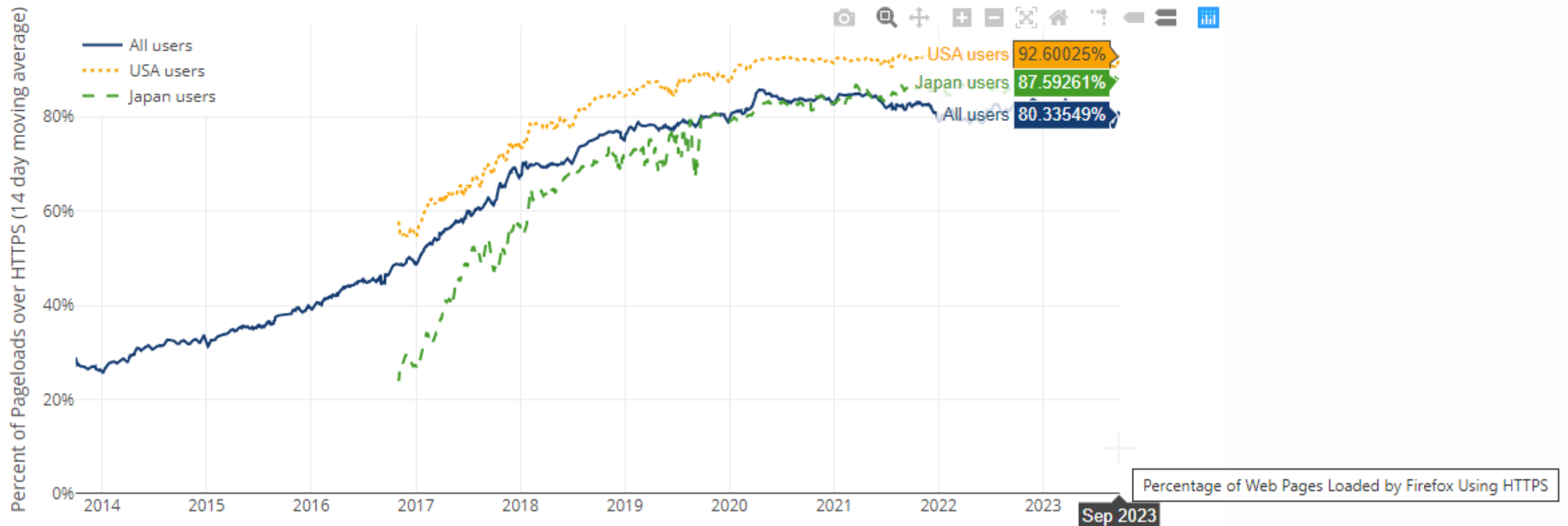
Let's Encrypt Growth



Freie CA - Let's Encrypt

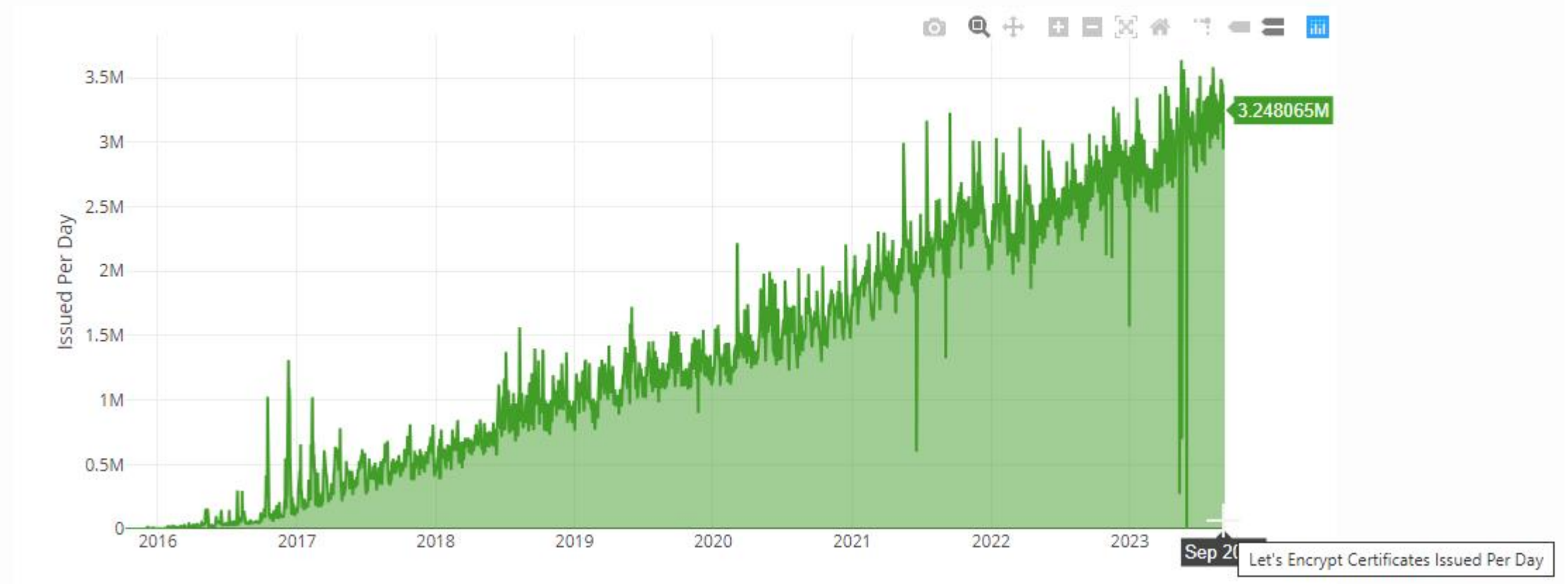
Percentage of Web Pages Loaded by Firefox Using HTTPS

(14-day moving average, source: [Firefox Telemetry](#))



Freie CA - Let's Encrypt

Let's Encrypt Certificates Issued Per Day



Freie CA - Let's Encrypt

- Protokoll zur Ausstellung von Zertifikaten: ACME
 - Aktuelle Version: v2
 - Mögliche Zertifikate:
 - Domain Validated Certificates
 - Domain Validated Wildcard Certificates
 - Beschreibt die Kommunikation zwischen den Servern der CA und den Servern der Anwender
 - Basis: Austausch von JSON Nachrichten über HTTPS
 - Basis sind so genannte Challenges:
 - HTTP-01 challenge
 - DNS-01 challenge
 - TLS-ALPN-01 challenge

Freie CA - Let's Encrypt

- HTTP-01 challenge
 - Anfrage an Let's Encrypt ACME API
 - Let's Encrypt ACME API liefert einen Token zurück
 - Url muss via Port 80 erreichbar sein (Datei mit Token + Fingerprint von Account-Key):
`http://<YOUR_DOMAIN>/.well-known/acme-challenge/<TOKEN>`
 - Rückmeldung an Let's Encrypt API
 - Let's Encrypt überprüft die Verfügbarkeit von mehreren Standorten weltweit
 - Zertifikat wird ausgestellt
 - Pro: Einfach zu automatisieren/Ohne Zugriff auf DNS verwendbar
 - Contra: Keine Wildcard Zertifikate / Port 80 erforderlich / Schwieriger bei lastverteilten Webservern

Freie CA - Let's Encrypt

- DNS-01 challenge
 - Anfrage an Let's Encrypt ACME API
 - Let's Encrypt ACME API liefert einen Token zurück
 - TXT Eintrag für `_acme-challenge.<YOUR_DOMAIN>` mit dem Token als Wert muss angelegt werden
 - Rückmeldung an Let's Encrypt API
 - Let's Encrypt überprüft die Verfügbarkeit von mehreren Standorten weltweit
 - Zertifikat wird ausgestellt
 - Pro: Ermöglicht Wildcard Zertifikate / Einfacher bei lastverteilten Webservern
 - Contra: Nur Sinnvoll, wenn DNS Anbieter eine API anbietet und Aktualisierungen schnell genug ausgerollt werden

Freie CA - Let's Encrypt

- TLS-ALPN-01 challenge
 - Nachfolger der TLS-SNI-01 challenge
 - Operiert auf Port 443 im Zuge des TLS Handshakes
 - Aktuell nicht stark verbreitet
 - Pro: Kann verwendet werden, wenn Port 80 nicht verfügbar ist
 - Contra: Aktuell nicht mit Apache/Nginx/Certbot unterstützt / Keine Wildcard Zertifikate möglich

Freie CA - Let's Encrypt

- Übung

Certificate Transparency Logs

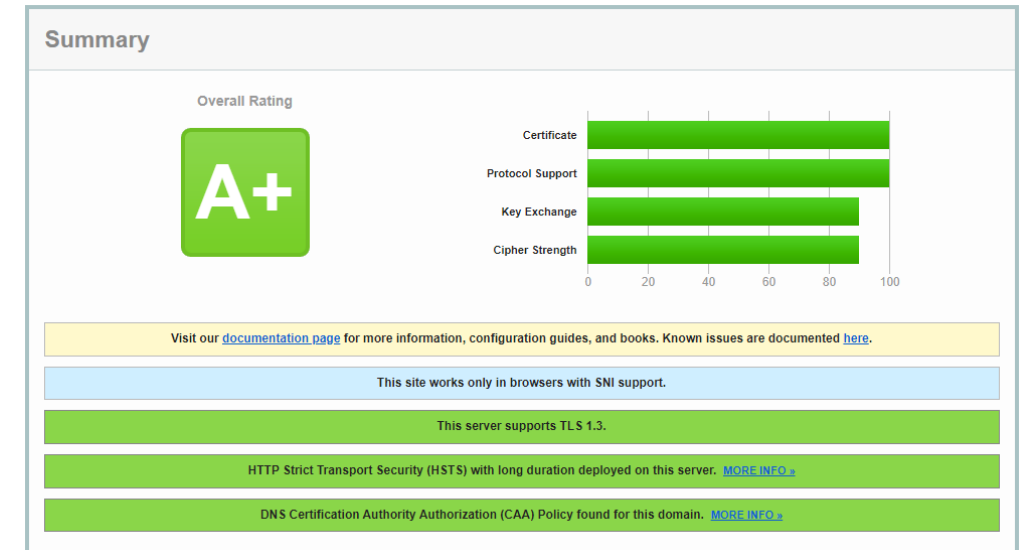
- CAs können bzw. müssen Informationen zu ausgestellten Zertifikaten in CTL ablegen
- CTLs werden von verschiedensten Anbietern bereitgestellt (Letsencrypt, Cloudflare, Google, ...)
- Browser prüfen, ob Zertifikat in genügend “passed” CTLs hinterlegt sind (Certificate Transparency Policy)
 - Google Chrome
 - Gültigkeitsdauer < 180Tage: Zertifikat muss in min. 2 CTL vorhanden sein
 - Gültigkeitsdauer > 180Tage: Zertifikat muss in min. 3 CTL vorhanden sein

Certificate Transparency Logs

- CTL manuell überprüfen
 - <https://crt.sh/>
 - https://sslmate.com/labs/ct_policy_analyzer/
 - <https://ct.cloudflare.com/>

Qualys SSL Server/Client Test

- <https://www.ssllabs.com/ssltest/>
 - Einfache Überprüfung der Konfiguration eines Webserver
 - SNI / HSTS / CAA
-
- <https://clienttest.ssllabs.com:8443/ssltest/viewMyClient.html>
 - Einfache Überprüfung des verwendeten Browsers



Protocol Features

| Protocols | |
|-----------|----------|
| TLS 1.3 | Yes |
| TLS 1.2 | Yes |
| TLS 1.1 | No |
| TLS 1.0 | Firewall |
| SSL 3 | Firewall |
| SSL 2 | Firewall |

| Cipher Suites (in order of preference) | |
|---|-----|
| TLS_GREASE_FA (0xfafa) | - |
| TLS_AES_128_GCM_SHA256 (0x1301) Forward Secrecy | 128 |
| TLS_AES_256_GCM_SHA384 (0x1302) Forward Secrecy | 256 |

Qualys SSL Server/Client Test

- Demo