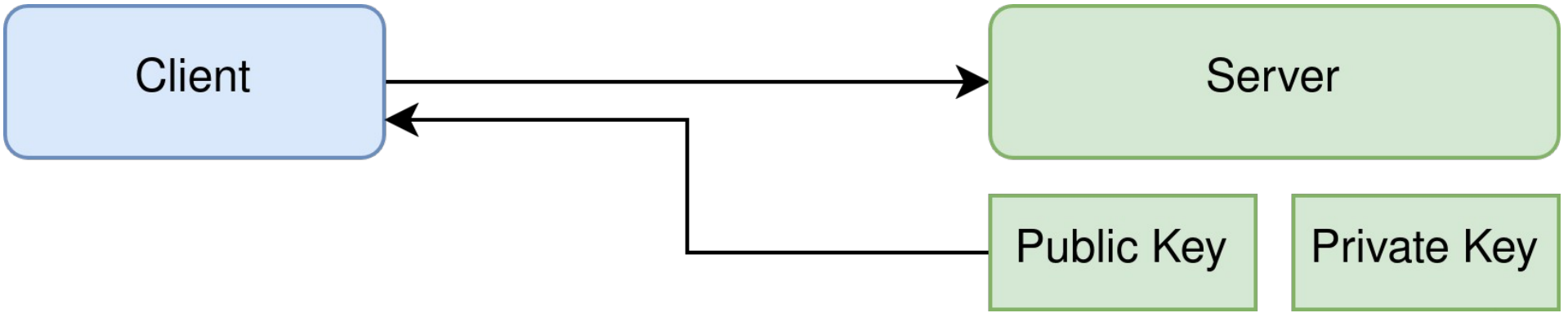
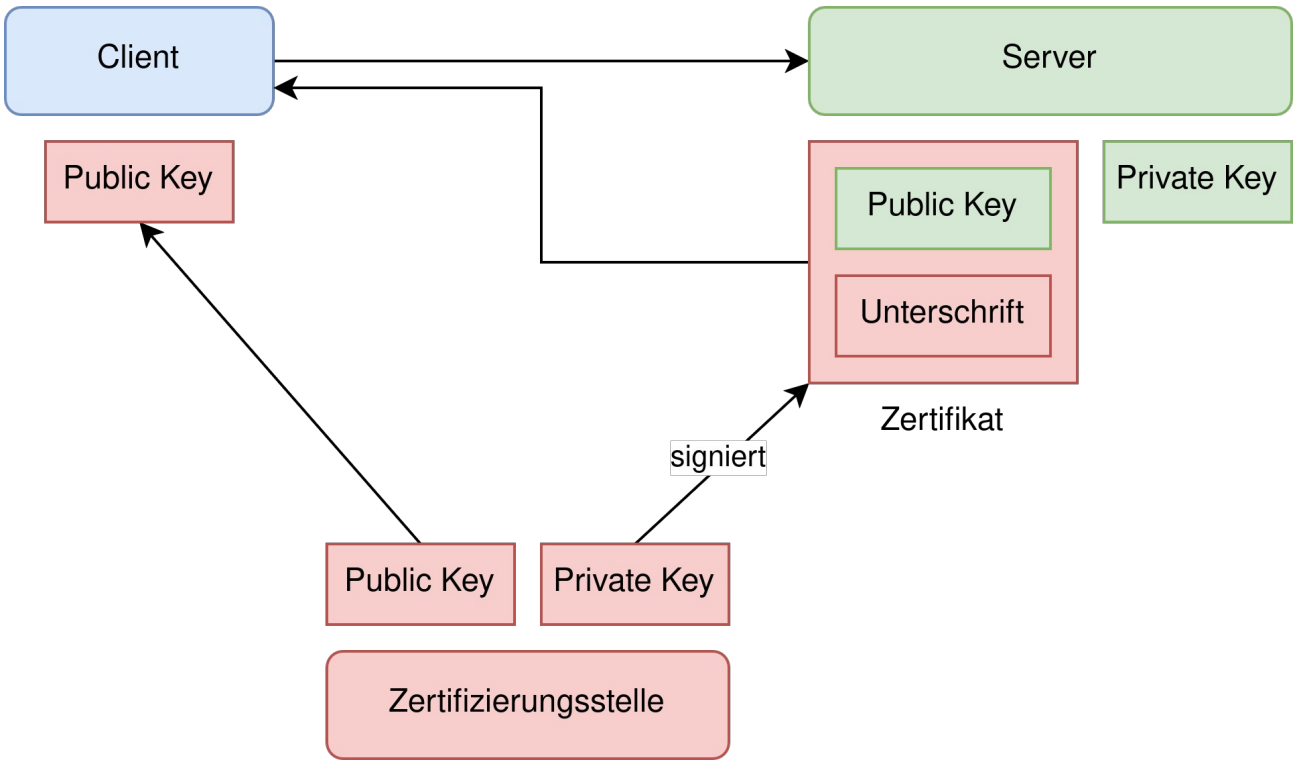
Let's-Encrypt-Zertifikate für Intranet-Server

Was sind X.509-Zertifikate?



Was sind X.509-Zertifikate?



Arten der Validierung

- Domain Validated (DV)
- Individual Validated (IV)
- Organization Validated (OV)
- Extended Validation (EV)


CLT2025 · Chemnitzer Linux-Tage 2025 – Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
CLT2025 · Chemnitzer Linux-Tage
https://chemnitzerlinux-tage.de/2025/de
Chemnitzer Linux-Tage
22. und 23. März 2025
the Culture of Open Source
ALLGEMEINES
PROGRAMM
ADD-ONS
SERVICE
CHEMNITZER LINUX-TAGE 2025
the Culture of Open Source
22. /23. März 2025
Hörsaalgebäude an der
Reichenhainer Straße 90
→ Links für den Schnelleinstieg
the Culture
#CLT2025
of Open
#CLT2025
Source
#CLT2025

Was ist Let’s Encrypt?

- Projekt der Internet Security Research Group (ISRG)
- Kostenlose Zertifikate
- Komplett automatisiert (ACME)
- Domain Validated
- 90 Tage Gültigkeit

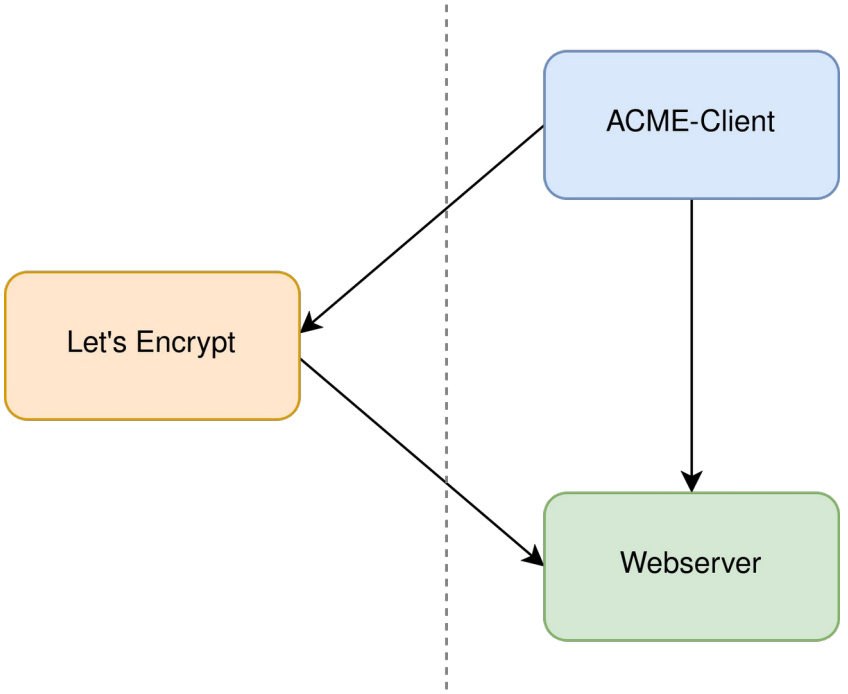
Warum Let’s-Encrypt im Intranet?

- Eigene PKI bedeutet Aufwand
- Benutzer verwenden eigene Geräte (BYOD)

Warum vielleicht auch nicht?

- Nur für öffentliche Domains
- Zertifikate sind im Certificate Transparency Log sichtbar

Domain Verification – HTTP-01 Challenge



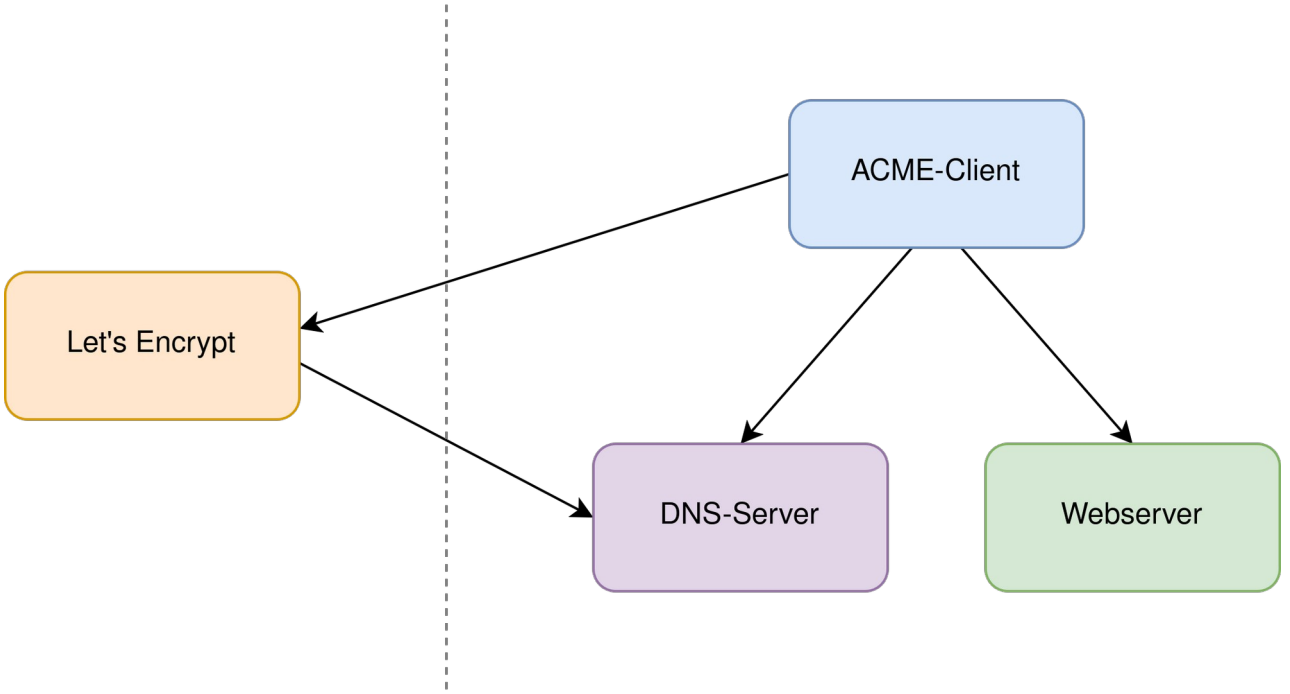
Domain Verification – HTTP-01 Challenge

- Der Client sendet Request an Let’s Encrypt und bekommt Challenge
- Der Client platziert die Challenge auf dem Webserver
- Let’s Encrypt überprüft die Challenge
- Der Client bekommt das signierte Zertifikat

Domain Verification – HTTP-01 Challenge

- Port 80 muss aus dem Internet erreichbar sein
- Workarounds für nicht-erreichbare Hosts:
  - Split DNS
  - DNAT

Domain Verification – DNS-01 Challenge



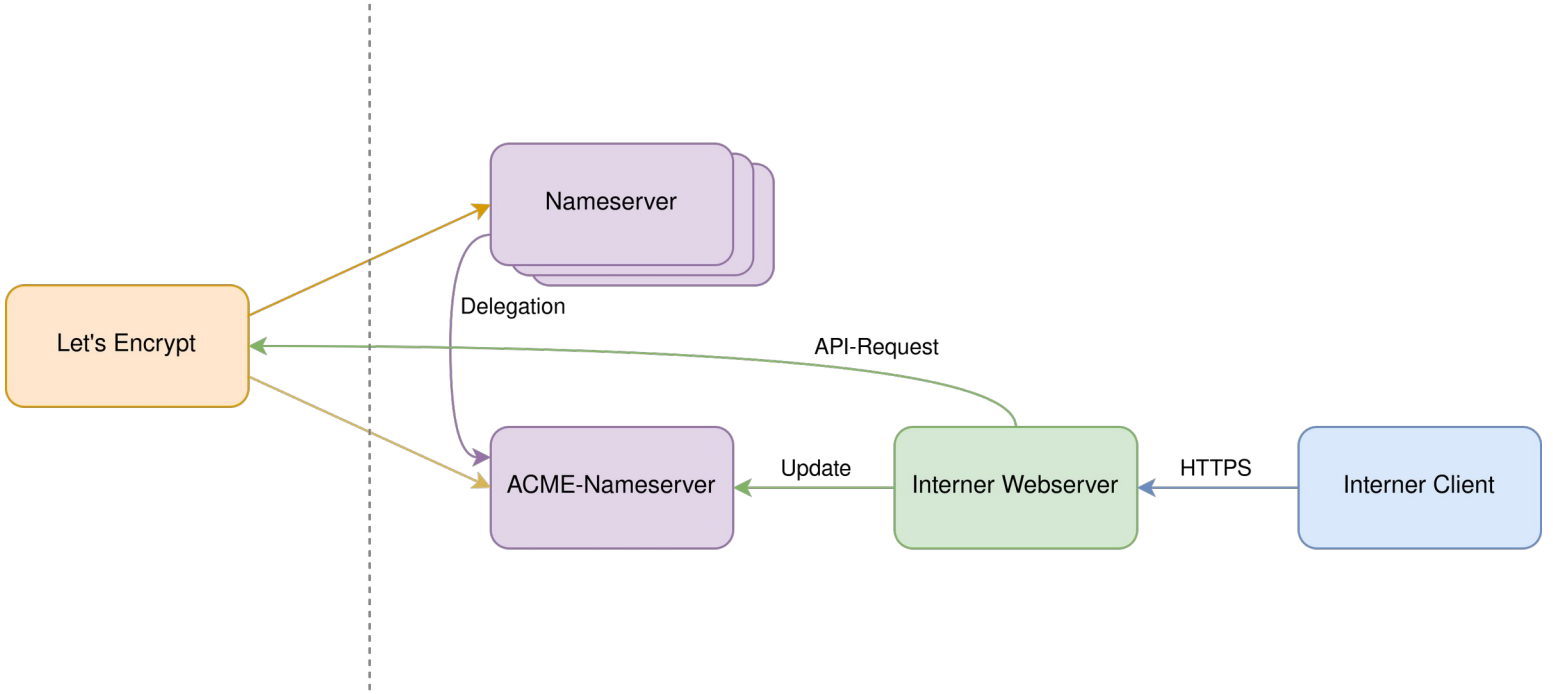
Domain Verification – DNS-01 Challenge

- Der Client sendet Request an Let’s Encrypt und bekommt Challenge
- Der Client erzeugt einen TXT-Eintrag im DNS
- Let’s Encrypt macht eine DNS-Abfrage und überprüft den TXT-Eintrag
- Der Client bekommt das signierte Zertifikat

Domain Verification – DNS-01 Challenge

- Subdomain _acme-challenge.<domain>
- DNS-Delegation möglich (NS-Record)
- Unterstützt Wildcard-Zertifikate (*.<domain>)

DNS-01 Challenge – Beispiel-Setup



Demo