Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
Conférence des directrices et directeurs cantonaux de la santé
Conferenza delle direttrici e dei direttori cantonali della sanità

eHealth Suisse

Sichere Kommunikation im EPD-Vertrauensraum

Authentifizierung und Autorisierung mittels TLS Klasse 2-Zertifikaten

Bern, 3. März 2025

ehealthsuisse
Kompetenz- und Koordinationsstelle von Bund und Kantonen
Centre de compétences et de coordination de la Confédération et des cantons
Centro di competenza e di coordinamento di Confederazione e Cantoni

Impressum

Weitere Informationen und Bezugsquelle: www.e-health-suisse.ch

Zweck und Positionierung dieses Dokuments:
Diese Umsetzungshilfe bietet eine technische Anleitung zur Verwendung von TLS-Zertifikaten der Klasse 2 bei mutual TLS (mTLS)-Handshakes, einschliesslich Authentifizierung, Autorisierung und der Ablage von Zertifikatsinformationen im Community Portal Index (CH:CPI), um sichere Verbindungen zwischen den Endpunkten der (Stamm-)Gemeinschaften zu gewährleisten. Die Zielgruppen sind somit die (Stamm-)Gemeinschaften, deren Mitglieder und ihre technischen Provider.
Die Empfehlungen gelten grundsätzlich auch für an die EPD-Plattformen der (Stamm-)Gemeinschaften angeschlossene Primärsysteme der Leistungserbringer, wobei diese den CH:CPI nicht nutzen. In diesem Dokument liegt der Fokus jedoch nicht auf den Primärsystemen, sondern auf der Kommunikation zwischen den (Stamm-)Gemeinschaften.

Im Interesse einer besseren Lesbarkeit wird auf die konsequente gemeinsame Nennung der männlichen und weiblichen Form verzichtet. Wo nicht anders angegeben, sind immer beide Geschlechter gemeint.

Inhaltsverzeichnis

Zusammenfassung

Zusammenfassung

Das Dokument dient als technische Umsetzungshilfe für die Verwendung von Transport Layer Security (TLS)-Zertifikaten der Klasse 2 mit Identitätsprüfung bei einem mutual TLS (mTLS)-Handshake zur Einrichtung einer sicheren Kommunikationsverbindung zwischen (Stamm-)Gemeinschaften im EPD-Vertrauensraum.

Es beleuchtet die spezifischen Merkmale von Klasse-2-Zertifikaten und ergänzt die allgemeine Beschreibung eines mTLS-Handshakes um detaillierte Informationen zur Authentifizierung und Autorisierung der eingesetzten Zertifikate. Besonderes Augenmerk liegt dabei auf der Ablage der Zertifikatsinformationen im Community Portal Index (CH:CPI).

Die Empfehlungen zur sicheren Kommunikation gelten grundsätzlich auch für an die EPD-Plattform der jeweiligen (Stamm-)Gemeinschaft angeschlossene Primärsysteme, wobei diese den CH:CPI nicht verwenden. Die Umsetzungshilfe legt den Fokus jedoch nicht auf die Primärsysteme, sondern auf die Kommunikation zwischen den (Stamm-)Gemeinschaften.

1 Einleitung

1.1 Ausgangslage

Sichere mTLS-Verbindungen zwischen (Stamm-) Gemeinschaften

Im EPD-Vertrauensraum erfolgt heute die Kommunikation zwischen den (Stamm-) Gemeinschaften über eine gesicherte mutual TLS (mTLS)-Verbindung. Die Zertifikate sowie weitere Informationen zu den (Stamm-) Gemeinschaften werden zentral im Community Portal Index (CH:CPI) (vgl. Art. 33 und 40 EPDV) verwaltet (siehe Abbildung 1). Jede zertifizierte (Stamm-) Gemeinschaft hat Zugang zum CH:CPI und erhält so die notwendigen Informationen über ihre Kommunikationspartner.

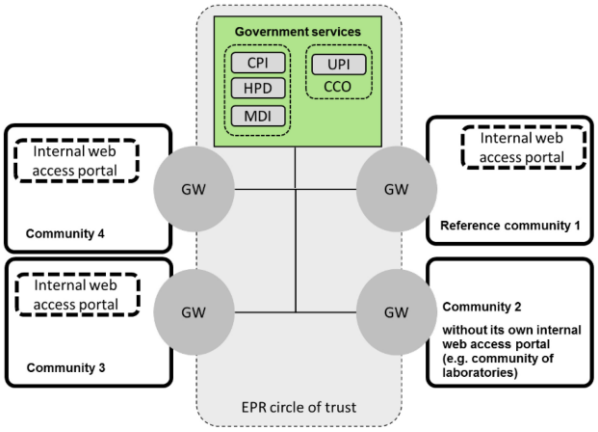

Abbildung 1: Kommunikation zwischen (Stamm-)Gemeinschaften

Jede zertifizierte (Stamm-) Gemeinschaft kommuniziert mit allen zertifizierten (Stamm-) Gemeinschaften. Der CH:CPI dient dabei als Vertrauensanker. Das BAG verwaltet die Informationen im CH:CPI. Die (Stamm-) Gemeinschaften rufen sie regelmässig ab und melden Änderungen dem BAG.

Klasse 2 – Zertifikate von akkreditierten Schweizer CAs

Es werden folgende Anforderungen an die verwendeten Zertifikate gestellt:

1. Es sind nur Zertifikate von in der Schweiz akkreditierten Zertifizierungsstellen (CAs) erlaubt. Das sind:
   - Bundesamt für Informatik und Telekommunikation (BIT)
   - QuoVadis Trustlink
   - Swisscom (Schweiz) AG
   - SwissSign AG
2. Nur TLS-Zertifikate der Zertifikatsklasse 2 oder höher[1] (gem. eCH-0048 PKI-Zertifikatsklassen, Version 2.0 vom 28.11.2018) sind zulässig.

[1] Geregelte (fortgeschrittene) Zertifikate oder EV-Zertifikate sind nicht erforderlich, können jedoch verwendet werden.

1.2 Auftrag und Vorgehen

Die sichere Kommunikation zwischen den Endpunkten der (Stamm-) Gemeinschaften ist essenziell für das reibungslose Funktionieren des EPD.

Es wird untersucht, welche TLS-Zertifikate zum Einsatz kommen und wie diese bei einem mTLS-Handshake für die Authentifizierung und Autorisierung verwendet werden.

Dazu wird auf folgende Punkte genauer eingegangen:

- Was ist ein Klasse-2-Zertifikat? Worauf muss man achten?
- Was muss bei einer gegenseitigen Authentifizierung mittels mTLS-Handshake beachtet werden?
- Welche Varianten gibt es bei der Autorisierung von Zertifikaten beim mTLS-Handshake?
- Welche Informationen zu den TLS-Zertifikaten sollte man im CH:CPI ablegen?

2 Grundlegende Herausforderungen

2.1 TLS-Zertifikate der Zertifikatsklasse 2

TLS-Zertifikate mit NCP und Subjekt-Informationen

TLS-Zertifikate der Zertifikatsklasse 2 garantieren eine Identitätsüberprüfung der Organisation, die das Zertifikat beantragt. Zusätzlich sind diese Zertifikate an eine „*Normalized Certificate Policy*“ (NCP) entsprechend den Anforderungen in „*ETSI EN 319 411-1: Part 1: General requirements*” gebunden, um sicherzustellen, dass das Zertifikat grundlegenden Sicherheitsstandards folgt. Diese NCP ist anhand einer Policy Object Identifier (OID) im Zertifikat erkennbar (siehe Abbildung 2).

```
[1]Certificate Policy:
    Policy Identifier=2.16.756.1.89.2.1.2  = SwissSign certificate policy
    [1,1]Policy Qualifier Info:
        Policy Qualifier Id=CPS
        Qualifier:
            https://repository.swisssign.com/SwissSign_CPS_TLS.pdf
[2]Certificate Policy:
    Policy Identifier=0.4.0.2042.1.7    = organizational-validation-certificate-policy
[3]Certificate Policy:
    Policy Identifier=2.23.140.1.2.2    = subject-identity-validated
```

Abbildung 2: Beispiel einer NCP (OID 0.4.0.2042.1.7) in einem TLS-Zertifikat

Subjekt-Informationen im Zertifikat

Bei den Klasse 2-Zertifikaten muss nach «*ETSI EN 319 411-1: Part 1: General requirements – Chap. 5.42.»* das überprüfte Subjekt im Zertifikat angegeben werden. Im Fall der Machine-to-Machine (M2M)-Kommunikation zwischen (Stamm-) Gemeinschaften handelt es sich um die Angaben der Kommunikations-Endpunkte (Gateways und Server). Ein Beispiel ist in Abbildung 3 angegeben.

```
CN = prod.epd.ch
OU = Community 1
O = Company CH AG
L = Bern
S = Bern
C = CH
```

Abbildung 3: Subjekt-Information im Zertifikat

Die Subjekt-Information enthält:

- den Fully Qualified Domain Name (FQDN) als *Common name (cn).*
- den vollständigen Namen der Organisation (hier der Name der (Stamm-) Gemeinschaft).
- (Optional) eine staatlich anerkannte Identitätsnummer, wie die Unternehmens-Identifikationsnummer (UID) aus dem UID-Register des Bundesamts für Statistik.

subjectAltName contains all FQDNs

Entsprechend den Vorgaben des **CA/Browser Forum** (Certification Authority Browser Forum, siehe Anhang 1) sollte das Feld *common name* (*cn*) im Zertifikat nicht mehr verwendet werden, sondern das Feld *subjectAltName* (siehe Abbildung 4) sollte alle FQDNs einer Gemeinschaft enthalten (die Verwendung von Wildcard * wird dabei unterstützt).

```
DNS Name=prod.epd.ch
DNS Name=prod-01.epd.ch
DNS Name=prod-02.epd.ch
DNS Name=prod-03.epd.ch
```

Abbildung 4: Beispiel subjectAltName

Kurzlebige Zertifikate empfohlen

Heute geht der Trend zu kurzlebigen Zertifikaten, um Sicherheitsrisiken zu minimieren und das Management zu vereinfachen. Durch die regelmässige automatische Erneuerung werden Kompromittierungen schneller behoben und die Abhängigkeit von widerrufsbezogenen Massnahmen verringert. Offen ist die Frage, ob CAs auch kurzlebige Klasse 2-Zertifikate unterstützen.

2.2 Authentifizierung mittels mTLS

Gegenseitige Authentifizierung durch mTLS-Handshake

Zum Aufbau einer gesicherten Kommunikationsverbindung zwischen (Stamm-) Gemeinschaften findet ein mTLS-Handshake statt, bei dem sich die beiden Parteien/Endpunkte gegenseitig authentifizieren. Entsprechend der Kommunikationsrichtung übernimmt dabei eine Partei die Rolle des Servers und die andere die Rolle des Clients.

In Abbildung 5 ist der generelle Ablauf eines mTLS-Handshakes dargestellt.

Zunächst sendet der Server sein Zertifikat an den Client (Schritt 2), der es überprüft (Schritt 3) und die Identität des Servers bestätigt. Dann sendet der Client sein eigenes Zertifikat an den Server (Schritt 4), der dieses ebenfalls überprüft (Schritt 3) und die Identität des Clients bestätigt.

Erst wenn beide Parteien gegenseitig die Identitäten bestätigt und ihre Schlüssel ausgetauscht haben, wird die sichere Verbindung aufgebaut.

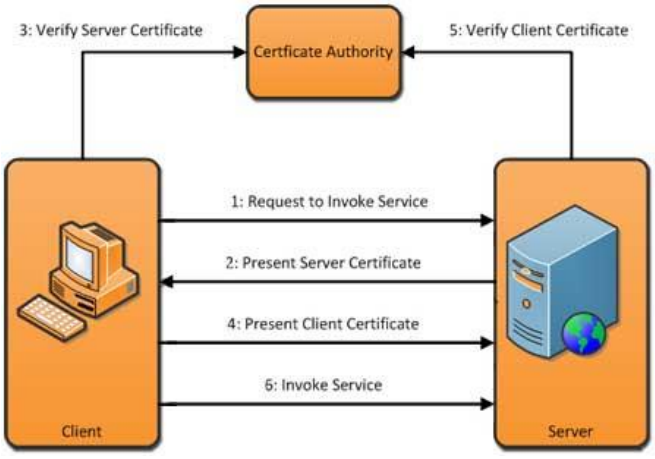

Abbildung 5: Schematischer mTLS-Ablauf

Überprüfung des Server-Zertifikats

Bei der Überprüfung des Server-Zertifikats geht der Client wie folgt vor:

1. Er überprüft, ob das Zertifikat erlaubt ist (siehe Kap. 2.3 Autorisierung).
2. Er überprüft, ob der *hostname* mit den FQDNs aus dem Server-Zertifikat übereinstimmt, um Man-In-Middle-Attacks zu vermeiden. Er verwendet dazu die FQDNs aus dem *subjectAltName* (mit dem Type *DNS Name*) und die Abgleichsregeln aus RFC2459.

Überprüfung des Client-Zertifikats

Bei der Überprüfung des Client-Zertifikats geht der Server wie folgt vor:

1. Er überprüft, ob das Zertifikat erlaubt ist (siehe Kap. 2.3 Autorisierung).
2. (Wenn möglich) Er überprüft, ob der *hostname* mit den FQDNs aus dem Server-Zertifikat übereinstimmt, um Man-In-Middle-Attacks zu vermeiden (wie bei der Überprüfung eines Server-Zertifikats).

Revokationsprüfung ist verpflichtend

Enthalten die Zertifikate Informationen über einen Online Certificate Status Protocol (OCSP)-Endpoint, muss dieser sowohl vom Client wie auch vom Server verwendet werden, um den Revokations-Status der Zertifikate abzufragen. In Abbildung 6 wird beispielhaft die Revokationsprüfung des Server-Zertifikats durch den Client gezeigt. Es sind verschiedene Verfahren möglich, um Latenzzeiten zu verringern und den möglichen Ausfall von Revokationsdiensten zu kompensieren.

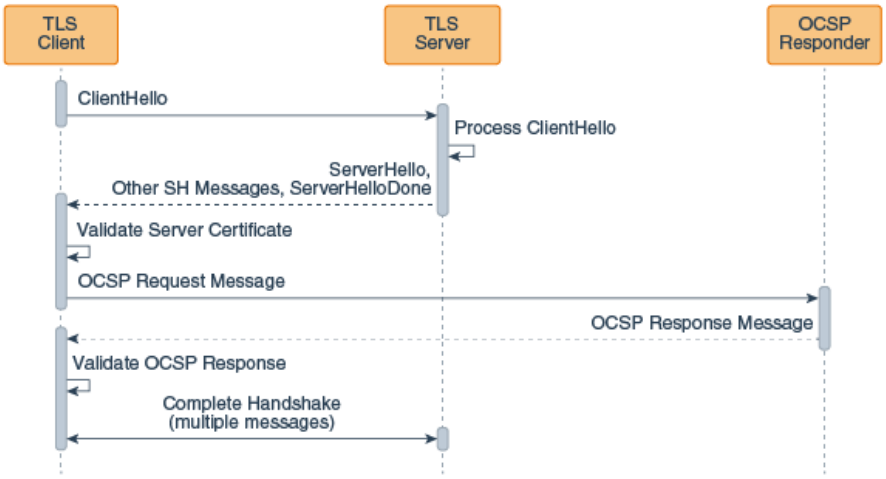

Abbildung 6: Schematische Revokationsprüfung eines Server-Zertifikats durch den Client[2]

2.3 Autorisierung

Nur Zertifikate aus dem CH:CPI sind berechtigt

Gemäss RFC 2818 (HTTP Over TLS, Section 3.1: "…*it is important to narrow the scope of acceptable certificates as much as possible*…") müssen die während des mTLS-Handshakes präsentierten Zertifikate überprüft werden, ob sie berechtigt sind. Die Grundlagen dafür sind die Informationen aus dem CH:CPI.

[2] Quelle: https://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/ocsp.html#client-driven-ocsp-and-certificate-revocation

2-stufige Autorisierung

Die Autorisierung erfolgt in 2 Phasen:

1. **Grobautorisierung**:
   - Nur Zertifikate, die von den oben erwähnten vier in der Schweiz akkreditierten CAs ausgestellt wurden, sind zugelassen.
   - Nur normalisierte TLS-Zertifikate der Zertifikatsklasse 2 mit Identitätsvalidierung (siehe Kap. 2.1) sind zulässig.
2. **Feinautorisierung:** Es sind nur Zertifikate erlaubt, zu denen Informationen im CH:CPI hinterlegt wurden.

Varianten der Feinautorisierung

Es gibt 2 verschiedenen Möglichkeiten, die Zertifikats-Informationen im CH:CPI abzulegen und zu verwenden:

1. **Pflege von Zertifikats-Listen (White-Lists):** Für jeden Endpunkt (Gateway) wird durch das BAG von der zuständigen (Stamm-) Gemeinschaft eine Liste von gültigen Zertifikaten mit Hilfe eines entsprechenden (De-) Registrierungsprozesses gepflegt. Diese Listen müssen regelmässig von den Kommunikationspartnern aus dem CH:CPI ausgelesen werden und beim mTLS-Handshake zum Abgleich des erhaltenen Zertifikats verwendet werden.
2. **Pflege von Organisation:** Anstatt Zertifikats-Listen für einzelne Endpunkte zu pflegen, wird nur eine Liste der autorisierten Organisationen (Gemeinschaften) mit ihren FQDNs geführt. Beim mTLS-Handshake werden die Informationen aus dem *Subject*- und dem *subjectAltName*-Feld des erhaltenen Zertifikats mit den Informationen aus dem CH:CPI abgeglichen. Die aufwändige Pflege von Zertifikats-Listen entfällt.

Aktuell werden im CH:CPI Zertifikats-Listen gepflegt, aber eine Umstellung auf die Pflege von Organisation mit FQDNs wäre vorteilhaft:

- Es müssen deutlich weniger Informationen im CH:CPI gepflegt werden. Aufwändige (De-) Registrierungsprozesse für Zertifikate entfallen.
- Alle Arten von Zertifikaten (Klasse 2 und höher) werden automatisch unterstützt, z.B. auch EV-Zertifikate oder Behördenzertifikate.
- Kurzlebige Zertifikate können unterstützt werden.

Voraussetzung ist, dass alle mTLS-Teilnehmer die Grob- und Feinautorisierung korrekt durchführen und die Organisations- und FQDN-Informationen in den Zertifikaten überprüfen.

3 Empfehlungen

3.1 Sichere M2M-Kommunikation

Für eine sichere Kommunikation im EPD-Vertrauensraum zwischen (Stamm-) Gemeinschaften müssen sich die beiden Parteien/Endpunkte mittels mutual TLS-Handshake gegenseitig authentifizieren.

mTLS ist ein MUSS

Dabei muss der Client das Server-Zertifikat überprüfen und der Server das Client-Zertifikat. Dabei ist eine Prüfung des Inhalts des Zertifikates mit dem CH:CPI eines Abgleichs mit White-Lists zu bevorzugen.

Gegenseitige Zertifikats-Überprüfung

Revokationschecks müssen von beiden Seiten (Client und Server) gemacht werden, wenn die Zertifikate entsprechende Informationen enthalten.

Revokationschecks nicht vernachlässigen

3.2 Anforderungen an Client- und Server-Zertifikate

Der Kreis der verwendeten Zertifikate sollten im Vertrauensraum so weit wie möglich eingeschränkt werden:

Einschränkung der erlaubten Zertifikate

- Es sollten nur vertrauenswürde Schweizer CAs verwendet werden.
- Klasse 2-Zertifikate oder höher beinhalten eine Identitätsprüfung der Organisation und reduzieren die Gefahr von Missbrauch, z. B. durch Angreifer, die gefälschte Zertifikate für Phishing oder Man-in-the-Middle-Angriffe nutzen könnten.
- Durch die Aufzählung von mehreren FQDNs im *subjectAltName* können mehrere Schnittstellen adressiert werden.

Idealerweise werden kurzlebige Zertifikate verwendet und die Rotation von Schlüsseln und Zertifikaten automatisiert. Kurzlebige Zertifikate vereinfachen auch die Revokationsprüfungen.

Kurzlebige Zertifikate bevorzugt

3.3 Zentrale Ablage von Zertifikaten

In einem System wie dem EPD-Vertrauensraum, in dem verschiedene Organisationen über M2M-Kommunikation verbunden sind, ist eine zentrale Instanz wie der CH:CPI erforderlich. Diese verwaltet die zugelassenen Zertifikate der Kommunikationspartner und stellt diese Informationen allen Beteiligten zur Verfügung.

Zentrale Verwaltung

Zertifikatsinformationen können über eine White-List bereitgestellt werden, indem alle Parteien ihre aktuellen Zertifikate regelmässig bei der zentralen Instanz (CH:CPI) registrieren. Die Kommunikationspartner müssen diese Informationen regelmässig abrufen und in ihren Systemen aktualisieren, was für alle Beteiligten einen erheblichen Aufwand bedeutet.

Aufwändige White-List-Verwaltung.

Ein alternativer Ansatz zur Reduzierung des Verwaltungsaufwands ist die Nutzung von Klasse-2-Zertifikaten in Kombination mit einer zentralen Verwaltung der zugelassenen Organisationen. Im Gegensatz zu Zertifikatsinformationen, die sich häufig, bei kurzlebigen Zertifikaten täglich, ändern, bleibt die Anzahl und Art der kooperierenden Organisationen in der Regel relativ stabil.

Abstützung auf Klasse2-Zertifikate und erlaubte Organisationen

4 Anhang 1

4.1 Weitere Informationen

- eCH. (2018). *eCH-0048 PKI-Zertifikatsklassen V2.0*. Verein eCH. https://ech.ch/de/ech/ech-0048/2.0

- Bundesamt für Gesundheit (BAG). (2024). *Nationales Integrationsprofil nach Artikel 5 Absatz 1 Buchstabe c EPDV-EDI*. Verfügbar unter https://www.bag.admin.ch/epdg, Registerkarte «Gesetze»

- ETSI. (2023). *EN 319 411-1:Part 1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*. European Telecommunications Standards Institute. https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.04.01_60/en_31941101v010401p.pdf

- CA/Browser Forum. (2022, April 23). *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* (Version 1.8.4). https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.8.4.pdf
    - Chap. 7.1.4.4 content of SAN and CN
    - Chap. 3.2.2.1 Identity verification