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

Communication sûre dans l’espace de confiance du DEP

Authentification et autorisation au moyen de certificats TLS de classe 2

Berne, le 3 mars 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

© eHealth Suisse, Centre de compétences et de coordination de la Confédération et des cantons

Licence : ce résultat appartient à eHealth Suisse (Centre de compétences et de coordination de la Confédération et des cantons). Le résultat final sera publié via des canaux d'information appropriés sous la licence Creative Commons de type « Attribution - Partage dans les mêmes conditions 4.0 ». Texte de la licence : http://creativecommons.org/licenses/by-sa/4.0

Autres informations et sources : www.e-health-suisse.ch

Objet et positionnement de ce document :
La présente aide à la mise en œuvre fournit des instructions techniques sur l'utilisation des certificats TLS de classe 2 dans les handshake TLS mutuels (mTLS), y compris l'authentification, l'autorisation et le stockage des informations relatives au certificat dans le *Community Portal Index* (CH:CPI), afin de garantir des connexions sécurisées entre les points terminaux des communautés (de référence). Les groupes cibles sont donc les communautés (de référence) et leurs membres ainsi que leurs providers techniques.
Les recommandations s'appliquent également aux systèmes primaires des prestataires de services connectés aux plateformes DEP des communautés (de référence), bien que ces derniers n'utilisent pas le CH:CPI. Toutefois, ce document ne se concentre pas sur les systèmes primaires, mais sur la communication entre les communautés (de référence).

Afin de faciliter la lecture et sauf mention contraire, la forme générique est utilisée pour désigner les deux sexes.

Table des matières

Résumé

Résumé

Le présent document explique comment utiliser des certificats TLS (*Transport Layer Security*) de classe 2, avec vérification d'identité, pour sécuriser la communication entre les communautés (de référence) dans l'espace de confiance DEP, en utilisant le handshake mTLS (*mutual* TLS).

Il met en lumière les caractéristiques spécifiques des certificats de classe 2 et complète la description générale d'un handshake mTLS par des informations détaillées sur l'authentification et l'autorisation des certificats utilisés. Une attention particulière est accordée au stockage des informations relatives aux certificats dans le *Community Portal Index* (CH:CPI).

Les recommandations pour une communication sécurisée s'appliquent également aux systèmes primaires connectés à la plateforme DEP de la communauté (de référence) concernée, même si ces systèmes n'utilisent pas le CH:CPI. Cependant, l'aide à la mise en œuvre ne se concentre pas sur les systèmes primaires, mais sur la communication entre les communautés (de référence).

1 Contexte et but du présent rapport

1.1 Contexte

Connexions mTLS sécurisées entre communautés (de référence)

Dans l'espace de confiance DEP, la communication entre les communautés (de référence) s'effectue aujourd'hui via une connexion TLS mutuelle sécurisée (mTLS). Les certificats et d'autres informations sur les communautés (de référence) sont gérés de manière centralisée dans le *Community Portal Index* (CH:CPI) (cf. art. 33 et 40 ODEP) (voir Figure 1). Chaque communauté (de référence) certifiée a accès au CH:CPI et reçoit ainsi les informations nécessaires sur ses partenaires de communication.

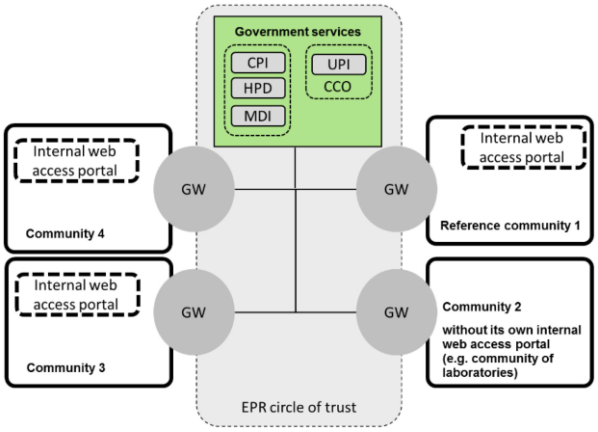

Figure 1 : Communication entre les communautés (de référence)

Chaque communauté (de référence) certifiée communique avec toutes les communautés (de référence) certifiées. Le CH:CPI sert de certificat approuvé. L'OFSP gère les informations dans le CH:CPI. Les communautés (de référence) les consultent régulièrement et signalent les changements à l'OFSP.

Classe 2 – Certificats délivrés par des CA suisses accrédités

Les exigences suivantes s'appliquent aux certificats utilisés :

1. Seuls les certificats délivrés par des autorités de certification (CA) accréditées en Suisse sont autorisés. Il s'agit de :
   - l'Office fédéral de l'informatique et de la télécommunication (OFIT)
   - QuoVadis Trustlink
   - Swisscom (Suisse) SA
   - SwissSign SA
2. Seuls les certificats TLS de classe 2 ou supérieure[1] (selon eCH-0048 Classes de certificats PKI, version 2.0 du 28.11.2018) sont autorisés.

[1] Les certificats réglementés (avancés) ou les certificats EV ne sont pas obligatoires, mais peuvent être utilisés.

1.2 Mission et procédure

Une communication sécurisée entre les points terminaux des communautés (de référence) est essentielle au bon fonctionnement du DEP.

On examine quels certificats TLS sont utilisés, et comment ils le sont, pour l'authentification et l'autorisation lors d'un handshake mTLS.

À cette fin, les points suivants sont examinés plus en détail :

- Qu'est-ce qu'un certificat de classe 2 ? À quoi faut-il prêter attention ?
- À quoi faut-il prêter attention lors d'une authentification mutuelle par handshake mTLS ?
- Quelles sont les variantes d'autorisation de certificats lors d'un handshake mTLS ?
- Quelles informations relatives aux certificats TLS faut-il enregistrer dans le CH:CPI ?

2 Défis principaux

2.1 Certificats TLS de classe 2

Certificats TLS avec NCP et informations sur le sujet

Les certificats TLS de classe 2 garantissent une vérification de l'identité de l'organisation qui demande le certificat. En outre, ces certificats sont liés à une « *Normalized Certificate Policy* » (NCP) conformément aux exigences de la norme « *ETSI EN 319 411-1: Part 1: General requirements* », afin de garantir que le certificat respecte les normes de sécurité fondamentales. Cette NCP est identifiable dans le certificat grâce à un *Policy Object Identifier* (OID) (voir Figure 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
```

Figure 2 : exemple d'une NCP (OID 0.4.0.2042.1.7) dans un certificat TLS

Informations sur le sujet dans le certificat

Pour les certificats de classe 2, le sujet vérifié doit y être indiqué conformément à la norme « *ETSI EN 319 411-1: Part 1: General requirements – Chap. 5.42. »*. Dans le cas de la communication de machine à machine (M2M) entre communautés (de référence), il s'agit des informations des points terminaux de communication (passerelles et serveurs). Un exemple est donné dans la Figure 3.

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

Figure 3: information sur le sujet dans le certificat

L'information sur le sujet contient :

- le Fully Qualified Domain Name (FQDN) en tant que nom commun (*common name (cn)).*
- le nom complet de l'organisation (ici le nom de la communauté (de référence)).
- (facultatif) un numéro d'identification reconnu par l'État, tel que le numéro d'identification des entreprises (IDE) du Registre IDE de l'Office fédéral de la statistique.

subjectAltName contient tous les FQDN

Conformément aux exigences du **CA/Browser Forum** (*Certification Authority Browser Forum*, voir Annexe 1), le champ *common name* (*cn*) ne devrait plus être utilisé dans le certificat, mais le champ *subjectAltName* (voir Figure 4) devrait contenir tous les FQDN d'une communauté (l'utilisation de caractères génériques * y est prise en charge).

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

Figure 4 : exemple subjectAltName

Certificats éphémères recommandés

Aujourd'hui, la tendance est aux certificats éphémères afin de minimiser les risques de sécurité et de simplifier la gestion. Grâce au renouvellement automatique régulier, les compromissions sont corrigées plus rapidement et la dépendance aux mesures liées à la révocation est réduite. Reste à déterminer si les autorités de certification prennent également en charge les certificats éphémères de classe 2.

2.2 Authentification par mTLS

Authentification mutuelle par handshake mTLS

Pour établir une connexion de communication sécurisée entre des communautés (de référence), un handshake mTLS a lieu, au cours duquel les deux parties/points terminaux s'authentifient mutuellement. Selon le sens de la communication, une partie assume le rôle de serveur et l'autre celui de client.

La Figure 5 illustre le déroulement général d'un handshake mTLS.

Le serveur envoie d'abord son certificat au client (étape 2), qui le vérifie (étape 3) et confirme l'identité du serveur. Le client envoie ensuite son propre certificat au serveur (étape 4), qui le vérifie également (étape 3) et confirme l'identité du client.

La connexion sécurisée est établie seulement lorsque les deux parties ont confirmé mutuellement leur identité et échangé leurs clés.

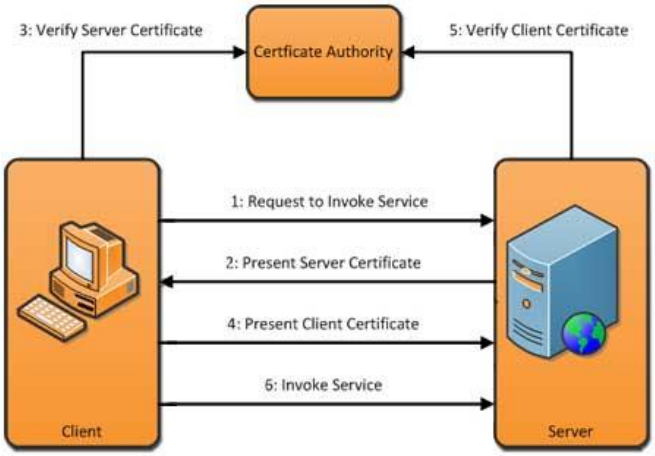

Figure 5: Schéma du processus mTLS

Vérification du certificat du serveur

Lors de la vérification du certificat du serveur, le client procède comme suit :

1. Il vérifie si le certificat est autorisé (voir chap. 2.3 Autorisation).
2. Il vérifie si le *hostname* correspond aux FQDN du certificat du serveur pour éviter les attaques de type « man-in-the-middle ». Pour ce faire, il utilise les FQDN du *subjectAltName* (avec le type *DNS Name*) et les règles de comparaison de la RFC2459.

Vérification du certificat client

Lors de la vérification du certificat client, le serveur procède comme suit :

1. Il vérifie si le certificat est autorisé (voir chap. 2.3 Autorisation).
2. (Si possible) Il vérifie si le *hostname* correspond aux FQDN du certificat du serveur afin d'éviter les attaques de type « man-in-the-middle » (comme lors de la vérification d'un certificat de serveur).

La vérification de la révocation est obligatoire

Si les certificats contiennent des informations sur un point terminal OCSP (*Online Certificate Status Protocol*), celui-ci doit être utilisé tant par le client que par le serveur pour vérifier le statut de révocation des certificats. La Figure 6 illustre un exemple de vérification de la révocation du certificat du serveur par le client. Différentes procédures sont possibles pour réduire les temps de latence et compenser une éventuelle panne des services de révocation.

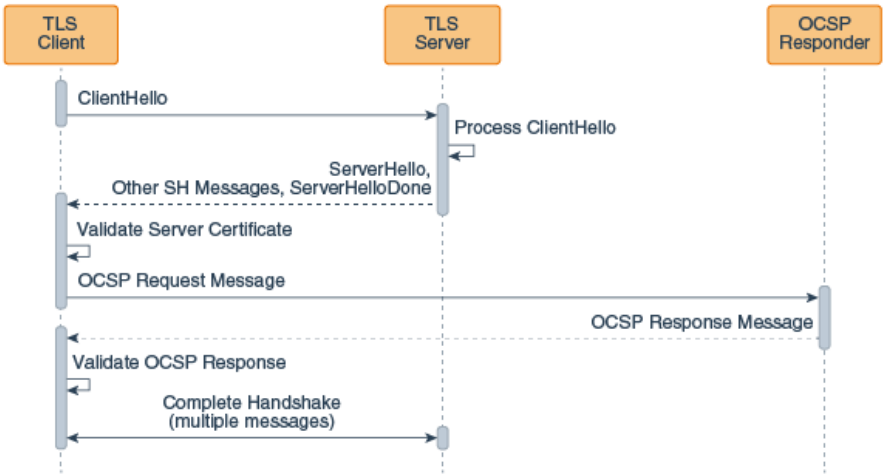

Figure 6: vérification schématique de révocation d'un certificat de serveur par le client[2]

2.3 Autorisation

Seuls les certificats du CH:CPI sont autorisés

Selon la RFC 2818 (HTTP Over TLS, section 3.1: «…*it is important to narrow the scope of acceptable certificates as much as possible*… ») il faut vérifier si les certificats présentés lors du mTLS-handshake sont autorisés. Les informations du CH:CPI servent de base à cette vérification.

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

Autorisation en deux étapes

L’autorisation se déroule en deux étapes :

1. **Autorisation générale** :
    - Seuls les certificats émis par les quatre autorités de certification accréditées en Suisse mentionnées ci-dessus sont autorisés.
    - Seuls les certificats TLS normalisés de classe 2 avec validation de l’identité (voir chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.**) sont autorisés.
2. **Autorisation détaillée :** seuls les certificats pour lesquels des informations ont été enregistrées dans le CH:CPI sont autorisés.

Variantes de l’autorisation détaillée

Il existe deux possibilités différentes pour stocker et utiliser les informations relatives au certificat dans le CH:CPI:

1. **Gestion des listes de certificats (listes blanches) :** pour chaque point terminal (passerelle), l’OFSP gère une liste de certificats valides provenant de la communauté (de référence) compétente, à l’aide d’un processus d’enregistrement et de désenregistrement approprié. Ces listes doivent être lues régulièrement par les partenaires de communication à partir du CH:CPI et utilisées lors du *handshake* mTLS pour comparer le certificat reçu.
2. **Gestion de l’organisation :** au lieu de gérer des listes de certificats pour chaque point terminal, on ne tient qu’une liste des organisations autorisées (communautés) avec leurs FQDN. Lors de la négociation mTLS, les informations des champs *Subject* et *subjectAltName* du certificat reçu sont comparées avec les informations du CH:CPI. La gestion fastidieuse des listes de certificats n’est plus nécessaire.

Actuellement, les listes de certificats sont gérées dans le CH:CPI, mais il serait avantageux de passer à la gestion de l’organisation avec des FQDN :

- Il convient de réduire nettement le nombre d’informations à gérer dans le CH:CPI et de supprimer les processus de (dé)enregistrement fastidieux pour les certificats.
- Tous les types de certificats (classe 2 et supérieures) seront alors automatiquement pris en charge, par exemple les certificats EV ou les certificats d’autorité.
- Les certificats éphémères peuvent être pris en charge.

La condition préalable est que tous les participants mTLS effectuent correctement l’autorisation générale et l’autorisation détaillée et vérifient les informations relatives à l’organisation et au FQDN dans les certificats.

3 Recommandations

3.1 Communication M2M sécurisée

Afin d'assurer une communication sécurisée dans l'espace de confiance DEP entre communautés (de référence), les deux parties/points terminaux doivent s'authentifier mutuellement au moyen d'un handshake TLS.

mTLS est un MUST

Le client doit vérifier le certificat du serveur et le serveur doit vérifier le certificat du client. Il est préférable de vérifier le contenu du certificat avec le CH:CPI ou de le comparer avec des listes blanches.

Vérification mutuelle des certificats

Les contrôles de révocation doivent être effectués par les deux parties (client et serveur) si les certificats contiennent des informations correspondantes.

Ne pas négliger les contrôles de révocation

3.2 Exigences relatives aux certificats client et serveur

Le cercle des certificats utilisés doit être limité autant que possible dans l'espace de confiance :

Limitation des certificats autorisés

- Seules les CA suisses dignes de confiance doivent être utilisées.
- Les certificats de classe 2 ou supérieure comprennent un contrôle d'identité de l'organisation et réduisent le risque d'utilisation abusive, par exemple par des pirates qui pourraient utiliser de faux certificats pour des attaques de phishing ou des attaques de type « man-in-the-middle ».
- En énumérant plusieurs FQDN dans le *subjectAltName*, il est possible d'adresser plusieurs interfaces.

Idéalement, on utilise des certificats éphémères et on automatise la rotation des clés et des certificats. Les certificats éphémères simplifient également les contrôles de révocation.

Préférer les certificats éphémères

3.3 Stockage centralisé des certificats

Dans un système tel que l'espace de confiance DEP, dans lequel différentes organisations sont reliées par communication M2M, une instance centrale telle que le CH:CPI est nécessaire. Celle-ci gère les certificats approuvés des partenaires de communication et met ces informations à la disposition de toutes les parties concernées.

Gestion centralisée

Les informations relatives aux certificats peuvent être mises à disposition via une liste blanche, toutes les parties enregistrant régulièrement leurs certificats actuels auprès de l'instance centrale (CH: CPI). Les partenaires de communication doivent régulièrement consulter ces informations et les mettre à jour dans leurs systèmes, ce qui représente une charge de travail considérable pour toutes les parties concernées.

Gestion complexe de la liste blanche

Une autre approche pour réduire la charge administrative consiste à utiliser des certificats de classe 2 en combinaison avec une gestion centralisée des organisations agréées. Contrairement aux informations sur les certificats, qui changent fréquemment, voire quotidiennement pour les certificats

Base : certificats de classe 2 et organisations autorisées

éphémères, le nombre et le type d’organisations coopérantes restent généralement relativement stables.

4 Annexe 1

4.1 Informations complémentaires

- eCH. (2018). *eCH-0048 Classes de certification PKI V2.0*. Association eCH. https://ech.ch/fr/ech/ech-0048/2.0

- Office fédéral de la santé publique (OFSP). (2024). *Profils d'intégration nationaux selon l'art. 5, al. 1, let. c, ODEP-DFI.* Disponible sous https://www.bag.admin.ch/ldep, rubrique « Législation »

- 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, avril 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