Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral de la santé publique (OFSP)
Division Transformation numérique

Fiche d'information
Certificats TLS dans le contexte du DEP

Date: 8 octobre 2025

Le tableau ci-dessous montre les différents composants du DEP et les exigences applicables aux certificats TLS :

Chiffre CTOC	2.9.26, let. a	2.9.26, let. b	2.9.26, let. c	4.15.3, let. b	4.15.4, let. a		
Composants	Points d'accès intercommunautaires communicants	Points d'accès pour les services de recherche	Points d'accès pour la base de données d'identification de la CdC	Systèmes accédant à un service par Internet	Portails d'accès	Points d'accès Points d'accès de la plateforme DEP auxquels accèdent des systèmes ou portails externes	Autres services Services au sein de la plateforme DEP qui communiquent entre eux
Systèmes et acteurs IHE (liste non exhaustive)	XCA(I) *Initiating* et *Responding Gateways*, *Authorization Decision Consumer* et *Provider*	*Value Set Consumer, Provider Information Consumer, Provider Information Source*	Client UPI via SEDEX	Système primaire ou intermédiaire, système PACS, utilisateur technique	Portail pour les patients, portail pour les professionnels de la santé	P. ex. : *Document Registry* auquel accède le *Document Consumer*	P. ex. : *Document Registry* avec *Document Repository, Secure Node* avec *Audit Repository*
Exigences applicables aux certificats	Loi fédérale du 18 mars 2016 sur la signature électronique (SCSE ; RS *943.03*)			- certificat électronique valable conformément aux dispositions du chapitre 2.3.4 - état de la technique	eCH-0048 classe 2 ou supérieure		Certificats valables uniquement au sein de la communauté

Informations complémentaires :
Office fédéral de la santé publique, Médias et communication, www.ofsp.admin.ch
Cette publication est également disponible en allemand et en italien.

Exigences concernant les certificats SSL/TLS

1 Introduction

L'OFSP reçoit de plus en plus de demandes de précisions concernant les exigences relatives au chiffrement TLS dans le cadre du dossier électronique du patient (DEP). Le présent document décrit les dispositions légales et, sur cette base, fournit des précisions pour les certificats TLS ainsi que pour la configuration TLS sécurisée des systèmes informatiques dans l'espace de confiance du DEP.

Les types de systèmes informatiques suivants font l'objet du présent document :

Systèmes informatiques	**Description**
Systèmes primaires (systèmes d'information des cabinets et des cliniques)	Les systèmes d'information des cabinets et des cliniques sont des systèmes primaires dans lesquels les hôpitaux, les cabinets médicaux, les pharmacies ou les thérapeutes gèrent le dossier médical informatisé interne des patients. Ces dossiers ou documents médicaux informatisés internes constituent la base primaire pour toutes les décisions concernant les traitements. À l'inverse, le dossier électronique du patient est considéré comme un système secondaire servant seulement de source pour d'autres données médicales.
Portails d'accès des communautés (de référence)	Les portails d'accès sont des portails Internet permettant aux patients et aux professionnels de la santé de disposer à tout moment et en tout lieu d'un accès sécurisé à leurs propres données, respectivement aux données des patients. Le portail d'accès pour les patients est mis en place par la communauté de référence des patients. Ces derniers peuvent en outre y gérer les droits d'accès à leur DEP. Le portail d'accès pour les professionnels de la santé est mis à disposition par la communauté ou la communauté de référence.
Plateforme DEP / systèmes internes des communautés (de référence)	Plateforme centrale DEP de la communauté et de ses système internes pour la mise à disposition du DEP.
Services de recherche centraux	Il s'agit de services pour la recherche de données en vertu de l'art. 39 ODEP. Ces services mettent à la disposition des communautés les données de référence nécessaires auxquelles les différents éléments d'infrastructure informatique des communautés peuvent accéder. Ces données sont nécessaires pour la communication entre les communautés. Les services de recherche centraux sont du ressort de l'OFSP.
Éditeurs de moyens d'identification en angl. : *Identity Provider* (IDP)	Instance mettant à disposition des moyens d'identification pour les professionnels de la santé et les patients.
CdC-UPI	Base de données d'identification de la Centrale de compensation de la Confédération (CdC) qui émet des numéros d'identification personnelle spécifiques à certains secteurs pour le DEP.

Informations complémentaires :
Office fédéral de la santé publique, Médias et communication, www.ofsp.admin.ch
Cette publication est également disponible en allemand et en italien.

2 Bases légales

2.1 Loi fédérale sur le dossier électronique du patient (LDEP)[1]

La LDEP décrit notamment l'accès au dossier électronique du patient et définit les critères de certification des communautés et des communautés de référence, des portails d'accès et des éditeurs de moyens d'identification. Le Conseil fédéral fixe les exigences permettant de garantir la protection et la sécurité des données. Il peut habiliter l'Office fédéral de la santé publique (OFSP) à adapter aux progrès techniques les critères en matière de protection et de sécurité des données.

2.2 Ordonnance sur le dossier électronique du patient (ODEP)[2]

Conformément à l'ODEP, les communautés doivent veiller à ce que le procédé de chiffrement utilisé pour l'enregistrement et le transfert des données soit conforme aux progrès techniques. Le Département fédéral de l'intérieur (DFI) fixe les prescriptions techniques et organisationnelles relatives au transfert des données du dossier et peut habiliter l'OFSP à adapter les prescriptions aux progrès techniques (cf. art. 10 ODEP). Il fixe les exigences techniques et organisationnelles applicables à la protection et à la sécurité des données (cf. art. 12 ODEP). En vertu de l'art. 31 ODEP, le DFI peut habiliter l'OFSP à adapter aux progrès techniques les critères de certification des éditeurs de moyens d'identification. Conformément à l'art. 40, al. 1, let. c, ODEP, le service de recherche des communautés et des communautés de référence contient les certificats assurant une authentification sûre par rapport aux autres communautés et communautés de référence.

2.3 Annexe 2[3] de l'ODEP-DFI (CTOC[4])

L'annexe 2 de l'ODEP-DFI contient les exigences en matière de certification à l'égard des communautés et communautés de référence.

2.3.1 Mesures cryptographiques lors de la transmission

Les **communautés** doivent garantir que des mesures cryptographiques adéquates, conformes à l'état actuel de la technique, assurent la confidentialité, l'authenticité et l'intégrité des données du dossier électronique du patient lors de chaque transmission (cf. ch. 2.5, let. a).

2.3.2 Certificats pour la communication entre les communautés et les services centraux

Les **communautés** doivent disposer d'un certificat numérique valable auprès d'un fournisseur de services de certification reconnu selon la SCSE pour l'authentification réciproque (cf. ch. 2.9.26) :

- Points d'accès intercommunautaires
- Points d'accès pour les services de recherche
- Points d'accès pour la base de données d'identification

[1] https://www.fedlex.admin.ch/eli/cc/2017/203/fr
[2] https://www.fedlex.admin.ch/eli/cc/2017/204/fr
[3] https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/oce/2025/56/fr/pdf-a/fedlex-data-admin-ch-eli-oce-2025-56-fr-pdf-a.pdf
[4] Conditions techniques et organisationnelles de certification

Informations complémentaires :
Office fédéral de la santé publique, Médias et communication, www.ofsp.admin.ch
Cette publication est également disponible en allemand et en italien.

2.3.3 Gestion des clés cryptographiques

Les **communautés** doivent garantir une gestion des clés cryptographiques (cf. ch. 4.12). Conformément aux aides à la mise en œuvre des CTOC, il s'agit de générer et distribuer les clés, de gérer les incidents de sécurité, d'appliquer le principe de la ségrégation des tâches, de sauvegarder les clés, de garantir les sauvegardes et de protéger les systèmes contre la compromission.

2.3.4 Certificat client

Les **systèmes** accédant à un service par Internet doivent s'authentifier auprès de celui-ci au moyen du protocole TLS, en utilisant un certificat électronique valable émis par un organe de certification fiable (*Certification Authority*, CA) conformément à l'état de la technique (cf. ch. 4.15.3, let b).

On entend par **« systèmes »** les systèmes qui communiquent depuis l'extérieur avec la plateforme centrale DEP de la communauté. Il s'agit, par exemple, des systèmes primaires ou intermédiaires, des systèmes PACS ou des utilisateurs techniques (TCU). Ces systèmes doivent communiquer de manière sécurisée avec les communautés et le fournisseur d'identité. Les bases légales exigent que tous les systèmes utilisant les services DEP accessibles à partir du réseau Internet public puissent prouver leur identité via l'authentification client TLS. Le protocole TLS avec authentification réciproque (mTLS) permet de garantir que seuls des systèmes légitimes puissent communiquer avec les communautés et les fournisseurs d'identité. Le certificat client n'est pas nécessaire en soi pour établir une connexion chiffrée, mais il garantit que, en complément aux systèmes de serveur des communautés et des fournisseurs d'identité, les systèmes qui s'y connectent s'authentifient également. En ce sens, les communautés et les fournisseurs d'identité doivent s'assurer que, lors de l'authentification client TLS avec le système, le certificat est correctement validé et qu'il a un sujet légitime (p. ex. un cabinet médical enregistré).

2.3.5 Authentification des systèmes appelants

Tous les **services** accessibles à partir d'Internet doivent authentifier le système appelant via *TLS-Client-Authentication* (cf. ch. 4.15.3, let. b, et 4.15.4, let. b).

Le terme de **« services »** se réfère aux services de la plateforme centrale DEP de la communauté, qui sont également appelés points d'accès dans les CTOC. Un point d'accès est par exemple un *Document Registry* central auquel peut accéder un *Document Consumer* du système primaire.

2.3.6 Portails d'accès et points d'accès

Pour les **portails** et les **points d'accès**, il convient d'utiliser des certificats TLS de la classe 2 ou supérieure (selon eCH-0048 Classes de certificat PKI, version 2.0 du 28.11.2018). Pour d'**autres services**, il faut utiliser au moins des certificats TLS de la classe 2 ou supérieure ou des certificats TLS uniquement valables au sein de la communauté (cf. ch. 4.15.4).

Les « **portails d'accès** » se rapportent au portail pour les patients et au portail pour les professionnels de la santé.

On entend par **« points d'accès »** les services de la plateforme DEP auxquels peuvent accéder, au sein de la communauté, des systèmes externes comme les systèmes primaires ou les portails d'accès. Font exception les points d'accès qui servent à la communication avec d'autres communautés ou communautés de référence, étant donné que, comme indiqué plus haut, celles-ci sont soumises à des exigences plus élevées (cf. chapitre 2.3.2).

Le terme **« autres services »** fait référence aux services au sein de la plateforme centrale du DEP qui communiquent entre eux. Citons, à titre d'exemple, l'acteur IHE *Document Registry* de la plateforme, qui communique avec le *Document Repository,* ou les acteurs *Secure Node* et *Audit Repository,* qui communiquent entre eux à l'interne.

3 Exigences applicables aux certificats dans le DEP

Les CTOC recensent quatre catégories de certificats TLS utilisés dans le cadre du DEP.

3.1 SCSE[5]

Pour les points d'accès intercommunautaires et les points d'accès pour les services de recherche et la base de données d'identification UPI, les communautés et les communautés de référence doivent utiliser des certificats au sens de la SCSE. Les éditeurs de certificats visés dans la SCSE doivent être reconnus par le Service d'accréditation suisse. L'objectif est de garantir que les certificats SCSE ne puissent être délivrés que par des institutions fiables qui satisfont aux exigences élevées conformément à la SCSE.

Les fournisseurs de certificats SCSE reconnus par le Service d'accréditation suisse[6], sont les suivants :

- Office fédéral de l'informatique et de la télécommunication (OFIT)
- DigiCert Switzerland SA
- Swisscom (Suisse) SA
- SwissSign AG

3.2 eCH-0048 classe 2 ou supérieure

Pour les portails et les points d'accès internes à la communauté, qui ne servent pas pour la communication intercommunautaire ou la communication avec les services centraux, il convient d'utiliser des certificats de la classe 2 ou supérieure selon la norme eCH-0048. Ces certificats peuvent également être utilisés pour d'autres services au sein de la plateforme centrale du DEP. Ces classes de certificat reposent sur la norme européenne (EN) ETSI EN 319 411 « *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificate*s »[7]. Cette norme exige que les fournisseurs de tels certificats se soumettent au moins tous les deux ans à un audit de conformité. Dans ce contexte, les exigences à l'égard des fournisseurs concernant l'exploitation, le personnel et les processus sont les mêmes que pour les fournisseurs soumis à la SCSE. En outre, lors de la demande de certificat, les personnes physiques doivent présenter une pièce d'identité reconnue au niveau national et, s'agissant des organisations, le pouvoir de représentation doit être justifié, par exemple au moyen d'un extrait du registre du commerce.

Contrairement à ce qui est décrit au prochain chapitre, les systèmes identifient ici la communauté non pas au moyen du certificat individuel, mais en se basant sur la fiabilité de l'éditeur (CA).

3.3 Certificats valables d'organes de certification fiables conformément à l'état de la technique

Les systèmes, par exemple les systèmes primaires ou intermédiaires, accédant aux services de la plateforme centrale du DEP doivent utiliser un certificat client valable en vertu des CTOC, émis par un organe de certification fiable conformément à l'état de la technique. Il doit donc être possible de consulter la validité actuelle du certificat auprès de l'éditeur. Les CTOC ne donnent pas davantage de précisions quant à la manière d'évaluer la fiabilité de l'organe de certification. À cet égard,

[5] https://www.fedlex.admin.ch/eli/cc/2016/752/fr
[6] https://www.sas.admin.ch/dam/sas/de/dokumente/Wer%20ist%20akkreditiert/pki-digitale-signatur.pdf.download.pdf/pki_digitale_signatur_liste_konsolidiert_20210716_link_angepasst.pdf
[7] https://www.etsi.org/standards#page=1&search=319%20411

Informations complémentaires :
Office fédéral de la santé publique, Médias et communication, www.ofsp.admin.ch
Cette publication est également disponible en allemand et en italien.

contrairement aux exigences mentionnées au chapitre 3.1, il ne doit pas nécessairement s'agir d'un fournisseur reconnu au sens de la SCSE ou d'une institution suisse. Il n'est pas non plus précisé quel justificatif d'identité doit être présenté lors de la demande d'un tel certificat. Dans ce contexte, il est tout à fait possible d'utiliser également des certificats à validation de domaine (*Domain Validated*), qui ne requièrent pas le contrôle de l'identité du requérant sur la base d'informations personnelles. Étant donné que, pour le moment, les communautés (de référence) doivent intégrer manuellement les certificats client des systèmes primaires, etc. dans leur plateforme DEP locale, la validation de l'organisation (*Organization Validation*) a lieu dans un second temps. Dans ce contexte, les certificats ainsi que les URL et les OID des systèmes au sein de la communauté sont enregistrés lors du processus d'onboarding. À chaque accès, la communauté identifie le système au moyen du certificat déposé, de l'URL ainsi que de l'OID. Le chapitre 4 aborde de manière approfondie l'état de la technique.

3.4 Certificats valables internes à la communauté

Pour d'autres services au sein de la plateforme centrale du DEP, il est possible d'utiliser soit des certificats selon la norme eCH-0048 classe 2 ou supérieure, soit des certificats qui ne sont valables qu'au sein de la communauté. Concernant ces derniers, il s'agit de certificats auto-signés. Bien que les CTOC ne formulent pas d'exigences plus précises, il va de soi que ces certificats doivent également être conformes à l'état de la technique et valables au moment de leur utilisation. En outre, il est fortement recommandé d'exploiter une infrastructure qui gère les certificats, comme la génération et le renouvellement de clés, et qui permet aux services de consulter la validité des certificats.

4 État de la technique

Étant donné que les bases légales concernant le DEP renvoient souvent à l'état de la technique, ce chapitre en résume les principaux éléments.

4.1 Gestion des clés cryptographiques

Pour la gestion des clés cryptographiques, il existe différentes normes et bonnes pratiques, en particulier NIST SP 800-57 et ISO/IEC 11770 ainsi que TR-02102-1 « *Technische Richtlinie Kryptographische Verfahren* »[8].

Durant l'ensemble de leur cycle de vie, les clés cryptographiques doivent être protégées de manière appropriée. Les principales phases du cycle de vie des clés sont la génération, l'activation, l'utilisation, le renouvellement, la révocation, l'archivage et la suppression.

Les principales exigences de sécurité pour la gestion des clés cryptographiques sont résumées dans le tableau ci-dessous.

8 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf;jsessionid=169A07F72938E162608F698F08B11E65.internet081?__blob=publicationFile&v=2

Informations complémentaires :
Office fédéral de la santé publique, Médias et communication, www.ofsp.admin.ch
Cette publication est également disponible en allemand et en italien.

Phase	Principales exigences de sécurité
Génération des clés	Les clés doivent être générées par le système informatique où elles seront utilisées. Les clés doivent être créées avec les paramètres cryptographiques sécurisés correspondants (cf. chapitre 3.3). Si les clés doivent être copiées et distribuées, il convient de garantir en tout temps leur confidentialité au moment de la transmission (p. ex. cryptage). Utilisation de bibliothèques standards permettant notamment une entropie suffisante pour générer une clé.
Activation des clés	Avant son activation, la clé doit être protégée au moins dans la même mesure que lors de son utilisation.
Utilisation des clés	Les clés doivent être sauvegardées avec un accès protégé et ne doivent être utilisées que par des personnes autorisées ou des processus informatiques aux fins des objectifs légitimes. Aucune utilisation simultanée de clés pour l'authentification, le cryptage et la signature numérique.
Renouvellement des clés	Les clés doivent être renouvelées périodiquement. Autrement dit : pas de nouveau certificat sur la base de clés existantes d'un ancien certificat.
Révocation des clés	Si une clé n'est plus nécessaire ou a été potentiellement compromise (p. ex. après une attaque informatique), elle devrait être révoquée, par exemple, au moyen d'une révocation du certificat.
Archivage des clés	Non pertinent dans le contexte de l'authentification.
Suppression des clés	Si une clé n'est plus nécessaire, il convient de l'effacer de façon sécurisée, en la supprimant notamment des supports de sauvegarde.

4.2 Certificats TLS

L'Office fédéral de la cybersécurité (OFCS) renvoie à des prescriptions de la Confédération qui ne sont toutefois applicables qu'aux systèmes informatiques de la Confédération. S'agissant des meilleures pratiques, la Confédération se réfère aux directives techniques correspondantes de l'office fédéral allemand de la sécurité des technologies et de l'information (*Bundesamt für Sicherheit in der Informationstechnik*, BSI).

La confiance dans les certificats repose sur les processus mis en place par un organe de certification avant l'émission d'un certificat. Les processus correspondants sont documentés dans une *Certificate Policy* (CP) et un *Certificate Practice Statement* (CPS). Le RFC 3647 « *Internet X.509 Public Key*

Infrastructure Certificate Policy and Certification Practices Framework »[9] documente notamment les éléments suivants devant faire l'objet d'une CP et d'un CPS.

- Procédure visant à authentifier le requérant du certificat avant l'émission du certificat
- Exigences pour l'organe de certification et le détenteur du certificat dans le cadre du cycle de vie du certificat
- Mesures organisationnelles et techniques de l'organe de certification (génération des clés, authentification du sujet, émission du certificat, révocation du certificat, audit et archivage)

Conformément au chapitre 8.2.2.2 de la directive technique **BSI TR-02103**[10], les certificats auto-signés ne garantissent aucunement leur intégrité étant donné qu'ils ne sont pas signés par une clé privée d'un organe de certification (CA) auquel on fait implicitement confiance. En outre, le nombre de CA fiables devrait être réduit au maximum.

Par ailleurs, les certificats auto-signés présentent fondamentalement les inconvénients suivants :

- Aucune relation de confiance implicite ne peut être établie sur la base d'une chaîne de confiance, et il faut accorder la confiance à chaque certificat séparément.
- Il n'existe aucun mécanisme permettant d'informer automatiquement les partenaires de la révocation d'un certificat.
- Il est plus compliqué de contrôler l'utilisation de clés cryptographiques « faibles » (p. ex. paramètres faibles connus).
- Il est difficile de suivre l'arrivée à échéance des certificats.

Lors du contrôle d'un certificat client ou serveur, il faut vérifier au moins les éléments suivants :

- Le certificat est émis par un organe de certification fiable.
- Le certificat est valable, c'est-à-dire non échu et non révoqué.
- Un certificat serveur a été émis pour le nom de domaine du service appelant.
- Un certificat client a été émis pour un sujet connu.

4.3 Configurations TLS

La directive technique du BSI TR-02102-2 « *Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)* »[11] recommande uniquement d'utiliser les versions du protocole TLS 1.2[12] et TLS 1.3[13]. Il est recommandé d'utiliser *TLS cipher suites* avec l'option « *perfect forward secrecy* » (PFS). La PFS empêche de déchiffrer a posteriori une communication, même si la clé de longue durée des partenaires est connue. Lorsque TLS est utilisé pour protéger les données personnelles, le BSI recommande les *cipher suites*, qui garantissent la PFS.

[9] https://datatracker.ietf.org/doc/html/rfc3647
[10] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02103/BSI-TR-02103.pdf;jsessionid=8F290B97DFB9A596CBA5FBC9536EC04A.internet462?__blob=publicationFile&v=2
[11] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html
[12] https://datatracker.ietf.org/doc/html/rfc5246
[13] https://datatracker.ietf.org/doc/html/rfc8446

Informations complémentaires :
Office fédéral de la santé publique, Médias et communication, www.ofsp.admin.ch
Cette publication est également disponible en allemand et en italien.