Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'interno DFI
Ufficio federale della sanità pubblica UFSP
Divisione Trasformazione digitale

Scheda informativa
Certificati TLS nel contesto della CIP

Data: 08.10.2025

La tabella seguente mostra i diversi componenti della CIP e i requisiti applicabili ai certificati TLS.

Numero CTO	2.9.26 lett. a	2.9.26 lett. b	2.9.26 lett. c	4.15.3 lett. b	4.15.4 lett. a		
Componenti	Punti d'accesso che comunicano a livello intercomunitario	Punti d'accesso nei confronti dei servizi di ricerca di dati	Punti d'accesso nei confronti della banca dati d'identificazione dell'UCC	Sistemi che accedono a un servizio attraverso Internet	Portali d'accesso	Punti d'accesso Punti d'accesso della piattaforma CIP utilizzati da sistemi o portali esterni	Altri servizi Servizi all'interno della piattaforma CIP che comunicano tra loro.
Sistemi e attori IHE (elenco non esaustivo)	XCA(I) Initiating and Responding Gateways, Authorization Decision Consumer and Provider	Value Set Consumer, Provider Information Consumer, Provider Information Source	UPI Client via Sedex	Sistema primario, intermediario, sistema PACS, utente tecnico	Portale per i pazienti, portale per i professionisti della salute	Ad es. Document Registry cui accede il Document Consumer	Ad es. Document Registry con Document Repository, Secure Node con Audit Repository
Requisiti per i certificati	Legge federale del 18 marzo 2016 sulla firma elettronica (FiEle; RS 943.03)			- Certificato elettronico valido secondo le disposizioni del cap. 2.3.4 - Stato della tecnica	Standard eCH-0048, classe 2 o superiore		Certificati validi solo all'interno della comunità

Per maggiori informazioni:
Ufficio federale della sanità pubblica, Comunicazione, www.ufsp.admin.ch
La presente pubblicazione è disponibile anche in tedesco e in francese.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'interno DFI
Ufficio federale della sanità pubblica UFSP
Divisione Trasformazione digitale

Requisiti SSL/TLS

1 Introduzione

L'UFSP riceve un numero crescente di richieste di chiarimento sui requisiti relativi alla crittografia TLS nel contesto della cartella informatizzata del paziente (CIP). Il presente documento illustra il quadro legale e, su questa base, fornisce precisazioni sui certificati TLS e sulla configurazione TLS sicura dei sistemi informatici nell'area riservata della CIP.

Sono oggetto del presente documento le tipologie di sistemi informatici di seguito descritte.

Tipologie di sistemi informatici	**Descrizione**
Sistemi primari (sistemi informatici degli studi medici e delle cliniche)	Sistemi d'informazione delle cliniche e degli studi medici in cui sono tenute le cartelle cliniche elettroniche interne di un ospedale, di uno studio medico, di una farmacia o di un terapeuta. Le cartelle cliniche elettroniche interne costituiscono la base primaria per tutte le decisioni terapeutiche. La cartella informatizzata del paziente è invece considerata un sistema secondario, che serve soltanto come fonte per altri dati medici.
Portali d'accesso delle comunità o delle comunità di riferimento	Portali Internet che consentono ai pazienti e ai professionisti della salute di accedere in modo sicuro rispettivamente ai propri dati e a quelli dei pazienti, indipendentemente dal luogo e dal momento. Il portale d'accesso per i pazienti è messo a disposizione dalla comunità di riferimento del paziente e gli permette tra l'altro di gestire i diritti d'accesso alla sua CIP. Il portale d'accesso per i professionisti della salute è messo a disposizione dalla comunità o dalla comunità di riferimento.
Piattaforma CIP / sistemi interni delle comunità e delle comunità di riferimento	Piattaforma CIP centralizzata della comunità e dei suoi sistemi interni per la messa a disposizione della CIP.
Servizi centralizzati di ricerca di dati	Servizi di ricerca di dati secondo l'articolo 39 dell'ordinanza sulla cartella informatizzata del paziente (OCIP; RS 816.11). Questi servizi mettono a disposizione delle comunità i dati di riferimento necessari, cui possono accedere i singoli elementi dell'infrastruttura IT di ciascuna comunità. I dati di riferimento sono necessari per la comunicazione tra le comunità. I servizi centralizzati di ricerca di dati sono di competenza dell'UFSP.
Emittente di strumenti d'identificazione (inglese: Identity Provider, IDP)	Organismo che rilascia strumenti d'identificazione a professionisti della salute e pazienti.
UCC-UPI	Banca dati d'identificazione dell'Ufficio centrale di compensazione della Confederazione (UCC), che rilascia numeri d'identificazione personale a livello di settore per la CIP.

Per maggiori informazioni:
Ufficio federale della sanità pubblica, Comunicazione, www.ufsp.admin.ch
La presente pubblicazione è disponibile anche in tedesco e in francese.

2 Basi legali

2.1 Legge federale sulla cartella informatizzata del paziente (LCIP)[1]

La LCIP descrive, tra l'altro, le modalità di accesso alla cartella informatizzata del paziente. Definisce i requisiti per la certificazione delle comunità, delle comunità di riferimento, dei portali d'accesso e degli emittenti di strumenti d'identificazione. Il Consiglio federale stabilisce come devono essere garantite la protezione e la sicurezza dei dati. L'Ufficio federale della sanità pubblica (UFSP) può essere autorizzato ad adeguare all'evoluzione della tecnica i requisiti di protezione e sicurezza dei dati.

2.2 Ordinanza sulla cartella informatizzata del paziente (OCIP)[2]

Secondo l'OCIP, le comunità devono garantire che per la memorizzazione e il trasferimento dei dati vengano utilizzati metodi di criptaggio secondo l'attuale stato della tecnica. Il Dipartimento federale dell'interno (DFI) stabilisce le prescrizioni tecniche e organizzative per la conservazione e la trasmissione dei dati e può autorizzare l'UFSP ad adeguare le prescrizioni allo stato della tecnica (cfr. art. 10 OCIP). Il DFI stabilisce i requisiti tecnici e organizzativi in materia di protezione e sicurezza dei dati (cfr. art. 12 OCIP). Sulla base dell'articolo 31 OCIP, il DFI può autorizzare l'UFSP ad adeguare allo stato della tecnica le prescrizioni per la certificazione degli emittenti di strumenti d'identificazione. Secondo l'articolo 40 OCIP, il servizio di ricerca di dati delle comunità e comunità di riferimento contiene i certificati per un'autenticazione sicura rispetto ad altre comunità e comunità di riferimento.

2.3 Allegato 2[3] (CTO)[4] dell'ordinanza del DFI sulla cartella informatizzata del paziente (OCIP-DFI)

L'allegato 2 OCIP-DFI contiene i requisiti per la certificazione delle comunità e delle comunità di riferimento.

2.3.1 Misure di criptaggio durante la trasmissione

Le **comunità** devono adottare misure di criptaggio adeguate e conformi allo stato attuale della tecnica affinché i dati della cartella informatizzata del paziente siano protetti dalla perdita di riservatezza, autenticità e integrità durante ogni trasmissione (cfr. n. 2.5 lett. a).

2.3.2 Certificati per la comunicazione tra le comunità e i servizi centrali

Le **comunità** devono essere in possesso di un certificato elettronico valido, rilasciato da un prestatore di servizi di certificazione riconosciuto secondo la legge sulla firma elettronica (FiEle; RS 943.03) per l'autenticazione reciproca di (cfr. n. 2.9.26):

- punti d'accesso a livello intercomunitario;
- punti d'accesso con i servizi di ricerca di dati;
- punti d'accesso con la banca dati d'identificazione.

[1]https://www.fedlex.admin.ch/eli/cc/2017/203/it
[2]https://www.fedlex.admin.ch/eli/cc/2017/204/it
[3]https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/oce/2023/50/it/pdf-a/fedlex-data-admin-ch-eli-oce-2023-50-it-pdf-a-1.pdf
[4]Condizioni tecniche e organizzative di certificazione

2.3.3 Gestione delle chiavi crittografiche

Le **comunità** devono garantire una gestione delle chiavi crittografiche (cfr. n. 4.12). Secondo l'ausilio per l'attuazione delle CTO, tale gestione comprende la generazione e la distribuzione di chiavi, la gestione di incidenti di sicurezza, il principio di separazione dei compiti, la memorizzazione di chiavi, i backup e la protezione da compromissioni.

2.3.4 Certificati client

I **sistemi** che accedono a un servizio attraverso Internet devono autenticarsi nei suoi confronti mediante sicurezza a livello di trasporto (TLS) con un certificato elettronico valido di un'autorità di certificazione affidabile (Certification Authority, CA) secondo lo stato della tecnica (cfr. n. 4.15.3 lett. b).

Con il termine **«sistemi»** si intendono sistemi che comunicano dall'esterno con la piattaforma CIP centralizzata della comunità. Si tratta, ad esempio, di sistemi primari, intermediari, sistemi PACS o utenti tecnici (technical user, TCU). Tali sistemi devono comunicare in modo sicuro con le comunità e con l'emittente di strumenti d'identificazione. Secondo le basi legali, tutti i sistemi che utilizzano servizi della CIP offerti attraverso l'Internet pubblico devono comprovare la propria identità mediante l'autenticazione client TLS. Il protocollo TLS con autenticazione reciproca (mTLS) garantisce che solo i sistemi legittimi possano comunicare con le comunità e con gli emittenti di strumenti d'identificazione. Il certificato client non è di per sé necessario per stabilire un collegamento criptato, ma garantisce che, oltre ai sistemi server delle comunità e degli emittenti di strumenti d'identificazione, anche i sistemi ad essi collegati si autentichino correttamente. Di conseguenza, le comunità e gli emittenti di strumenti d'identificazione devono garantire da un lato che i certificati siano validati correttamente e dall'altro che un soggetto legittimo (ad es. uno studio medico registrato) esegua l'autenticazione client TLS con il proprio sistema.

2.3.5 Autenticazione di sistemi richiedenti

Tutti i sistemi ai quali è possibile collegarsi attraverso Internet devono autenticare il sistema richiedente mediante l'autenticazione client TLS (cfr. n. 4.15.3 lett. b e n. 4.15.4 lett. b).

Il termine **«servizi»** si riferisce ai servizi della piattaforma CIP centralizzata della comunità, denominati anche punti d'accesso nelle CTO. Un punto d'accesso è, ad esempio, un Document Registry centralizzato cui accede un Document Consumer di un sistema primario.

2.3.6 Portali d'accesso e punti d'accesso

Per i **portali d'accesso** e i **punti d'accesso** si utilizzano certificati TLS della classe 2 o superiore (secondo le classi di certificato PKI eCH-0048, versione 2.0 del 28 novembre 2018), per **altri servizi** certificati TLS almeno della classe 2 o certificati TLS validi solo all'interno della comunità (cfr. n. 4.15.4).

Con **«portali d'accesso»** s'intendono il portale d'accesso per i pazienti e quello per i professionisti della salute.

I **«punti d'accesso»**, invece, costituiscono i servizi della piattaforma CIP che, all'interno della comunità, sono utilizzati da sistemi esterni, come i sistemi primari, o da portali d'accesso. Sono esclusi i punti d'accesso destinati alla comunicazione con altre comunità o con la comunità di riferimento, poiché per questi ultimi, come menzionato sopra, vigono requisiti più restrittivi (cfr. cap. 2.3.2).

Infine, l'espressione **«altri servizi»** è riferita ai servizi che comunicano tra loro all'interno della piattaforma CIP centralizzata. Si pensi ad esempio all'attore IHE Document Registry della piattaforma che comunica con il Document Repository o agli attori Secure Note e Audit Repository che comunicano tra loro internamente.

3 Requisiti per i certificati nel contesto della CIP

Nelle CTO sono descritte quattro diverse categorie di certificati TLS.

3.1 Legge sulla firma elettronica (FiEle)[5]

Per i punti d'accesso intercomunitari e per i punti d'accesso ai servizi di ricerca di dati e alla banca dati d'identificazione UPI, le comunità e le comunità di riferimento devono utilizzare certificati conformi alla FiEle. Gli emittenti di certificati secondo la FiEle devono essere riconosciuti dal Servizio di accreditamento svizzero. Ciò consente di garantire che i certificati possano essere rilasciati soltanto da istituzioni affidabili che soddisfano i severi requisiti previsti dalla FiEle.

Secondo il Servizio di accreditamento svizzero, gli emittenti riconosciuti di certificati conformi alla FiEle sono i seguenti[6]:

- Ufficio federale dell'informatica e della telecomunicazione (UFIT)
- DigiCert Switzerland SA
- Swisscom (Svizzera) SA
- SwissSign AG

3.2 Standard eCH-0048 della classe 2 o superiore

Per i portali d'accesso interni alla comunità e per i punti d'accesso non utilizzati per la comunicazione tra comunità o con i servizi centrali sono richiesti certificati della classe 2 o superiore conformi allo standard eCH-0048. Questi certificati possono essere utilizzati anche per altri servizi all'interno della piattaforma CIP centralizzata. Lo standard si basa sulla norma europea ETSI EN 319 411 «Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates»[7], ai sensi della quale gli emittenti di tali certificati devono sottoporsi a un audit di conformità almeno ogni due anni. I requisiti per l'emittente in termini di gestione, personale e processi sono dello stesso livello di quelli previsti per i prestatori secondo la FiEle. Inoltre, al momento della richiesta di un certificato, occorre presentare per le persone fisiche un documento d'identità riconosciuto a livello nazionale e per le organizzazioni una prova del potere di rappresentanza (ad es. estratto del registro di commercio).

Contrariamente a quanto esposto nel seguente capitolo, in questo caso i sistemi identificano la comunità non in base al certificato individuale, ma in base all'affidabilità dell'emittente (Certification Authority, CA).

3.3 Certificati validi di autorità di certificazione affidabili secondo lo stato della tecnica

Secondo le CTO, i sistemi come i sistemi primari o gli intermediari che accedono ai servizi della piattaforma CIP centralizzata devono utilizzare un certificato client valido, rilasciato da un'autorità di certificazione affidabile secondo lo stato della tecnica. Ciò presuppone la possibilità di verificare la validità corrente del certificato presso l'emittente. Le CTO non specificano la procedura da seguire per valutare l'affidabilità dell'autorità di certificazione. A differenza di quanto indicato nel capitolo 3.1, non deve trattarsi di un fornitore riconosciuto secondo la FiEle né di un'istituzione svizzera. Le CTO non precisano nemmeno il documento d'identificazione da presentare al momento della richiesta di tale certificato. Si possono quindi utilizzare anche certificati «Domain Validated», per i quali l'identità del richiedente non viene verificata mediante informazioni personali. Dato che le comunità (di riferimento)

[5] https://www.fedlex.admin.ch/eli/cc/2016/752/it
[6] https://www.sas.admin.ch/dam/sas/it/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

devono comunque integrare manualmente i certificati client dei sistemi primari ecc. nella piattaforma CIP centralizzata, durante tale processo viene già effettuata una sorta di «Organization Validation»: durante il processo di onboarding vengono così registrati i certificati, l'URL e l'OID dei sistemi primari all'interno della comunità. A ogni accesso, la comunità identifica il sistema basandosi sul certificato registrato, sull'URL e sull'OID. Per maggiori informazioni sullo stato della tecnica si rimanda al capitolo 4.

3.4 Certificati validi all'interno della comunità

Per altri servizi all'interno della piattaforma CIP centralizzata si possono utilizzare certificati conformi allo standard eCH-0048 della classe 2 o superiore, oppure certificati validi solo all'interno della comunità. In quest'ultimo caso si tratta di cosiddetti certificati autofirmati. Sebbene le CTO non definiscano requisiti dettagliati per tali certificati, è implicito che debbano essere emessi in conformità allo stato della tecnica ed essere validi al momento del loro utilizzo. È inoltre fortemente raccomandato disporre di un'infrastruttura in grado di gestire i certificati, in particolare per quanto riguarda la generazione e il rinnovo delle chiavi, e che consenta ai servizi di verificare la validità dei certificati.

4 Stato della tecnica

Poiché le basi legali della CIP fanno spesso riferimento allo stato della tecnica, in questo capitolo se ne presenta una sintesi.

4.1 Gestione delle chiavi crittografiche

Per la gestione delle chiavi crittografiche esistono diversi standard e buone prassi, tra cui gli standard NIST SP 800-57 e ISO/IEC 11770 nonché la direttiva tecnica TR-02102-1 «Technische Richtlinie Kryptographische Verfahren»[8].

Le chiavi crittografiche devono essere adeguatamente protette durante l'intero ciclo di vita. Le principali fasi del ciclo di vita sono: generazione, attivazione, utilizzo, rinnovo, disattivazione, archiviazione e cancellazione della chiave.

I principali requisiti di sicurezza per la gestione delle chiavi crittografiche sono riepilogati nella tabella seguente.

Fase	**Principali requisiti di sicurezza**
Generazione della chiave	Le chiavi devono essere generate nel sistema informatico in cui verranno utilizzate. Le chiavi devono essere generate con parametri crittografici appropriati e sicuri (cfr. cap. 3.3).

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

	In caso di copia o distribuzione delle chiavi, durante il trasferimento deve sempre essere garantita la riservatezza (ad es. mediante criptaggio). È raccomandato l'uso di librerie standard che garantiscano tra l'altro un'adeguata entropia nella generazione delle chiavi.
Attivazione della chiave	Prima dell'attivazione, la chiave dovrebbe beneficiare di una protezione almeno equivalente a quella prevista per il suo utilizzo.
Utilizzo della chiave	Le chiavi devono essere conservate con misure di sicurezza che ne impediscano l'accesso non autorizzato ed essere utilizzate soltanto da persone o processi informatici legittimi per lo scopo consentito. Non è consentito l'uso simultaneo delle chiavi per l'autenticazione, il criptaggio e la firma digitale.
Rinnovo della chiave	Le chiavi devono essere sostituite a intervalli regolari. Non è consentito generare un nuovo certificato basato sul materiale chiave di un certificato precedente.
Disattivazione della chiave	Se una chiave non è più necessaria o è potenzialmente compromessa (ad es. a seguito di un attacco informatico), dovrebbe essere disattivata, ad esempio mediante la revoca del certificato.
Archiviazione della chiave	Non rilevante nel contesto dell'autenticazione.
Cancellazione della chiave	Una chiave non più necessaria deve essere eliminata in modo sicuro, inclusi eventuali backup.

4.2 Certificati TLS

L'Ufficio federale della cibersicurezza (UFCS) rimanda alle prescrizioni della Confederazione, le quali tuttavia si applicano soltanto ai sistemi TIC della Confederazione. Per le buone prassi, la Confederazione rimanda all'Ufficio federale tedesco per la sicurezza informatica (Bundesamt für Sicherheit in der Informationstechnik, BSI) e alle corrispondenti direttive tecniche.

L'affidabilità dei certificati è garantita dai processi che un'autorità di certificazione esegue prima di emettere un certificato. Tali processi sono documentati in una Certificate Policy (CP) e in un Certificate Practice Statement (CPS). L'RFC 3647 «Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework»[9] documenta, tra l'altro, i seguenti aspetti che dovrebbero essere trattati in una CP e in un CPS:

- procedura per l'autenticazione del soggetto richiedente prima dell'emissione del certificato;
- requisiti per l'autorità di certificazione e per i titolari dei certificati nell'ambito del ciclo di vita dei certificati;

[9] https://datatracker.ietf.org/doc/html/rfc3647

- misure organizzative e tecniche dell'autorità di certificazione (generazione delle chiavi, autenticazione dei soggetti, emissione dei certificati, revoca dei certificati, audit e archiviazione).

Secondo il capitolo 8.2.2.2 della direttiva tecnica TR-02103 del BSI[10], i certificati autofirmati non offrono alcuna protezione dell'integrità, dato che non sono firmati mediante una chiave privata di un'autorità di certificazione considerata implicitamente affidabile. Inoltre, il numero delle autorità di certificazione considerate affidabili dovrebbe essere mantenuto il più basso possibile.

In genere, i certificati autofirmati presentano altri svantaggi:

- non è possibile stabilire un rapporto di fiducia implicita attraverso una catena di fiducia; la fiducia dev'essere concessa in modo specifico per ciascun certificato;
- non esiste un meccanismo che consenta di informare automaticamente i partner di comunicazione in merito alla revoca di un certificato;
- risulta più difficile controllare l'utilizzo di chiavi crittografiche «deboli» (ad es. parametri notoriamente insicuri);
- è più complicato monitorare la scadenza dei certificati.

Durante la verifica di un certificato client o server si devono controllare almeno i seguenti aspetti:

- il certificato è stato emesso da un'autorità di certificazione considerata affidabile;
- il certificato è valido, ossia non è scaduto né revocato;
- il certificato server corrisponde al nome di dominio del servizio richiesto;
- il certificato client è stato emesso per un soggetto noto.

4.3 Configurazioni TLS

La direttiva tecnica TR-02102-2 del BSI «Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)»[11] raccomanda l'uso esclusivo delle versioni del protocollo TLS 1.2[12] e TLS 1.3[13]. È inoltre consigliato l'uso di suite di crittografia TLS che offrano la proprietà Perfect Forward Secrecy (PFS), grazie alla quale un collegamento non può essere decifrato retroattivamente nemmeno nel caso in cui le chiavi a lungo termine dei partner di comunicazione siano compromesse. Quando il protocollo TLS viene utilizzato per la protezione di dati personali, il BSI raccomanda l'uso di suite di crittografia che garantiscano la Perfect Forward Secrecy (PFS).

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