



Faktenblatt TLS Zertifikate im EPD

Datum: 06.02.2026

Die folgende Tabelle zeigt die verschiedenen Komponenten im EPD und welche Anforderungen bezüglich TLS-Zertifikate für diese gelten:

TOZ Ziffer	2.9.26 Bst. a	2.9.26 Bst. b	2.9.26 Bst. c	4.15.3 Bst. b	4.15.4 Bst. a		
Komponente	Gemeinschafts- übergreifend kommunizierend e Zugangs- punkte	Zugangspunkte gegenüber den Abfragediensten	Zugangspunkte gegenüber der Identifikationsdat enbank der ZAS	Systeme, die über das Internet auf einen Dienst zugreifen.	Zugangsportale	Zugangspunkte Zugangspunkte der EPD- Plattform, die von externen Systemen oder Portalen angesprochen werden.	Andere Dienste Dienste innerhalb der EPD-Plattform, die miteinander kommunizieren.
Systeme und IHE Akteure (nicht abschliessend)	XCA(I) Initiating und Responding Gateways, Authorization Decision Consumer und Provider	Value Set Consumer, Provider Information Consumer, Provider Information Source	UPI Client via Sedex	Primärsystem, Intermediär, PACS- System, Technischer User	Patientenportal, GFP-Portal	z.B.: Document Registry, die vom Document Consumer angesprochen wird.	z.B.: Document Registry mit Document Repository, Secure Node mit Audit Repository
Anforderungen an Zertifikate	Bundesgesetz vom 18. März 2016 über die elektronische Signatur (ZertES, SR 943.03)			-Gültiges elektronisches Zertifikat, gemäss Vorgaben im Kap. 2.3.4. -Stand der Technik	eCH-0048 Klasse 2 oder höher		Zertifikate, die nur innerhalb der Gemein- schaft gültig sind.

Weitere Informationen:

Bundesamt für Gesundheit, Kommunikation, www.bag.admin.ch

Diese Publikation erscheint ebenfalls in französischer und italienischer Sprache.



Herleitung, Anforderungen zu SSL/TLS

1 Einleitung

Das BAG erhält vermehrt Anfragen zur Präzisierung der Anforderungen zur TLS-Transportverschlüsselung im Rahmen des Elektronischen Patientendossiers (EPD). Dieses Dokument beschreibt die rechtlichen Vorgaben und gibt auf dieser Basis Präzisierungen für TLS-Zertifikate sowie für die sichere TLS-Konfiguration der jeweiligen IT-Systeme im EPD-Vertrauensraum.

Folgende IT-Systemarten sind im Scope dieses Dokuments:

IT-Systemarten	Beschreibung
Primärsysteme (Praxis-, Klinik-Informationssysteme)	Als Primärsysteme werden die Praxis- und Klinikinformationssysteme bezeichnet, in denen die interne elektronische Krankengeschichte eines Spitals, einer Arztpraxis oder Apotheke oder Therapeuten geführt wird. Diese interne elektronische Krankengeschichte oder -Akte ist die primäre Basis für alle behandlungsrelevanten Entscheidungen. Im Gegensatz dazu wird das elektronische Patientendossier als 'Sekundärsystem' positioniert, welches lediglich als Quelle für weitere medizinische Daten dienen soll.
Zugangsportale von (Stamm-)Gemeinschaften	Zugangsportale sind Internetportale, die Patientinnen und Patienten und Gesundheitsfachpersonen einen von Ort und Zeit unabhängigen und sicheren Zugriff auf die eigenen Daten, bzw. auf die Daten des Patienten/der Patientin ermöglichen. Das Zugangportal für Patienten/innen wird von der Stammgemeinschaft des Patienten/der Patientin bereitgestellt. Darüber hinaus kann der Patient/die Patientin über sein Zugangportal die Zugriffsrechte auf sein elektronisches Patientendossier verwalten. Das Zugangportal für Gesundheitsfachpersonen wird von der Gemeinschaft oder Stammgemeinschaft zur Verfügung gestellt.
EPD-Plattform / Interne Systeme von (Stamm-)Gemeinschaften	Zentrale EPD-Plattform der Gemeinschaft und deren internen Systeme zur Bereitstellung des EPD.
Zentrale Abfragedienste	Bei den zentralen Abfragediensten handelt es sich um die Dienste zur Abfrage gemäss Art. 39 EPDV. Diese stellen den Gemeinschaften notwendige Referenzdaten zur Verfügung, welche von einzelnen IT-Infrastrukturelementen der Gemeinschaften abgefragt werden können. Die Referenzdaten sind für die Kommunikation zwischen Gemeinschaften nötig. Die zentralen Abfragedienste sind in der Verantwortung des BAG.
Herausgeber von Identifikationsmitteln engl. Identity Provider (IDP)	Instanz, welche Identifikationsmittel für Gesundheitsfachpersonen und Patienten bereitstellt.
ZAS UPI	Identifikationsdatenbank der Zentralen Ausgleichsstelle des Bundes (ZAS), die für das EPD sektorielle Personenidentifikationsnummern herausgibt.

Weitere Informationen:

Bundesamt für Gesundheit, Kommunikation, www.bag.admin.ch

Diese Publikation erscheint ebenfalls in französischer und italienischer Sprache.

2 Rechtsgrundlagen

2.1 Bundesgesetz über das elektronische Patientendossier (EPDG)¹

Im EPDG wird u.a. der Zugang zum elektronischen Patientendossier beschrieben. Es werden Anforderungen für die Zertifizierung von Gemeinschaften, Stammgemeinschaften, Zugangsportale und die Herausgeber von Identifikationsmitteln festgelegt. Der Bundesrat legt die Anforderungen fest wie der Datenschutz und die Datensicherheit zu gewährleisten sind. Das Bundesamt für Gesundheit (BAG) kann ermächtigt werden, die Anforderungen für Datenschutz und Datensicherheit dem jeweiligen Stand der Technik anzupassen.

2.2 Verordnung über das elektronische Patientendossier (EPDV)²

Gemäss EPDV müssen Gemeinschaften sicherstellen, dass für die Speicherung und Übertragung der Daten Verschlüsselungsverfahren nach aktuellem Stand der Technik verwendet werden. Das Eidgenössische Department des Innern (EDI) legt die technischen und organisatorischen Vorgaben für die Datenübertragung fest und kann das BAG ermächtigen die Vorgaben nach dem Stand der Technik anzupassen (siehe Artikel 10 EPDV). Das EDI legt die technischen und organisatorischen Anforderungen in Bezug auf Datenschutz und Datensicherheit fest (siehe Artikel 12 EPDV). Auf Basis von Artikel 31 EPDV kann das EDI das BAG ermächtigen, die Vorgaben für die Zertifizierung von Herausgebern von Identifikationsmitteln dem Stand der Technik anzupassen. Gemäss Artikel 40 enthält der Dienst zur Abfrage der Gemeinschaften und Stammgemeinschaften die Zertifikate zur sichern Authentifizierung gegenüber anderen Gemeinschaften und Stammgemeinschaften.

2.3 EPDV-EDI Anhang 2³ (TOZ⁴)

Anhang 2 der EPDV-EDI enthält die Zertifizierungsanforderungen für Gemeinschaften und Stammgemeinschaften.

2.3.1 Kryptografische Massnahmen bei der Übertragung

Gemeinschaften müssen sicherstellen, dass Daten des elektronischen Patientendossiers mit geeigneten und dem aktuellen Stand der Technik entsprechenden kryptografischen Massnahmen bei der Übertragung gegen den Verlust der Vertraulichkeit, Authentizität und Integrität abgesichert werden (siehe Ziffer 2.5 Buchstabe a).

¹ <https://www.fedlex.admin.ch/eli/cc/2017/203/de>

² <https://www.fedlex.admin.ch/eli/cc/2017/204/de>

³ <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/oce/2025/56/de/pdf-a/fedlex-data-admin-ch-eli-oce-2025-56-de-pdf-a.pdf>

⁴ Technische und Organisatorische Zertifizierungsvoraussetzungen

Weitere Informationen:

Bundesamt für Gesundheit, Kommunikation, www.bag.admin.ch

Diese Publikation erscheint ebenfalls in französischer und italienischer Sprache.

2.3.2 Zertifikate für Kommunikation zwischen Gemeinschaften und den zentralen Diensten

Gemeinschaften müssen über ein gültiges digitales Zertifikat von einem anerkannten Anbieter von Zertifikatsdiensten gemäss ZertES verfügen zur gegenseitigen Authentisierung von (siehe Ziffer 2.9.26):

- Gemeinschaftsübergreifenden Zugangspunkten
- Zugangspunkten mit den Abfragediensten
- Zugangspunkten mit der Identifikationsdatenbank

2.3.3 Verwaltung kryptografischer Schlüssel

Gemeinschaften müssen eine Verwaltung kryptographischer Schlüssel sicherstellen (siehe Ziffer 4.12). Gemäss Hilfestellung zur Umsetzung TOZ beinhaltet diese Schlüsselgenerierung, Schlüsselverteilung, Behandlung von Sicherheitsvorfällen, Prinzip der Aufgabentrennung, Schlüsselspeicherung, Backup, Schutz vor Kompromittierung.

2.3.4 Client Zertifikate

Systeme, die über das Internet auf einen Dienst zugreifen, müssen sich diesem gegenüber mittels Transportschichtssicherheit (TLS) mit einem gültigen elektronischen Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (Certification Authority, CA) nach dem Stand der Technik authentisieren (siehe Ziffer 4.15.3 Buchstabe b).

Mit dem Begriff «**Systeme**» sind dabei Systeme gemeint, die von ausserhalb mit der zentralen EPD-Plattform der Gemeinschaft kommunizieren. Also zum Beispiel Primärsysteme, Intermediäre, PACS-Systeme oder technische User. Solche sollen auf sichere Art- und Weise mit den Gemeinschaften und dem Identity Provider kommunizieren. Die Rechtsgrundlagen fordern, dass alle Systeme, die über das öffentliche Internet angebotene Dienste des EPD nutzen, ihre Identität durch eine TLS Client-Authentisierung nachweisen sollen. Durch das TLS-Protokoll mit gegenseitiger Authentisierung (mTLS) wird sichergestellt, dass nur legitime Systeme mit den Gemeinschaften und Identity Providern kommunizieren können. Das Client-Zertifikat ist an sich nicht notwendig, um eine verschlüsselte Verbindung aufzubauen, sondern gewährleistet, dass ergänzend zu den Server-Systemen der Gemeinschaften und der IDPs auch die jeweils dazu verbindenden Systeme sich authentisieren. Insofern muss auf der Seite der Gemeinschaften und der IDPs sichergestellt sein, dass sowohl eine korrekte Zertifikatsvalidierung als auch ein legitimes Subject (z.B. eine registrierte Praxis) eine TLS-Client-Authentisierung mit seinem System durchführt.

2.3.5 Authentisierung von aufrufenden Systemen

Alle **Dienste**, die aus dem Internet aufrufbar sind, müssen das aufrufende System mittels TLS-Client-Authentication authentisieren (siehe Ziffern 4.15.3 Buchstabe b, 4.15.4 Buchstabe b).

Der Begriff «**Dienste**» bezieht sich dabei auf die Dienste der zentralen EPD-Plattform der Gemeinschaft, die in der TOZ auch Zugangspunkte genannt werden. So ein Zugangspunkt ist zum Beispiel eine zentrale Document Registry, die von einem Document Consumer des Primärsystems angesprochen wird.

2.3.6 Zugangsportale und Zugangspunkte

Für **Zugangsportale** sowie **Zugangspunkte** werden TLS-Zertifikate der Zertifikatsklasse 2 oder höher (gem. eCH-0048 PKI-Zertifikatsklassen, Version 2.0 vom 28.11.2018) eingesetzt. Für **andere Dienste** entweder mindestens TLS-Zertifikate der Zertifikatsklasse 2 oder TLS-Zertifikate, die nur innerhalb der Gemeinschaft gültig sind (siehe Ziffer 4.15.4).

Mit «**Zugangsportale**» sind das Patienten- und GFP-Portal gemeint.

Weitere Informationen:

Bundesamt für Gesundheit, Kommunikation, www.bag.admin.ch

Diese Publikation erscheint ebenfalls in französischer und italienischer Sprache.

Unter «**Zugangspunkte**» sind die Dienste der EPD-Plattform zu verstehen, die innerhalb der Gemeinschaft von externen Systemen wie zum Beispiel Primärsystemen oder Zugangsportalen angesprochen werden. Hier ausgenommen sind Zugangspunkte die zur Kommunikation mit anderen Gemeinschaften oder Stammgemeinschaft dienen, da für diese wie oben erwähnt erhöhte Anforderungen gelten (siehe Kapitel 2.3.2).

Der Begriff «**andere Dienste**» bezieht sich auf Dienste innerhalb der zentralen EPD-Plattform, die miteinander kommunizieren. Wie zum Beispiel der IHE Akteur Document Registry der Plattform mit dem Document Repository kommuniziert oder die Akteure Secure Node und Audit Repository, die intern miteinander kommunizieren.

3 Anforderungen an Zertifikate im EPD

In der TOZ werden vier verschiedene Kategorien von TLS Zertifikaten beschrieben, die zum Einsatz kommen.

3.1 ZertES⁵

Für gemeinschaftsübergreifende Zugangspunkte sowie Zugangspunkte zu den Abfragediensten und zur Identifikationsdatenbank UPI müssen Gemeinschaften und Stammgemeinschaften Zertifikate gemäss ZertES einsetzen. Die Herausgeber von Zertifikaten gemäss ZertES müssen durch die schweizerische Akkreditierungsstelle anerkannt sein. Dadurch wird sichergestellt, dass ZertES Zertifikate nur von vertrauenswürdigen Institutionen herausgegeben werden können, welche die hohen Anforderungen gemäss ZertES erfüllen.

Anerkannte Anbieter von ZertES Zertifikaten sind gemäss der schweizerischen Akkreditierungsstelle⁶ die folgenden:

- Bundesamt für Informatik und Telekommunikation (BIT)
- DigiCert Switzerland AG
- Swisscom (Schweiz) AG
- SwissSign AG

3.2 eCH-0048 Klasse 2 oder höher

Für gemeinschaftsinterne Zugangsportale und Zugangspunkte, die nicht für die gemeinschaftsübergreifende Kommunikation oder die Kommunikation mit den zentralen Diensten, verwendet werden, müssen Zertifikate der Klasse 2 oder höher nach dem eCH-0048 Standard eingesetzt werden. Ebenfalls können solche Zertifikate für andere Dienste innerhalb der zentralen EPD-Plattform eingesetzt werden. Der Standard basiert auf der Europäischen Norm (EN) ETSI EN 319 411 „Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates“⁷. Diese Norm verlangt, dass sich ein Anbieter solcher Zertifikate mindestens alle zwei Jahre einem Compliance Audit unterziehen muss. Die Anforderungen an den Anbieter hinsichtlich Betrieb, Personal und Prozesse sind dabei auf demselben Niveau wie für Anbieter gemäss ZertES. Weiter muss bei Beantragung eines Zertifikats als Identitätsnachweis für

⁵ <https://www.fedlex.admin.ch/eli/cc/2016/752/de>

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>

Weitere Informationen:

Bundesamt für Gesundheit, Kommunikation, www.bag.admin.ch

Diese Publikation erscheint ebenfalls in französischer und italienischer Sprache.

natürliche Personen ein national anerkanntes Ausweisdokument vorgezeigt werden, bei Organisationen eine Vertretungsbefugnis z.B. mittels Handelsregisterauszug.

Im Gegensatz zum nachfolgenden Kapitel identifizieren die Systeme die Gemeinschaft hier nicht anhand des individuellen Zertifikates, sondern anhand der Vertrauenswürdigkeit des Herausgebers (CA).

3.3 Gültige Zertifikate vertrauenswürdiger Zertifizierungsstellen nach Stand der Technik

Systeme wie zum Beispiel Primärsysteme oder Intermediäre, die auf die Dienste der zentralen EPD-Plattform zugreifen, müssen gemäss TOZ ein gültiges Client-Zertifikat verwenden, das von einer vertrauenswürdigen Zertifizierungsstelle nach Stand der Technik ausgestellt wurde. Dies bedingt die Möglichkeit, die aktuelle Gültigkeit des Zertifikats beim Herausgeber abfragen zu können. Wie die Vertrauenswürdigkeit der Zertifizierungsstelle zu beurteilen ist, wird in der TOZ nicht weiter beschrieben. Es muss sich dabei aber anders als in Kapitel 3.1 nicht um einen anerkannten Anbieter gemäss ZertES oder gar eine schweizerische Institution handeln. Auch offengelassen ist, welcher Identifikationsnachweis bei Beantragung eines solchen Zertifikats vorgewiesen werden muss. Hier können also durchaus auch «Domain Validated» Zertifikate zum Einsatz kommen, wo die Identität des Antragsstellers nicht auf personenbezogene Informationen überprüft wird. Da die (Stamm-)Gemeinschaften die Client-Zertifikate von Primärsystemen etc. momentan sowieso in einem manuellen Prozess, bei sich in der zentralen EPD-Plattform integrieren müssen, erfolgt eine Art «Organization Validation» in einem zweiten Schritt. Dabei werden die Zertifikate sowie URL und OID der Systeme in der Gemeinschaft beim Onboarding Prozess registriert. Bei jedem Zugriff identifiziert die Gemeinschaft das System so anhand des hinterlegten Zertifikates, der URL sowie der OID. Bezüglich des Stands der Technik wird in Kapitel 4 vertieft darauf eingegangen.

3.4 Gemeinschaftsintern gültige Zertifikate

Für andere Dienste innerhalb der zentralen EPD-Plattform können entweder Zertifikate gemäss eCH-0048 Klasse 2 oder höher eingesetzt werden oder Zertifikate, die nur innerhalb der Gemeinschaft gültig sind. Bei letzterem handelt es sich um sogenannte selbstsignierte Zertifikate. Obwohl die TOZ keine genaueren Anforderungen nennt, ist es selbstsprechend, dass diese Zertifikate ebenfalls gemäss dem Stand der Technik ausgestellt werden und bei Verwendung gültig sein sollen. Zudem ist es stark empfohlen eine Infrastruktur zu betreiben, welche das Management der Zertifikate wie zum Beispiel Schlüsselgenerierung und Schlüsselerneuerung übernimmt und wo die Dienste die Gültigkeit der Zertifikate abfragen können.

4 Stand der Technik

Vor dem Hintergrund, dass die Rechtsgrundlagen für das EPD häufig auf den Stand der Technik verweisen, wird dieser in diesem Kapitel zusammengefasst.

Weitere Informationen:

Bundesamt für Gesundheit, Kommunikation, www.bag.admin.ch

Diese Publikation erscheint ebenfalls in französischer und italienischer Sprache.

4.1 Management kryptographischer Schlüssel

Für das Management kryptographischer Schlüssel existieren verschiedene Standards und good practices u.a. NIST SP 800-57 und ISO/IEC 11770 sowie TR-02102-1 «Technische Richtlinie Kryptographische Verfahren»⁸.

Kryptographische Schlüssel müssen während ihres gesamten Lebenszyklus angemessen geschützt werden. Die wesentlichen Lebenszyklusphasen sind Schlüsselgenerierung, Schlüsselaktivierung, Schlüsselnutzung, Schlüsselerneuerung, Schlüsselrückzug, Schlüsselarchivierung und Schlüssellöschung.

Die wesentlichen Sicherheitsanforderungen für das Management von kryptographischen Schlüsseln sind in der folgenden Tabelle zusammengefasst.

Phase	Wesentliche Sicherheitsanforderungen
Schlüsselgenerierung	<p>Schlüssel sollen auf dem IT-System generiert werden, wo diese auch genutzt werden.</p> <p>Schlüssel sollen mit den entsprechenden sicheren kryptographischen Parametern erstellt werden (siehe Kapitel 3.3).</p> <p>Sofern Schlüssel kopiert und verteilt werden sollen, ist die Vertraulichkeit des Schlüssels bei der Übertragung stets zu bewahren (z.B. Verschlüsselung).</p> <p>Nutzung von Standard-Bibliotheken, welche u.a. genügend Entropie bei der Generierung eines Schlüssels erlaubt.</p>
Schlüsselaktivierung	<p>Vor der Aktivierung sollte der Schlüssel mindestens so geschützt sein, wie während der Nutzung.</p>
Schlüsselnutzung	<p>Schlüssel sollen zugriffsgeschützt gespeichert sein und nur durch legitime Personen oder Computer-Prozesse für den legitimen Zweck eingesetzt werden.</p> <p>Keine gleichzeitige Nutzung von Schlüsseln für Authentisierung, Verschlüsselung und digitale Signatur.</p>
Schlüsselerneuerung	<p>Schlüssel sollen periodisch gewechselt werden. D.h. kein neues Zertifikat auf Basis des bestehenden Schlüsselmaterials eines alten Zertifikats.</p>
Schlüsselrückziehung	<p>Sofern ein Schlüssel nicht mehr benötigt oder potentiell kompromittiert wurde (z.B. nach einem IT-Angriff) sollte der Schlüssel zurückgezogen werden z.B. durch Zertifikatsrevozierung.</p>

⁸

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

Weitere Informationen:

Bundesamt für Gesundheit, Kommunikation, www.bag.admin.ch

Diese Publikation erscheint ebenfalls in französischer und italienischer Sprache.

Schlüsselarchivierung	Im Kontext von Authentisierung nicht relevant.
Schlüssellöschung	Sofern ein Schlüssel nicht mehr benötigt wird, ist dieser sicher zu löschen u.a. auch auf Backup-Medien.

4.2 TLS-Zertifikate

Das Bundesamt für Cybersicherheit (BACS) verweist auf Vorgaben des Bundes, die jedoch nur für IKT-Systeme des Bundes gelten. Bei «best practices» verweist der Bund auf das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) mit den entsprechenden technischen Richtlinien.

Das Vertrauen in Zertifikate basiert auf den Prozessen, die eine Certificate Authority durchläuft, bevor ein angefragtes Zertifikat ausgestellt wird. Dokumentiert werden entsprechende Prozesse in einer Certificate Policy (CP) und einem Certificate Practice Statement (CPS). Der RFC 3647 «Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework»⁹ dokumentiert u.a. die folgenden Themen, welche in einem CP/CPS adressiert werden sollten:

- Verfahren zur Authentifizierung des Zertifikatsantragstellers vor der Ausstellung des Zertifikats
- Anforderungen für die CA und Zertifikatnehmer im Rahmen des Zertifikats-Lebenszyklus
- Organisatorische und technische Massnahmen der CA (Schlüsselgenerierung, Subjekt-Authentifizierung, Zertifikatsausstellung, Zertifikatswiderruf, Auditierung und Archivierung)

Gemäss Kapitel 8.2.2.2 der **BSI TR-02103**¹⁰ bieten selbstsignierte Zertifikate an sich keinerlei Integritätsschutz, da diese nicht durch einen privaten Schlüssel einer Certificate Authority (CA) signiert werden, der man implizit vertraut. Darüber hinaus sollte die Zahl der vertrauten CAs so gering wie möglich gehalten werden.

Des Weiteren haben selbstsignierte Zertifikate grundsätzlich die weiteren Nachteile:

- Es kann kein implizites Vertrauensverhältnis über eine Vertrauenskette etabliert werden, sondern es muss jedem einzelnen Zertifikat dediziert vertraut werden.
- Es existiert kein Mechanismus, um Kommunikationspartnern ein Zurückziehen eines Zertifikats automatisiert mitzuteilen.
- Die Kontrolle bzgl. des Einsatz «schwacher» kryptographischer Schlüssel (z.B. bekannt schwache Parameter) wird erschwert.
- Das Tracking des Ablaufs der Gültigkeit von Zertifikaten wird erschwert.

Bei der Prüfung eines Client- oder Server-Zertifikats sollen mindestens die folgenden Parameter geprüft werden:

- Das Zertifikat ist ausgestellt von einer vertrauenswürdigen Certificate Authority (CA).
- Das Zertifikat ist gültig, das heisst nicht abgelaufen und nicht gesperrt.

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

Weitere Informationen:

Bundesamt für Gesundheit, Kommunikation, www.bag.admin.ch

Diese Publikation erscheint ebenfalls in französischer und italienischer Sprache.

- Es wird geprüft, ob ein Server-Zertifikat auf den Domain-Namen des aufgerufenen Service ausgestellt wurde.
- Es wird geprüft, ob ein Client-Zertifikat für ein bekanntes Subjekt ausgestellt wurde.

4.3 TLS-Konfigurationen

Die technische Richtlinie vom BSI TR-02102-2 "Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)"¹¹ empfiehlt nur den Einsatz der TLS-Protokollversionen TLS 1.2¹² und TLS 1.3¹³. Es wird der Einsatz von TLS cipher suites mit der Eigenschaft «Perfect forward secrecy» (PFS) empfohlen. Durch PFS kann eine Verbindung auch bei Kenntnis der Langzeit-Schlüssel der Kommunikationspartner nicht nachträglich entschlüsselt werden. Bei der Verwendung von TLS zum Schutz personenbezogener Daten wird der Einsatz von cipher suites, die PFS gewährleisten, vom BSI empfohlen.

4.4 Verkürzung der Lebensdauer von der TLS-Zertifikate

Das internationale CA/Browser-Forum hat Änderungen bei der Gültigkeitsdauer von TLS-Zertifikaten angekündigt. Die wichtigsten nationalen und internationalen Anbieter von TLS-Zertifikaten sind bereits dabei, ihre eigenen Angebote und Prozesse entsprechend anzupassen¹⁴.

Auch das Bundesamt für Gesundheit (BAG) weiss von diesen Änderungen. Erste Analysen und die Suche nach möglichen Lösungen werden derzeit zusammen mit dem Bundesamt für Informatik und Telekommunikation (BIT) geprüft. Das BAG wird die verschiedenen Beteiligten proaktiv informieren, sobald erste Zwischenergebnisse vorliegen. Bis dahin bleiben die bekannten Abläufe für den Austausch von TLS-Zertifikaten zwischen den (Stamm-)Gemeinschaften, ihren IT-Lieferanten und dem BAG unverändert.

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>

¹⁴ Siehe zum Beispiel <https://www.swisssign.com/blog/47-days-ssl-tls-laufzeit.html> oder <https://www.digicert.com/de/blog/tls-certificate-lifetimes-will-officially-reduce-to-47-days>

Weitere Informationen:

Bundesamt für Gesundheit, Kommunikation, www.bag.admin.ch

Diese Publikation erscheint ebenfalls in französischer und italienischer Sprache.