

Bestimmungen zur Informationstechniksicherheit gemäß § 2 Anlage 31b zum Bundesmantelvertrag - Ärzte SGB V - ips - Videosprechstunde - IT

datenschutz cert GmbH
15.04.2024

Inhaltsverzeichnis

1. Einleitung.....	5
2. Der Zertifizierungsstandard „ips - Videosprechstunde - IT“	7
2.1. Was kann zertifiziert werden?	7
2.2. Abgrenzung.....	8
2.3. Konkretisierung des Bewertungsgegenstands	8
2.4. Räumlicher Anwendungsbereich.....	10
2.5. Konformitätsaussage	10
3. Anwendung des Zertifizierungsstandards „ips - Videosprechstunde - IT“	11
3.1. Scope-Beschreibung	11
3.2. Realisierungsbeschreibung.....	13
4. Der Kriterienkatalog „ips - Videosprechstunde - IT“	15
4.1. P.1 Grundlagen	15
4.2. P.2 Übertragung	17
4.3. P.3 Verschlüsselung	19
4.4. P.4 Absicherung der Inhalte	21
4.5. P.5 Ausschluss schwerwiegender Sicherheitsrisiken OWASP Top 10	24
5. Zertifizierungsprozess.....	26
5.1. Übersicht.....	26
5.2. Antrag	26
5.3. Angebot mit Kalkulation.....	27
5.4. Referenzdokumentation der Kunden	27
5.5. Evaluierungsprozess	28
5.6. Stichprobenverfahren	29
5.7. Bewertungsschema	29
5.8. Evaluierungsbericht.....	29
5.9. Anerkennung bestehender Zertifikate.....	29
5.10. Zertifizierung	30
5.11. Jährliche Überwachung	32
5.12. Re-Zertifizierung.....	32
5.13. Anlassbezogene Prüfungen.....	32
5.14. Änderungen, die sich auf die Zertifizierung auswirken.....	32
5.15. Beendigung, Einschränkung, Aussetzung oder Zurückziehung der Zertifizierung.....	33
6. Referenzen.....	34
7. Glossar	35
8. datenschutz cert GmbH	37

Historie

Version	Datum	Grund der Änderung	Geändert durch
0.1	06.07.2019	erste Version zur Vorlage bei DAkkS und Aufsichtsbehörden	Dr. Sönke Maseberg, Alisha Gühr
0.2	06.07.2021	Überarbeitung wegen Änderungen im Konformitätsbewertungsprogramm	Alisha Gühr
0.3	19.10.2021	Berücksichtigung von Anmerkungen der DAkkS-Programmprüfung	Alisha Gühr
0.4	01.01.2022	Berücksichtigung der neuen Anlage 31b zum BMV-Ä	Alisha Gühr
0.5	16.08.2022	Berücksichtigung der DAkkS Fachberichtsprüfung	Alisha Gühr
0.6	01.12.2022	Berücksichtigung der DAkkS Fachberichtsprüfung	Alisha Gühr
0.7	19.01.2023	Berücksichtigung der DAkkS Geschäftsstellenprüfung	Dr. Sönke Maseberg, Alisha Gühr
0.8	07.03.2023	Berücksichtigung der DAkkS Geschäftsstellenprüfung	Dr. Sönke Maseberg, Alisha Gühr
1.0	15.05.2023	Finale Fassung nach Akkreditierung	Dr. Sönke Maseberg, Alisha Gühr
1.1.	15.04.2024	Berücksichtigung der DAkkS Fachbegutachtung	Dr. Sönke Maseberg, Alisha Gühr

Dokumenten-Überwachungsverfahren

Status	Prozess-/Dokumentenbesitzer	Version
Final	Dr. Sönke Maseberg	1.1

Verteilerliste

- datenschutz cert GmbH
- Zertifizierungsstellen und Interessierte (Lizenznehmer des Programms)
- DAkKS

1. Einleitung

Die „Vereinbarung über die Anforderungen an die technischen Verfahren zur Videosprechstunde gemäß § 365 SGB V“ zwischen dem GKV-Spitzenverband und der Kassenärztlichen Bundesvereinigung (Anlage 31b zum Bundesmantelvertrag - Ärzte) [Anlage 31b BMV-Ä] sieht ein Zertifizierungsverfahren für Videosprechstunden vor.

Gemäß § 5 Abs. 2 Anlage 31b müssen Videodienstanbieter den Nachweis führen, dass der angebotene Videodienst die Anforderungen an die Gewährleistung der Schutzziele (Vertraulichkeit, Integrität und Verfügbarkeit) gemäß § 2 und § 2a erfüllt. Zudem muss der Videodienstanbieter gemäß Buchstabe c) bestätigen, dass er bzw. der angebotene Videodienst die inhaltlichen Anforderungen gemäß Absatz 1 erfüllt.“ Der Nachweis für die Informationstechniksicherheit gemäß § 2 Abs. 2 lit. a) Anlage 31b BMV-Ä ist möglich durch:

- „Ein Zertifikat einer gemäß der VO (EG) 765/2008 nach ISO/IEC 17065 für den Geltungsbereich der technischen Verfahren zur Videosprechstunde gemäß § 365 Absatz 1 SGB V akkreditierten Zertifizierungsstelle. Im Rahmen der fachlichen Prüfung der Akkreditierungsfähigkeit von entsprechenden Konformitätsbewertungsprogrammen durch die Akkreditierungsstelle ist das Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik herzustellen.“

Ein solches Zertifikat besteht zum Zeitpunkt der Erstellung dieses Programms nicht. Die Kriterien und das dahinterliegende Zertifizierungsprogramm dient daher dem Zweck, ein solches Zertifikat über die Informationstechniksicherheit bereitzustellen.

Mit der ips-Videosprechstunde kann ein Zertifizierungsverfahren für die Informationstechniksicherheit für Videosprechstunden als Nachweis der Einhaltung der Anforderungen zur Informationstechniksicherheit in § 2 Anlage 31b BMV-Ä realisiert werden.

Werden die Kriterien von ips - Videosprechstunde - IT erfüllt erhält der Videodienst Zertifikat einer gemäß der VO (EG) 765/2008 nach ISO/IEC 17065 für den Geltungsbereich der technischen Verfahren zur Videosprechstunde gemäß § 365 Absatz 1 SGB V akkreditierten Zertifizierungsstelle.

Für eine Listung bei der Kassenärztlichen Bundesvereinigung ist zusätzlich ein Zertifikat gemäß Art. 42 DSGVO für den Geltungsbereich der Verarbeitung personenbezogener Daten bei Videodiensten in der vertragsärztlichen Versorgung zur Durchführung von Videosprechstunde gemäß § 365 Absatz 1 SGB V erforderlich. Das Zertifikat wird erteilt von einer nach ISO/IEC 17065 akkreditierten und zugelassenen Zertifizierungsstelle. Dies kann z.B. durch eine Zertifizierung einer IT-gestützten Verarbeitung personenbezogener Daten gem. Art. 42 DSGVO gemäß („ips - Videosprechstunde - IT“) angestrebt werden.

Das vorliegende Dokument gliedert sich wie folgt auf:

- zunächst wird in Abs. 2 der Zertifizierungsstandard „ips - Videosprechstunde - IT“ vorgestellt, hier wird insbesondere erläutert, was gem. „ips - Videosprechstunde - IT“ zertifiziert werden kann,

- anschließend wird in Abs. 3 die Anwendung des Zertifizierungsstandards im Detail erläutert, bevor
- in Abs. 4 der eigentliche Kriterienkatalog mit den Anforderungselementen folgt.

Der vorliegende Kriterienkatalog schließt mit einer Beschreibung des Zertifizierungsprozesses 5 mit Referenzen und Glossar in den Abs. 6 und 7 sowie den Kontaktdaten der datenschutz cert GmbH in Abs. 8.

Dieses Dokument ist Eigentum der datenschutz cert GmbH! Eine Weitergabe ist nicht zulässig.

2. Der Zertifizierungsstandard „ips - Videosprechstunde - IT“

2.1. Was kann zertifiziert werden?

Zunächst wird die wichtige Frage erörtert, was eigentlich im Rahmen einer „Videosprechstunde“ zertifiziert werden kann. Die Erbringung von Videosprechstunden wird gemäß § 365 SGB V definiert als:

- Synchroner Kommunikation über die den Patienten zur Verfügung stehende technische Ausstattung, ggf. unter Assistenz, z. B. durch eine Bezugsperson, im Sinne einer Videosprechstunde in Echtzeit, die Vertragsärzte den Patienten anbieten können.
- Als Videodienstleister werden Unternehmen bezeichnet, die Vertragsärzte Dienste zur Durchführung von Videosprechstunden gemäß § 1 Abs 2 Anlage 31b BMV-Ä anbieten.

Der Bewertungsgegenstand umfasst somit die synchrone Videokommunikation¹, welche über eine technische Infrastruktur realisiert wird. Zur Durchführung der Videokommunikation bedarf es einer technischen Infrastruktur², die eine solche synchrone Kommunikation zwischen zwei oder mehr Teilnehmenden ermöglicht.

Der Bewertungsgegenstand beginnt bei der Eröffnung der Videoverbindung zwischen den Teilnehmenden, umfasst die Durchführung der Videokommunikation von Anfang bis Ende der Verbindung und endet bei der Löschung der entstandenen Metadaten.

Neben der direkten Kommunikation umfasst der Bewertungsgegenstand die vorübergehende Speicherung und Löschung der Metadaten/Verbindungsdaten, als wesentlichen Bestandteil des Verbindungsaufbaus und der Durchführung der Videosprechstunde.

Der technische Geltungsbereich umfasst alle Systeme und Komponenten der Betreiber, die zur Durchführung, zum Betrieb sowie zur Wartung der zu zertifizierenden Videosprechstunde und zur Vermittlung von Informationen zwischen den o.g. Systemen und Komponenten notwendig sind.

Schnittstellen zur Übertragung von Informationen aus oder in den Geltungsbereich der Videosprechstunde stellen Risiken für weitere Systeme und Komponenten im Netzsegment dar. Schnittstellen zur Informationsübertragung³ sind somit Bestandteil des Geltungsbereichs. Weitere Schnittstellen zu externen Systemen, wie z.B. Mail- oder SMS-Server sind ebenfalls Teil des Geltungsbereichs.

¹ Die beteiligten Kommunikationspartner tauschen in Echtzeit Informationen aus, z.B. Angesicht zu Angesicht, über Videokonferenzsysteme.

² Dies erfolgt in der Regel über eine Weblösung (Webseite), eine mobile Applikation oder ein bestimmtes technisches Gerät mit integrierter Software.

³ Diese umfassen sämtliche Systeme und Komponenten des Betreibers, welche Metadaten und Verbindungsdaten speichern oder verarbeiten, die als wesentlichen Bestandteil des Verbindungsaufbaus und der Durchführung der Videosprechstunde notwendig sind.

Clients, die Teil des Netzwerksegments der zu zertifizierenden Videosprechstunde sein könnten, sind dem Geltungsbereich hinzuzählen.

Wird eine PKI betrieben, die zur internen Kommunikation notwendig ist, ist diese Teil des Geltungsbereichs.

2.2. Abgrenzung

Der Bewertungsgegenstand umfasst dabei lediglich die vom Videodienstanbieter bereitgestellte Lösung mit ihren vom Geltungsbereich umfassten Bestandteilen. Nicht zum Bewertungsgegenstand zählt die Nutzung der Videosprechstunde durch die Anwender, insbesondere bei nicht ordnungsgemäßer Nutzung.

Die technische Lösung zur Planung (Terminierung) einer solchen Kommunikation, inklusive der Bereitstellung oder Übermittlung der technischen Zugangsdaten für die Teilnehmenden zur Durchführung einer Videosprechstunde hingegen ist nicht Teil des Bewertungsgegenstandes. Hierbei werden zwar auch schützenswerte Daten verarbeitet, welche im Rahmen einer datenschutzrechtlichen Prüfung auf den Schutz der Daten geprüft werden sollten, die Kriterien des § 2 der Anlage 31b zum BMV-Ä hingegen zielen klar auf die technische Sicherheit der Videoverbindung ab.

Systeme und Komponenten außerhalb des internen Netzwerks, der zu zertifizierenden Videosprechstunde sind kein Teil des Bewertungsgegenstandes. So sind externe Mail- oder SMS-Server vom Geltungsbereich auszunehmen. Weiter sind sämtliche Komponenten und Systeme vom Geltungsbereich ausgegrenzt, die auf Seiten der Kommunikationspartner, und nicht vom Betreiber, betrieben werden.

Auch die Entwicklungsumgebung stellt keinen Bestandteil des Zertifizierungsgegenstandes dar.

Systeme, Komponenten und Anwendungen, die kein Risiko für die zu zertifizierende Videosprechstunde darstellen, können begründet vom Geltungsbereich abgegrenzt werden.

2.3. Konkretisierung des Bewertungsgegenstands

Der Bewertungsgegenstand der Zertifizierung – muss eindeutig festgelegt sein. Es muss eindeutig beschrieben sein, welche Tätigkeiten exakt zum Scope gehören, an welchen Standorten diese Tätigkeiten erbracht werden, welche IT-Komponenten erforderlich sind und auch welche Prozesse in einer Organisation etabliert sind, um die Videosprechstunde insgesamt darstellen zu können. Diese eindeutige Festlegung ist nicht nur für die Organisation wichtig, sondern auch für das Evaluationsteam und die Zertifizierungsstelle.

Eine nach diesem Programm zu zertifizierende „Videosprechstunde“ wird durch folgende Elemente charakterisiert:

- Videoübertragung über das Internet zum Zwecke der Durchführung einer Videosprechstunde mittels eines technischen Verfahrens (technische Umsetzung des Verbindungsaufbaus, der Durchführung einer Videokommunikation und Verbindung der Gesprächsteilnehmer) (TV);

- Prozesse (PRZ) mit den fachlichen Tätigkeiten, die für die Videosprechstunde benötigt werden;
- Informationen (Verbindungsdaten, Videodaten (INFO));
- IT-Infrastruktur (IT) mit Servern, Clients, Netzkomponenten, Datenbanken, Speichersystemen und Schnittstellen;
- Applikationen (APPL), über die die Videosprechstunde realisiert wird (URL der Webseite, Versionsstand und Betriebssystem der App oder Software);

Die Gesamtheit dieser Zielobjektkategorien stellen somit die Videosprechstunde und den Bewertungsgegenstand dar.

Kunde ist der Betreiber der Videosprechstunde.

Das Zertifikat trägt den Titel „ips - Videosprechstunde - IT“.

Für eine konkrete Zertifizierung sind alle nachfolgenden Zielobjekte (Zielobjekte) aufzulisten, die für den zu Bewertungsgegenstand (Scope) zwingend erforderlich sind:

- Technisches Verfahren (TV):
 - Beschreibung der technischen Umsetzung bzw. des technischen Verfahrens welches zur Durchführung der Videoübertragung über das Internet eingesetzt wird (Verbindungsaufbau, der Durchführung einer Videokommunikation und Verbindung der Gesprächsteilnehmer);
- Prozesse (PRZ):
 - Beschreibung der fachlichen Prozesse, die für die Videosprechstunde benötigt werden;
- Informationen (Verbindungsdaten, Videodaten (INFO))
 - Beschreibung der Informationen bzw. Daten welche im Geltungsbereich anfallen (hierbei ist nicht von der datenschutzrechtlichen Definition von Daten auszugehen);
- IT-Infrastruktur (IT):
 - exakte Angabe der IT-Systeme (Servern, Clients, Netzkomponenten, Datenbanken, Speichersystemen und Schnittstellen), die für die Videosprechstunde erforderlich sind, mit Netzstrukturplan;
- Applikationen (APPL):
 - exakte Angabe der Applikationen – sowohl interne Anwendungen als auch von Extern verfügbare Anwendungen, wie etwa Webseiten oder Apps –, die im Rahmen der Videosprechstunde genutzt werden.

Zur Definition der Begriffe wird auf das Glossar in Abs. 9 verwiesen.

Die Zertifizierungsstelle muss sicherstellen, dass der Bewertungsgegenstand unmissverständlich festgelegt ist.

In dieser Übersicht sind zunächst alle Zielobjekte aufzunehmen, auch solche, die durch Dienstleister und externe Dritte wahrgenommen werden; diese Zielobjekte sind dann entsprechend zu kennzeichnen.

Diese exakt definierten Videosprechstunde stellen damit den Bewertungsgegenstand und somit den Geltungsbereich der Zertifizierung dar. Ein Ausschluss einzelner Zielobjekte, die für die zu zertifizierenden technischen Verfahren zur Videosprechstunde erforderlich sind, ist nicht zulässig.

2.4. Räumlicher Anwendungsbereich

Die Verarbeitung von Informationen im Rahmen der Videosprechstunde darf nur im Inland, in einem Mitgliedsstaat der Europäischen Union oder in einem diesem nach § 35 Absatz 7 des Ersten Buches Sozialgesetzbuch gleichgestellten Staat, oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat erfolgen.

Dies ist eine zwingende Anforderung an Videosprechstunden im Rahmen der datenschutzrechtlichen Zertifizierung. Logischerweise können Videosprechstunde somit nur innerhalb dieser räumlichen Begrenzung stattfinden.

Somit ist der räumliche Anwendungsbereich auch für diesen Zertifizierungsstandard eingeschränkt.

2.5. Konformitätsaussage

Mit einem „ips - Videosprechstunde - IT“ -Zertifikat wird folgende Konformitätsaussage getroffen:

Die Zertifizierungsstelle bestätigt,

- dass die angegebene Organisation als Videodienstanbieter
- den definierten Bewertungsgegenstand – die „Videosprechstunde“ –
- konform zu folgenden Anforderungen betreibt:
 - § 2 der Anlage 31b BMV-Ä, und dass
- folgende Prüfgrundlagen genutzt wurden:
 - der vorliegende ips - Videosprechstunde - IT -Kriterienkatalog.

3. Anwendung des Zertifizierungsstandards „ips - Videosprechstunde - IT“

Der Zertifizierungsstandard „ips - Videosprechstunde - IT“ ist geeignet, eine Videosprechstunde so zu modellieren, dass eine anschließende Zertifizierung/ ein Nachweis gemäß § 5 Abs. 2 lit. a) Anlage 31b BMV-Ä möglich ist.

In diesem Abschnitt wird die Vorgehensweise zur Beschreibung eines technischen Verfahrens zur Videosprechstunde gem. „ips - Videosprechstunde - IT“ beschrieben.

3.1. Scope-Beschreibung

Im ersten Schritt ist der Geltungsbereich – der Scope – exakt festzulegen; hierzu sind die nachfolgenden Angaben erforderlich. Wenn möglich, können Informationen gruppiert werden.

Es muss die „gesamte Kette“, die zu einem technischen Verfahren zur Videosprechstunde gehört, beschrieben sein. Alle Informationen müssen klar, präzise und eindeutig sein.

3.1.1. Antragsteller

Angabe des Antragstellers:

NAME (JURISTISCHE PERSON)
Straße, Ort, Land
Tel, Fax, E-Mail, Webseite
Ansprechpartner mit Kontaktdaten

Darlegung der Organisationsstruktur, etwa anhand eines Organigramms sowie Vorlage eines Handelsregisterauszugs.

3.1.2. Art der Videosprechstunde (TV)

Beschreibung der zu zertifizierenden technischen Verfahren zur Videosprechstunde unter Angabe von:

- Beschreibung der technischen Umsetzung bzw. des technischen Verfahrens welches zur Durchführung der Videoübertragung über das Internet eingesetzt wird (Verbindungsaufbau, der Durchführung einer Videokommunikation und Verbindung der Gesprächsteilnehmer) (TV).

3.1.3. Informationen (Verbindungsdaten, Videodaten (INFO))

Beschreibung der Informationen bzw. Daten welche im Geltungsbereich anfallen (hierbei ist nicht von der datenschutzrechtlichen Definition von Daten auszugehen).

ID	BESCHREIBUNG	ART DER INFORMATIONEN
INFO-01		
INFO-02		

3.1.4. Prozesse (PRZ)

Beschreibung der Prozesse (PRZ), die für die konkrete Videosprechstunde benötigt werden; ggf. Verweis auf beigefügte Regelungen, Anleitungen, Prozessbeschreibungen, etc.

3.1.5. Applikationen (APPL)

Beschreibung aller für die zu zertifizierenden technischen Verfahren zur Videosprechstunde relevanten Applikationen (APPL), die in der Videosprechstunde genutzt werden; dies sind sowohl interne Anwendungen als auch extern verfügbare Anwendungen, wie etwa Webseiten oder Apps; mit Angabe der Art der Applikation und Zuordnung zu den in der Applikation verwendeten Informationen mit Netzstrukturplan.

ID	BESCHREIBUNG	ART DER APPLIKATION	RELEVANTE INFORMATIONEN	BEMERKUNG
Appl-01				
Appl-02				

3.1.6. IT-Infrastruktur (IT)

Beschreibung aller für die zu zertifizierenden technischen Verfahren zur Videosprechstunde relevanten IT-Systeme (Client, Server, Netzkomponenten, Datenbanken, Speichersystemen); mit: Angabe der Art der Systeme und Zuordnung zu den Applikationen.

ID	BESCHREIBUNG	ART DES IT-SYSTEMS	RELEVANTE APPLIKATION	BEMERKUNG
Client-01				
Client -02				

ID	BESCHREIBUNG	ART DES SYSTEMS	IT-RELEVANTE APPLIKATION	BEMERKUNG
Serv-01				
Serv-03				
Netz-01				
Netz-02				
DB-01				
DB-02				
Speicher-01				
Speicher-02				

3.1.7. Schnittstellen

Beschreibung aller für die zu zertifizierenden technischen Verfahren zur Videosprechstunde relevanten Schnittstellen zu anderen Systemen und Organisationen (Außenverbindungen):

ID	BESCHREIBUNG	ART DER SCHNITTSTELLE	BEMERKUNG
Int-01			
Int-02			

Graphische Darlegung, etwa als Netzstrukturplan und Datenflussdiagramm.

3.2. Realisierungsbeschreibung

Nachdem im vorherigen Schritt die dem generischen Ansatz des Zertifizierungsstandards „ips - Videosprechstunde - IT“ geschuldeten „Freiheitsgrade“

eliminiert wurden – also der konkrete Sicherheitsmaßstab für den konkreten Scope festgestellt wurde –, kann im nächsten Schritt die inhaltliche Auseinandersetzung des konkreten Bewertungsgegenstand mit den Anforderungen der Anlage 31b zum BMV-Ä erfolgen.

Dazu ist zu allen Anforderungselementen anzugeben und zu beschreiben, wie diese Anforderungen umgesetzt werden.

Den Kriterienkatalog mit den Anforderungselementen findet sich in Abs. 4. Darüber hinaus werden weiterführende Informationen und Vorgaben von der Programmeignerin vorgegeben und von den Zertifizierungsstellen zur einheitlichen Anwendbarkeit zur Verfügung gestellt.

Wichtig: Die Anforderungen beziehen sich stets auf den gesamten Bewertungsgegenstand und insb. auf die jeweils angegebenen Zielobjekte. Und zwar dann auf alle Zielobjekte.

Insgesamt müssen alle Informationen klar, präzise und eindeutig sein.

4. Der Kriterienkatalog „ips - Videosprechstunde - IT“

Der vorliegende Kriterienkatalog „ips - Videosprechstunde - IT“ enthält die folgenden Kriterien, die im Nachfolgenden im Detail dargelegt werden:

- P.1 Grundlagen
 - P.1.1 Verpflichtung zur Einhaltung der Sicherheit bei Behandelnden
 - P.1.2 Risikoanalyse
- P.2 Übertragung
 - P.2.1 Übertragung der Videosprechstunde
 - P.2.2 Authentifizierung
- P.3 Verschlüsselung
 - P.3.1 Transportverschlüsselung
 - P.3.2 Ende-zu-Ende-Verschlüsselung
- P.4 Absicherung der Inhalte
 - P.4.1 Absicherung der Inhalte der Videosprechstunde & Metadaten
 - P.4.2 Löschung
- P.5 Ausschluss schwerwiegender Sicherheitsrisiken

Alle Kriterien des vorliegenden Kriterienkatalogs sind wie folgt aufgebaut:

- eindeutige ID und Name des Anforderungselementes;
- Anforderung: hier findet sich die normative Anforderung dieses Anforderungselementes;
- Verweis Anlage 31b zum BMV-Ä: Verweis auf die (gesetzliche) Anforderung;
- Nachweise: hier findet sich ein Mindestsatz an Nachweisen, die der Kunde zur Verfügung stellt, um die Umsetzung nachzuweisen;
- Zielobjektkategorie: Zuordnung zu den relevanten Zielobjekten, vgl. Ausführungen in Abs. 3.1;
- Evaluierungsmethode: Vorgabe an das Evaluationsteam im Rahmen eines Zertifizierungsverfahrens.

4.1. P.1 Grundlagen

4.1.1. P.1.1 Verpflichtung zur Einhaltung der Sicherheit bei Behandelnden

Anforderung

Der Videodienstanbieter muss die Behandelnden oder behandelnden Institutionen schriftlich vertraglich verpflichten bei der Nutzung der Videosprechstunde im Hinblick auf die Sicherheit der Verarbeitung der Informationen (INFO) in seinen Räumlichkeiten und IT-Systemen zu gewährleisten, dass die erforderlichen technischen und organisatorischen Maßnahmen eingehalten werden. Der Videodienstanbieter muss sicherstellen, dass die Applikation erst nach Abschluss einer entsprechenden vertraglichen Regelung genutzt werden kann.

Verweis

§ 2 Abs. 1 Anlage BMV-Ä

Nachweise

Vertragliche Verpflichtung, AGB

Zur Verfügungstellung der Applikation

Prozess- und Verfahrensbeschreibung

Zielobjektkategorie

APPL

PRZ

INFO

Evaluierungsmethode

Inspektion für die Zielobjektkategorie APPL, INFO ergänzend analysiert das Evaluationsteam

- Vertragliche Verpflichtungen/AGB

Auditierung für die Zielobjektkategorie PRZ, ergänzend analysiert das Evaluationsteam

- abgeschlossene Verpflichtungen.

4.1.2. P.1.2 Risikoanalyse

Anforderung

Der Videodienstanbieter muss eine Risikoanalyse unter Betrachtung der Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität durchführen. Diese muss den „Signalisierungsserver“ als Vertrauensanker innerhalb der Videosprechstunde sowie die technischen und organisatorischen Maßnahmen zur Absicherung der Videosprechstunde adressieren. Die Risikoanalyse muss nachvollziehbar, korrekt und dokumentiert vorliegen und regelmäßig – mindestens jährlich – sowie anlassbezogen aktualisiert werden.

Verweis

§ 2 Abs. 2 und § 2 Abs. 3 Anlage BMV-Ä

Nachweise

Risikoanalyse

Zielobjektkategorie

PRZ

Evaluierungsmethode

Auditierung für die Zielobjektkategorie PRZ, ergänzend analysiert das Evaluationsteam

- Risikoanalyse

4.2. P.2 Übertragung

4.2.1. P.2.1 Übertragung der Videosprechstunde

Anforderung

Der Videodiensteanbieter muss nachweisen, dass die Übertragung der Inhalte der Videosprechstunde nach dem Stand der Technik geschützt ist.

Die Übertragung der Videosprechstunde soll über eine Peer-to-Peer-Verbindung zwischen Behandelnden und Patienten oder der Pflegekraft, ohne Nutzung eines zentralen Servers, erfolgen.

Erfolgt die Übertragung über eine Peer-to-Peer-Verbindung muss der Videodiensteanbieter nachweisen, dass für die Verbindung zwischen den Teilnehmenden eine Transportverschlüsselung, bspw. TLS und dTLS, nach dem Stand der Technik gem. [TR-02102-2] verwendet wird.

Bei einem Abweichen von einem Peer-to-Peer-Verfahren muss der Videodiensteanbieter nachweisen, dass er durch geeignete technische und organisatorische Maßnahmen ein angemessenes Schutzniveau gewährleistet. Hierbei darf die Erfüllung von der Anforderung an die Ende-zu-Ende-Verschlüsselung gemäß 4.3.2 nicht beeinträchtigt werden. Der Videodiensteanbieter muss zudem nachweisen, dass das durch das eingesetzte Verfahren bei einem Abweichen von Peer-to-Peer-Verfahren die Authentizität und die Übertragung der Daten nicht beeinträchtigt wird.

Verweis

§ 2 Abs. 2 Anlage BMV-Ä

Nachweise

Verfahrens- und Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibungen, Beschreibung der technischen Umsetzung der Implementierung der Videofunktion)

Netzplan

Architekturdiagramm

Kommunikationsdiagramm

Autorisierungskonzept

Zielobjektkategorie

IT

APPL

TV

PRZ

INFO

Evaluierungsmethode

Inspektion für die Zielobjektkategorie APPL, IT, INFO und TV. Ergänzend analysiert das Evaluationsteam

- Objektive Nachweise zur Umsetzung und Konfiguration der Übertragung

Inspektion durch das Evaluationsteam für Penetrationstests unter Anwendung des OWASP TOP 10 Testing Guide in der jeweils aktuellen Fassung, für die Zielobjektkategorie APPL, IT und TV, insbesondere wie obige Darlegung des Sachverhalts technisch umgesetzt wurde.

Auditierung für die Zielobjektkategorie PRZ (sofern vorliegend), ergänzend analysiert das Evaluationsteam

- Verfahrens- und Prozessbeschreibungen

4.2.2. P.2.2 Authentifizierung

Anforderung

Der Videodiensteanbieter muss gewährleisten, dass sich die Teilnehmenden gegenüber dem Signalisierungsserver authentifizieren.

Verweis

§ 2 Abs. 2 und § 2 Abs. 3 Anlage BMV-Ä

Nachweise

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibungen, Beschreibung der technischen Umsetzung der Implementierung der Videofunktion)

Netzplan

Architekturdiagramm

Kommunikationsdiagramm

Autorisierungskonzept

Zielobjektkategorie

IT

APPL

TV

INFO

Evaluierungsmethode

Inspektion für die Zielobjektkategorie APPL, IT, INFO und TV. Ergänzend analysiert das Evaluationsteam

- Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung
- Objektive Nachweise zur Umsetzung und Konfiguration

Inspektion durch das Evaluationsteam für Penetrationstests unter Anwendung des OWASP TOP 10 Testing Guide in der jeweils aktuellen Fassung, für die Zielobjektkategorie APPL, IT und TV, insbesondere wie obige Darlegung des Sachverhalts technisch umgesetzt wurde.

4.3. P.3 Verschlüsselung

4.3.1. P.3.1 Transportverschlüsselung

Der Videodienstanbieter muss entsprechend folgender Maßgaben verschlüsseln:

- Erfolgt die Übertragung über eine Peer-to-Peer-Verbindung muss der Videodienstanbieter nachweisen, dass für die Verbindung zwischen den Teilnehmenden eine Transportverschlüsselung, bspw. TLS und dTLS, nach dem Stand der Technik gem. [TR-02102-2] verwendet wird.
- Die Verbindung zu dem für den Verbindungsaufbau eingesetzte Signalisierungsserver zum Austausch der Metainformationen muss nach dem Stand der Technik gem. [TR-02102-2] in der aktuellen Fassung geschützt werden.
- Der Videodienstanbieter muss die Verbindung zu Signalisierungsservern, welche zum für den Verbindungsaufbau zum Austausch der Metadaten eingesetzt werden, nach dem Stand der Technik gem. [TR-02102-2] in der aktuellen Fassung transportverschlüsseln.
- Der Videodienstanbieter muss sämtliche Übertragungswege für Metadaten nach dem Stand der Technik gem. [TR-02102-2] transportverschlüsseln.

Verweis Anlage 31b zum BMV-Ä

§ 2 Abs. 2 und § 2 Abs. 3 Anlage BMV-Ä

Nachweise

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibungen, Beschreibung der technischen Umsetzung der Implementierung der Videofunktion)

Netzplan

Architekturdiagramm

Kommunikationsdiagramm

Autorisierungskonzept

Zielobjektkategorie

IT

APPL

TV

INFO

Evaluierungsmethode

Inspektion für die Zielobjektkategorie APPL, IT, INFO und TV. Ergänzend analysiert das Evaluationsteam

- Objektive Nachweise für Konfiguration

Inspektion durch das Evaluationsteam für Penetrationstests unter Anwendung des OWASP TOP 10 Testing Guide in der jeweils aktuellen Fassung, für die Zielobjektkategorie APPL, IT und TV, insbesondere wie obige Darlegung des Sachverhalts technisch umgesetzt wurde.

4.3.2. P.3.2 Ende-zu-Ende-Verschlüsselung

Anforderung

Der Videodiensteanbieter muss sicherstellen, dass ausgetauschte Video- und Audiodaten Ende-zu-Ende, nach dem Stand der Technik gem. [TR-02102] verschlüsselt werden.

Darüber hinaus muss der Videodiensteanbieter sicherstellen, dass, sofern vorhanden, sämtliche Funktionen zur Datenübermittlung, im Rahmen der Videosprechstunde, wie z.B. Chat oder Dateiaustausch, Ende-zu-Ende, nach dem Stand der Technik. [TR-02102-1] oder [TR-02102-2] in der jeweils aktuellen Fassung, verschlüsselt werden.

Verweis

§ 2 Abs. 3 Anlage BMV-Ä

Nachweise

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibungen, Beschreibung der technischen Umsetzung der Implementierung der Videofunktion)

Netzplan

Architekturdiagramm

Kommunikationsdiagramm

Autorisierungskonzept

Zielobjektkategorie

IT

APPL

TV

Evaluierungsmethode

Inspektion für die Zielobjektkategorie APPL, IT und TV. Ergänzend analysiert das Evaluationsteam

- Objektive Nachweise zur Konfiguration

Inspektion durch das Evaluationsteam für Penetrationstests unter Anwendung des OWASP TOP 10 Testing Guide in der jeweils aktuellen Fassung, für die Zielobjektkategorie APPL, IT und TV, insbesondere wie obige Darlegung des Sachverhalts technisch umgesetzt wurde.

4.4. P.4 Absicherung der Inhalte

4.4.1. P.4.1 Absicherung der Inhalte der Videosprechstunde & Metadaten

Anforderung

Der Videodiensteanbieter muss sicherstellen, dass die Inhalte der Videosprechstunde weder durch ihn noch Andere eingesehen oder gespeichert werden können. Er muss zudem gewährleisten, dass Protokollinformationen und Protokollierungseinrichtungen vor Manipulation und unbefugtem Zugriff geschützt sind.

Der Videodiensteanbieter muss sicherstellen, dass die Informationen (INFO) nicht weitergegeben werden.

Der Videodiensteanbieter muss ein Berechtigungskonzept dokumentiert haben, welches die Zugriffsmöglichkeiten auf die Videosprechstunde adressiert. Das Berechtigungskonzept muss nachvollziehbar, korrekt und dokumentiert vorliegen und regelmäßig – mindestens jährlich – sowie anlassbezogen aktualisiert werden.

Verweis Anlage 31b zum BMV-Ä

§ 2 Abs. 4 Anlage BMV-Ä

Nachweise

Darlegung des Sachverhalts mit Begründung

Verfahrens- und Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibungen, Löschkonzept, Berechtigungskonzept)

Objektive Nachweise (z.B. vergebene Berechtigungen)

Berechtigungskonzept

Netzplan

Architekturdiagramm

Kommunikationsdiagramm

Zielobjektkategorie

PRZ

IT

APPL

INFO

Evaluierungsmethode

Auditierung für die Zielobjektkategorie PRZ, ergänzend analysiert das Evaluationsteam

- Verfahrens- und Prozessbeschreibungen
- Berechtigungskonzept
- objektive Nachweise (z.B. vergebene Berechtigungen)

Inspektion für die Zielobjektkategorie APPL, IT. Ergänzend analysiert das Evaluationsteam

- Objektive Nachweise zur Konfiguration
- Inspektion durch das Evaluationsteam für Penetrationstests unter Anwendung des OWASP TOP 10 Testing Guide in der jeweils aktuellen Fassung, für die Zielobjektkategorie APPL, IT, INFO und TV, insbesondere wie obige Darlegung des Sachverhalts technisch umgesetzt wurde.

4.4.2. P.4.2 Löschung

Anforderung

Der Videodienstanbieter muss sicherstellen, dass die Metadaten/technischen Verbindungsdaten nach spätestens drei Monaten gelöscht werden und nur für die zur Abwicklung der Videosprechstunde notwendigen Abläufe genutzt werden. Der

Videodiensteanbieter muss ein Löschkonzept dokumentiert haben, welches die Löschung sämtlicher Informationen der Videosprechstunde adressiert. Das Löschkonzept muss nachvollziehbar, korrekt und dokumentiert vorliegen und regelmäßig – mindestens jährlich – sowie anlassbezogen aktualisiert werden.

Verweis Anlage 31b zum BMV-Ä

§ 2 Abs. 4 Anlage BMV-Ä

Nachweise

Darlegung des Sachverhalts mit Begründung

Verfahrens- und Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibungen, Löschkonzept, Berechtigungskonzept)

Objektive Nachweise über durchgeführte Löschungen

Löschkonzept

Zielobjektkategorie

PRZ

TV

IT

APPL

INFO

Evaluierungsmethode

Inspektion für die Zielobjektkategorie APPL, IT, TV und INFO. Ergänzend analysiert das Evaluationsteam

- Objektive Nachweise zur Konfiguration
- Löschkonzept

Auditierung für die Zielobjektkategorie PRZ ergänzend analysiert das Evaluationsteam

- Verfahrens- und Prozessbeschreibungen
- Berechtigungskonzept
- objektive Nachweise zu durchgeführten Löschungen / Löschprotokolle
- Löschkonzept

4.5. P.5 Ausschluss schwerwiegender Sicherheitsrisiken OWASP Top 10

Anforderung

Der Videodiensteanbieter muss gewährleisten, dass der Videodienst hinsichtlich der eingesetzten Applikationen (APPL) keine schwerwiegenden Sicherheitsrisiken aufweist. Hierzu muss der Videodiensteanbieter gewährleisten, dass die Beeinträchtigung des Videodienstes durch Risiken gemäß den aktuellen Fassungen der, für die Applikation (APPL) einschlägigen, OWASP Richtlinien (OWASP TOP 10 in der jeweils aktuellen Fassung bzw. OWASP Mobile Top 10) durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen ausgeschlossen ist.

Der Videodiensteanbieter muss nachweisen, dass der Videodienst hinsichtlich der eingesetzten Applikationen (APPL) regelmäßig – mindestens jedoch einmal jährlich – sowie anlassbezogen dahingehend überprüft wird, dass keine schwerwiegenden Sicherheitsrisiken vorliegen.

In dem Penetrationstest muss eine Bewertung des Schadenspotentials hinsichtlich der Beeinträchtigung der Gewährleistung der Schutzziele gemäß der OWASP-Risikobewertung (OWASP Risk Rating Methodology in der jeweils aktuellen Fassung) vornehmen. Der Penetrationstest darf zum Evaluierungszeitpunkt max. 3 Monate alt sein.

Der Videodiensteanbieter muss Prozesse aufrechterhalten, um umgehend Schwachstellen zu beheben.

Ein schwerwiegendes Sicherheitsrisiko betrifft eine Schwachstelle, nach der OWASP-Risikobewertung eine Schwachstelle, welche eine hohe Eintrittswahrscheinlichkeit aufweist und/oder zu umfangreichen Verlusten der Vertraulichkeit, Integrität und Verfügbarkeit der Daten oder Funktionen führt bzw. der Organisation oder Einzelpersonen, die die Anwendung nutzen, erheblichen Schaden zufügt. Ein solches Sicherheitsrisiko muss umgehend geschlossen werden und die Wirksamkeit der Gegenmaßnahmen muss im Rahmen eines Nachttests bestätigt werden.

Ein mittleres Sicherheitsrisiko bezieht sich auf Sicherheitslücken, welche eine moderate Eintrittswahrscheinlichkeit und/oder moderate Auswirkungen aufweisen. Weiterhin resultiert eine hohe Eintrittswahrscheinlichkeit mit geringen Auswirkungen sowie eine niedrige Eintrittswahrscheinlichkeit mit einem hohem Schadenspotential hinsichtlich der Auswirkungen ebenfalls in einem mittleren Risiko. Hierfür ist eine Schließung der entsprechenden Sicherheitslücken bis zum Ende der Evaluation unter Beschreibung der Maßnahmen erforderlich.

Ein niedriges Sicherheitsrisiko betrifft eine Schwachstelle, mit niedriger Eintrittswahrscheinlichkeit und moderaten Auswirkungen oder mit moderater Eintrittswahrscheinlichkeit und niedrigen Auswirkungen. Ein solches Sicherheitsrisiko mit einem Schadenspotential muss innerhalb einer Frist von 3 Monaten ab dem Zeitpunkt an dem der Videodiensteanbieter Kenntnis von der Schwachstelle erhält behoben werden. Ein solches Sicherheitsrisiko mit einem geringen Schadenspotential muss jedoch umgehend behoben werden sofern hieraus eine Beeinträchtigung der Gewährleistung der Schutzziele hervorgeht.

Verweis Anlage 31b zum BMV-Ä

§ 2 Abs. 5 Anlage BMV-Ä

Nachweise

Ergebnisse des Penetrationstests

Maßnahmenplan der die Behebung von gefundenen Schwachstellen beschreibt (mit Maßnahmen und Zeithorizont)

Verfahrens- und Prozessbeschreibungen

Objektive Nachweise für die Behebung von gefundenen Schwachstellen

Netzplan

Architekturdiagramm

Kommunikationsdiagramm

Autorisierungskonzept

Zielobjektkategorie

PRZ

APPL

IT

TV

INFO

Evaluierungsmethode

Inspektion unter Anwendung des OWASP TOP 10 Testing Guide in der jeweils aktuellen Fassung, für die Zielobjektkategorie APPL, IT, INFO und TV, insbesondere wie obige Darlegung des Sachverhalts technisch umgesetzt wurde. Ergänzend analysiert der Evaluator für Penetrationstest, ob gilt:

- Es liegen keine Schwachstellen mit schwerwiegendem Sicherheitsrisiko vor.

Ergänzend analysiert das Evaluationsteam

- Objektive Nachweise zur Umsetzung und Konfiguration

Auditierung für die Zielobjektkategorie PRZ ergänzend analysiert das Evaluationsteam

- Verfahrens- und Prozessbeschreibungen
- Verfahrens- und Prozessbeschreibungen zum Umgang mit Ergebnissen von Penetrationstests
- Maßnahmenplan der die Behebung von gefundenen Schwachstellen beschreibt (mit Maßnahmen und Zeithorizont)
- Objektive Nachweise für die Behebung von gefundenen Schwachstellen

5. Zertifizierungsprozess

In diesem Abschnitt wird der Zertifizierungsprozess zur Erlangung eines „ips - Videosprechstunde - IT“ -Zertifikates erläutert.

5.1. Übersicht

Der grundsätzliche Zertifizierungsprozess gestaltet sich wie folgt:

- Antrag: Ein Kunde bekundet Interesse an einer Zertifizierung und reicht ein Antragsformular mit den Eckdaten zum Geltungsbereich ein; antragsberechtigt für eine Zertifizierung ist der Videodienstanbieter;
- Aufwandskalkulation: Die Zertifizierungsstelle erstellt auf Grundlage des Antrags eine Aufwandschätzung und unterbreitet den Kunden ein Angebot;
- Beauftragung durch Kunden;
- Kunde stellt Referenzdokumentation zur Verfügung;
- Zertifizierungsstelle startet die Evaluierung:
 - Beauftragung des Evaluationsteams mit Prüfung der Unabhängigkeit des Evaluationsteam;
 - Begleitung des Evaluierungsverfahrens mit Abnahme der Berichte;
- Zertifizierung inkl. Zertifizierungsentscheidung;
- Veröffentlichung des Zertifikates;
- Zertifikatsbegleitung über die Laufzeit mit Überwachungstätigkeiten und ggf. Beendigung, Einschränkung, Aussetzung oder Zurückziehung der Zertifizierung.

5.2. Antrag

Der Antrag umfasst insbesondere die folgenden Informationen:

- Kunde:
 - exakte Angabe der antragstellenden Organisation;
 - Ansprechpartner;
- Geltungsbereich (Scope):
 - exakte Scope-Bezeichnung der Videosprechstunde; diese Bezeichnung wird abschließend typischerweise im Zertifikat aufgenommen;
- Details zum Geltungsbereich:
 - IT-Systeme (IT): Übersicht über eingesetzte IT-Systeme (Servern, Clients, Netzkomponenten, Datenbanken, Speichersystemen und Schnittstellen samt Netzstrukturplan), die für die IT-gestützte Verarbeitung erforderlich sind;
 - Applikationen (APPL): Übersicht über eingesetzte Applikationen – sowohl interne Anwendungen als auch von Extern verfügbare Anwendungen, wie etwa Webseiten oder Apps –, die für die Dienstleistung genutzt werden;
 - Anzahl Beschäftigte im Geltungsbereich;
 - bereits vorliegende Zertifizierungen;

- etwaige Beratungsdienstleistungen bzgl. des Geltungsbereiches in Anspruch genommen;
- allgemeine Informationen bezüglich des antragstellenden Kunden und der Videosprechstunde, die für den beantragten Zertifizierungsbereich relevant sind;
- Informationen bezüglich aller ausgegliederten Prozesse, die von den Kunden genutzt werden und die die Konformität mit den Anforderungen beeinflussen;
- erforderliche einzureichende Anlagen, z. B. die Ergebnisse eines Penetrationstests ggf. vorliegende Zertifizierungen (in Form der Zertifizierung und/oder Prüfbericht).

5.3. Angebot mit Kalkulation

Die Zertifizierungsstelle prüft, ob eine Zertifizierung gemäß Antrag durchgeführt werden kann. Die Zertifizierungsstelle muss hierbei sicherstellen, dass der Bewertungsgegenstand angemessen ist und die Videosprechstunde adressiert. Ferner muss sichergestellt werden, dass die Beschreibung des Bewertungsgegenstand unmissverständlich ist.

Die Aufwandskalkulation sieht für einzelne Tätigkeiten feste Minimalwerte vor und orientiert sich ferner an folgenden Faktoren:

- Anzahl der eingesetzten Applikationen im Scope.
- Bei der Aufwandskalkulation können auch gültige Zertifikate akkreditierter und anerkannter Stellen berücksichtigt werden.

Die Aufwandskalkulation orientiert sich an folgender Tabelle, wobei die nachfolgend beschriebenen Evaluierungsmethoden zum Einsatz kommen:

TÄTIGKEIT	AUFWAND	BEMERKUNG
Prüfung und Evaluierung	n Tage, mind. 6 Tage	Kalkulation orientiert sich an Art und Umfang des Geltungsbereiches sowie der anwendbaren Anforderungen des Kriterienkatalogs.
Vor- und Nachbereitung Dokumentation Projektmanagement	mind. 0,5 Tag	

Da bei Re-Zertifizierungsverfahren die Basisprüfung entfallen kann, sofern Scope-Beschreibung unverändert, kann sich der Aufwand hier entsprechend reduzieren; ferner sind hier etwaige inhaltliche Veränderungen bei der Kalkulation einzubeziehen.

Bei der Überwachung wird grob ein Drittel des Aufwands der Erst-Zertifizierung veranschlagt.

5.4. Referenzdokumentation der Kunden

Der Kunde verpflichtet sich, der Zertifizierungsstelle eine hinreichende Referenzdokumentation zur Verfügung zu stellen. Die Referenzdokumentation der Kunden umfasst die folgenden Dokumente:

- Scope-Beschreibung: exakte Beschreibung des Geltungsbereiches mit folgenden Informationen: technische Verfahren (TV), Informationen (INFO), Prozesse (PRZ) zur Realisierung der Videosprechstunde, Schnittstellen, IT-Infrastruktur (IT), Applikationen (APPL).
- Realisierungsbeschreibung: ausführliche Umsetzungsbeschreibung für alle Anforderungen. Die Realisierungsbeschreibung ist so ausführlich, dass die Umsetzung zu den relevanten Anforderungen eindeutig hervorgeht. Die Realisierungsbeschreibung ist die verbindliche Zusicherung der Kunden, wie er die Anforderungen des vorliegenden Kriteriums konkret umsetzt. Ein Verweis auf andere Dokumente ist möglich, die Darstellung muss aber eindeutig und leicht möglich sein.

Der Kunde verpflichtet sich, die Dokumente Scope-Beschreibung und Realisierungsbeschreibung laufend aktuell zu halten und für die Aktualität einen entsprechenden Prozess etabliert zu haben.

Ferner verpflichtet sich der Kunde, alle weiteren, für die Evaluierung und Zertifizierung benötigten Unterlagen und Nachweise vollständig zur Verfügung zu stellen; die erforderlichen Nachweise sind im Kriterienkatalog angegeben. Ferner verpflichtet sich der Kunde, die Evaluierung und Zertifizierung aktiv zu unterstützen und alle Zielobjekte zugänglich zu machen, die für die Prüfung erforderlich sind.

5.4.1. Scope-Beschreibung

Die Scope-Beschreibung ist in Abs. 3.1 erläutert.

Die Scope-Beschreibung muss von den Kunden rechtsverbindlich unterschrieben werden; sie stellt damit die Grundlage für die Evaluierung und Zertifizierung dar. Es wird eine Vorlage zur Verfügung gestellt werden.

5.4.2. Realisierungsbeschreibung

Die Realisierungsbeschreibung ist in Abs. 3.2 beschrieben.

Die Realisierungsbeschreibung muss von den Kunden rechtsverbindlich unterschrieben werden; es stellt damit als Zusicherung der Kunden die Grundlage für die Evaluierung und Zertifizierung dar. Es wird eine Vorlage zur Verfügung gestellt werden.

5.5. Evaluierungsprozess

Als Konformitätsbewertungstätigkeiten werden folgende Evaluierungsmethoden angewendet:

- Basisprüfung: Analyse der Referenzdokumentation der Kunden;
- Auditierung: Prüfung der Prozesse;
- Inspektion: Prüfung technisch geprägten Anforderungen und weiterer Aspekte des Kriterienkatalogs.

Die Evaluierung insgesamt soll als ein gemeinsames Verfahren durchgeführt werden, das alle o.g. Evaluierungsmethoden „umschließt“. Selbstverständlich können dabei

Einzelaspekte durch eine bestimmte Evaluierungsmethode und/oder einen bestimmten Evaluator, der beispielsweise über die erforderlichen Kompetenzen verfügt, separat evaluiert werden, beispielsweise können alle Anforderungen, die mit der Prüfung (rechtl.) evaluiert werden, in einem Block zusammengefasst evaluiert werden.

Die Evaluierung erfolgt gegen die Anforderungen des vorliegenden Kriterienkatalogs.

Es wird ein zwei-stufiger Evaluierungsprozess etabliert:

1. Basisprüfung;
2. Auditierung und Inspektion.

5.6. Stichprobenverfahren

Grundsätzlich ist jede Evaluierung eine Stichprobe; die Stichprobe muss repräsentativ sein.

5.7. Bewertungsschema

Im vorliegenden Konformitätsbewertungsprogramm wird das folgende Bewertungsschema durchgesetzt:

- 1: Anforderung erfüllt;
- 2: Anforderung grundsätzlich erfüllt, aber es gibt Verbesserungspotential;
- 3: Anforderung nicht erfüllt (Abweichung).

Zur anschließenden Zertifizierung sind keinerlei Abweichungen von den Anforderungen zulässig, d.h. vor Zertifikatserteilung müssen alle Anforderungen stets erfüllt sein; es dürfen also nur die Bewertungen 1 oder 2 auftreten. Eine Abweichung (Bewertung 3) kann zu keiner Zertifizierung führen.

5.8. Evaluierungsbericht

Das Evaluationsteam dokumentiert seine Tätigkeiten.

5.9. Anerkennung bestehender Zertifikate

Es können bereits vorliegende Zertifizierungen nach § 5 Abs. 2 S. 3 lit. a Anlage 31b BMV-Ä durch eine akkreditierte Zertifizierungsstelle, die bereits einen Teil des Zertifizierungsgegenstands abdeckt, als Teilevaluierung berücksichtigt werden.

Hierbei gilt: Die Zertifizierungsstelle ist weiterhin verpflichtet, die aktuelle Einhaltung der Anforderungen (der vorgelegten Zertifizierung) zumindest stichprobenartig zu überprüfen und zu bewerten.

Notwendig für eine solche Beachtung ist das Vorliegen eines vollständigen Zertifizierungsgutachtens oder von Informationen, die eine Bewertung der Zertifizierungstätigkeit und -ergebnisse ermöglicht. Die Ergebnisse müssen auf einem Zertifizierungsverfahren beruhen. Eine Zertifizierungsurkunde oder ähnliche Bescheinigungen über eine Zertifizierung sind hierbei nicht ausreichend. Dabei müssen die in 6.2.2 enthaltenen Anforderungen erfüllt sein. Ergeben sich bei einer solchen Prüfung Abweichungen von den Anforderungen, die von dem vorliegenden

Zertifizierungsprogramm festgelegt sind, oder sonstige Unregelmäßigkeiten, so ist die Evaluierung im Rahmen des laufenden Zertifizierungsverfahrens zu erweitern und ggf. auf den gesamten, bereits zertifizierten Gegenstand auszudehnen.

5.10. Zertifizierung

5.10.1. Zweistufiges Verfahren

Es wird ein klassisches zwei-stufiges Verfahren eingesetzt:

- Evaluierung durch das Evaluationsteam, das bei der Zertifizierungsstelle lizenziert ist;
- Zertifizierung.

5.10.2. Laufzeit

Das Zertifikat ist drei Jahre gültig und erfordert zur Aufrechterhaltung zwei jährliche Überwachungen.

5.10.3. Zertifikat

Das Zertifikat weist folgende Informationen auf und kann ferner um das ips - Videosprechstunde - IT-Logo ergänzt werden.

Die datenschutz cert GmbH bestätigt hiermit, dass das nachfolgend spezifizierte technische Verfahren:

Geltungsbereich:

[Bezeichnung EVG gemäß Produktbezeichnung des Anbieters] gemäß Anlage des Videoanbieters:

[Antragsteller]

<exakter Name und Anschrift des Kunden>

konform ist zu den Anforderungen an die Informationstechniksicherheit gemäß § 2 der Anlage 31b zum BMV-Ä.

Prüfgrundlagen

Konformitätsbewertungsprogramm zur Zertifizierung einer Videosprechstunde gem. § 5 Abs. 2 lit. a Anlage 31b zum Bundesmanteltarifvertrag - Ärzte SGB V („ips - Videosprechstunde - IT“), Version x.x

Regelwerk:

Bestimmungen zur Informationstechniksicherheit gemäß § 2 Anlage 31b zum Bundesmantelvertrag – Ärzte SGB V - ips - Videosprechstunde – IT“, Version x.x.

Fassung der Anlage 31b zum BMV-Ä:

Anlage 31b zum Bundesmantelvertrag-Ärzte (BMV-Ä) i.V.m. der Vereinbarung über die Anforderungen an die technischen Verfahren zur Videosprechstunde

*gemäß § 365 Absatz 1 SGB V vom 21. Oktober 2016 in der Fassung vom TT. Monat
JJJJ.*

Ips – Videosprechstunde - IT

Zertifikats-ID: DSC.xxx.xx.xxxx

Referenzdokument: Version vom tt.mm.jjjj

Abschluss der Evaluierung: tt.mm.jjjj

Zertifizierungsentscheidung: tt.mm.jjjj

Datum der Ausstellung:

Laufzeit bis: tt.mm.jjjj

Unterschrift Leiter Zertifizierungsstelle

Infos zur Zertifizierungsstelle (Name, Adresse, Kontaktdaten, Webseite)

Darüber hinaus werden als Anhang zum Zertifikat in Form eines Kurzgutachtens weitere Informationen bestätigt:

Zertifikatsdetails

Anhang zum Zertifikat mit Zertifikats-ID <ID>

zum Geltungsbereich:

- Kontaktdaten der Kunden: <xxx>
- Beschreibung der Videosprechstunde: <xxx>
- Referenzdokument: <Version 1.0, tt.mm.jjjj>

zur Evaluierung:

- Prüfverfahren, inklusive der Zertifizierung zugrundeliegender Kriterien (ggf. mit Versionsangabe): <xxx>
- Prüfergebnis: <xxx>
- eingebundenes Evaluationsteam: <xxx>

zur Zertifizierung:

- Informationen über die Erst-bzw. Re-Zertifizierung: <xxx>
- Angaben zu möglichen Überwachungstätigkeiten zur Aufrechterhaltung der Zertifizierung: <xxx>

5.10.4. Verzeichnis zertifizierter Videosprechstunden

Die Zertifizierungsstelle hält eine öffentlich verfügbare Zertifikatsliste vor, aus der hervorgeht:

- Kunde, Geltungsbereich, Regelwerk, Zert-ID, Gültigkeitsdauer, Link auf Zertifikat samt Anlage (Zertifikatsdetails)

5.11. Jährliche Überwachung

Es sind jährliche Überwachungen vorgesehen. Überwachungen erfolgen grundsätzlich analog zur Erst-Zertifizierung, wobei jedoch nur eine Auswahl der Kriterien zu evaluieren ist.

5.12. Re-Zertifizierung

Nach einer Laufzeit von 3 Jahren endet der Zertifikatszyklus, der über ein Re-Zertifizierungsverfahren erneut gestartet werden kann. Die Re-Evaluierung erfolgt analog zur Erst-Evaluierung mit dem Unterschied, dass die Basisprüfung entfallen kann, sofern Scope-Beschreibung unverändert ist; andernfalls wird eine Basisprüfung mit dem Schwerpunkt der Veränderungen durchgeführt.

5.13. Anlassbezogene Prüfungen

Darüber hinaus können anlassbezogene Prüfungen (Evaluierung aus besonderem Anlass) stattfinden:

- Erweiterung oder Änderung des Geltungsbereichs;
- kurzfristig angekündigte Evaluierungen.

5.14. Änderungen, die sich auf die Zertifizierung auswirken

Die Zertifizierungsstelle informiert ihre Kunden zeitnah über Änderungen am Zertifizierungsstandard und -anforderungen und wie in diesem Fall vergleichbare Evaluierungen durchgeführt werden (müssen).

Der Kunde ist ferner verpflichtet, signifikante tatsächliche oder rechtliche Änderungen am zertifizierten Bewertungsgegenstand unverzüglich der Zertifizierungsstelle anzuzeigen. Welche tatsächlichen oder rechtlichen Änderungen als signifikant einzustufen sind, erfolgt nach folgender Maßgabe:

- Es liegt eine Änderung hinsichtlich der Videosprechstunde mit Relevanz für die Erfüllung der Kriterien des § 2 Anlage 31b BMV-Ä vor,
- es liegt eine Änderung der Einsatzumgebung vor,
- es liegt eine Änderung der (rechtlichen) Rahmenbedingungen vor oder
- es liegt eine Änderung am Stand der Technik vor,

die relevant für die Zertifizierungsaussage sind. Dies liegt insbesondere dann vor, wenn die Änderung eine Aktualisierung der Scope-Beschreibung und/oder Realisierungsbeschreibung erforderlich macht.

Die Zertifizierungsstelle ist bei Hinweisen über solche Änderungen, die Einfluss auf die Konformitätsbewertungsaussage haben könnten, verpflichtet, den Sachverhalt innerhalb von 4 Wochen zu ermitteln und geeignete Maßnahmen zu ergreifen. Die Zertifizierungsstelle hat auch hier zu definieren, wie sichergestellt wird, dass in vergleichbaren Fällen vergleichbare Maßnahmen ergriffen werden.

Ziel dieser Maßnahmen ist, dass auch eine veränderte Videosprechstunde seinen zertifizierten Status behält. Damit die Zertifizierungsstelle das erteilte Zertifikat anpassen kann, sind folgende Tätigkeiten notwendig:

- Der Kunde legt eine aktualisierte Referenzdokumentation vor (Scope-Beschreibung, Realisierungsbeschreibung), aus der insb. die Veränderungen deutlich erkennbar sind.
- Der Kunde legt eine Impact-Analyse vor, aus der die Konsequenzen seiner Änderungen dargestellt werden.
- Der Kunde legt aktuelle objektive Nachweise vor, sofern erforderlich.
- Die Zertifizierungsstelle überprüft die Unterlagen und entscheidet, ob eine Evaluierung aus besonderem Anlass erforderlich ist, um die Einhaltung der Anforderungen feststellen zu können.

5.15. Beendigung, Einschränkung, Aussetzung oder Zurückziehung der Zertifizierung

Es müssen alle Anforderungen erfüllt werden; ein Umgang mit Nicht-Konformitäten ist nicht vorgesehen. Wird bei einer Überwachung eine Hauptabweichung (Nicht-Konformität der Bewertung 3) identifiziert, ergeben sich folgende Möglichkeiten:

- Weiterführung der Zertifizierung unter Bedingungen, die von der Zertifizierungsstelle festgelegt werden (z. B. dokumentierte Ursachenanalyse, autorisierte Maßnahmenplanung mit zeitnaher Behebungsfrist, zeitnahe Behebung, fristgemäße Einreichung einer vollständigen Dokumentation des Sachverhaltes, Begutachtung durch außerordentliche Evaluierung);
- Einschränkung des Geltungsbereichs der Zertifizierung, um eine nichtkonforme Videosprechstunde zu entfernen;
- Aussetzen der Zertifizierung vorbehaltlich der Abstellmaßnahmen durch den Kunden;
- Zurückziehung der Zertifizierung.

Wird der Geltungsbereich einer Zertifizierung eingeschränkt, müssen alle zertifizierungsrelevanten Unterlagen (inkl. Zertifikat und Zertifikatsliste) angepasst werden. Außerdem muss den Kunden der Sachverhalt und die Folgen für seine Werbung mit dem Zertifikat und Logo klar und eindeutig mitgeteilt werden.

Wird ein Zertifikat ausgesetzt, muss der Kunde darüber informiert werden, durch welche Maßnahmen er die Aussetzung beenden kann. Die Maßnahmen legt die Zertifizierungsstelle fest, die sind z.B. dokumentierte Ursachenanalyse, autorisierte Maßnahmenplanung mit zeitnaher Behebungsfrist, zeitnahe Behebung, fristgemäße Einreichung einer vollständigen Dokumentation des Sachverhaltes, Begutachtung durch außerordentliche Evaluierung.

6. Referenzen

[Anlage 31b]

Vereinbarung über die Anforderungen an die technischen Verfahren zur Videosprechstunde gemäß § 365 Absatz 1 SGB V vom 21. Oktober 2016 in der Fassung vom 13. November 2023 (Anlage 31b zum Bundesmantelvertrag - Ärzte).

7. Glossar

BEGRIFF	ERLÄUTERUNG
Applikationen (APPL)	Gesamtheit der Applikationen – sowohl interne Anwendungen als auch von Extern verfügbare Anwendungen, wie etwa Webseiten oder Apps –, die im Rahmen der Videosprechstunde genutzt werden
Bewertungsgegenstand	Gegenstand eines konkreten Zertifizierungsverfahrens synonym zu Bewertungsgegenstand, Scope, Target of Evaluation (ToE)
Evaluator	Prüfer, der eine Evaluierung durchführt
Evaluierung (engl. Evaluation)	Prüfung, durchgeführt durch: <ul style="list-style-type: none"> - Inspektion - Auditierung
Informationen	Informationen, die im Rahmen der Videosprechstunde verarbeitet werden (inkl. Primär- und Sekundärinformationen)
IT-Infrastruktur (IT)	Gesamtheit der IT-Systeme (Servern, Clients, Netzkomponenten, Datenbanken, Speichersystemen und Schnittstellen), die für die Videosprechstunde erforderlich sind, mit Netzstrukturplan
Kunde	eine Organisation, die als Anbieter einer Videosprechstunde ein Zertifikat anstrebt
Organisation	Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre Ziele zu erreichen. Anmerkung: Der Begriff Organisation umfasst unter anderem Einzelunternehmer, Gesellschaft, Konzern, Firma, Unternehmen, Behörde, Handelsgesellschaft, Verband, Wohltätigkeitsorganisation, Institution, oder Teile oder eine Kombination der genannten, ob eingetragen oder nicht, öffentlich oder privat. (lt. Definition aus ISO 9000)
Primärinformationen	Primärinformationen sind die Informationen, die im Kontext der Videosprechstunde zusätzlich zu den Primärinformationen anfallen, z.B. Protokolldaten, Verbindungsdaten, Autorisierungsdaten, Metadaten
Prozesse (PRZ)	Gesamtheit der fachlichen Tätigkeiten, die zur Realisierung der zu zertifizierenden Videosprechstunde benötigt werden
Sekundärinformationen	Primärinformationen sind die Informationen, die in der Videosprechstunde vornehmlich verarbeitet werden, z.B.
Zielobjektkategorien	Zielobjektkategorie charakterisiert den Scope: <ul style="list-style-type: none"> - Technische Verfahren (TV)

BEGRIFF	ERLÄUTERUNG
	<ul style="list-style-type: none">- Informationen (INFO)- IT-Infrastruktur (IT)- Applikationen (APPL)

8. datenschutz cert GmbH

Verantwortlich für den Zertifizierungsstandard „ips - Videosprechstunde - IT“ mit dem „Konformitätsbewertungsprogramm zur Zertifizierung einer Online-Videosprechstunde gem. § 5 Abs. 2 lit. a) Anlage 31b zum Bundesmanteltarifvertrag - Ärzte SGB V („ips - Videosprechstunde - IT“)“ sowie dem vorliegenden „Bestimmungen zur Informationstechniksicherheit gemäß § 2 Anlage 31b zum Bundesmantelvertrag - Ärzte SGB V - ips - Videosprechstunde - IT“ ist die datenschutz cert GmbH.

datenschutz cert GmbH

Standort Bremen

Konsul-Smidt-Str. 88a

28217 Bremen

Tel.: 0421 / 69 66 32 - 550

Fax: 0421 / 69 66 32 - 551

Niederlassung Offenbach/Main

Mainstr. 143

63065 Offenbach am Main

Tel.: 069 / 87 00 783 - 580

Fax: 069 / 87 00 783 - 581

E-Mail: office@datenschutz-cert.de

Internet: www.datenschutz-cert.de