Gemeinsame Policy für die Ausgabe der Heilberufsausweise

Zertifikatsrichtlinie Heilberufsausweis

Version: 2.2.0

18.06.2021

Bundesapothekerkammer

Bundesärztekammer

Bundespsychotherapeutenkammer

Bundeszahnärztekammer

gematik GmbH

Bezirksregierung Münster - eGBR

Impressum

Herausgeber **Bundesapothekerkammer**
Bundesärztekammer
Bundespsychotherapeutenkammer
Bundeszahnärztekammer
gematik GmbH
Bezirksregierung Münster - eGBR

Versionshistorie

Version	Datum	Änderungen	Editor
0.1	05.11.2004	Initiale Version	cs
0.9.1	06.05.2005	Übernahme der Bearbeitung durch die Herausgeber	ds
0.9.3	25.10.2005	Konsolidierung der Arbeitsfassung, Freigabe zur Veröffentlichung und Kommentierung	Bergen
0.9.3.w1	10.02.2006	Einarbeitung der Kommentare der Vertrauensdiensteanbieter und Herausgeber	Bergen
0.9.3.w2	**03.03.2006**	**Freigabe durch die Herausgabe zur erneuten Kommentierung**	**Bergen**
0.9.4.w1	15.06.2007	Einarbeitung der Kommentare der Herausgeber als Diskussionsgrundlage für den 04.07.2007	Bergen
0.9.4.w2	19.05.2008	Redaktionelle Komplettüberarbeitung: (Durchgängige Seitenzahl; Umstrukturierung einiger Kapitel; Neue Begriffsdefinition der Rollen; Singularform der Beziehungen zwischen den Rollen; Karte heißt jetzt Ausweis; Zertifikatsabkürzungen eingeführt; Verkürzung des Literaturverzeichnis; Präzisierung zwischen ausgeben und ausstellen; Präzisierung weiterer Sachverhalte) Inhaltliche Anpassungen: (Klärung der Zuständigkeiten zwischen HPC-Herausgeber und Policy-Herausgeber; Informationspflicht des ZDA ggü. HPC-Herausgeber bei Zertifikatsausstellung und -sperrung)	Bergen
0.9.5	27.04.2009	Abstimmung durch die HPC-Herausgeber	Bergen
0.9.6	12.05.2009	Fassung zur Kommentierung durch die ZDA (keine Kommentare eingegangen)	Bergen
1.0.0	**08.06.2009**	**Freigabe durch die Herausgeber**	**Bergen**
1.0.5	30.07.2012 04.10.2012 **06.11.2012**	Anpassungen gemäß Kryptokonzept der Gematik, online Identifizierung mit ePA möglich, editorische Korrekturen, Umgebungsanforderungen für AUT/ENC, neue OID, **Freigabe durch die Herausgeber**	Raptis
2.0.0	**24.09.2018**	Anpassungen auf eIDAS und VDG, Begriffsanpassung HPC → HBA,	Schladweiler, Gottsmann

		Anpassungen an aktuelle Gegebenheiten, Löschen der Abschnitte zu Haftung und Verpflichtungen der Überprüfer, **Freigabe durch die Herausgeber**	
2.1.0	**28.05.2021**	Aufnahme der gematik GmbH als Herausgeber Anpassung an die geänderten gesetzlichen Grundlagen gemäß SGB V **Freigabe durch die Herausgeber**	gematik
2.2.0	**18.06.2021**	Aufnahme der Bezirksregierung Münster, eGBR - elektronisches Gesundheitsberuferegister als Herausgeber **Freigabe durch die Herausgeber**	eGBR/gematik

Veröffentlichte Versionen sind **fett** markiert.

Inhaltsverzeichnis

1 Einleitung und Begriffsbestimmung

In dieser gemeinsamen Zertifikatsrichtlinie (*Certificate Policy – CP*) wird ein Regelwerk mit Sicherheitsanforderungen zur Ausstellung von Zertifikaten und der Ausgabe elektronischer Heilberufsausweise (HBA), die insbesondere zur sicheren Erzeugung elektronischer Signaturen verwendet werden, definiert. Als Signaturerstellungseinheit und Trägermedium für die Schlüssel und die ausgegebenen Zertifikate wird eine Chipkarte verwendet, welche dem Anhang II der „VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG“, im Folgenden in der Kurzform „eIDAS“ benannt, entspricht. Ausgestellt werden dabei neben den X.509-Zertifikaten auch *Card Verifiable Certificates* (CV-Zertifikate), wobei CV-Zertifikate in ISO/IEC 7816-8 beschrieben sind.

Die ausgestellten X.509- und CV-Zertifikate der Ausweisinhaber decken zusammen die Anwendungsgebiete Signaturerstellung (Unterschrift), Authentifizierung sowie Ver- bzw. Entschlüsselung sowie den CV-basierten Kartenzugriff auf elektronische Gesundheitskarten ab. Diese Policy behandelt nur Aspekte der X.509-Zertifikate, die CV-Zertifikate sind nicht Gegenstand dieser Policy.

Die qualifizierten Zertifikate erfüllen die Anforderungen nach eIDAS bzw. dem „Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG“, im Folgenden stets in der Kurzform Vertrauensdienstegesetz (VDG) genannt, und sind somit für die sichere Erzeugung qualifizierter elektronischer Signaturen geeignet. Diese Anforderung ist durch § 291a [SGB V] begründet.

Gemäß Kap. III Abschnitt 4 Art. 28 Abs. (3) eIDAS können zusätzlich fakultative Attribute des Ausweisinhabers (bspw. die Berufsgruppeneigenschaft) bei entsprechender Bestätigung durch die zuständige Stelle in den Zertifikaten verankert werden.

1.1 Rechtliche Einordnung

Die jeweils aktuell gültigen Regelungen und Vorgaben nach eIDAS, des VDG sowie des *Sozialgesetzbuches – Fünftes Buch* – [SGB V], des *Bundesdatenschutzgesetzes* [BDSG] und der EU-Datenschutzgrundverordnung [DSGVO] finden Anwendung und sind dieser Policy übergeordnet.

Die Kartenherausgeber werden durch § 340 [SGB V], die Heilberufsgesetze der Länder und die jeweiligen Spitzenorganisationen der Leistungserbringer näher bestimmt.

1.2 Dokumentenidentifikation

Dokumententyp:	Certificate Policy
Name dieses Dokumentes:	Gemeinsame Policy für die Ausgabe der Heilberufsausweise
Kurzname dieses Dokumentes:	Zertifikatsrichtlinie HBA
Referenz für dieses Dokument:	[CP-HBA]
Version:	2.2.0 vom 18.06.2021
Object Identifier:	1.2.276.0.76.4.145 {policy-hba-010005-cp}

1.3 Begriffsdefinition

Es wird grundlegend zwischen dem *Policy-Herausgeber*, dem *Kartenherausgeber*, dem *Antragsteller*, dem *Ausweisinhaber*, dem *Anwender,* und dem *Anbieter* als Akteur unterschieden. Dabei stehen diese in einem bestimmten Verhältnis zueinander: Ein Antragsteller beantragt bei einem Anbieter die Ausstellung von Zertifikaten. Ein Kartenherausgeber lässt einen (oder mehrere) Anbieter in seinem Bereich zu. Ein Policy-Herausgeber koordiniert die bundesweit einheitlichen Vorgaben der Kartenherausgeber seines Sektors. Die Policy-Herausgeber koordinieren sich untereinander auf Bundesebene.

Es existieren damit mehrere Policy-Herausgeber, mehrere Anbieter und mehrere Kartenherausgeber. Für einen Antragsteller ist jedoch immer nur ein bestimmter Kartenherausgeber zuständig, der wiederum nur einem bestimmten Policy-Herausgeber zugeordnet ist. Für einen Kartenherausgeber können mehrere Anbieter - als Verwaltungshelfer - tätig sein. Sofern der Antragsteller einen Heilberufsausweis erhalten hat, wird er als Ausweisinhaber bezeichnet.

Die Ausstellung der Zertifikate eines Heilberufsausweises beantragt der Antragsteller bei einem Anbieter, den er sich unter den vom jeweiligen Kartenherausgeber zugelassenen Anbietern frei auswählen kann. Der Text dieser Policy orientiert sich daher aus Sicht des Antragstellers an der Singularform der verschiedenen Parteien, auch wenn z.B. mehrere Anbieter oder Kartenherausgeber parallel (unabhängig) zueinander existieren. Sollte eine Aufgabe durch mehrere bzw. alle z. B. Policy-Herausgeber in Zusammenarbeit erfüllt werden, wird dies besonders kenntlich gemacht.

Es werden folgende Rollen und Begriffe definiert

- Der **Policy-Herausgeber** im Sinne dieser Policy entspricht einem der Herausgeber dieses Dokumentes. Die Gesamtheit aller Policy-Herausgeber ist für die Herausgabe dieser Policy verantwortlich. Im Impressum sind die Policy-Herausgeber unter Herausgeber aufgeführt. Die Policy-Herausgeber koordinieren die bundesweiten Vorgaben der ihnen jeweils zugeordneten Kartenherausgeber.

- Der **Kartenherausgeber** im Sinne dieser Policy ist eine für die Ausgabe eines Heilberufsausweises zuständige Stelle gemäß § 340 [SGB V] (i.d.R. sind das die Länderberufskammern). Ein Kartenherausgeber gibt den Heilberufsausweis nur für einen bestimmten Kreis an Antragstellern heraus und bedient sich dabei der Hilfe eines oder mehrerer Anbieter. Diese Zusammenarbeit ist vertraglich vereinbart.

- Der **Antragsteller** im Sinne dieser Policy ist eine natürliche Person, die einen HBA nach dieser Policy bei einem für ihn zuständigen Kartenherausgeber bzw. Anbieter beantragt. Mit Besitz eines HBAs ergeben sich im Sinne der vorliegenden Policy folgende zusätzliche Rollen für den Antragsteller:

    - Der **Ausweisinhaber** im Sinne dieser Policy ist eine natürliche Person, die einen nach dieser Policy ausgegebenen Heilberufsausweis erhält und für dessen Verwendung alleinig verantwortlich ist. Aufgrund der persönlichen Bindung sind Ausweisinhaber, Zertifikatsinhaber und Antragsteller identisch.

    - Der **Zertifikatsinhaber** im Sinne dieser Policy ist die natürliche Person, auf die ein Zertifikat gemäß dieser Policy ausgestellt wurde und in der alleinigen Kontrolle über den diesem Zertifikat zugeordneten privaten Schlüssel ist.

    - Der **Anwender** im Sinne dieser Policy ist eine natürliche Person, die ein Zertifikat und den damit verbundenen privaten Schlüssel, welche nach dieser Policy ausgestellt wurden, verwendet. Der Anwender ist immer auch der Ausweisinhaber und Zertifikatsinhaber.

- Der **Überprüfer** im Sinne dieser Policy ist eine Person, die ein signiertes Element und insbesondere das verwendete Zertifikat überprüft.

- Der **Anbieter** im Sinne dieser Policy ist ein qualifizierter Vertrauensdiensteanbieter (VDA) nach [eIDAS], der für einen Kartenherausgeber tätig ist und Zertifikate nach dieser Policy ausstellt. Ein Anbieter kann sich auch eines qualifizierten Vertrauensdiensteanbieters bedienen. In diesem Fall sorgt der Anbieter dafür, dass die Rechte und Pflichten, die durch [eIDAS] geregelt sind, auch für diese Vertragskonstellation gewährleistet werden. Ein Anbieter kann für mehrere Kartenherausgeber, auch unterschiedlicher Sektoren, tätig sein.

- Der **Heilberufsausweis** im Sinne dieser Policy ist eine Chipkarte, die X.509-Zertifikate enthält, die nach dieser Policy ausgestellt wurden. Die Zertifikate des Heilberufsausweises bilden hierbei die kryptografische Identität einer Person in der elektronischen Welt ab. Die Nutzung der privaten Schlüssel eines Heilberufsausweises sind nur nach vorheriger und erfolgreicher PIN-Eingabe möglich.

- Ein **Endnutzerzertifikat** ist ein Zertifikat, das zu einem im Heilberufsausweis gespeicherten privaten Schlüssel gehört und auf den Ausweisinhaber als Zertifikatsinhaber ausgestellt ist.

1.4 Organisatorisches

Nur die Policy-Herausgeber gemeinsam haben die Entscheidungsbefugnis über die Inhalte dieser Policy. Sie diskutieren alle Änderungen an der Policy im Vorfeld mit den entsprechenden VDA und legen gemeinsam Migrationsfristen fest.

1.5 Übereinstimmung des Object Identifier

Der in Kapitel 1.2 aufgeführte *Object Identifier* (OID) wird nur für die Erstellung von Zertifikaten gemäß dieser Policy verwendet und wird in das jeweilige Zertifikat (in die Extension c*ertificatePolicies*) gemäß [gemSpec_PKI] aufgenommen.

1.6 Aufteilung der Kapitel

Die nachfolgenden Kapitel dienen insbesondere dazu, die Mindestanforderungen an die für Authentifizierung und Ver- und Entschlüsselung benötigten Zertifikate zu definieren. Für qualifizierte Zertifikate bestehen zusätzlich weitergehende Anforderungen aus [eIDAS] und [VDG].

In Kapitel 2 werden die Verpflichtungen beschrieben, denen die einzelnen Rollen unterworfen sind.

In Kapitel 3 werden die Vorgaben für einen Anbieter festgelegt, nach denen dieser seine Vertrauensdienstleistung zu erfüllen hat. Implizit werden dabei Vorgaben an den Antragsprozess und die Ausweisinhaber getroffen.

In Kapitel 4 werden als Anhang A die in diesem Dokument verwendeten Verzeichnisse aufgeführt.

In Kapitel 5 werden als Anlage B die Beziehungen zwischen den Policy-Herausgebern und den Kartenherausgebern informativ aufgeführt.

2 Verpflichtungen

In diesem Kapitel werden die Verpflichtungen geklärt.

2.1 Verpflichtungen des Policy-Herausgebers und des Kartenherausgebers

Der Policy-Herausgeber ist für die Einhaltung der in dieser Policy aufgestellten Richtlinien in seinem jeweiligen Sektor verantwortlich.

Der Kartenherausgeber hat die Pflicht, seinerseits verwalteten Antragstellern die Beantragung eines Heilberufsausweises bei jedem Anbieter, der für seinen Sektor zugelassen ist, zu ermöglichen.

2.2 Verpflichtungen des Anbieters bzw. dem jeweils beauftragten VDA

Der Anbieter bzw. der vom Anbieter beauftragte VDA ist verpflichtet, seine Vertrauensdienstleistungen gemäß dieser Zertifikatsrichtlinie (*Certificate Policy* – CP) sowie seinem *Certification Practice Statement* (CPS) anzubieten und auszuführen. Dies dokumentiert er gemäß Kapitel 1.5 unter anderem durch die Aufnahme der in Kapitel 1.2 angegebenen OID in die Endnutzerzertifikate.

Der Gültigkeitszeitraum der X.509-Zertifikate für Authentifizierung (C.HP.AUT) und Verschlüsselung (C.HP.ENC) soll den Gültigkeitszeitraum ihrer Aussteller-Zertifikate (CA- und Root-Zertifikate) nicht übersteigen.

Die Gültigkeitszeiträume aller Zertifikate eines Ausweises sollen grundsätzlich gleichzeitig enden. Im Falle eines Algorithmenwechsels sind unterschiedliche Gültigkeitszeiträume bei unterschiedlichen Algorithmen zulässig. Bei Sperrungen, bspw. nach Verlust oder im Falle des Entzuges der Berufserlaubnis bzw. Approbation, werden stets sämtliche (sperrbaren) Zertifikate eines Ausweises gemeinsam gesperrt.

Der Anbieter muss entsprechend der Regelungen des §13 [VDG] die Antragsteller über Sicherheitsmaßnahmen und Rechtswirkungen unterrichten.

2.3 Verpflichtungen des Antragstellers, des Ausweisinhabers und des Anwenders

Der Antragsteller wird vertraglich zur Einhaltung der nachfolgend aufgeführten Verpflichtungen im Rahmen des Registrierungsprozesses (siehe dazu auch Kapitel 3.3.2) verpflichtet. Das Akzeptieren der Vertragsbedingungen wird durch den Anbieter dokumentiert.

Aufgrund der persönlichen Bindung sind beim Heilberufsausweis der Antragsteller, der Ausweisinhaber und der Anwender identisch.

Die Verpflichtungen beinhalten insbesondere:

a. Der Antragsteller macht korrekte, wahrheitsgetreue und vollständige Angaben zu den benötigten Informationen. Dies gilt insbesondere für den Registrierungsprozess.

b. Der Ausweisinhaber ergreift die notwendigen Vorsichtsmaßnahmen, um einen unbefugten Einsatz seiner privaten Schlüssel zu verhindern. Nach Ablauf des Gültigkeitszeitraums oder nach Sperrung der Karte darf er die privaten Schlüssel nicht mehr nutzen. Er muss den Heilberufsausweis sicher vernichten bzw. unbrauchbar machen (beispielsweise durch das physische Zerstören des Chips des HBAs).

c. Der Ausweisinhaber hat den zuständigen Anbieter umgehend zu informieren, wenn

   - der Heilberufsausweis nicht mehr unter seiner alleinigen Kontrolle steht,
   - der begründete Verdacht auf eine Kompromittierung besteht
   - sowie wesentliche Informationen im Zertifikat fehlerhaft sind oder sich geändert haben (Name, Berufsgruppenattribut).

   (Der Anbieter ist wiederum verpflichtet, bei einer Sperrung auch den Kartenherausgeber zu informieren. Näheres dazu regelt Kapitel 3.3.7)

d. Der Anwender nutzt die ausgestellten Schlüssel bzw. Zertifikate nur für die jeweils vorgesehenen Anwendungsbereiche:

Anwendungsbereich	**Schlüsselpaar bzw. Zertifikat**
Qualifizierte elektronische Signatur	**C.HP.QES**
Authentifizierung	**C.HP.AUT**
Ver- bzw. Entschlüsselung	**C.HP.ENC**

Tabelle 1: Anwendungsbereiche der Schlüsselpaare und Zertifikate

   Insbesondere ist das qualifizierte Zertifikat ausschließlich für qualifizierte elektronische Signaturen im Sinne der Nicht-Abstreitbarkeit (non-repudiation bzw. content commitment) einzusetzen.

e. Der Anwender berücksichtigt die Anforderungen an die Einsatzumgebung, die der Anbieter für den Einsatz der Zertifikate definiert.

3 Anforderungen an die Erbringung von Vertrauensdiensten

Es werden die Anforderungen an die Erbringung von Vertrauensdiensten (z. B. das Ausstellen von Zertifikaten) festgelegt. Die nachfolgend beschriebenen Prozesse erfüllen insbesondere die Vorgaben aus [eIDAS] und [VDG] sowie [gemSpec_PKI].

3.1 Certification Practice Statement (CPS)

Die Prozesse und Verfahren zur Einhaltung und Erfüllung der in der Policy aufgeführten Anforderungen werden in einem von dem VDA erstellten CPS festgelegt und den jeweiligen Policy-Herausgebern erläutert.

Anwender-relevante Änderungen an dem CPS werden frühzeitig durch den VDA veröffentlicht.

Sämtliche weiteren Anforderungen sind durch den VDA ebenfalls in seinem Certification Practice Statement (CPS) aufzunehmen.

3.2 Verwaltung von Schlüsseln zur Erbringung von Vertrauensdiensten

Die Anforderungen aus [eIDAS] und [VDG] an Schlüssel für Zertifikate sowohl der Certificate Authority (CA) als auch der Anwender sind einzuhalten.

In den nachfolgenden Unterabschnitten werden daher nur Anforderungen an die weiteren Schlüssel (bspw. CA-Schlüssel für Authentifizierung bzw. Ver- und Entschlüsselung) als Mindestanforderung aufgeführt.

3.2.1 Erzeugung der CA-Schlüssel

Die Generierung der weiteren CA-Schlüssel (nach Kapitel 3.2) erfolgt nur durch entsprechend autorisiertes Personal in einer physisch gesicherten Umgebung. Zudem wird mindestens das Vier-Augen-Prinzip angewendet. Die verwendeten Algorithmen und Schlüssellängen erfüllen dabei die Vorgaben aus [gemSpec_PKI].

CA-Schlüssel für die Ausstellung der Endnutzerzertifikate C.HP.ENC und C.HP.AUT müssen eine vergleichbare Sicherheit wie die CA-Schlüssel für qualifizierte Signaturzertifikate (z. B. C.HP.QES) bieten.

> Maßgeblich sind die Vorgaben bzgl. verwendbarer kryptographischer Algorithmen aus dem Dokument [gemSpec_Krypt].

3.2.2 Speicherung und Backup von CA-Schlüsseln

Der VDA sorgt für die Geheimhaltung und Integrität der privaten CA-Schlüssel. Ein optionales Backup ist unter Einhaltung mindestens derselben Anforderungen wie für den privaten Originalschlüssel möglich.

3.2.3 Verteilung und Veröffentlichung der öffentlichen CA-Schlüssel

Der VDA gewährleistet die Authentizität und Integrität der von ihm erzeugten und verwalteten öffentlichen Schlüssel bei der Verteilung. Hierfür werden neben den CA-Zertifikaten das dazugehörige Root-Zertifikat sowie die zugehörigen Fingerprints zur Überprüfung veröffentlicht.

3.2.4 Verteilung und Veröffentlichung der privaten CA-Schlüssel

Der VDA hat sicherzustellen, dass seine privaten CA-Schlüssel weder verteilt noch offen gelegt werden.

3.2.5 Verwendungszweck der CA-Schlüssel

Private CA-Schlüssel dürfen u.a. für die Ausstellung von Zertifikaten gemäß dieser Policy eingesetzt werden.

Die Verwendung findet nur in physisch abgesicherten Räumlichkeiten durch autorisiertes Personal und mindestens unter der Anwendung des Vier-Augen-Prinzips gemäß dem im CPS oder Sicherheitskonzept des VDA definierten Rollenkonzept statt.

Benötigte Anwendungsbereiche diesbezüglich sind:

Anwendungsbereich	**Schlüssel bzw. Zertifikat**
Ausstellung der Zertifikate C.HP.QES	C.CA.QES
Ausstellung der Zertifikate C.HP.AUT	C.CA.AUT
Ausstellung der Zertifikate C.HP.ENC	C.CA.ENC

Tabelle 2: Anwendungsbereich der Schlüssel und Zertifikate der CA

Die privaten CA-Schlüssel dürfen für die o.g. Anwendungsbereiche benutzt werden. Die Schlüsselpaare C.CA.AUT und C.CA.ENC dürfen identisch sein.

3.2.6 Ende des Gültigkeitszeitraums von CA-Schlüsseln

Mit Ablauf des Gültigkeitszeitraums kann ein neues Zertifikat für den CA-Schlüssel erstellt werden, wenn die empfohlenen Algorithmen und Schlüssellängen dies noch erlauben. Ist

dies nicht der Fall, werden neue CA-Schlüssel nach den dann gültigen Vorgaben gemäß Kapitel 3.2.1 generiert. Ein Einsatz über den Gültigkeitszeitraum hinaus ist nicht gestattet.

CA-Zertifikate werden gesperrt, wenn die zugrunde liegenden Algorithmen und Schlüssellängen gemäß Kapitel 3.2.1 nicht mehr zugelassen sind.

3.2.7 Verwaltung und Lebenszyklen der Hardware Security Module für die Zertifizierung

Seitens des VDA darf ein Hardware Security Module (HSM) eingesetzt werden, sofern die gesetzlichen Anforderungen dies ermöglichen.

Die Hardware Security Module für die Zertifizierung unterliegen während ihres gesamten Lebenszyklus folgenden Sicherheitsmaßnahmen:

a. Alle Arbeiten an einem HSM werden nach dem Vier-Augen-Prinzip und nur von autorisiertem Personal durchgeführt.

b. Bei der Inbetriebnahme eines HSM erfolgt eine umfassende Überprüfung der korrekten Funktionsweise.

c. Vor Außerbetriebnahme eines HSM werden alle enthaltenen privaten Schlüssel gelöscht.

Die genannten Maßnahmen werden von dem VDA in seinem CPS beschrieben.

3.2.8 Erzeugung der Schlüssel für den Heilberufsausweis

Die Schlüsselgenerierung für die Anwender unterliegt nachfolgenden Anforderungen, durch welche die Geheimhaltung und Sicherheit gewährleistet wird:

a. Die in [gemSpec_PKI] sowie in [gemSpec_Krypt] genannten Anforderungen an Schlüssellänge und verwendete Algorithmen für die Schlüsselpaare für Verschlüsselung oder Authentifizierung sind einzuhalten. Darüber hinaus gelten die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik gemäß [VDG].

b. Die Schlüsselpaare der Zertifikate für Authentifizierung (C.HP.AUT) und Verschlüsselung (C.HP.ENC) des HBAs werden innerhalb der sicheren Signaturerstellungseinheit selbst erzeugt bzw. durch vergleichbare Verfahren, soweit die Sicherheit nicht reduziert wird, außerhalb der Signaturerstellungseinheit erzeugt und sicher in die Karten eingebracht. Die privaten Schlüssel können aus der Signaturerstellungseinheit nicht ausgelesen werden. Entsprechendes gilt für das Schlüsselpaar des Zertifikates für die qualifizierte Signatur (C.HP.QES), für das weitere rechtliche Auflagen gelten können.

3.2.9 Sicherheit der Heilberufsausweise

Die Sicherheitsanforderungen an Transport, Produktion und Auslieferung des Heilberufsausweises durch den VDA bzw. im Auftrag des VDA an den Antragsteller sind regelmäßig hinsichtlich ihrer Konformität zum Sicherheitskonzept des VDA durch eine Konformitätsbewertungsstelle gemäß [eIDAS] zu überprüfen.

3.2.10 Aufbringung weiterer Anwendungen

Applikationsfremde Daten oder weitere, über die in [gemSpec_PKI] beschriebenen hinausgehende, Anwendungen dürfen nur nach ausdrücklicher Genehmigung durch den Policy-Herausgeber nutzbar gemacht werden.

3.3 Lebenszyklus der Endnutzerzertifikate des HBAs

Im Folgenden wird der Lebenszyklus der Zertifikate des Antragstellers (Endnutzerzertifikate) beschrieben, die gemäß dieser Policy ausgestellt werden.

3.3.1 Bekanntmachung der Vertragsbedingungen

Der Policy- bzw. Kartenherausgeber stellt durch Veröffentlichung für die Antragsteller insbesondere die folgenden Dokumente zur Verfügung:

- Diese Certificate Policy (CP),
- eine Liste mit den Anbietern, die seinen Anforderungen genügen (siehe auch Kapitel 2.1).

Der Anbieter ist für die Veröffentlichung seiner allgemeinen Vertragsbedingungen verantwortlich und muss diese dem Antragsteller zugänglich machen.

3.3.2 Registrierung des Antragstellers

Der Ablauf während der Registrierung des Antragstellers enthält mindestens folgende Kernpunkte:

a. Identifizierung des Antragstellers,

b. Überprüfung der Antragsdaten,

c. Bestätigung des Berufsgruppenattributs,

d. Produktionsfreigabe durch den Kartenherausgeber.

3.3.2.1 Standardablauf und Identifizierung

Der Antrag auf einen Heilberufsausweis enthält auch einen Antrag auf Ausstellung von Zertifikaten und muss durch den Antragsteller rechtsverbindlich unterschrieben werden. Dies kann entweder handschriftlich oder elektronisch, unter Nutzung einer gültigen, qualifizierten Signatur, die dem Antragsteller zugeordnet ist, erfolgen.

Die Identifikation und Registrierung eines Antragstellers erfolgt gemäß den Vorgaben aus [eIDAS] und [VDG] für qualifizierte elektronische Zertifikate.

Dabei gelten insbesondere die nachfolgenden Punkte:

a. Dem Antragsteller werden vom Anbieter neben den erforderlichen Formularen auch die Rechtsbelehrung, die Unterrichtungsunterlagen, die Allgemeinen Geschäftsbedingungen, sowie Merkblätter und alle weiteren Bestimmungen zur Zertifikatsnutzung verfügbar gemacht.

b. Der Antrag auf Ausstellung eines Zertifikats muss mindestens den vollständigen Namen, die aktuelle Anschrift sowie Geburtsdatum und -ort des Antragstellers enthalten. Insbesondere müssen die Angaben geeignet sein, die X.509-Zertifikate des Heilberufsausweises gemäß [gemSpec_PKI] zweifelsfrei zu befüllen.

c. Der Antrag ist vom Antragsteller auf die Korrektheit der gemachten Angaben hin zu überprüfen und anschließend rechtsgültig zu unterschreiben.

d. Der Antragsteller ist durch einen amtlichen Lichtbildausweis oder Dokumente mit gleichwertiger Sicherheit eindeutig zu identifizieren. Bei der Identifizierung muss der Antragsteller persönlich anwesend sein. Alternativ kann die Identifizierung mittels der eID-Funktion des Personalausweises oder anderen onlinebasierten Identifizierungsvarianten, sofern diese die für qualifizierte Zertifikate sicherheitstechnisch und gemäß den Anforderungen des Abschnitt III Artikel 24 [eIDAS] sowie Teil 2 §11 [VDG] geeignet sind, durchgeführt werden.

e. Im Rahmen der Antragsprüfung ist eine Überprüfung der Berechtigung der Antragstellung notwendig. Hierzu hat der Antragsteller ggf. zusätzliche Dokumente vorzulegen, die durch den Kartenherausgeber gefordert werden.

f. Im Verlauf des Registrierungsprozesses hat der Antragsteller unter anderem folgende Punkte in geeigneter Form anzuerkennen:

    - Von dem Policy-Herausgeber und dem Kartenherausgeber aufgestellte Verpflichtungen,

    - von dem Kartenherausgeber aufgestellte zusätzliche Verpflichtungen,

- Zustimmung oder Verweigerung, die beantragten Zertifikate in weiteren Suchdiensten abrufbar zu halten,

- Auskunftserteilung der zuständigen Stelle für den Nachweis eines berufsbezogenen Attributes gegenüber dem VDA.

g. Alle relevanten Dokumente des Registrierungsprozesses für qualifizierte Zertifikate werden mindestens über den gesetzlich vorgeschriebenen Zeitraum gemäß [eIDAS] sowie darüber hinaus gemäß Teil 2 §16 [VDG] im Sinne der „auf Dauer prüfbaren Vertrauensdiensteanbieter“ hinweg archiviert. Die Archivierung muss den Anforderungen des [BDSG] und der [DSGVO] genügen.

Der Antragsteller kann entweder einen Erstantrag oder einen Folgeantrag stellen. Der VDA hat beide Verfahren in seinem CPS zu beschreiben.

3.3.2.2 Erstantrag

Als Erstantrag werden alle Anträge eines Antragstellers bezeichnet, die keine Folgeanträge sind. Bei einem Erstantrag muss die vollständige Registrierung gemäß Kapitel 3.3.2 durchlaufen werden. Insbesondere ist eine Identifizierung des Antragstellers gemäß Kapitel 3.3.2.1 zwingend notwendig.

3.3.2.3 Folgeantrag

Ein Folgeantrag ist ein Antrag, der auf Grundlage einer bereits abgeschlossenen Identifizierung eines anderen Antrags gestellt wird. Der Ausweisinhaber wird bei auslaufender Gültigkeit der Zertifikate seines Heilberufsausweises entsprechend durch den VDA informiert (z. B. per E-Mail oder Brief). Dabei muss der VDA mitteilen, unter welchen Umständen und bis wann ein Folgeantrag gestellt werden kann. Bei einem Folgeantrag können die bei einem Erstantrag angefallenen Daten wiederverwendet werden. Insbesondere kann auf eine erneute Identifizierung des Antragstellers verzichtet werden, sofern die vorherige Identifizierung noch gemäß Kapitel 3.3.2.1 verwendbar ist. Der Nachweis eines berufsbezogenen Attributes durch den Kartenherausgeber gegenüber dem VDA ist zu erneuern.

Weiterhin muss für einen Folgeantrag die erneute Freigabe zur Produktion des Heilberufsausweises durch den Kartenherausgeber ggü. dem VDA erfolgen. Ausnahme bilden Austauschausweise gemäß Kapitel 3.3.2.4.

3.3.2.4 Austauschausweis

Ein Anbieter kann einen „Austauschausweis“ bis 6 Monate nach Ausstellung des Heilberufsausweises ohne Freigabe durch den Kartenherausgeber produzieren und versenden. Die Produktionsrückmeldung des Austauschausweises geht dem Herausgeber wie üblich zu und kann der ursprünglichen Freigabe zugeordnet werden.

3.3.3 Freigabe zur Produktion

Der jeweilige Kartenherausgeber besitzt die Entscheidungsbefugnis über die Freigabe zur Produktion eines Heilberufsausweises. Insbesondere behalten sich die Kartenherausgeber vor, die Anzahl der gleichzeitig gültigen HBAs pro Antragsteller ggf. zu begrenzen.

Ohne Freigabe zur Produktion dürfen X.509-Zertifikate für den Heilberufsausweis nicht ausgestellt werden.

3.3.4 Ausstellung der Zertifikate

Der Kartenherausgeber und der VDA gewährleisten durch Einhaltung der nachfolgenden Punkte eine sichere Zertifikatsausstellung:

a. Alle sicherheitskritischen Tätigkeiten werden nur von autorisiertem, fachkundigem und zuverlässigem Personal und – sofern notwendig – unter Einhaltung des Vier-Augen-Prinzips durchgeführt.

b. Zur Gewährleistung der Vertraulichkeit und Integrität der aufgenommenen Daten werden diese nur mit einem geeigneten Verfahren gesichert zwischen dem Kartenherausgeber oder einer von diesem beauftragten Stelle und dem VDA übertragen.

c. Die X.509-Zertifikate werden durch den VDA gemäß den gesetzlichen Bestimmungen aus [eIDAS] und [VDG] sowie unter Einhaltung der [gemSpec_PKI] erstellt. Die maximale Gültigkeitsdauer der X.509-Zertifikate eines Heilberufsausweises richtet sich nach [gemSpec_Krypt].

d. Die Ausstellung der X.509-Zertifikate der Heilberufsausweise durch den VDA erfolgt erst nach expliziter Freigabe zur Produktion gemäß Kapitel 3.3.3 in Schriftform oder elektronischer Form mit Hilfe einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels durch den jeweiligen Kartenherausgeber.

e. Der Kartenherausgeber wird schriftlich und/oder elektronisch durch den VDA über das Ausstellen eines Zertifikates für einen Heilberufsausweis informiert. Dabei werden mindestens die folgenden Informationen bereitgestellt, die eine zweifelsfreie Zuordnung des ausgestellten Zertifikates zu dem Zertifikatsinhaber ermöglichen:

    - Vorgangsnummer,
    - Seriennummer des Zertifikates,
    - Gültigkeitszeitraum des Zertifikates,
    - Ausweisnummer des Heilberufsausweises, der das Zertifikat enthält,
    - vollständiger Name (Vornamen, Nachname, Geburtsname) des Zertifikatsinhabers,

- Geburtsdatum und Geburtsort des Zertifikatsinhabers.

Entsprechend werden weitere attributbestätigende Stellen informiert, wenn diese nicht der Kartenherausgeber ist.

f. Die Übergabe des Heilberufsausweises an den Antragsteller erfolgt auf sichere Art und Weise durch den VDA, so dass gewährleistet ist, dass nur der Antragsteller den Heilberufsausweis in Betrieb nehmen kann. Der Ausweisinhaber hat den Erhalt des Heilberufsausweises gegenüber dem VDA ggf. zu bestätigten. Das Vorgehen hat der VDA in seinem CPS zu beschreiben.

3.3.5 Veröffentlichung der Zertifikate

Der VDA stellt einen Verzeichnisdienst zur Verfügung, der von ihm gemäß dieser Policy ausgestellte Zertifikate bereitstellt. Die Veröffentlichung betrifft mindestens die Verschlüsselungszertifikate, die auf Wunsch des Karteninhabers abrufbar gehalten werden sollen.

3.3.6 Überprüfbarkeit der Zertifikate

Der VDA hat die von ihm nach dieser Policy ausgestellten Zertifikate gemäß den Anforderungen aus [eIDAS] und [VDG] für qualifizierte Zertifikate (C.HP.QES) überprüfbar zu halten. Dies gilt auch für das Zertifikat für Verschlüsselung (C.HP.ENC) sowie Authentifizierung (C.HP.AUT) des Heilberufsausweises.

3.3.7 Sperrung von Zertifikaten

Das Sperren von Zertifikaten kennzeichnet diese ab dem Zeitpunkt der Sperrung als ungültig. Eine Sperrung kann nicht aufgehoben oder rückgängig gemacht werden. Sie kann auch nicht rückwirkend erfolgen. Es ist nicht notwendig, Zertifikate nach Ablauf ihrer Gültigkeit zu sperren. Insbesondere gelten folgende Punkte:

a. Der Sperrantrag kann telefonisch oder schriftlich an den VDA gestellt werden. Der VDA kann auch weitere Verfahren anbieten.

b. Es wird ein Sperrkennwort oder eine andere zuverlässige Identifizierung für den Absender eines Sperrantrags verwendet.

c. Neben dem Ausweisinhaber können zuständige Stellen für den Nachweis eines berufsbezogenen Attributes (gemäß Teil 2 § 12 [VDG]) einen Sperrantrag stellen. Dies ist insbesondere der Kartenherausgeber sowie gesondert berechtigte Stellen.

d. Vor der Sperrung hat der entsprechend autorisierte Mitarbeiter des VDA den Antrag auf seine Korrektheit hin zu prüfen, insbesondere die Berechtigung des Absenders des Sperrantrags.

e. Die Durchführung der Sperrung muss gemäß [eIDAS] und [VDG] für qualifizierte Zertifikate unverzüglich erfolgen. Insbesondere ist die Online-Statusabfrage für die Überprüfung der Zertifikate umgehend zu aktualisieren.

f. Eine optionale Sperrliste kann durch ein *CRL-Signer-Zertifikat* signiert werden (indirekte CRL). Online-Statusabfragen müssen mittels eines *OCSP-Signer-Zertifikates* signiert werden.

g. Das Aktualisierungsintervall der Sperrliste wird vom VDA festgelegt.

h. Wird ein Zertifikat gesperrt, informiert der VDA den Zertifikatsinhaber, den Kartenherausgeber sowie ggf. weitere attributbestätigende Stellen in Schriftform, Textform oder elektronischer Form über die Sperrung des Zertifikats.

Es werden stets sämtliche X.509-Zertifikate gleichzeitig gesperrt, die sich auf demselben Heilberufsausweis befinden und nach dieser Policy ausgestellt wurden.

3.4 Verwaltung und Betrieb der Zertifizierungsstelle

Neben den Auflagen aus [eIDAS] und [VDG] für qualifizierte Zertifikate ist ein VDA verpflichtet, die im Folgenden beschriebenen Punkte zu gewährleisten. Begründete Abweichungen sind zulässig, benötigen jedoch die schriftliche Genehmigung der Policy-Herausgeber.

3.4.1 Sicherheitsmanagement

Für das Sicherheitsmanagement gelten die nachfolgenden Punkte:

a. Der VDA ist für alle Abläufe und Prozesse der von ihm angebotenen Dienste verantwortlich. An den VDA werden klare Forderungen gestellt, deren Einhaltung durch entsprechende Kontrollfunktionen überprüft wird. Die für die Einhaltung der Sicherheit relevanten Maßnahmen werden im CPS des VDA definiert und dem Kartenherausgeber sowie dessen Policy-Herausgeber zugänglich gemacht.

b. Die Sicherheitsrichtlinien und -vorgaben werden regelmäßig kontrolliert und müssen bei Bedarf an die aktuellen Gegebenheiten angepasst werden. Der VDA ist in seinem Wirkungsbereich für die Definition der Sicherheitsrichtlinien und deren Weitergabe an das betroffene Personal verantwortlich.

c. Der VDA führt eine umfassende Dokumentation über alle sicherheitsrelevanten Maßnahmen sowie deren korrekte Umsetzung und legt diese dem Kartenherausgeber und dessen Policy-Herausgeber vor. Näheres regelt jeder Kartenherausgeber in Rücksprache mit seinem Policy-Herausgeber in den Ausschreibungs- bzw. Zulassungsunterlagen.

3.4.2 Informationsklassifizierung und -verwaltung

Im Gesamtsicherheitskonzept des VDA, welches eine Bedrohungs- und Risikoanalyse beinhaltet, werden alle Informationskategorien definiert und nach ihrem Schutzbedarf klassifiziert. Der VDA gewährleistet dabei durch geeignete Maßnahmen die Absicherung aller schutzwürdigen Daten und Informationen.

3.4.3 Personelle Sicherheitsmaßnahmen

Mit den Anforderungen nach [eIDAS] und [VDG] stellen sich mindestens die folgenden Anforderungen an das eingesetzte Personal:

a. Der VDA beschäftigt nur Mitarbeiter, welche das erforderliche Wissen sowie die notwendige Qualifikation und Erfahrung für die Ausübung der jeweiligen Tätigkeit besitzen. Mitarbeiter für vertrauenswürdige Positionen müssen ein polizeiliches Führungszeugnis vorlegen. Erst nach einer Unbedenklichkeitseinstufung darf die Position vergeben werden.

b. Die genauen Aufgabengebiete und deren zugehörige Tätigkeiten – insbesondere bei sicherheitsrelevanten Punkten – werden in einem Rollenkonzept des VDA ausführlich beschrieben. Diese Beschreibungen umfassen unter anderem neben den Pflichten auch die Rechte und erforderlichen Kompetenzen.

c. In dem CPS des VDA werden alle vertrauenswürdigen Rollen ausführlich beschrieben.

d. Alle Aktivitäten erfolgen gemäß den aufgestellten Sicherheitsrichtlinien.

e. Mitarbeiter in vertrauenswürdigen Positionen werden vor Rollen- und Interessenkonflikten bezüglich ihrer Tätigkeiten bewahrt, damit eine unvoreingenommene Ausübung dieser Tätigkeiten ermöglicht wird.

3.4.4 Physikalische und organisatorische Sicherheitsmaßnahmen

Zur Absicherung von sicherheitskritischen Bereichen werden Maßnahmen vom VDA zur Verhinderung von Verlusten, Kompromittierungen und Beschädigungen sowie der Unterbrechung des laufenden Betriebs ergriffen. Diese umfassen insbesondere:

a. Nur autorisiertes Personal hat Zutritt zu den sicherheitskritischen Bereichen, um eine Kompromittierung durch unautorisierte Zugriffe zu verhindern. Diese Bereiche umfassen insbesondere die Räumlichkeiten, in denen die Zertifizierungs- und Sperrprozesse sowie (je nach Sicherheitskonzept bzw. CPS) die Chipkartenpersonalisierung durchgeführt wird.

b. Die Systeme für die Zertifizierungs- und Sperrprozesse sowie (je nach Sicherheitskonzept) die Chipkartenpersonalisierung bilden eigene Sicherheitsbereiche, welche

von anderen organisatorischen Einheiten räumlich abgegrenzt und durch einen physischen Zutrittsschutz abgesichert sind.

c. Hinsichtlich der Systeme für die Zertifizierungs- und Sperrprozesse sowie die (je nach Sicherheitskonzept) Chipkartenpersonalisierung müssen Sicherheitsmaßnahmen zur Abwendung von Gefahren durch Feuer, Wasserschäden und Naturgewalten sowie Schutz vor Einbruch und Diebstahl, Ausfällen von Versorgungseinheiten und Systemausfällen getroffen werden.

d. Die Zertifizierungsprozesse müssen durch geeignete Kontrollen vor unautorisierter Entnahme von Gegenständen und Daten geschützt werden.

Die notwendigen Maßnahmen werden im CPS und insbesondere dem Sicherheitskonzept des VDA geregelt.

3.4.5 Management des Betriebes

Der VDA gewährleistet, dass die Systeme für die Zertifizierungsprozesse korrekt betrieben werden. Dazu gelten insbesondere die folgenden Punkte:

a. Auf einen Zwischenfall wird zeitnah reagiert. Zwischenfall und Reaktion werden ausführlich dokumentiert und der Policy-Herausgeber informiert.

b. Schäden werden durch Backups und definierte Prozeduren zur Fehlerbeseitigung minimiert.

c. Die eingesetzten Systeme werden gegen schadhafte Software und unautorisierte Zugriffe geschützt.

d. Datenträger werden vor Diebstahl und unautorisiertem Zugriff geschützt.

e. Alle Datenträger werden gemäß ihrer Sicherheitsstufe aufbewahrt. Datenträger, die sicherheitsrelevante oder vertrauliche Informationen beinhalten, werden bei ihrer Ausmusterung auf sichere Weise vernichtet.

Zur weiteren Minimierung von Zwischenfällen werden die sicherheitskritischen Funktionen von den anderen Funktionen getrennt. Alle genannten sicherheitskritischen Funktionen werden (gemäß des Rollenkonzepts im Gesamtsicherheitskonzept des VDA) nur von autorisiertem Personal durchgeführt. Zu den Tätigkeiten gehören insbesondere der Betrieb, die Wartung sowie die Administration der Systeme. Dazu gehört der Schutz vor schadhafter Software, die regelmäßige Kontrolle und Analyse von Log-Dateien sowie erhöhte Sicherheitsmaßnahmen bei der Datenträgerverwaltung und dem Datenaustausch.

3.4.6 Zugriffsverwaltung

Der Zugriff auf die Systeme für die Zertifizierungs- und Sperrprozesse sowie die dazugehörigen Dienste erfolgt nur durch autorisiertes Personal. Dies wird durch die folgenden Punkte gewährleistet:

a. Der Zugriff auf die Systeme ist nur autorisiertem Personal möglich. Dazu werden verschiedene Kategorien von Zugriffsrechten eingerichtet, welche insbesondere die sicherheitskritischen von den unkritischen Funktionen trennen.

b. Vor jedem Zugriff auf ein System muss sich das Personal authentifizieren. Alle Zugriffe – insbesondere unautorisierte Zugriffsversuche – werden protokolliert.

c. Alle sicherheitskritischen Zugriffe bezüglich des Zertifikatsmanagements sind zusätzlich durch sichere Authentifizierungsmechanismen geschützt.

d. Alle vertraulichen Daten werden bei der Übertragung über unsichere Netzwerke geschützt.

e. Die Systeme werden vor Zugriffen durch unbefugte Dritte geschützt. Die Systemkomponenten befinden sich in physisch gesicherten Räumlichkeiten.

f. Bei der Entdeckung unautorisierter Zugriffsversuche auf das System müssen unverzüglich Gegenmaßnahmen ergriffen werden.

3.4.7 Einsatz vertrauenswürdiger Systeme

Der VDA ergreift geeignete technische und organisatorische Maßnahmen zur Beherrschung der Sicherheitsrisiken im Zusammenhang mit den von ihm erbrachten Vertrauensdiensten. Diese Maßnahmen müssen unter Berücksichtigung des jeweils neuesten Standes der Technik gewährleisten, dass das Sicherheitsniveau der Höhe des Risikos angemessen ist. Insbesondere sind Maßnahmen zu ergreifen, um Auswirkungen von Sicherheitsverletzungen zu vermeiden bzw. so gering wie möglich zu halten und die Beteiligten über die nachteiligen Folgen solcher Vorfälle zu informieren.

3.4.8 Aufrechterhaltung des ungestörten Betriebes und Behandlung von Zwischenfällen

Nach dem Eintreten von Katastrophenfällen sind der Kartenherausgeber und der VDA darum bemüht, möglichst kurzfristig den sicheren, geregelten Betrieb wieder aufzunehmen. Der zugrunde liegende Notfallplan ist Bestandteil des Sicherheitskonzepts bzw. CPS des VDA. Die Kartenherausgeber und Policy-Herausgeber werden in die dann notwendigen Kommunikationsmaßnahmen eingebunden.

3.4.9 Einstellung der Tätigkeit

Der VDA meldet gemäß Teil II §16 [VDG] die Einstellung der Tätigkeit rechtzeitig der zuständigen Behörde, dem Kartenherausgeber und allen Policy-Herausgebern. Für den Fall der Einstellung der Tätigkeit erarbeitet der VDA unter Einbeziehung der betroffenen Policy-Herausgeber eine Verfahrensbeschreibung zur Abwicklung bzw. zur Übernahme der Tätigkeit in Bezug auf diese Policy. Das Verfahren wird im CPS des VDA beschrieben. Insbesondere muss die Übergabe der Zertifikate an einen weiteren VDA sichergestellt sein, gemäß den Anforderungen der Vertrauensdiensteverordnung. Die Anforderungen gelten für alle Zertifikatsklassen. Dies beinhaltet mindestens:

a. die Zertifikate,

b. die Sperrlisten,

c. Informationen über freigeschaltete oder nicht freigeschaltete Zertifikate,

d. Registrierungsanträge,

e. Informationen für den Zugang und die Benutzung der Sperrpasswörter:

    - Art der Verschlüsselung,
    - Kodierung, ggf. Hashing,
    - Schlüssel für den Zugriff (falls erforderlich: im verschlossenen Umschlag, bei einem Notar hinterlegt, bis sie benötigt werden),
    - Kommunikations-Informationen (z.B. Weiterleitung / Überlassung einer Sperrhotline).

f. Sperrpasswörter in verwertbarer Form auf sichere Art und Weise.

Die Übergabe muss effizient erfolgen können.

3.4.10 Übereinstimmung mit gesetzlichen Anforderungen

Der Kartenherausgeber und der VDA gewährleisten die Einhaltung der gesetzlichen Vorgaben aus [eIDAS], [VDG], [BDSG] und [DSGVO] sowie die sich aus [gemSpec_PKI] und dieser Policy ergebenden Anforderungen, in ihrer jeweils gültigen Fassung.

Dabei wird insbesondere auf die Einhaltung der Datenschutzanforderungen im [BDSG] und der [DSGVO] geachtet. Hierzu werden wichtige Informationen vor Verfälschung sowie Verlust geschützt. Die Daten der Antragsteller werden nur mit deren ausdrücklichem Einverständnis, auf Grund gesetzlicher Bestimmungen oder richterlichen Anordnungen offengelegt.

3.4.11 Aufbewahrung von Informationen zu Zertifikaten

Der Kartenherausgeber und der VDA bewahren alle Informationen zu Zertifikaten gemäß den gesetzlichen Vorgaben aus [eIDAS] und [VDG] für qualifizierte Zertifikate und dem [BDSG] und der [DSGVO] auf. Dabei gelten insbesondere nachfolgende Punkte:

a. Die zu archivierenden Daten müssen in dem CPS des VDA definiert werden. Mindestens werden die Unterlagen nach Kapitel 3.3.2 archiviert.

b. Die Archivierung der Daten erfolgt gemäß den Richtlinien des CPS des VDA.

c. Die Integrität und Vertraulichkeit der archivierten Daten werden gewahrt.

d. Nur autorisiertes Personal kann archivierte Daten löschen. Die Löschung darf erst nach erfolgreicher Authentifizierung und Autorisierung erfolgen. Die Löschung ist zu dokumentieren.

e. Für mindestens fünf Jahre ab Ablauf der Gültigkeit (ungeachtet einer Sperrung) eines der X.509-Zertifikate (C.HP.QES, C.HP.AUT, C.HP.ENC) des Heilberufsausweises werden archiviert:

    a. das Zertifikat,

    b. ggf. Sperrinformationen zum Zertifikat (inkl. Zeitpunkt der Sperrung) z.B. – falls vorhanden – die Sperrlisten, die das Zertifikat enthalten könnten,

    c. die Zuordnung zwischen Zertifikat und Personendaten inkl. Originalantrag zur Identifizierung. Sofern ein ersetzendes Scannen des Originalantrags erfolgte, kann auch diese Information archiviert werden.

f. CA-Zertifikate werden mindestens so lange aufbewahrt, wie davon ausgestellte Zertifikate aufbewahrt werden.

4 Anhang A – Verzeichnisse

4.1 Abkürzungsverzeichnis

BAK	Bundesapothekerkammer
BÄK	Bundesärztekammer
BDSG	Bundesdatenschutzgesetz
BPtK	Bundespsychotherapeutenkammer
BSI	Bundesamt für Sicherheit in der Informationstechnik
BZÄK	Bundeszahnärztekammer
C.HP.AUT	Das Zertifikat der Anwendung “Authentifizierung” des HBA
C.HP.ENC	Das Zertifikat der Anwendung „Ent- und Verschlüsselung“ des HBA (engl. encode)
C.HP.QES	Das Zertifikat der Anwendung „Qualifizierte Elektronische Signatur“ des HBA
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CVC	Card Verifiable Certificate
CV-Zertifikat	Card-Verifiable-Zertifikat
DSGVO	Datenschutzgrundverordnung
eGBR	Bezirksregierung Münster, elektronisches Gesundheitsberuferegister
HBA	Heilberufsausweis
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number / Persönliche Identifikationsnummer
VDA	Vertrauensdiensteanbieter

4.2 Literaturverzeichnis

Externe Dokumente	
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_PKI]	gematik: Übergreifende Spezifikation Spezifikation PKI;
[BDSG]	Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097)
[SGB V]	Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), zuletzt geändert durch Artikel 3 G. v. 22.04.2021
[eIDAS]	Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.
[VDG]	Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist
[VDV]	Verordnung zu Vertrauensdiensten (Vertrauensdiensteverordnung – VDV), Bundesministerium für Wirtschaft und Energie.
[DSGVO]	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

4.3 Abbildungsverzeichnis

4.4 Tabellenverzeichnis

5 Anhang B – Verhältnis Karten- zu Policy-Herausgeber (informativ)

Die nachfolgende Abbildung zeigt informativ die Beziehungen zwischen den Policy-Herausgebern, den Kartenherausgebern und den Anbietern / VDA.

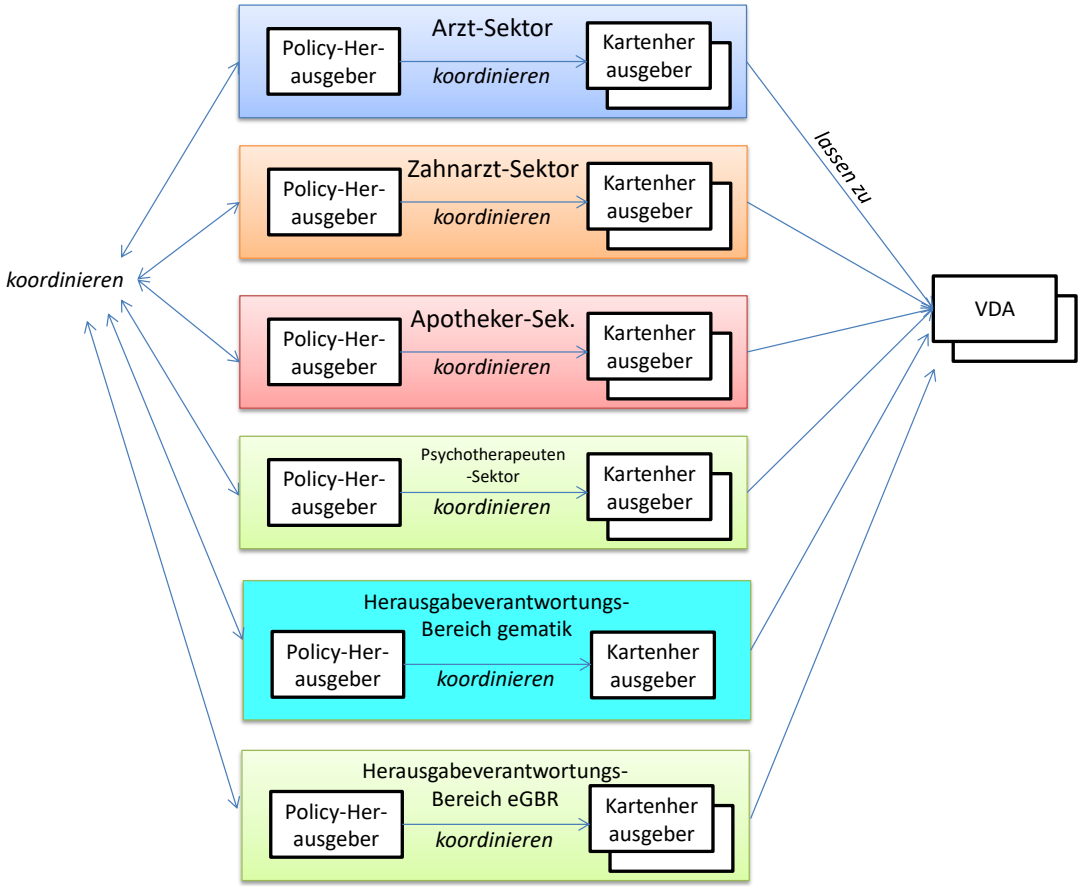

Abbildung 1: Beziehungen zwischen Policy- und Kartenherausgebern und den VDA (informativ)