Gemeinsame Policy für die Ausgabe der HPC

Zertifikatsrichtlinie HPC

Version: 1.0.5

06.11.2012

Bundesapothekerkammer

Bundesärztekammer

Bundespsychotherapeutenkammer

Bundeszahnärztekammer

Kassenzahnärztliche Bundesvereinigung

Impressum

Herausgeber **Bundesapothekerkammer**
Bundesärztekammer
Bundespsychotherapeutenkammer
Bundeszahnärztekammer
Kassenzahnärztliche Bundesvereinigung

Editor Bundesapothekerkammer
c/o Apothekerhaus Eschborn
Martin Bergen
Carl-Mannich-Str. 26
65760 Eschborn

1 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 Zertifizierungsdiensteanbieter 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 Veröffentlichte Versionen sind **fett** markiert.

3

Inhaltsverzeichnis

1 Einleitung und Begriffsbestimmung

In dieser gemeinsamen Zertifikatsrichtlinie (*Certificate Policy – CP*) wird ein Regelwerk mit Sicherheitsanforderungen zur Ausstellung von Zertifikaten und der Ausgabe der *Health Professional Card* (HPC), die insbesondere zur sicheren Erzeugung elektronischer Signaturen geeignet ist, definiert. Als sichere Signaturerstellungseinheit (SSEE) und Trägermedium für die Schlüssel und die ausgegebenen Zertifikate wird ausschließlich eine Chipkarte verwendet. Ausgestellt werden dabei – gemäß der HPC-Spezifikation [HPC-Spec] – neben den X.509-Zertifikaten auch *Card Verifiable Certificates* (CV-Zertifikate), wobei die Verwendung der CV-Zertifikate in ISO/IEC 7816-8 beschrieben ist.

Die gemäß [HPC-Spec] ausgestellten X.509- und CV-Zertifikate[1] der Ausweisinhaber decken zusammen die Anwendungsgebiete Signaturerstellung (Unterschrift), Authentifizierung sowie Ver- bzw. Entschlüsselung ab. Jedes Zertifikat wird dabei nur für fest vorgegebene Anwendungsgebiete eingesetzt (vgl. Kapitel 2.3 und 3.2.5).

Die generierten X.509-Signaturschlüssel-Zertifikate erfüllen mindestens die Anforderungen aus dem *Gesetz über Rahmenbedingungen für elektronische Signaturen* (Signaturgesetz – [SigG]) und der *Verordnung zur elektronischen Signatur* (Signaturverordnung – [SigV]) für qualifizierte elektronische Signaturen und sind somit für die sichere Erzeugung elektronischer Signaturen geeignet. Gemäß Rechtslage § 291a [SGB V] sowie der [HPC-Spec] werden für die HPC insbesondere X.509-Zertifikate für qualifizierte Signaturen ausgestellt.

Zusätzliche Attribute des Ausweisinhabers (bspw. Approbation) können gemäß [HPC-Spec] bei entsprechender Bestätigung durch die zuständige Stelle im X.509-Basiszertifikat oder in weiteren, dem Basiszertifikat zugeordneten, Attributzertifikaten oder in beiden verankert werden. Auch Attributzertifikate folgen den Anforderungen aus X.509 und sollen bei qualifiziertem Niveau in der Chipkarte gespeichert werden. Die Anforderungen an Attribut-Zertifikate sind im Anhang der [HPC-Spec] beschrieben.

Die in der HPC-Spezifikation beschriebene SMC ist Gegenstand einer eigenen Policy.

1.1 Rechtliche Einordnung

Soweit zutreffend finden die jeweils aktuell gültigen Regelungen und Vorgaben des *Signaturgesetzes* [SigG], der *Signaturverordnung* [SigV], des *Sozialgesetzbuches – Fünftes Buch* – [SGB V] sowie des *Bundesdatenschutzgesetzes* [BDSG] Anwendung und sind dieser Policy übergeordnet.

Der bzw. die HPC-Herausgeber werden durch § 291a [SGB V], die Heilberufsgesetze der Länder und die jeweiligen Spitzenorganisationen der Leistungserbringer näher bestimmt.

[1] CV-Zertifikate werden in weiteren Dokumenten geregelt. Diese Policy betrachtet CV-Zertifikate nur informativ.

1.2 Dokumentenidentifikation

Dokumententyp:	Certificate Policy
Name dieses Dokumentes:	Gemeinsame Policy für die Ausgabe der HPC
Kurzname dieses Dokumentes:	Zertifikatsrichtlinie HPC
Referenz für dieses Dokument:	[CP-HPC]
Version:	1.0.5 vom 06.11.2012
Object Identifier:	1.2.276.0.76.4.145 {policy-hba-010005-cp}

1.3 Begriffsdefinition

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

Es existieren damit mehrere Policy-Herausgeber, mehrere ZDA und mehrere HPC-Herausgeber. Für einen Antragsteller ist jedoch immer nur ein bestimmter HPC-Herausgeber zuständig, der wiederum nur einem bestimmten Policy-Herausgeber zugeordnet ist. Für einen HPC-Herausgeber können mehrere ZDA tätig sein.

Die Ausstellung der Zertifikate einer HPC beantragt der Antragsteller bei einem ganz konkreten ZDA. Der Text dieser Policy orientiert sich daher aus Sicht des Antragstellers an der Singularform der verschiedenen Parteien, auch wenn z.B. mehrere HPC-Herausgeber 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 HPC-Herausgeber. (Vgl. dazu *Anhang C – Verhältnis HPC- zu Policy-Herausgeber (informativ)*).

- Der **HPC-Herausgeber** im Sinne dieser Policy ist eine für die Ausgabe einer HPC zuständige Stelle gemäß § 291a Absatz 5a Nr. 1 [SGB V]. Ein HPC-Herausgeber gibt die HPCs nur für einen bestimmten Kreis an Antragstellern heraus und bedient sich dabei der Hilfe eines oder mehrerer Zertifizierungsdiensteanbieter. Er muss den für

ihn zuständigen Policy-Herausgeber über die Aufnahme seiner Tätigkeit informieren der die bundesweit einheitlichen Vorgaben für seinen Bereich koordiniert.

- Der **Antragsteller** im Sinne dieser Policy ist eine natürliche Person, die eine HPC nach dieser Policy bei einem für ihn zuständigen HPC-Herausgeber bzw. ZDA beantragt. Eine Liste der möglichen Antragsteller (z.B. Apotheker, Ärzte, Psychotherapeuten und Zahnärzte) wird durch den jeweiligen HPC-Herausgeber veröffentlicht. Mit Besitz einer HPC ergeben sich im Sinne der vorliegenden Policy folgende zusätzliche Rollen für den Antragsteller:
  - Der **Ausweisinhaber** im Sinne dieser Policy ist eine natürliche Person, die eine nach dieser Policy ausgegebene HPC erhält und für deren Verwendung alleinig verantwortlich ist. Aufgrund der persönlichen Bindung sind Ausweisinhaber 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 **Zertifizierungsdiensteanbieter (ZDA)** im Sinne dieser Policy ist ein akkreditierter Zertifizierungsdiensteanbieter nach [SigG], der für einen HPC-Herausgeber tätig ist und Zertifikate nach dieser Policy ausstellt. Ein ZDA kann für mehrere HPC-Herausgeber tätig sein.
- Die **HPC** im Sinne dieser Policy ist eine Chipkarte gemäß [HPC-Spec], die mindestens X.509-Zertifikate enthält, die nach dieser Policy ausgestellt wurden. Die Zertifikate der HPC bilden hierbei die kryptografische Identität einer Person in der elektronischen Welt ab. Der Zugriff auf die privaten Schlüssel einer HPC ist nur nach vorheriger und erfolgreicher Eingabe einer PIN möglich. Eine HPC im Sinne dieser Policy wird auch Heilberufsausweis oder Berufsausweis genannt.
- Ein **Endnutzerzertifikat** ist ein Zertifikat, dass zu einem in der HPC 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 ZDA und legen gemeinsam entsprechende Migrationsfristen fest.

Ein HPC-Herausgeber kann für seinen Bereich spezifische Anforderungen aufstellen, die nur verschärfenden bzw. präzisierenden Charakter haben. Dies ist jeweils mit dem für ihn zuständigen Policy-Herausgeber abzustimmen.

Vorgaben, Anforderungen, weitere Bestimmungen u. ä. trifft der HPC-Herausgeber gegenüber dem ZDA nur nach vorheriger Absprache mit seinem Policy-Herausgeber, der ggf. sich wiederum auf Bundesebene mit den übrigen Policy-Herausgebern abstimmen muss.

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 [HPC-Spec] 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 dem [SigG] und [SigV].

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

In Kapitel 3 werden die Vorgaben für einen ZDA festgelegt, nach denen dieser seine Zertifizierungsdienstleistung 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 abweichenden Bestimmungen für den Test- und Übergangszeitraum festgelegt.

In Kapitel 6 werden als Anlage C die Beziehungen zwischen den Policy-Herausgebern und den HPC-Herausgebern informativ aufgeführt.

2 Verpflichtungen und Haftungsbestimmungen

In diesem Kapitel werden die Verpflichtungen und Haftungsbedingungen geklärt.

2.1 Verpflichtungen des Policy-Herausgebers und des HPC-Herausgebers

Der HPC-Herausgeber ist für die Einhaltung der in dieser Policy aufgestellten Richtlinien verantwortlich. Er hat insbesondere die Pflicht, eine Übersicht der ZDA zu erstellen, mit denen er zusammenarbeitet bzw. die durch ihn zugelassen sind. Er muss diese Übersicht auf einem aktuellen Stand halten sowie den Anwendern zugänglich machen. Die Übersicht ist an seinen zuständigen Policy-Herausgeber zu melden.

2.2 Verpflichtungen des ZDA

Der ZDA ist verpflichtet, seine Zertifizierungsdienstleistungen 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 ZDA stellt insbesondere eine Liste mit Komponenten und Verfahren zur sicheren Erstellung insbesondere einer qualifizierten elektronischen Signatur und zur Signaturprüfung bereit und macht diese dem Ausweisinhaber zugänglich.

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 dabei durch Leisten einer rechtsgültigen Unterschrift des Antragstellers dokumentiert.

Aufgrund der persönlichen Bindung sind bei der HPC 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 die sichere Signaturerstellungseinheit sicher vernichten bzw. un-

brauchbar machen[2] (beispielsweise durch das physische Zerstören des Chips der HPC).

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

- die HPC nicht mehr unter seiner alleinigen Kontrolle steht,
- der begründete Verdacht auf eine Kompromittierung besteht,
- sowie die Informationen im Zertifikat fehlerhaft sind oder sich geändert haben.

(Der ZDA ist wiederum verpflichtet, bei einer Sperrung auch den HPC-Herausgeber 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 Schlüsselpaar und Zertifikate der HPC

Insbesondere setzt er den privaten Signaturschlüssel des Zertifikates C.HP.QES nur zur Erzeugung qualifizierter elektronischer Signaturen gemäß [SigG] ein. Der Anwendungsbereich Authentifizierung umfasst auch die Signatur von Nachrichten und Dateien im Sinne des Nachweises des Ursprungs, nicht aber im Sinne einer rechtlichen Bindung an den signierten Inhalt (Beispiel: Signierte E-Mail).

e. Der Anwender soll für die qualifizierte elektronische Signatur ausschließlich Komponenten und Verfahren einsetzen, welche nach [SigG] bestätigt sind.

f. Der Anwender hat dafür Sorge zu tragen, dass in der Arbeitsumgebung, in der eine qualifizierte elektronische Signatur erstellt wird, die geforderten Rahmenbedingungen der nach [SigG] bestätigten Komponenten und Verfahren eingehalten werden. Dazu hat er sowohl alle technischen als auch organisatorischen Maßnahmen zu ergreifen, welche nur einen befugten Zugriff auf diese Arbeitsumgebung ermöglichen.

g. Der Anwender muss bei Nutzung der Schlüssel in den Anwendungsbereichen Authentifizierung und Ver- bzw. Entschlüsselung alle technischen und organisatorischen

[2] Dies ist notwendig, um den Missbrauch von CV-Zertifikaten zu verhindern.

Maßnahmen ergreifen, welche nur einen befugten Zugriff auf die genutzte Arbeitsumgebung ermöglichen.

2.4 Verpflichtungen des Überprüfers

Ein Überprüfer, welcher ein gemäß dieser Policy ausgestelltes Zertifikat zur Überprüfung einer ausgeführten Sicherheitsfunktion (beispielsweise einer Signatur) einsetzen will, muss folgende Punkte einhalten:

a. Der Überprüfer kontrolliert die Gültigkeit des Zertifikats in Bezug auf den Signaturerstellungszeitpunkt bzw. Authentifizierungszeitpunkt und dem zu Grunde liegenden Gültigkeitsmodell. Als Gültigkeitsmodell für alle Zertifikatsklassen wird das Kettenmodell definiert. Der Gültigkeitszeitraum der X.509-Zertifikate für Authentisierung (C.HP.AUT) und Verschlüsselung (C.HP.ENC) soll den Gültigkeitszeitraum ihrer Aussteller-Zertifikate (CA- und Root-Zertifikate) nicht übersteigen.

b. Der Überprüfer kontrolliert den Status des Zertifikats. Der das Zertifikat ausstellende ZDA stellt dazu entsprechende Abfragedienste zur Verfügung.

c. Der Überprüfer achtet auf die Anwendungsbereiche des Zertifikats und die damit verbundenen Einschränkungen.

d. Die Schlüsselpaare und Zertifikate dürfen nur für ihren jeweiligen Anwendungsbereich benutzt werden. Eine Benutzung außerhalb des zugehörigen Anwendungsbereichs ist nicht zulässig. Insbesondere ist das Schlüsselpaar bzw. Zertifikat C.HP.QES ausschließlich für die qualifizierte elektronische Signatur nach [SigG] im Sinne der *Nicht-Abstreitbarkeit* (*non-repudiation* bzw. *content commitment*) einzusetzen.

e. Der Überprüfer hat die Sorgfaltspflicht, seine IT-Infrastruktur zu schützen. Insbesondere gilt:

   - Er muss die Auflagen des Software-Herstellers der Signaturanwendungskomponente, wie sie in der Bedienungsanleitung beschrieben sind, erfüllen.

   - Er darf neue Root-Zertifikate nur nach sorgfältiger Prüfung (Vergleich des *Fingerprints* des Root-Zertifikats mit dem vertrauenswürdig veröffentlichten Fingerprint des echten Root-Zertifikats) im Rechner-Betriebssystem und in die Software installieren. Ein automatisiertes Verfahren setzt voraus, dass die Signaturanwendungskomponente dies sicher unterstützt. Dabei verlagert sich dann die Prüfpflicht des Überprüfers vom Root-Zertifikat auf den verwendeten Vertrauensanker (z.B. ein TSL-Signaturzertifikat).

f. Er muss evtl. Nutzungsbeschränkungen im Zertifikat berücksichtigen.

g. Eine Aussage über die Gültigkeit der qualifizierten elektronischen Signatur wird über eine zugelassene, im Amtsblatt der BNetzA aufgeführte, Signaturanwendungskomponente getroffen.

2.5 Haftungsbestimmungen

Grundsätzlich gelten mindestens die nachfolgend aufgeführten Haftungsbestimmungen.

2.5.1 Haftung des ZDA

Als Aussteller von Zertifikaten haftet der ZDA nach den Bestimmungen für qualifizierte elektronische Signaturzertifikate gemäß [SigG]. Analog haftet der ZDA auch für Schäden, die in Zusammenhang mit der Ausstellung der in dieser Policy aufgeführten weiteren Zertifikate (Authentisierungs-, Verschlüsselungszertifikate, Attributzertifikate sowie qualifizierte Signaturzertifikate) entstehen.

2.5.2 Haftung des HPC-Herausgebers

Der HPC-Herausgeber haftet im Rahmen der Herausgabe der HPC für Schäden – gleich aus welchem Rechtsgrund – nur bei Vorsatz oder grober Fahrlässigkeit sowie im Falle schuldhafter Verletzung wesentlicher Pflichten. Die voran genannten Haftungsbeschränkungen gelten nicht für schuldhaft verursachte Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit sowie die Haftung nach dem Produkthaftungsgesetz.

2.5.3 Haftung des Ausweisinhabers

Der Ausweisinhaber haftet für die sichere Aufbewahrung und die Nutzung seiner HPC.

2.5.4 Haftungsausschluss des Policy-Herausgebers

Der Policy-Herausgeber haftet für Schäden, die mit der Umsetzung dieser Policy verbunden sind, nur bei Vorsatz und grober Fahrlässigkeit.

3 Anforderungen an die Erbringung von Zertifizierungsdiensten

Es werden die Anforderungen an die Erbringung von Zertifizierungsdiensten (z. B. das Ausstellen von Zertifikaten) festgelegt. Die nachfolgend beschriebenen Prozesse erfüllen insbesondere die Vorgaben aus [SigG] und [SigV] sowie der HPC-Spezifikation [HPC-Spec].

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 ZDA erstellten CPS festgelegt und den jeweiligen Policy-Herausgebern erläutert.

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

Der HPC-Herausgeber kann in Rücksprache mit seinem Policy-Herausgeber weitere Anforderungen im Rahmen seiner Zulassung bzw. Ausschreibung festlegen. Sämtliche weitere Anforderungen sind durch den ZDA ebenfalls in einem *Certification Practice Statement* (CPS) aufzunehmen.

3.2 Verwaltung von Schlüsseln zur Erbringung von Zertifizierungsdiensten

Die Anforderungen aus [SigG] und [SigV] an Schlüssel für qualifizierte elektronischen Signaturzertifikate sowohl der CA als auch der Anwender sind einzuhalten.

In den nachfolgenden Unterabschnitten werden daher nur Anforderungen an die weiteren Schlüssel (bspw. CA-Schlüssel für Authentifikation 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 [HPC-Spec].

Insbesondere gelten dabei folgende Vorgaben bezüglich Schlüssellänge und Algorithmus:

a. Die Schlüssellängen und Algorithmen für alle X.509-CA-Zertifikate müssen mindestens eine vergleichbare Sicherheit bieten, wie die Schlüssellängen und Algorithmen der davon ausgestellten Endnutzerzertifikate.

b. Die Schlüssellängen müssen mindestens so groß sein, wie die empfohlenen Schlüssellängen im jeweiligen aktuellen Algorithmenkatalog der Bundesnetzagentur.

c. CA-Schlüssel für die Ausstellung der Endnutzerzertifikate C.HP.ENC und C.HP.AUT müssen eine vergleichbare Sicherheit bieten, wie die CA-Schlüssel für qualifizierte Signaturzertifikate (z. B. C.HP.QES). Aktuell empfohlene Algorithmen sind:

- RSA mit einer Mindestlänge von 2048 Bit.
- ECDSA mit einer Mindestlänge von 256 Bit.

Maßgeblich sind die Vorgaben der Policy-Herausgeber.

d. Für CV-CA-Zertifikate (C.CA.CVC) gelten die Bestimmungen der [HPC-Spec].

3.2.2 Speicherung und Backup von CA-Schlüsseln

Der ZDA 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 ZDA gewährleistet die Authentizität und Integrität der von ihm erzeugten und verwalteten öffentlichen Schlüssel bei der Verteilung. Hierfür wird neben den CA-Zertifikaten das dazugehörige Root-Zertifikat sowie die zugehörigen Fingerprints zur Überprüfung veröffentlicht. Die Veröffentlichung der Root-Zertifikate erfolgt mindestens über geeignete, von den HPC-Herausgebern festgelegte Printmedien.

3.2.4 Verteilung und Veröffentlichung der privaten CA-Schlüssel

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

3.2.5 Verwendungszweck der CA-Schlüssel

Private CA-Schlüssel werden nur für die Ausstellung von Zertifikaten gemäß dieser Policy eingesetzt.

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

1 Benötigte Anwendungsbereiche sind:

Anwendungsbereich	**Schlüssel bzw. Zertifikat**
Ausstellung der Zertifikate C.HP.QES und C.HP.ATTR	C.CA.QES
Ausstellung der Zertifikate C.HP.AUT	C.CA.AUT
Ausstellung der Zertifikate C.HP.ENC	C.CA.ENC
Ausstellung der Zertifikate C.HP.CVC (nicht Gegenstand dieser Policy)	C.CA.CVC

2 ***Tabelle 2: Anwendungsbereich der Schlüssel und Zertifikate der CA***

3 Die privaten CA-Schlüssel dürfen nur für ihren jeweiligen Anwendungsbereich benutzt wer-
4 den. Eine Benutzung außerhalb des zugehörigen Anwendungsbereichs ist grundsätzlich
5 nicht zulässig. Ausnahmen bedürfen der ausdrücklichen Genehmigung durch den Policy-
6 Herausgeber. Die Schlüsselpaare C.CA.AUT und C.CA.ENC dürfen identisch sein.

7 3.2.6 Ende des Gültigkeitszeitraums von CA-Schlüsseln

8 Mit Ablauf des Gültigkeitszeitraums kann ein neues Zertifikat für den CA-Schlüssel erstellt
9 werden, wenn die empfohlenen Algorithmen und Schlüssellängen dies noch erlauben. Ist
10 dies nicht der Fall, werden neue CA-Schlüssel nach den dann gültigen Vorgaben gemäß
11 Kapitel 3.2.1 generiert und die alten privaten CA-Schlüssel sowie deren Backup gelöscht. Ein
12 Einsatz über den Gültigkeitszeitraum hinaus ist nicht gestattet.

13 CA-Zertifikate werden gesperrt, wenn die zugrunde liegenden Algorithmen und Schlüssel-
14 längen vom Algorithmenkatalog der Bundesnetzagentur nicht mehr zugelassen sind.

15 3.2.7 Verwaltung und Lebenszyklen der Hardware Security Module für die Zertifizie-
16 rung

17 Die Art und Stufe der Sicherheitsbestätigung des Hardware Security Module[3] (HSM) werden
18 durch den Policy-Herausgeber festgelegt.

19 a. Die Hardware Security Module für die Zertifizierung unterliegen während ihres ge-
20 samten Lebenszyklus folgenden Sicherheitsmaßnahmen:

21 b. Alle Arbeiten an einem HSM werden nach dem Vier-Augen-Prinzip und nur von auto-
22 risiertem Personal durchgeführt.

[3] Das Hardware Security Module kann auch eine Chipkarte sein.

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

d. Vor der Außerbetriebnahme eines HSM werden alle enthaltenen privaten Schlüssel gelöscht.

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

3.2.8 Erzeugung der Schlüssel für die HPC

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

a. Die in Tabelle 3 genannten Anforderungen an Schlüssellänge und verwendete Algorithmen für die Schlüsselpaare für Verschlüsselung oder Authentifizierung sind einzuhalten.

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

Schlüssellängen und Algorithmen für X.509-Zertifikate für den **Produktiveinsatz**:

Schlüsselpaar bzw. Zertifikat	**Algorithmus und Länge**	**Anmerkung**
C.HP.QES	Die Schlüssellängen müssen mindestens so groß sein, wie die empfohlenen Schlüssellängen im jeweiligen aktuellen Algorithmenkatalog der Bundesnetzagentur.	Mindestlänge für RSA derzeit 2048 Bit oder Algorithmen und Schlüssellängen mit vergleichbarer Sicherheit.
C.HP.ENC	wie C.HP.QES (Mindestlänge für RSA: derzeit 2048 Bit)	Ausnahme: wenn für C.HP.QES ECDSA verwendet wird, dann soll für das C.HP.ENC RSA ab 2048 Bit oder vergleichbar Sicheres verwendet werden.
C.HP.AUT	wie C.HP.QES (Mindestlänge für RSA: derzeit 2048 Bit)	

Tabelle 3: Schlüssellängen und Algorithmen für den Produktiveinsatz

3.2.9 Sicherheit der HPC

Die Sicherheitsanforderungen an die Chipkartenproduktion, Transport zum ZDA und Auslieferung an den Ausweisinhaber sind im, nach [SigG] bestätigten, Sicherheitskonzept des ZDA beschrieben.

3.2.10 Aufbringung weiterer Anwendungen

Applikationsfremde Daten oder Anwendungen[4] dürfen nur nach ausdrücklicher Genehmigung durch den Policy-Herausgeber in den verfügbaren Speicher der Chipkarte geladen werden.

3.3 Lebenszyklus der Endnutzerzertifikate der HPC

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-Herausgeber stellt durch Veröffentlichung insbesondere die folgenden Dokumente zur Verfügung:

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

Der ZDA ist für die Veröffentlichung seiner allgemeinen Vertragsbedingungen verantwortlich und muss diese den 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. Einholung der Bestätigung des Berufsgruppenattributs.

d. Einholung der Bestätigung ggf. weiterer Attribute.

e. Produktionsfreigabe durch den HPC-Herausgeber.

[4] Zusätzlich zu den verpflichtenden Anwendungen der [HPC-Spec].

3.3.2.1 Standardablauf und Identifizierung

Der Antrag für die Herausgabe der HPC 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 elektronischen Signatur, die dem Antragsteller zugeordnet ist, erfolgen. Der Antrag für die Herausgabe der HPC kann dabei auch zusammen mit einem Antrag für die Herausgabe der SMC kombiniert erfolgen.

Die Identifikation und Registrierung eines Antragstellers erfolgt gemäß den Vorgaben aus [SigG] und [SigV] für qualifizierte elektronische Signaturzertifikate. Damit wird gewährleistet, dass der Antrag für die Zertifikatsausstellung vollständig, korrekt sowie berechtigt ist.

Dabei gelten insbesondere die nachfolgenden Punkte:

a. Dem Antragsteller werden von dem ZDA neben den erforderlichen Formularen auch die Rechtsbelehrung, die Unterrichtungsunterlagen, die Allgemeinen Geschäftsbedingungen, sowie Merkblätter und alle weiteren Bestimmungen zur Zertifikatsnutzung schriftlich (z. B. in elektronischer Form oder gemäß den gesetzlichen Bestimmungen) zur Verfügung gestellt.

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 der HPC gemäß [HPC-Spec] 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 bei Antragstellung oder Ausweisübergabe zu identifizieren. Bei der Identifizierung muss der Antragsteller physisch anwesend sein. Alternativ kann – auch unter Verzicht der physischen Anwesenheit – eine Identifizierung mittels der eID-Funktion des Personalausweises vorgenommen werden.

e. Im Rahmen der Antragsprüfung ist eine Überprüfung der Berechtigung der Antragstellung notwendig. Hierzu hat der Antragsteller die entsprechenden Dokumente vorzulegen, die durch den HPC-Herausgeber gefordert werden.

f. Im Verlauf des Registrierungsprozesses hat der Antragsteller unter anderem folgende Punkte zu erfüllen:

    - Annahme der von dem Policy-Herausgeber und dem HPC-Herausgeber aufgestellten Verpflichtungen des Antragstellers, des Ausweisinhabers und des Anwenders,

- Annahme der von dem HPC-Herausgeber aufgestellten zusätzlichen Verpflichtungen des Antragstellers, des Ausweisinhabers und des Anwenders,
- Zustimmung zur Archivierung aller relevanten Dokumente des Registrierungsprozesses,
- Zustimmung, die beantragten Zertifikate in den entsprechenden Zertifikatsdiensten des ZDA überprüfbar zu halten,
- Zustimmung oder Verweigerung, die beantragten Zertifikate in weiteren Suchdiensten abrufbar zu halten,
- Jeweils Zustimmung zur Auskunftserteilung der bestätigenden Stelle eines Attributes gegenüber dem ZDA.

g. Alle relevanten Dokumente des Registrierungsprozesses für qualifizierte elektronische Signaturzertifikate werden mindestens über den gesetzlich vorgeschriebenen Zeitraum gemäß [SigG] und [SigV] hinweg archiviert. Die Archivierung muss den Anforderungen des [BDSG] genügen.

Der Antragsteller kann entweder einen Erstantrag oder einen Folgeantrag stellen. Der ZDA 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 Identifizierung eines anderen Antrags gestellt wird. Der Ausweisinhaber wird bei auslaufender Gültigkeit der Zertifikate seiner HPC entsprechend durch den ZDA informiert (z. B. per E-Mail, Fax oder Brief). Dabei muss der ZDA mitteilen, unter welchen Umständen und bis wann ein Folgeantrag gestellt werden kann. Bei einem Folgeantrag können die bei einem Erstantrag angefallenen Daten wieder verwendet werden. Insbesondere kann auf eine erneute Identifizierung des Antragstellers verzichtet werden, sofern die vorherige Identifizierung noch gemäß [SigG] und [SigV] verwendbar ist. Die Attributsbestätigungen sind gemäß dem CPS des ZDA zu erneuern.

Bei einem Folgeantrag muss die erneute Freigabe zur Produktion der HPC durch den HPC-Herausgeber erfolgen.

3.3.3 Freigabe zur Produktion

Der jeweilige HPC-Herausgeber besitzt die Entscheidungsbefugnis über die Freigabe zur Produktion einer HPC. Insbesondere behalten sich die HPC-Herausgeber vor, die Anzahl der gleichzeitig gültigen HPCs pro Antragsteller zu begrenzen.

Ohne Freigabe zur Produktion der HPC dürfen die X.509-Zertifikate der HPC nicht ausgestellt werden.

3.3.4 Ausstellung der Zertifikate

Der HPC-Herausgeber und der ZDA gewährleisten durch Einhaltung der nachfolgenden Punkte eine sichere Zertifikatsausstellung:

a. Alle sicherheitskritischen Tätigkeiten werden nur von autorisiertem Personal und 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 HPC-Herausgeber oder einer von diesem beauftragten Stelle und dem ZDA übertragen.

c. Die X.509-Zertifikate werden durch den ZDA gemäß den gesetzlichen Bestimmungen aus [SigG] und [SigV] sowie unter Einhaltung der [HPC-Spec] erstellt. Die X.509-Zertifikate einer HPC dürfen maximal fünf Jahre gültig sein.

d. Die Ausstellung der X.509-Zertifikate der HPC durch den ZDA erfolgt erst nach expliziter Freigabe in Schriftform oder elektronischer Form mit Hilfe einer qualifizierten elektronischen Signatur durch den jeweiligen HPC-Herausgeber.

e. Der HPC-Herausgeber wird schriftlich und/oder elektronisch durch den ZDA über das Ausstellen eines Zertifikates für die HPC informiert. Dabei werden mindestens die folgenden Informationen übermittelt, die eine zweifelsfreie Zuordnung des ausgestellten Zertifikates zu dem Zertifikatsinhaber ermöglichen:

   - Die Seriennummer des Zertifikates,
   - Der Gültigkeitszeitraum des Zertifikates,
   - Die Nummer der HPC, die das Zertifikat enthält; bei einem Attributzertifikat (C.HP.ATTR) ist dies die Nummer der HPC, die das dem Attributzertifikat zugeordnete qualifizierte elektronische Signaturzertifikat (C.HP.QES) enthält.
   - Der vollständige Name (Vornamen, Nachname, Geburtsname) des Zertifikatsinhabers.
   - Das Geburtsdatum und der Geburtsort des Zertifikatsinhabers.

Entsprechend wird auch die attributsbestätigende Stelle informiert, wenn diese nicht ebenfalls der HPC-Herausgeber ist.

f. Die Übergabe der HPC an den Antragsteller erfolgt auf sichere Art und Weise durch den ZDA, so dass gewährleistet ist, dass nur der Antragsteller die HPC, insbesondere den darin enthaltenen privaten Schlüssel des CV-Zertifikates (C.HP.CV), in Betrieb nehmen kann. Der Ausweisinhaber hat den Erhalt der HPC gegenüber dem ZDA revisionssicher zu bestätigten. Das Vorgehen hat der ZDA in seinem CPS zu beschreiben.

3.3.5 Veröffentlichung der Zertifikate

Der ZDA stellt einen Verzeichnisdienst zur Verfügung, der abrufbare Zertifikate[5] bereitstellt. Die Veröffentlichung betrifft nur die X.509-Zertifikate, die abrufbar gehalten werden sollen. Näheres dazu regelt der Policy-Herausgeber.

Für Dritte wird die Möglichkeit geschaffen, übergreifend in den Verzeichnisdiensten des Gesundheitswesens nach einem abrufbaren Zertifikat zu suchen. Als Ergebnis dieser Suche wird der Verweis auf das Zertifikat im Verzeichnisdienst des ZDA geliefert.

3.3.6 Überprüfbarkeit der Zertifikate

Der ZDA hat die von ihm nach dieser Policy ausgestellten Zertifikate gemäß den Anforderungen aus [SigG] für qualifizierte elektronische Signaturzertifikate (C.HP.QES) überprüfbar zu halten. Dies gilt auch für die Zertifikate für Verschlüsselung (C.HPC.ENC), Authentifizierung (C.HPC.AUT) sowie eventuelle Attributzertifikate (C.HP.ATTR) der HPC.

3.3.7 Sperrung von Zertifikaten

Das Sperren eines Zertifikats ist die vorzeitige Beendigung der Gültigkeit des Zertifikats. Eine Sperrung ist nur für X.509-Zertifikate vorgesehen. Insbesondere gelten folgende Punkte:

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

b. Es wird ein Sperrkennwort oder eine andere zuverlässige Identifizierung verwendet.

c. Neben den Ausweisinhaber können zuständige und Attribute bestätigende Stellen (gemäß § 8 [SigG]) einen Sperrantrag stellen. Dies ist insbesondere der HPC-Herausgeber sowie die von ihm beauftragten Stellen.

d. Vor der Sperrung hat der autorisierte Mitarbeiter des ZDA den Antrag auf seine Korrektheit hin zu prüfen, insbesondere die Berechtigung des Sperrenden.

[5] Zertifikate, die von diesem ZDA stammen und im Sinne dieser Policy ausgestellt wurden.

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

f. Eine 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 von dem HPC-Herausgeber in Rücksprache mit seinem Policy-Herausgeber festgelegt.

h. Wird ein Zertifikat gesperrt, informiert der ZDA den Zertifikatsinhaber (sofern zutreffend ist dies der Ausweisinhaber), den HPC-Herausgeber sowie ggf. die Attributsbestätigende Stelle in Schriftform, Textform oder elektronischer Form (mit Hilfe einer qualifizierten elektronischen Signatur) über die Sperrung des Zertifikats. Dies umfasst mindestens die folgenden Angaben:

   - Seriennummer des Zertifikates,
   - Sperrzeitpunkt.

Wenn entweder das qualifizierte elektronische Signaturzertifikat (C.HP.QES), das Authentifizierungszertifikat (C.HP.AUT) oder das Verschlüsselungszertifikat (C.HP.ENC) gesperrt wird, werden automatisch alle anderen X.509-Zertifikate gesperrt, die sich auf der selben HPC befinden und nach dieser Policy ausgestellt wurden.

3.3.8 Zertifikatserneuerung bei Schlüsselbeibehaltung

Es ist möglich, dass unter Beibehaltung der Schlüsselpaare neue Zertifikate für eine HPC auf Antrag des Ausweisinhabers ausgestellt werden. Dies darf aber nur erfolgen, wenn die betroffenen Schlüsselpaare bzw. die Schlüssellängen und Algorithmen noch hinreichend sicher sind. Eine neue Produktionsfreigabe durch den HPC-Herausgeber ist hierbei zwingend notwendig.

Die neu ausgestellten Zertifikate können in einem sicheren Verfahren in die HPC eingebracht (ausgetauscht) werden. Dies gilt vor allem für die Zertifikate für Authentifizierung (C.HP.AUT), Verschlüsselung (C.HP.ENC) sowie eventuell vorhandene Attributzertifikate (C.HP.ATTR). Die Zulässigkeit für das qualifizierte elektronische Signaturzertifikat (C.HP.QES) unterliegt dabei den Auflagen aus [SigG] und [SigV]. Sofern der ZDA den Austausch von Zertifikaten in der HPC ermöglicht, hat er das Verfahren in seinem CPS zu beschreiben.

3.4 Verwaltung und Betrieb der Zertifizierungsstelle

Neben den Auflagen aus [SigG] und [SigV] für qualifizierte elektronische Signaturzertifikate ist ein ZDA verpflichtet, die im Folgenden beschriebenen Punkte zu gewährleisten. Begründete Abweichungen sind zulässig, benötigen jedoch der schriftlichen Genehmigung durch den Policy-Herausgeber.

3.4.1 Sicherheitsmanagement

Für das Sicherheitsmanagement gelten die nachfolgenden Punkte:

a. Der ZDA ist für alle Abläufe und Prozesse der von ihm angebotenen Dienste verantwortlich. An den ZDA werden klare Forderungen gestellt, deren Einhaltung durch entsprechende Kontrollfunktionen überprüft wird. Die für die Einhaltung der Sicherheit relevanten Maßnahmen werden im CPS des ZDA definiert und dem HPC-Herausgeber 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 ZDA ist in seinem Wirkungsbereich für die Definition der Sicherheitsrichtlinien und deren Weitergabe an das betroffene Personal verantwortlich.

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

3.4.2 Informationsklassifizierung und –verwaltung

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

3.4.3 Personelle Sicherheitsmaßnahmen

Neben den Anforderungen nach [SigG] und [SigV] stellen die Herausgeber die folgenden Anforderungen an das eingesetzte Personal:

a. Der ZDA 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 ZDA ausführlich beschrieben. Diese Beschreibungen umfassen unter anderem neben den Pflichten auch die Rechte und erforderlichen Kompetenzen.

c. In dem CPS des ZDA 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 ZDA 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 werden.

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 ZDA geregelt.

3.4.5 Management des Betriebes

Der ZDA 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 die Anwender-relevanten Teile dem HPC-Herausgeber zur Verfügung gestellt.

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 ZDA) 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 Zertifikatsmanagement 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 Entwicklung und Wartung vertrauenswürdiger Systeme

Der HPC-Herausgeber und der ZDA setzen in den vertrauenswürdigen Systemen Komponenten ein, die ausreichend gegen unautorisierte Veränderungen geschützt sind. Bei der Entwicklung vertrauenswürdiger Systeme erfolgt in der Designphase und der Spezifikation der Anforderungen eine Analyse der Sicherheitsanforderungen. Dies gilt auch, wenn für die Entwicklung ein Dritter beauftragt wird. Alle Änderungen an vertrauenswürdigen Systemen unterliegen einem vom ZDA festgelegten Verfahren mit Kontrolle und Dokumentation der einzelnen Schritte. Die benötigten Maßnahmen dazu werden im CPS bzw. Sicherheitskonzept des ZDA beschrieben.

3.4.8 Aufrechterhaltung des ungestörten Betriebes und Behandlung von Zwischenfällen

Nach dem Eintreten von Katastrophenfällen sind der HPC-Herausgeber und der ZDA darum bemüht, möglichst kurzfristig den sicheren, geregelten Betrieb wieder aufzunehmen. Dabei gilt insbesondere, dass die Policy-Herausgeber schon einen begründeten Kompromittierungsverdacht eines Zertifizierungsschlüssels als Katastrophenfall einstufen. Sollte dieser Fall eintreten, ergreift der betroffene ZDA Maßnahmen, welche zusammen mit dem HPC-Herausgeber ggf. mit Unterstützung des entsprechenden Policy-Herausgebers in einem Notfallplan festgelegt werden. Der Notfallplan ist Bestandteil des Sicherheitskonzepts bzw. CPS des ZDA.

3.4.9 Einstellung der Tätigkeit

Der ZDA meldet gemäß [SigG] die Einstellung der Tätigkeit rechtzeitig der zuständigen Behörde, dem HPC-Herausgeber und allen Policy-Herausgebern. Für den Fall der Einstellung der Tätigkeit erarbeitet der ZDA 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 ZDA beschrieben. Insbesondere muss die Übergabe der Zertifikate an einen weiteren ZDA sichergestellt sein. 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 HPC-Herausgeber und der ZDA gewährleisten die Einhaltung der gesetzlichen Vorgaben aus [SigG] und [SigV], dem [BDSG], sowie die sich aus [HPC-Spec] und dieser Policy ergebenden Anforderungen, in ihrer jeweils gültigen Fassung. Dabei wird insbesondere auf die Einhaltung der Datenschutzanforderungen im [BDSG] 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 offen gelegt.

3.4.11 Aufbewahrung von Informationen zu Zertifikaten

Der HPC-Herausgeber und der ZDA bewahren alle Informationen zu Zertifikaten gemäß den gesetzlichen Vorgaben aus [SigG] und [SigV] für qualifizierte elektronische Signaturzertifikate und dem [BDSG] auf. Dabei gelten insbesondere nachfolgende Punkte:

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

b. Die Archivierung der Daten erfolgt gemäß den Richtlinien des in Punkt a genannten CPS.

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

d. Nur autorisiertes Personal kann archivierte Daten löschen. Die Löschung darf erst nach erfolgreicher Authentisierung 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, C.HP.ATTR) der HPC werden archiviert:

a. Das Zertifikat,

b. 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,

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

g. Die Seriennummer des Chips der HPC (ICCSN) und die Zuordnung zum Ausweisinhaber werden für drei zusätzliche Jahre aufbewahrt, nachdem sie von sämtlichen gültigen elektronischen Gesundheitskarten nicht mehr akzeptiert werden. Der ZDA hat dem HPC-Herausgeber bei Bedarf Auskunft über diese Daten zu geben.

4 Anhang A – Verzeichnisse

4.1 Abkürzungsverzeichnis

BAK	Bundesapothekerkammer
BÄK	Bundesärztekammer
BDSG	Bundesdatenschutzgesetz
BPtK	Bundespsychotherapeutenkammer
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	Beispielsweise
BZÄK	Bundeszahnärztekammer
bzw.	beziehungsweise
C.HP.ATTR	Ein Attributzertifikat der HPC
C.HP.AUT	Das Zertifikat der Anwendung “Authentifizierung” der HPC
C.HP.CVC	Das CV-Zertifikat der HPC
C.HP.ENC	Das Zertifikat der Anwendung „Ent- und Verschlüsselung“ der HPC (engl. encode)
C.HP.QES	Das Zertifikat der Anwendung „Qualifizierte Elektronische Signatur“ der HPC
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practise Statement
CRL	Certificate Revocation List
CV	Card Verifiable
CV-AUT	Card Verifiable Authentication Certificates
CVC	Card Verifiable Certificate
CV-Zertifikat	Card Verifiable Zertifikat
evtl.	Eventuell
HPA	Health Professional Application
HPC	Health Professional Card
HSM	Hardware Security Module
ICCSN	Integrated Circuit Card Serial Number
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KZBV	Kassenzahnärztliche Bundesvereinigung
OCSP	Online Certificate Status Protocol
OID	Object Identifier

PIN	Personal Identification Number / Persönliche Identifikationsnummer
PUK	PIN Unblocking Key
SGB V	Sozialgesetzbuch, Fünftes Buch
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz)
SigV	Verordnung zur elektronischen Signatur (Signaturverordnung)
SMC	Security Module Card
ZDA	Zertifizierungsdiensteanbieter

4.2 Literaturverzeichnis

Zugehörige Dokumente der Policy-Herausgeber	
[HPC-Spec]	Bundesapothekerkammer, Bundesärztekammer, Bundespsychotherapeutenkammer, Bundeszahnärztekammer, Deutsche Krankenhausgesellschaft, Kassenärztliche Vereinigung, Kassenzahnärztliche Vereinigung: *„German Health Professional Card and Security Module Card, Part 1, Part 2 und Part 3“, in Version 2.3.1 und neuer*

Externe Dokumente	
[BDSG]	Bundesdatenschutzgesetz
[SGB V]	Sozialgesetzbuch Nummer Fünf (SGB V)
[SigG]	Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16.05.2001 (BGBl. I Nr. 22 2001 S. 876 ff) zuletzt geändert durch: Artikel 4 des Gesetzes vom 17.07.2009 (BGBl. I S. 2091)
[SigV]	Verordnung zur elektronischen Signatur vom 16.11.2001 BGBl. I Nr. 59 2001 S. 3074 ff) zuletzt geändert durch die Zweite Verordnung zur Änderung der Signaturverordnung vom 15. November 2010, (BGBl I Nr. 57 S. 1542ff vom 22.11.2010)

4.3 Abbildungsverzeichnis

4.4 Tabellenverzeichnis

1

5 Anhang B – Abweichungen im Test- und Übergangszeitraum

Für die HPC müssen Chipkarten zum Einsatz kommen, die konform zu einer von den Policy-Herausgebern vorgegebenen HPC-Spezifikation [HPC-Spec] sind. Im Realbetrieb müssen diese Chipkarten zusätzlich bestätigt sein. Aufgrund der Natur der Testmaßnamen kann während des Testzeitraumes von der Notwendigkeit der Bestätigung der Chipkarte sowie einer Akkreditierung der Gesamtprozesse abgewichen werden. Dabei müssen jedoch insbesondere folgende Randbedingungen beachtet werden:

- CV-Zertifikate müssen unterstützt werden.
- Die logische Struktur der Files auf der Chipkarte und die standardisierten Applikationen gemäß [HPC-Spec] müssen implementiert sein.

Für den Test- und Übergangszeitraum können auch ZDA tätig werden und Zertifikate nach dieser Policy ausstellen, die eine Akkreditierung anstreben und sich in der Bestätigung durch eine Prüf- bzw. Bestätigungsstelle nach [SigG] befinden. Naturgemäß bezieht sich diese Akkreditierung auf eine qualifizierte Signaturkarte, die nicht notwendiger Weise eine HPC ist.

5.1 Abweichende Bestimmungen für den Testzeitraum

Von den regulären Anforderungen abweichend können in einem von den Policy-Herausgebern zu definierenden Testzeitraum für die HPC auch Zertifikate für fortgeschrittene Signaturen (C.HP.SIG) erstellt werden. Bei der Verwendung von Signaturen auf Basis dieser fortgeschrittenen Zertifikate ist jederzeit die erforderliche Rechtssicherheit entsprechend dem Formerfordernis ggf. über ein paralleles oder zusätzliches Verfahren (notfalls papierbasiert mit Unterschrift) sicherzustellen.

Die Konformität mit dieser Policy kann im Testzeitraum durch den ZDA schriftlich erklärt werden. Für die Angabe der Zertifikatspolicy in den Zertifikaten des Testzeitraums kann die selbe OID (dieser Zertifikatspolicy, siehe Kapitel 1.5) verwendet werden. Die Policy-Herausgeber behalten sich vor, zu prüfen, ob die Anforderungen der Policy erfüllt werden.

Die Anforderungen an das Ausstellen von Zertifikaten für qualifizierte Signaturen werden auch für den Testzeitraum angestrebt. Der Testzeitraum dient damit zur endgültigen Ausgestaltung der signaturgesetzkonformen Prozesse zur Ausgabe von qualifizierten Zertifikaten und ist in § 291a [SGB V] geregelt.

Nachdem Ausgabeprozesse und die Chipkarte der HPC nach [SigG] auf qualifiziertem Niveau bestätigt sind, werden für das Signatur-Zertifikat der HPC ausschließlich Zertifikate für qualifizierte Signaturen ausgestellt.

5.2 Abweichende Bestimmungen für den Übergangszeitraum

Sobald die HPC mit Signaturzertifikaten auf qualifiziertem Niveau erstellt und ausgegeben wird, dürfen nach einer von den Policy-Herausgebern zu definierenden Übergangszeit im heilberuflichen Kontext mit der HPC als Heilberufs- bzw. Berufsausweis ausschließlich elektronische Unterschriften auf Basis von qualifizierten Zertifikaten (C.HP.QES) erstellt werden; eine weitere Verwendung der fortgeschrittenen Zertifikate der HPC (C.HP.SIG) ist in diesem Kontext nicht zulässig.

Das Ende des Übergangszeitraums wird öffentlich erklärt.

6 Anhang C – Verhältnis HPC- zu Policy-Herausgeber (informativ)

Die nachfolgende Abbildung zeigt informativ die Beziehungen zwischen den Policy-Herausgebern, den HPC-Herausgebern und den ZDA.

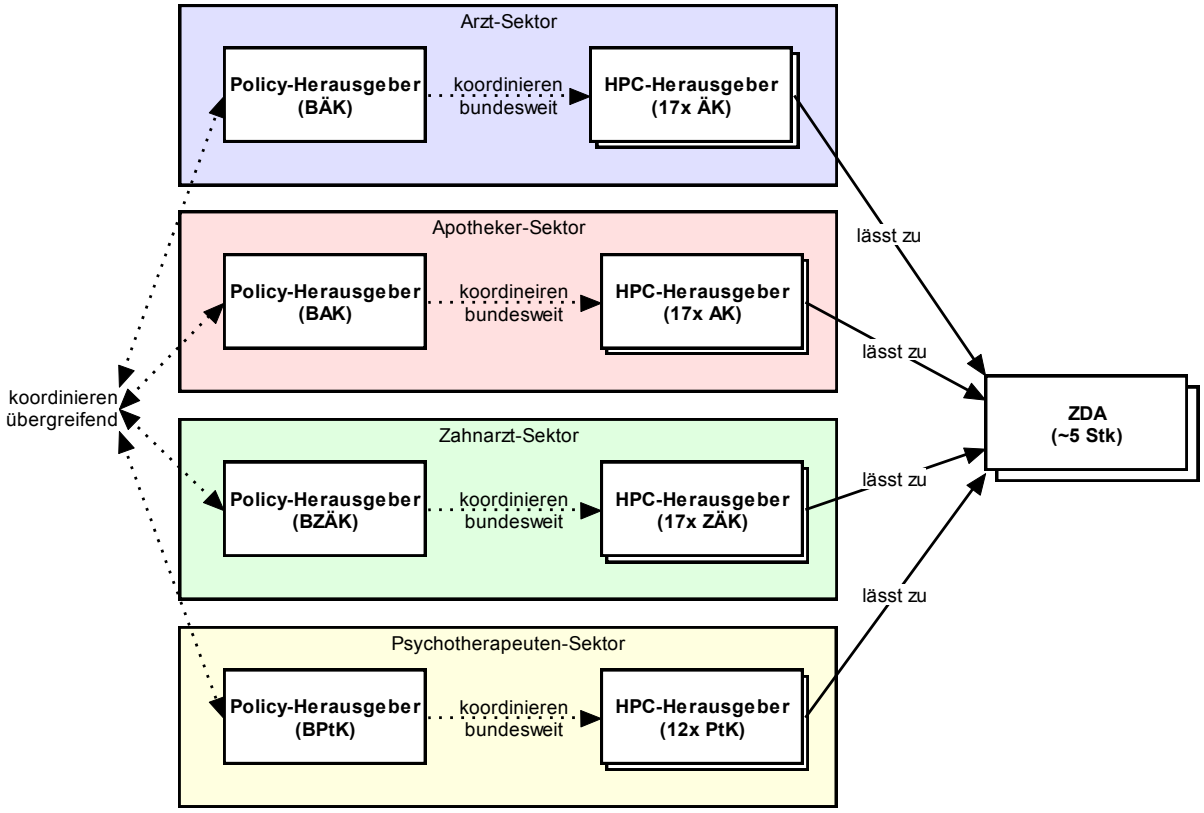

Abbildung 1: Beziehungen zwischen Policy- und HPC-Herausgebern und den ZDA (informativ)

Zur Zeit existieren fünf Policy-Herausgeber. Dies macht für den ärztlichen, den pharmazeutischen, den psychotherapeutischen und den zahnärztlichen Bereich 63 (=3x17 + 1x12) verschiedene HPC-Herausgeber.