

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

Gemeinsame Policy für die Ausgabe der HPC

Zertifikatsrichtlinie HPC

Version: 1.0.0

08.06.2009



Bundesapothekerkammer

Bundesärztekammer

Bundespsychotherapeutenkammer

Bundeszahnärztekammer

Kassenzahnärztliche Bundesvereinigung

1 **Impressum**

2

3 Herausgeber **Bundesapothekerkammer**
4 **Bundesärztekammer**
5 **Bundespsychotherapeutenkammer**
6 **Bundeszahnärztekammer**
7 **Kassenzahnärztliche Bundesvereinigung**

8

9 Editor Bundesapothekerkammer
10 c/o Apothekerhaus Eschborn
11 Martin Bergen
12 Carl-Mannich-Str. 26
13 65760 Eschborn

14

15 © 2009 Copyright Bundesapothekerkammer,
16 Bundesärztekammer
17 Bundespsychotherapeutenkammer
18 Bundeszahnärztekammer
19 Kassenzahnärztliche Bundesvereinigung

20

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

2 Veröffentlichte Versionen sind **fett** markiert.

3

1	Inhaltsverzeichnis	
2	Impressum	2
3	Versionshistorie	3
4	Inhaltsverzeichnis	4
5	1 Einleitung und Begriffsbestimmung	6
6	1.1 Rechtliche Einordnung	6
7	1.2 Dokumentenidentifikation	7
8	1.3 Begriffsdefinition	7
9	1.4 Organisatorisches	9
10	1.5 Übereinstimmung des Object Identifier	9
11	1.6 Aufteilung der Kapitel	9
12	2 Verpflichtungen und Haftungsbestimmungen	10
13	2.1 Verpflichtungen des Policy-Herausgebers und des HPC-Herausgebers	10
14	2.2 Verpflichtungen des ZDA	10
15	2.3 Verpflichtungen des Antragstellers, des Ausweisinhabers und des Anwenders	10
16	2.4 Verpflichtungen des Überprüfers	12
17	2.5 Haftungsbestimmungen	13
18	2.5.1 Haftung des ZDA	13
19	2.5.2 Haftung des HPC-Herausgebers	13
20	2.5.3 Haftung des Ausweisinhabers	13
21	2.5.4 Haftungsausschluss des Policy-Herausgebers	13
22	3 Anforderungen an die Erbringung von Zertifizierungsdiensten	14
23	3.1 Certification Practice Statement (CPS)	14
24	3.2 Verwaltung von Schlüsseln zur Erbringung von Zertifizierungsdiensten	14
25	3.2.1 Erzeugung der CA-Schlüssel	14
26	3.2.2 Speicherung und Backup von CA-Schlüsseln	15
27	3.2.3 Verteilung und Veröffentlichung der öffentlichen CA-Schlüssel	15
28	3.2.4 Verteilung und Veröffentlichung der privaten CA-Schlüssel	15
29	3.2.5 Verwendungszweck der CA-Schlüssel	15
30	3.2.6 Ende des Gültigkeitszeitraums von CA-Schlüsseln	16
31	3.2.7 Verwaltung und Lebenszyklen der Hardware Security Module für die Zertifizierung	16
32	3.2.8 Erzeugung der Schlüssel für die HPC	17
33	3.2.9 Sicherheit der HPC	18
34	3.2.10 Aufbringung weiterer Anwendungen	18
35	3.3 Lebenszyklus der Endnutzerzertifikate der HPC	18
36	3.3.1 Bekanntmachung der Vertragsbedingungen	18
37	3.3.2 Registrierung des Antragstellers	18
38	3.3.3 Freigabe zur Produktion	20
39	3.3.4 Ausstellung der Zertifikate	21
40	3.3.5 Veröffentlichung der Zertifikate	22
41	3.3.6 Überprüfbarkeit der Zertifikate	22
42	3.3.7 Sperrung von Zertifikaten	22
43	3.3.8 Zertifikatserneuerung bei Schlüsselbeibehaltung	23

1	3.4	Verwaltung und Betrieb der Zertifizierungsstelle.....	23
2	3.4.1	Sicherheitsmanagement.....	24
3	3.4.2	Informationsklassifizierung und –verwaltung.....	24
4	3.4.3	Personelle Sicherheitsmaßnahmen.....	24
5	3.4.4	Physikalische und organisatorische Sicherheitsmaßnahmen	25
6	3.4.5	Management des Betriebes.....	25
7	3.4.6	Zugriffsverwaltung	26
8	3.4.7	Entwicklung und Wartung vertrauenswürdiger Systeme.....	26
9	3.4.8	Aufrechterhaltung des ungestörten Betriebes und Behandlung von Zwischenfällen	27
10	3.4.9	Einstellung der Tätigkeit	27
11	3.4.10	Übereinstimmung mit gesetzlichen Anforderungen.....	28
12	3.4.11	Aufbewahrung von Informationen zu Zertifikaten.....	28
13	4	Anhang A – Verzeichnisse.....	30
14	4.1	Abkürzungsverzeichnis.....	30
15	4.2	Literaturverzeichnis	31
16	4.3	Abbildungsverzeichnis.....	31
17	4.4	Tabellenverzeichnis	31
18	5	Anhang B – Abweichungen im Test- und Übergangszeitraum	32
19	5.1	Abweichende Bestimmungen für den Testzeitraum.....	32
20	5.2	Abweichende Bestimmungen für den Übergangszeitraum	33
21	6	Anhang C – Verhältnis HPC- zu Policy-Herausgeber (informativ)	34
22			
23			

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-Zertifikate¹ 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 *Bundesdatenschutzgesetz* [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 1.2 Dokumentenidentifikation

2	Dokumententyp:	Certificate Policy
3	Name dieses Dokumentes:	Gemeinsame Policy für die Ausgabe der HPC
4	Kurzname dieses Dokumentes:	Zertifikatsrichtlinie HPC
5	Referenz für dieses Dokument:	[CP-HPC]
6	Version:	1.0.0 vom 08.06.2009
7	Object Identifier:	1.2.276.0.76.4.62 {policy-hba-010000-cp}

8 1.3 Begriffsdefinition

9 Es wird grundlegend zwischen dem *Policy-Herausgeber*, dem *HPC-Herausgeber*, dem *An-*
10 *tragsteller*, dem *Ausweisinhaber* (Endnutzer), dem *Anwender* und dem *Zertifizierungsdienst-*
11 *eanbieter* (ZDA) als Akteure unterschieden. Dabei stehen diese in einem bestimmten Ver-
12 hältnis zueinander: Ein Antragsteller beantragt bei einem ZDA die Ausstellung von Zertifika-
13 ten. Ein HPC-Herausgeber lässt einen (oder mehrere) ZDA in seinem Bereich zu. Ein Policy-
14 Herausgeber koordiniert die bundesweit einheitlichen Vorgaben der HPC-Herausgeber sei-
15 nes Bereichs. Die Policy-Herausgeber koordinieren sich untereinander auf Bundesebene.

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

20 Die Ausstellung der Zertifikate einer HPC beantragt der Antragsteller bei einem ganz konkre-
21 ten ZDA. Der Text dieser Policy orientiert sich daher aus Sicht des Antragstellers an der Sin-
22 gularform der verschiedenen Parteien, auch wenn z.B. mehrere HPC-Herausgeber parallel
23 (unabhängig) zueinander existieren. Sollte eine Aufgabe durch mehrere bzw. alle z. B. Poli-
24 cy-Herausgeber in Zusammenarbeit erfüllt werden, wird dies besonders kenntlich gemacht.

25 Es werden folgende Rollen und Begriffe definiert

26 • Der **Policy-Herausgeber** im Sinne dieser Policy entspricht einem der Herausgeber
27 dieses Dokumentes. Die Gesamtheit aller Policy-Herausgeber ist für die Herausgabe
28 dieser Policy verantwortlich. Im Impressum sind die Policy-Herausgeber unter Her-
29 ausgeber aufgeführt. Die Policy-Herausgeber koordinieren die bundesweiten Vorga-
30 ben der ihnen jeweils zugeordneten HPC-Herausgeber. (Vgl. dazu *Anhang C – Ver-*
31 *hältnis HPC- zu Policy-Herausgeber (informativ)*).

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

- 1 ihn zuständigen Policy-Herausgeber über die Aufnahme seiner Tätigkeit informieren
2 der die bundesweit einheitlichen Vorgaben für seinen Bereich koordiniert.
- 3 • Der **Antragsteller** im Sinne dieser Policy ist eine natürliche Person, die eine HPC
4 nach dieser Policy bei einem für ihn zuständigen HPC-Herausgeber bzw. ZDA bean-
5 tragt. Eine Liste der möglichen Antragsteller (z.B. Apotheker, Ärzte, Psychotherapeu-
6 ten und Zahnärzte) wird durch den jeweiligen HPC-Herausgeber veröffentlicht. Mit
7 Besitz einer HPC ergeben sich im Sinne der vorliegenden Policy folgende zusätzliche
8 Rollen für den Antragsteller:
 - 9 ○ Der **Ausweisinhaber** im Sinne dieser Policy ist eine natürliche Person, die
10 eine nach dieser Policy ausgegebene HPC erhält und für deren Verwendung
11 alleinig verantwortlich ist. Aufgrund der persönlichen Bindung sind Ausweisin-
12 haber und Antragsteller identisch.
 - 13 ○ Der **Zertifikatsinhaber** im Sinne dieser Policy ist die natürliche Person, auf
14 die ein Zertifikat gemäß dieser Policy ausgestellt wurde und in der alleinigen
15 Kontrolle über den diesem Zertifikat zugeordneten privaten Schlüssel ist.
 - 16 ○ Der **Anwender** im Sinne dieser Policy ist eine natürliche Person, die ein Zerti-
17 fikate und den damit verbundenen privaten Schlüssel, welche nach dieser Poli-
18 cy ausgestellt wurden, verwendet. Der Anwender ist immer auch der Ausweis-
19 inhaber und Zertifikatsinhaber.
 - 20 • Der **Überprüfer** im Sinne dieser Policy ist eine Person, die ein signiertes Element
21 und insbesondere das verwendete Zertifikat überprüft.
 - 22 • Der **Zertifizierungsdiensteanbieter (ZDA)** im Sinne dieser Policy ist ein akkreditier-
23 ter Zertifizierungsdiensteanbieter nach [SigG], der für einen HPC-Herausgeber tätig
24 ist und Zertifikate nach dieser Policy ausstellt. Ein ZDA kann für mehrere HPC-
25 Herausgeber tätig sein.
 - 26 • Die **HPC** im Sinne dieser Policy ist eine Chipkarte gemäß [HPC-Spec], die mindes-
27 tens X.509-Zertifikate enthält, die nach dieser Policy ausgestellt wurden. Die Zertifika-
28 te der HPC bilden hierbei die kryptografische Identität einer Person in der elektroni-
29 schen Welt ab. Der Zugriff auf die privaten Schlüssel einer HPC ist nur nach vorheri-
30 ger und erfolgreicher Eingabe einer PIN möglich. Eine HPC im Sinne dieser Policy
31 wird auch Heilberufsausweis oder Berufsausweis genannt.
 - 32 • Ein **Endnutzerzertifikat** ist ein Zertifikat, dass zu einem in der HPC gespeicherten
33 privaten Schlüssel gehört und auf den Ausweisinhaber als Zertifikatsinhaber ausge-
34 stellt ist.

1 1.4 Organisatorisches

2 Nur die Policy-Herausgeber gemeinsam haben die Entscheidungsbefugnis über die Inhalte
3 dieser Policy. Sie diskutieren alle Änderungen an der Policy im Vorfeld mit den entsprechen-
4 den ZDA und legen gemeinsam entsprechende Migrationsfristen fest.

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

8 Vorgaben, Anforderung, weitere Bestimmungen u. ä. trifft der HPC-Herausgeber gegenüber
9 dem ZDA nur nach vorheriger Absprache mit seinem Policy-Herausgeber, der ggf. sich wie-
10 derum auf Bundesebene mit den übrigen Policy-Herausgebern abstimmen muss.

11 1.5 Übereinstimmung des Object Identifier

12 Der in Kapitel 1.2 aufgeführte *Object Identifier* (OID) wird nur für die Erstellung von Zertifika-
13 ten gemäß dieser Policy verwendet und wird in das jeweilige Zertifikat (in die Extension
14 *certificatePolicies*) gemäß [HPC-Spec] aufgenommen.

15 1.6 Aufteilung der Kapitel

16 Die nachfolgenden Kapitel dienen insbesondere dazu, die Mindestanforderungen an die für
17 Authentifizierung und Ver- und Entschlüsselung benötigten Zertifikate zu definieren. Für qua-
18 lifizierte Zertifikate bestehen zusätzlich weitergehende Anforderungen aus dem [SigG] und
19 [SigV].

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

22 In Kapitel 3 werden die Vorgaben für einen ZDA festgelegt, nach denen dieser seine Zerti-
23 fizierungsdienstleistung zu erfüllen hat. Implizit werden dabei Vorgaben an den Antragspro-
24 zess und die Ausweisinhaber getroffen.

25 In Kapitel 4 werden als Anhang A die in diesem Dokument verwendeten Verzeichnisse auf-
26 geführt.

27 In Kapitel 5 werden als Anlage B die abweichenden Bestimmungen für den Test- und Über-
28 gangszeitraum festgelegt.

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

1 **2 Verpflichtungen und Haftungsbestimmungen**

2 In diesem Kapitel werden die Verpflichtungen und Haftungsbedingungen geklärt.

3 **2.1 Verpflichtungen des Policy-Herausgebers und des HPC-Herausgebers**

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

9 **2.2 Verpflichtungen des ZDA**

10 Der ZDA ist verpflichtet, seine Zertifizierungsdienstleistungen gemäß dieser Zertifikatsrichtli-
11 nie (*Certificate Policy* – CP) sowie seinem *Certification Practice Statement* (CPS) anzubieten
12 und auszuführen. Dies dokumentiert er gemäß Kapitel 1.5 unter anderem durch die Aufnah-
13 me der in Kapitel 1.2 angegebenen OID in die Endnutzerzertifikate.

14 Der ZDA stellt insbesondere eine Liste mit Komponenten und Verfahren zur sicheren Erstel-
15 lung insbesondere einer qualifizierten elektronischen Signatur und zur Signaturprüfung bereit
16 und macht diese dem Ausweisinhaber zugänglich.

17 **2.3 Verpflichtungen des Antragstellers, des Ausweisinhabers und des An-** 18 **wenders**

19 Der Antragsteller wird vertraglich zur Einhaltung der nachfolgend aufgeführten Verpflichtun-
20 gen im Rahmen des Registrierungsprozesses (siehe dazu auch Kapitel 3.3.2) verpflichtet.
21 Das Akzeptieren der Vertragsbedingungen wird dabei durch Leisten einer rechtsgültigen
22 Unterschrift des Antragstellers dokumentiert.

23 Aufgrund der persönlichen Bindung sind bei der HPC der Antragsteller, der Ausweisinhaber
24 und der Anwender identisch.

25 Die Verpflichtungen beinhalten insbesondere:

- 26 a. Der Antragsteller macht korrekte, wahrheitsgetreue und vollständige Angaben zu den
27 benötigten Informationen. Dies gilt insbesondere für den Registrierungsprozess.
- 28 b. Der Ausweisinhaber ergreift die notwendigen Vorsichtsmaßnahmen, um einen unbe-
29 fugten Einsatz seiner privaten Schlüssel zu verhindern. Auch nach Ablauf des Gültig-
30 keitszeitraums hat er dafür zu sorgen, dass seine privaten Schlüssel sowie die zuge-
31 hörige sichere Signaturerstellungseinheit (die HPC) nicht missbräuchlich verwendet

1 werden kann. Bei Entsorgung muss die sichere Signaturerstellungseinheit sicher ver-
2 nichtet bzw. unbrauchbar gemacht werden² (beispielsweise durch das physische Zer-
3 stören des Chips der HPC).

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

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

8 (Der ZDA ist wiederum verpflichtet, bei einer Sperrung auch den HPC-Herausgeber
9 zu informieren. Näheres dazu regelt Kapitel 3.3.7)

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

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

12 ***Tabelle 1: Anwendungsbereiche der Schlüsselpaar und Zertifikate der HPC***

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

18 e. Der Anwender soll für die qualifizierte elektronische Signatur ausschließlich Kompo-
19 nenten und Verfahren einsetzen, welche nach [SigG] bestätigt sind.

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

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

1 2.4 Verpflichtungen des Überprüfers

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

- 5 a. Der Überprüfer kontrolliert die Gültigkeit des Zertifikats in Bezug auf den Signaturers-
6 tellungszeitpunkt bzw. Authentifizierungszeitpunkt und dem zu Grunde liegenden Gül-
7 tigkeitsmodell. Als Gültigkeitsmodell für alle Zertifikatsklassen wird das Kettenmodell
8 definiert. Der Gültigkeitszeitraum der X.509-Zertifikate für Authentisierung
9 (C.HP.AUT) und Verschlüsselung (C.HP.ENC) soll den Gültigkeitszeitraum ihrer Aus-
10 steller-Zertifikate (CA- und Root-Zertifikate) nicht übersteigen.
- 11 b. Der Überprüfer kontrolliert den Status des Zertifikats. Der das Zertifikat ausstellende
12 ZDA stellt dazu entsprechende Abfragedienste zur Verfügung.
- 13 c. Der Überprüfer achtet auf die Anwendungsbereiche des Zertifikats und die damit ver-
14 bundenen Einschränkungen .
- 15 d. Die Schlüsselpaare und Zertifikate dürfen nur für ihren jeweiligen Anwendungsbe-
16 reich benutzt werden. Eine Benutzung außerhalb des zugehörigen Anwendungsbe-
17 reichs ist nicht zulässig. Insbesondere ist das Schlüsselpaar bzw. Zertifikat
18 C.HP.QES ausschließlich für die qualifizierte elektronische Signatur nach [SigG] im
19 Sinne der *Nicht-Abstreitbarkeit (non-repudiation bzw. content commitment)* einzuset-
20 zen.
- 21 e. Der Überprüfer hat die Sorgfaltspflicht, seine IT-Infrastruktur zu schützen. Insbeson-
22 dere gilt:
- 23 • Er muss die Auflagen des Software-Herstellers der Signaturanwendungs-
24 komponente, wie sie in der Bedienungsanleitung beschrieben sind, erfüllen.
 - 25 • Er darf neue Root-Zertifikate nur nach sorgfältiger Prüfung (Vergleich des
26 *Fingerprints* des Root-Zertifikats mit dem vertrauenswürdig veröffentlichten
27 Fingerprint des echten Root-Zertifikats) im Rechner-Betriebssystem und in die
28 Software installieren. Ein automatisiertes Verfahren setzt voraus, dass die
29 Signaturanwendungskomponente dies sicher unterstützt. Dabei verlagert sich
30 dann die Prüfpflicht des Überprüfers vom Root-Zertifikat auf den verwendeten
31 Vertrauensanker (z.B. ein TSL-Signaturzertifikat).
- 32 f. Er muss evtl. Nutzungsbeschränkungen im Zertifikat berücksichtigen.
- 33 g. Eine Aussage über die Gültigkeit der qualifizierten elektronischen Signatur wird über
34 eine zugelassene, im Amtsblatt der BNetzA aufgeführte, Signaturanwendungs-
35 komponente getroffen.

1 **2.5 Haftungsbestimmungen**

2 Grundsätzlich gelten mindestens die nachfolgend aufgeführten Haftungsbestimmungen.

3 **2.5.1 Haftung des ZDA**

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

9 **2.5.2 Haftung des HPC-Herausgebers**

10 Der HPC-Herausgeber haftet für Schäden – gleich aus welchem Rechtsgrund – nur bei Vor-
11 satz oder grober Fahrlässigkeit sowie im Falle schuldhafter Verletzung wesentlicher Pflich-
12 ten. Die voran genannten Haftungsbeschränkungen gelten nicht für schuldhaft verursachte
13 Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit sowie die Haf-
14 tung nach dem Produkthaftungsgesetz.

15 **2.5.3 Haftung des Ausweisinhabers**

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

17 **2.5.4 Haftungsausschluss des Policy-Herausgebers**

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

20

1 **3 Anforderungen an die Erbringung von Zertifizierungsdiensten**

2 Es werden die Anforderungen an die Erbringung von Zertifizierungsdiensten (z. B. das Aus-
3 stellen von Zertifikaten) festgelegt. Die nachfolgend beschriebenen Prozesse erfüllen insbe-
4 sondere die Vorgaben aus [SigG] und [SigV] sowie der HPC-Spezifikation [HPC-Spec].

5 **3.1 Certification Practice Statement (CPS)**

6 Die Prozesse und Verfahren zur Einhaltung und Erfüllung der in der Policy aufgeführten An-
7 forderungen werden in einem, von dem ZDA erstellten CPS festgelegt und den jeweiligen
8 Policy-Herausgebern erläutert.

9 Anwender-relevante Änderungen an dem CPS werden frühzeitig durch den ZDA veröffent-
10 licht.

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

15 **3.2 Verwaltung von Schlüsseln zur Erbringung von Zertifizierungsdiensten**

16 Die Anforderungen aus [SigG] und [SigV] an Schlüssel für qualifizierte elektronischen Signa-
17 turzertifikate sowohl der CA als auch der Anwender sind einzuhalten.

18 In den nachfolgenden Unterabschnitten werden daher nur Anforderungen an die weiteren
19 Schlüssel (bspw. CA-Schlüssel für Authentifikation bzw. Ver- und Entschlüsselung) als Min-
20 destanforderung aufgeführt.

21 **3.2.1 Erzeugung der CA-Schlüssel**

22 Die Generierung der weiteren CA-Schlüssel (nach Kapitel 3.2) erfolgt nur durch entspre-
23 chend autorisiertes Personal in einer physisch gesicherten Umgebung. Zudem wird mindes-
24 tens das Vier-Augen-Prinzip angewendet. Die verwendeten Algorithmen und Schlüssellän-
25 gen erfüllen dabei die Vorgaben aus [HPC-Spec].

26 Insbesondere gelten dabei folgende Vorgaben bezüglich Schlüssellänge und Algorithmus:

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

30 b. Die Schlüssellängen müssen mindestens so groß sein, wie die empfohlenen Schlüs-
31 sellängen im jeweiligen aktuellen Algorithmenkatalog der Bundesnetzagentur.

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

4 • RSA mit einer Mindestlänge von 2048 Bit.

5 • ECDSA mit einer Mindestlänge von 256 Bit.

6 Maßgeblich sind die Vorgaben der Policy-Herausgeber.

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

8 **3.2.2 Speicherung und Backup von CA-Schlüsseln**

9 Der ZDA sorgt für die Geheimhaltung und Integrität der privaten CA-Schlüssel. Ein optiona-
10 les Backup ist unter Einhaltung mindestens derselben Anforderungen wie für den privaten
11 Originalschlüssel möglich.

12 **3.2.3 Verteilung und Veröffentlichung der öffentlichen CA-Schlüssel**

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

18 **3.2.4 Verteilung und Veröffentlichung der privaten CA-Schlüssel**

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

21 **3.2.5 Verwendungszweck der CA-Schlüssel**

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

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

27

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 Anwendungsbereich ist grundsätzlich nicht
5 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 Module³ (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.

1 c. Bei der Inbetriebnahme eines HSM erfolgt eine umfassende Überprüfung der korrek-
2 ten Funktionsweise.

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

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

6 3.2.8 Erzeugung der Schlüssel für die HPC

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

9 a. Die in Tabelle 3 genannten Anforderungen an Schlüssellänge und verwendete Algo-
10 rithmen für die Schlüsselpaare für Verschlüsselung oder Authentifizierung sind einzu-
11 halten.

12 b. Die Schlüsselpaare der Zertifikate für Authentifizierung (C.HP.AUT) und Verschlüsse-
13 lung (C.HP.ENC) der HPC werden innerhalb der sicheren Signaturerstellungseinheit
14 selbst erzeugt bzw. durch vergleichbare Verfahren, soweit die Sicherheit nicht redu-
15 ziert wird, außerhalb der Signaturerstellungseinheit erzeugt. Die privaten Schlüssel
16 können aus der Signaturerstellungseinheit nicht ausgelesen werden. Entsprechendes
17 gilt für das Schlüsselpaar des Zertifikates für die qualifizierte elektronische Signatur
18 (C.HP.QES), für das weitere rechtliche Auflagen gelten können.

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

Schlüsselpaar bzw. Zertifikat	Algorithmus und Länge	Anmerkung
C.HP.QES	Die Schlüssellängen müssen mindes- tens so groß sein, wie die empfohlenen Schlüssellängen im jeweiligen aktuellen Algorithmenkatalog der Bundesnetz- agentur.	Mindestlänge für RSA derzeit 2048 Bit oder Algorithmen und Schlüssellängen mit vergleichba- rer 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 Siche- res verwendet werden.
C.HP.AUT	wie C.HP.QES (Mindestlänge für RSA: derzeit 2048 Bit)	

20 **Tabelle 3: Schlüssellängen und Algorithmen für den Produktiveinsatz**

1 **3.2.9 Sicherheit der HPC**

2 Die Sicherheitsanforderungen an die Chipkartenproduktion, Transport zum ZDA und Auslie-
3 ferung an den Ausweisinhaber sind im, nach [SigG] bestätigten, Sicherheitskonzept des ZDA
4 beschrieben.

5 **3.2.10 Aufbringung weiterer Anwendungen**

6 Applikationsfremde Daten oder Anwendungen⁴ dürfen nur nach ausdrücklicher Genehmi-
7 gung durch den Policy-Herausgeber in den verfügbaren Speicher der Chipkarte geladen
8 werden.

9 **3.3 Lebenszyklus der Endnutzerzertifikate der HPC**

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

12 **3.3.1 Bekanntmachung der Vertragsbedingungen**

13 Der Policy-Herausgeber stellt durch Veröffentlichung insbesondere die folgenden Dokumen-
14 te zur Verfügung:

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

17 Der ZDA ist für die Veröffentlichung seiner allgemeinen Vertragsbedingungen verantwortlich
18 und muss diese den Antragsteller zugänglich machen.

19 **3.3.2 Registrierung des Antragstellers**

20 Der Ablauf während der Registrierung des Antragstellers enthält mindestens folgende Kern-
21 punkte:

- 22 a. Identifizierung des Antragstellers.
- 23 b. Überprüfung der Antragsdaten.
- 24 c. Einholung der Bestätigung des Berufsgruppenattributs.
- 25 d. Einholung der Bestätigung ggf. weiterer Attribute.
- 26 e. Produktionsfreigabe durch den HPC-Herausgeber.

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

1 3.3.2.1 Standardablauf und Identifizierung

2 Der Antrag für die Herausgabe der HPC enthält auch einen Antrag auf Ausstellung von Zerti-
3 fikaten und muss durch den Antragsteller rechtsverbindlich unterschrieben werden. Dies
4 kann entweder handschriftlich oder elektronisch unter Nutzung einer gültigen, qualifizierten
5 elektronischen Signatur, die dem Antragsteller zugeordnet ist, erfolgen. Der Antrag für die
6 Herausgabe der HPC kann dabei auch zusammen mit einem Antrag für die Herausgabe der
7 SMC kombiniert erfolgen.

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

11 Dabei gelten insbesondere die nachfolgenden Punkte:

12 a. Dem Antragsteller werden von dem ZDA neben den erforderlichen Formularen auch
13 die Rechtsbelehrung, die Unterrichtsunterlagen, die Allgemeinen Geschäftsbed-
14 dingungen, sowie Merkblätter und alle weiteren Bestimmungen zur Zertifikatsnutzung
15 schriftlich (z. B. in elektronischer Form oder gemäß den gesetzlichen Bestimmungen)
16 zur Verfügung gestellt.

17 b. Der Antrag auf Ausstellung eines Zertifikats muss mindestens den vollständigen Na-
18 men, die aktuelle Anschrift sowie Geburtsdatum und –ort des Antragstellers enthal-
19 ten. Insbesondere müssen die Angaben geeignet sein, die X.509-Zertifikate der HPC
20 gemäß [HPC-Spec] zweifelsfrei zu befüllen.

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

23 d. Der Antragsteller ist durch einen amtlichen Lichtbildausweis oder Dokumente mit
24 gleichwertiger Sicherheit eindeutig bei Antragstellung oder Ausweisübergabe zu iden-
25 tifizieren. Bei der Identifizierung muss der Antragsteller physisch anwesend sein.

26 e. Im Rahmen der Antragsprüfung ist eine Überprüfung der Berechtigung der Antrag-
27 stellung notwendig. Hierzu hat der Antragsteller die entsprechenden Dokumente vor-
28 zulegen, die durch den HPC-Herausgeber gefordert werden.

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

31 • Annahme der von dem Policy-Herausgeber und dem HPC-Herausgeber auf-
32 gestellten Verpflichtungen des Antragstellers, des Ausweisinhabers und des
33 Anwenders,

34 • Annahme der von dem HPC-Herausgeber aufgestellten zusätzlichen Ver-
35 pflichtungen des Antragstellers, des Ausweisinhabers und des Anwenders,

- 1 • Zustimmung zur Archivierung aller relevanten Dokumente des Registrie-
2 rungsprozesses,
- 3 • Zustimmung, die beantragten Zertifikate in den entsprechenden Zertifikats-
4 diensten des ZDA überprüfbar zu halten,
- 5 • Zustimmung oder Verweigerung, die beantragten Zertifikate in weiteren Such-
6 diensten abrufbar zu halten,
- 7 • Jeweils Zustimmung zur Auskunftserteilung der bestätigenden Stelle eines At-
8 tributes gegenüber dem ZDA.

9 g. Alle relevanten Dokumente des Registrierungsprozesses für qualifizierte elektroni-
10 sche Signaturzertifikate werden mindestens über den gesetzlich vorgeschriebenen
11 Zeitraum gemäß [SigG] und [SigV] hinweg archiviert. Die Archivierung muss den An-
12 forderungen des [BDSG] genügen.

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

15 **3.3.2.2 Erstantrag**

16 Als Erstantrag werden alle Anträge eines Antragstellers bezeichnet, die keine Folgeanträge
17 sind. Bei einem Erstantrag muss die vollständige Registrierung gemäß Kapitel 3.3.2 durch-
18 laufen werden. Insbesondere ist eine Identifizierung des Antragstellers gemäß Kapitel 3.3.2.1
19 zwingend notwendig.

20 **3.3.2.3 Folgeantrag**

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

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

31 **3.3.3 Freigabe zur Produktion**

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

1 Ohne Freigabe zur Produktion der HPC dürfen die X.509-Zertifikate der HPC nicht ausge-
2 stellt werden.

3 **3.3.4 Ausstellung der Zertifikate**

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

6 a. Alle sicherheitskritischen Tätigkeiten werden nur von autorisiertem Personal und un-
7 ter Einhaltung des Vier-Augen-Prinzips durchgeführt.

8 b. Zur Gewährleistung der Vertraulichkeit und Integrität der aufgenommenen Daten
9 werden diese nur mit einem geeigneten Verfahren gesichert zwischen dem HPC-
10 Herausgeber oder einer von diesem beauftragten Stelle und dem ZDA übertragen.

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

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

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

- 21 • Die Seriennummer des Zertifikates,
- 22 • Der Gültigkeitszeitraum des Zertifikates,
- 23 • Die Nummer der HPC, die das Zertifikat enthält; bei einem Attributzertifikat
24 (C.HP.ATTR) ist dies die Nummer der HPC, die das dem Attributzertifikat zu-
25 geordnete qualifizierte elektronische Signaturzertifikat (C.HP.QES) enthält.
- 26 • Der vollständige Name (Vornamen, Nachname, Geburtsname) des Zertifikats-
27 inhabers.
- 28 • Das Geburtsdatum und der Geburtsort des Zertifikatsinhabers.

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

31 f. Die Übergabe der HPC an den Antragsteller erfolgt auf sichere Art und Weise durch
32 den ZDA, so dass gewährleistet ist, dass nur der Antragsteller die HPC, insbesonde-
33 re den darin enthaltenen privaten Schlüssel des CV-Zertifikates (C.HP.CV), in Betrieb

1 nehmen kann. Der Ausweisinhaber hat den Erhalt der HPC gegenüber dem ZDA re-
2 visionssicher zu bestätigen. Das Vorgehen hat der ZDA in seinem CPS zu beschrei-
3 ben.

4 **3.3.5 Veröffentlichung der Zertifikate**

5 Der ZDA stellt einen Verzeichnisdienst zur Verfügung, der abrufbare Zertifikate⁵ bereitstellt.
6 Die Veröffentlichung betrifft nur die X.509-Zertifikate, die abrufbar gehalten werden sollen.
7 Näheres dazu regelt der Policy-Herausgeber.

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

11 **3.3.6 Überprüfbarkeit der Zertifikate**

12 Der ZDA hat die von ihm nach dieser Policy ausgestellten Zertifikate gemäß den Anforde-
13 rungen aus [SigG] für qualifizierte elektronische Signaturzertifikate (C.HP.QES) überprüfbar
14 zu halten. Dies gilt auch für die Zertifikate für Verschlüsselung (C.HPC.ENC), Authentifizie-
15 rung (C.HPC.AUT) sowie eventuelle Attributzertifikate (C.HP.ATTR) der HPC.

16 **3.3.7 Sperrung von Zertifikaten**

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

- 19 a. Der Sperrantrag kann telefonisch oder schriftlich an den ZDA gestellt werden. Der
20 ZDA kann auch weitere, bestätigte Verfahren anbieten.
- 21 b. Es wird ein Sperrkennwort oder eine andere zuverlässige Identifizierung verwendet.
- 22 c. Neben den Ausweisinhaber können zuständige und Attribute bestätigende Stellen
23 (gemäß § 8 [SigG]) einen Sperrantrag stellen. Dies ist insbesondere der HPC-
24 Herausgeber sowie die von ihm beauftragten Stellen.
- 25 d. Vor der Sperrung hat der autorisierte Mitarbeiter des ZDA den Antrag auf seine Kor-
26 rektheit hin zu prüfen, insbesondere die Berechtigung des Sperrenden.
- 27 e. Die Durchführung der Sperrung muss gemäß [SigG] und [SigV] für qualifizierte elekt-
28 ronische Signaturzertifikate unverzüglich erfolgen. Insbesondere ist die Online-
29 Statusabfrage für die Überprüfung der Zertifikate umgehend zu aktualisieren.
- 30 f. Eine Sperrliste kann durch ein *CRL-Signer-Zertifikat* signiert werden (indirekte CRL).
31 Online-Statusabfragen müssen mittels eines *OCSP-Signer-Zertifikates* signiert wer-
32 den.

1 g. Das Aktualisierungsintervall der Sperrliste wird von dem HPC-Herausgeber in Rück-
2 sprache mit seinem Policy-Herausgeber festgelegt.

3 h. Wird ein Zertifikat gesperrt, informiert der ZDA den Zertifikatsinhaber (sofern zutref-
4 fend ist dies der den Ausweisinhaber), den HPC-Herausgeber sowie ggf. die Attri-
5 butsbestätigende Stelle in Schriftform oder elektronischer Form (mit Hilfe einer quali-
6 fizierten elektronischen Signatur) über die Sperrung des Zertifikats. Dies umfasst
7 mindestens die folgenden Angaben:

- 8 • Seriennummer des Zertifikates,
- 9 • Sperrzeitpunkt.

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

14 **3.3.8 Zertifikatserneuerung bei Schlüsselbeibehaltung**

15 Es ist möglich, dass unter Beibehaltung der Schlüsselpaare neue Zertifikate für eine HPC auf
16 Antrag des Ausweisinhabers ausgestellt werden. Dies darf aber nur erfolgen, wenn die be-
17 troffenen Schlüsselpaare bzw. die Schlüssellängen und Algorithmen noch hinreichend sicher
18 sind. Eine neue Produktionsfreigabe durch den HPC-Herausgeber ist hierbei zwingend not-
19 wendig.

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

27 **3.4 Verwaltung und Betrieb der Zertifizierungsstelle**

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

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

1 **3.4.1 Sicherheitsmanagement**

2 Für das Sicherheitsmanagement gelten die nachfolgenden Punkte:

- 3 a. Der ZDA ist für alle Abläufe und Prozesse der von ihm angebotenen Dienste verant-
4 wortlich. An den ZDA werden klare Forderungen gestellt, deren Einhaltung durch ent-
5 sprechende Kontrollfunktionen überprüft werden. Die für die Einhaltung der Sicherheit
6 relevanten Maßnahmen werden im CPS des ZDA definiert und dem HPC-
7 Herausgeber sowie dessen Policy-Herausgeber zugänglich gemacht.
- 8 b. Die Sicherheitsrichtlinien und –vorgaben werden regelmäßig kontrolliert und müssen
9 bei Bedarf an die aktuellen Gegebenheiten angepasst werden. Der ZDA ist in seinem
10 Wirkungsbereich für die Definition der Sicherheitsrichtlinien und deren Weitergabe an
11 das betroffene Personal verantwortlich.
- 12 c. Der ZDA führt eine umfassende Dokumentation über alle sicherheitsrelevanten Maß-
13 nahmen sowie deren korrekten Umsetzung und legt diese dem HPC-Herausgeber
14 und dessen Policy-Herausgeber vor. Näheres regelt jeder HPC-Herausgeber in
15 Rücksprache mit seinem Policy-Herausgeber in den Ausschreibungs- bzw. Zulas-
16 sungsunterlagen.

17 **3.4.2 Informationsklassifizierung und –verwaltung**

18 In den Gesamtsicherheitskonzept des ZDA, welches eine Bedrohungs- und Risikoanalyse
19 beinhaltet, werden alle Informationskategorien definiert und nach ihrem Schutzbedarf klassi-
20 fiziert. Der ZDA gewährleisten dabei durch geeignete Maßnahmen die Absicherung aller
21 schutzwürdigen Daten und Informationen.

22 **3.4.3 Personelle Sicherheitsmaßnahmen**

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

- 25 a. Der ZDA beschäftigt nur Mitarbeiter, welche das erforderliche Wissen sowie die not-
26 wendige Qualifikation und Erfahrung für die Ausübung der jeweiligen Tätigkeit besit-
27 zen. Mitarbeiter für vertrauenswürdige Positionen müssen ein polizeiliches Führungs-
28 zeugnis vorlegen. Erst nach einer Unbedenklichkeitseinstufung darf die Position ver-
29 geben werden.
- 30 b. Die genauen Aufgabengebiete und deren zugehörige Tätigkeiten – insbesondere bei
31 sicherheitsrelevanten Punkten – werden in einem Rollenkonzept des ZDA ausführlich
32 beschrieben. Diese Beschreibungen umfassen unter anderem neben den Pflichten
33 auch die Rechte und erforderlichen Kompetenzen.
- 34 c. In dem CPS des ZDA werden alle vertrauenswürdigen Rollen ausführlich beschrie-
35 ben.

- 1 d. Alle Aktivitäten erfolgen gemäß den aufgestellten Sicherheitsrichtlinien.
- 2 e. Mitarbeiter in vertrauenswürdigen Positionen werden vor Rollen- und Interessenkon-
- 3 flikten bezüglich ihrer Tätigkeiten bewahrt, damit eine unvoreingenommene Aus-
- 4 übung dieser Tätigkeiten ermöglicht wird.

5 **3.4.4 Physikalische und organisatorische Sicherheitsmaßnahmen**

6 Zur Absicherung von sicherheitskritischen Bereichen werden Maßnahmen vom ZDA zur

7 Verhinderung von Verlusten, Kompromittierungen und Beschädigungen sowie der Unterbre-

8 chung des laufenden Betriebs ergriffen. Diese umfassen insbesondere:

- 9 a. Nur autorisiertes Personal hat Zutritt zu den sicherheitskritischen Bereichen, um eine
- 10 Kompromittierung durch unautorisierte Zugriffe zu verhindern. Diese Bereiche umfas-
- 11 sen insbesondere die Räumlichkeiten, in denen die Zertifizierungs- und Sperrprozes-
- 12 se sowie (je nach Sicherheitskonzept bzw. CPS) die Chipkartenpersonalisierung
- 13 durchgeführt werden.
- 14 b. Die Systeme für die Zertifizierungs- und Sperrprozesse sowie (je nach Sicherheits-
- 15 konzept) die Chipkartenpersonalisierung bilden eigene Sicherheitsbereiche, welche
- 16 von anderen organisatorischen Einheiten räumlich abgegrenzt und durch einen phy-
- 17 sischen Zutrittsschutz abgesichert sind.
- 18 c. Hinsichtlich der Systeme für die Zertifizierungs- und Sperrprozesse sowie die (je nach
- 19 Sicherheitskonzept) Chipkartenpersonalisierung müssen Sicherheitsmaßnahmen zur
- 20 Abwendung von Gefahren durch Feuer, Wasserschäden und Naturgewalten sowie
- 21 Schutz vor Einbruch und Diebstahl, Ausfällen von Versorgungseinheiten und Sys-
- 22 temausfällen getroffen werden.
- 23 d. Die Zertifizierungsprozesse müssen durch geeignete Kontrollen vor unautorisierter
- 24 Entnahme von Gegenständen und Daten geschützt werden.

25 Die notwendigen Maßnahmen werden im CPS und insbesondere dem Sicherheitskonzept

26 des ZDA geregelt.

27 **3.4.5 Management des Betriebes**

28 Der ZDA gewährleistet, dass die Systeme für die Zertifizierungsprozesse korrekt betrieben

29 werden. Dazu gelten insbesondere die folgenden Punkte:

- 30 a. Auf einen Zwischenfall wird zeitnah reagiert. Zwischenfall und Reaktion werden aus-
- 31 führlich dokumentiert und die Anwender-relevanten Teile dem HPC-Herausgeber zur
- 32 Verfügung gestellt.
- 33 b. Schäden werden durch Backups und definierte Prozeduren zur Fehlerbeseitigung
- 34 minimiert.

- 1 c. Die eingesetzten Systeme werden gegen schadhafte Software und unautorisierte Zu-
2 griffe geschützt.
- 3 d. Datenträger werden vor Diebstahl und unautorisiertem Zugriff geschützt.
- 4 e. Alle Datenträger werden gemäß ihrer Sicherheitsstufe aufbewahrt. Datenträger, die
5 sicherheitsrelevante oder vertrauliche Informationen beinhalten, werden bei ihrer
6 Ausmusterung auf sichere Weise vernichtet.

7 Zur weiteren Minimierung von Zwischenfällen werden die sicherheitskritischen Funktionen
8 von den anderen Funktionen getrennt. Alle genannten sicherheitskritischen Funktionen wer-
9 den (gemäß des Rollenkonzepts im Gesamtsicherheitskonzept des ZDA) nur von autorisier-
10 tem Personal durchgeführt. Zu den Tätigkeiten gehören insbesondere der Betrieb, die War-
11 tung sowie die Administration der Systeme. Dazu gehört der Schutz vor schadhafter Soft-
12 ware, die regelmäßige Kontrolle und Analyse von Log-Dateien sowie erhöhte Sicherheits-
13 maßnahmen bei der Datenträgerverwaltung und dem Datenaustausch.

14 **3.4.6 Zugriffsverwaltung**

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

- 18 a. Der Zugriff auf die Systeme ist nur autorisiertem Personal möglich. Dazu werden ver-
19 schiedene Kategorien von Zugriffsrechten eingerichtet, welche insbesondere die
20 sicherheitskritischen von den unkritischen Funktionen trennen.
- 21 b. Vor jedem Zugriff auf ein System muss sich das Personal authentifizieren. Alle Zugrif-
22 fe – insbesondere unautorisierte Zugriffsversuche – werden protokolliert.
- 23 c. Alle sicherheitskritischen Zugriffe bezüglich Zertifikatsmanagement sind zusätzlich
24 durch sichere Authentifizierungsmechanismen geschützt.
- 25 d. Alle vertraulichen Daten werden bei der Übertragung über unsichere Netzwerke ge-
26 schützt.
- 27 e. Die Systeme werden vor Zugriffen durch unbefugte Dritte geschützt. Die System-
28 komponenten befinden sich in physisch gesicherten Räumlichkeiten.
- 29 f. Bei der Entdeckung unautorisierter Zugriffsversuche auf das System müssen unver-
30 züglich Gegenmaßnahmen ergriffen werden.

31 **3.4.7 Entwicklung und Wartung vertrauenswürdiger Systeme**

32 Der HPC-Herausgeber und der ZDA setzen in den vertrauenswürdigen Systemen Kompo-
33 nenten ein, die ausreichend gegen unautorisierte Veränderungen geschützt sind. Bei der

1 Entwicklung vertrauenswürdiger Systeme erfolgt in der Designphase und der Spezifikation
2 der Anforderungen eine Analyse der Sicherheitsanforderungen. Dies gilt auch, wenn für die
3 Entwicklung ein Dritter beauftragt wird. Alle Änderungen an vertrauenswürdigen Systemen
4 unterliegen einem vom ZDA festgelegten Verfahren mit Kontrolle und Dokumentation der
5 einzelnen Schritte. Die benötigten Maßnahmen dazu werden im CPS bzw. Sicherheitskon-
6 zept des ZDA beschrieben.

7 **3.4.8 Aufrechterhaltung des ungestörten Betriebes und Behandlung von Zwischen-** 8 **fällen**

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

17 **3.4.9 Einstellung der Tätigkeit**

18 Der ZDA meldet gemäß [SigG] die Einstellung der Tätigkeit rechtzeitig der zuständigen Be-
19 hörde, dem HPC-Herausgeber und allen Policy-Herausgebern. Für den Fall der Einstellung
20 der Tätigkeit erarbeitet der ZDA unter Einbeziehung der betroffenen Policy-Herausgeber eine
21 Verfahrensbeschreibung zur Abwicklung bzw. zur Übernahme der Tätigkeit in Bezug auf
22 diese Policy. Das Verfahren wird im CPS des ZDA beschrieben. Insbesondere muss die
23 Übergabe der Zertifikate an einen weiteren ZDA sichergestellt sein. Dies beinhaltet mindes-
24 tens:

- 25 a. Die Zertifikate,
- 26 b. Die Sperrlisten,
- 27 c. Informationen über freigeschaltete oder nicht freigeschaltete Zertifikate,
- 28 d. Registrierungsanträge,
- 29 e. Informationen für den Zugang und die Benutzung der Sperrpasswörter:
 - 30 • Art der Verschlüsselung,
 - 31 • Kodierung, ggf. Hashing,
 - 32 • Schlüssel für den Zugriff (falls erforderlich: im verschlossenen Umschlag, bei
33 einem Notar hinterlegt, bis sie benötigt werden),

- 1 • Kommunikations-Informationen (z.B. Weiterleitung / Überlassung einer Sperr-
2 hotline).

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

4 Die Übergabe muss effizient erfolgen können.

5 **3.4.10 Übereinstimmung mit gesetzlichen Anforderungen**

6 Der HPC-Herausgeber und der ZDA gewährleisten die Einhaltung der gesetzlichen Vorga-
7 ben aus [SigG] und [SigV], dem [BDSG], sowie die sich aus [HPC-Spec] und dieser Policy
8 ergebenden Anforderungen, in ihrer jeweils gültigen Fassung. Dabei wird insbesondere auf
9 die Einhaltung der Datenschutzerfordernungen im [BDSG] geachtet. Hierzu werden wichtige
10 Informationen vor Verfälschung sowie Verlust geschützt. Die Daten der Antragsteller werden
11 nur mit deren ausdrücklichem Einverständnis, auf Grund gesetzlicher Bestimmungen oder
12 richterlichen Anordnungen offen gelegt.

13 **3.4.11 Aufbewahrung von Informationen zu Zertifikaten**

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

17 a. Die zu archivierenden Daten müssen in dem CPS des ZDA definiert werden. Mindes-
18 tens werden die Unterlagen nach Kapitel 3.3.2 archiviert.

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

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

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

25 e. Für mindestens fünf Jahre ab Ablauf der Gültigkeit (ungeachtet einer Sperrung) eines
26 der X.509-Zertifikate (C.HP.QES, C.HP.AUT, C.HP.ENC, C.HP.ATTR) der HPC wer-
27 den archiviert:

28 a. Das Zertifikat,

29 b. Die Sperrlisten, die das Zertifikat enthalten könnten,

30 c. Die Zuordnung zwischen Zertifikat und Personendaten inkl. Originalantrag
31 und der Kopie des Ausweisdokumentes zur Identifizierung,

- 1 f. CA-Zertifikate werden mindestens solange aufbewahrt, wie davon ausgestellte Zerti-
2 fikate aufbewahrt werden.
- 3 g. Die Seriennummer des Chips der HPC und die Zuordnung zum Ausweisinhaber wer-
4 den für drei zusätzliche Jahre aufbewahrt, nachdem sie von sämtlichen gültigen
5 elektronischen Gesundheitskarten nicht mehr akzeptiert werden. Der ZDA hat dem
6 HPC-Herausgeber bei Bedarf Auskunft über diese Daten zu geben.
- 7

1 4 Anhang A – Verzeichnisse

2 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

1

2 4.2 Literaturverzeichnis

Zugehörige Dokumente der Policy-Herausgeber

[HPC-Spec]	Bundesapothekerkammer, Bundesärztekammer, Bundespsychotherapeutenkammer, Bundeszahnärztekammer, Deutsche Krankenhausgesellschaft, Kassenärztliche Vereinigung, Kassenzahnärztliche Vereinigung: <i>„German Health Professional Card and Security Module Card, Part 1, Part 2 und Part 3“, in Version 2.3.1 und neuer</i> (z. B.: http://www.sit.fraunhofer.de/forschungsbereich/tad/HBA-Spezifikation.jsp)
------------	--

3

Externe Dokumente

[BDSG]	Bundesdatenschutzgesetz
[SGB V]	Sozialgesetzbuch Nummer Fünf (SGB V)
[SigG]	Gesetz über Rahmenbedingungen für elektronische Signaturen; 12.05.2001, Novellierung zum Signaturgesetz erfolgte im November 2004 (SigG)
[SigV]	Verordnung zu elektronischen Signatur; 16.11.2001 (SigV)

4 4.3 Abbildungsverzeichnis

5	ABBILDUNG 1: BEZIEHUNGEN ZWISCHEN POLICY- UND HPC-HERAUSGEBERN UND DEN ZDA	
6	(INFORMATIV).....	34

7 4.4 Tabellenverzeichnis

8	TABELLE 1: ANWENDUNGSBEREICHE DER SCHLÜSSELPAAR UND ZERTIFIKATE DER HPC.....	11
9	TABELLE 2: ANWENDUNGSBEREICH DER SCHLÜSSEL UND ZERTIFIKATE DER CA	16
10	TABELLE 3: SCHLÜSSELLÄNGEN UND ALGORITHMEN FÜR DEN PRODUKTIVEINSATZ	17

11

1 **5 Anhang B – Abweichungen im Test- und Übergangszeitraum**

2 Für die HPC müssen Chipkarten zum Einsatz kommen, die konform zu einer von dem Poli-
3 cy-Herausgebern vorgegebenen HPC-Spezifikation [HPC-Spec] sind. Im Realbetrieb müs-
4 sen diese Chipkarten zusätzlich bestätigt sein. Aufgrund der Natur der Testmaßnahmen kann
5 während des Testzeitraumes von der Notwendigkeit der Bestätigung der Chipkarte sowie
6 einer Akkreditierung der Gesamtprozesse abgewichen werden. Dabei müssen jedoch insbe-
7 sondere folgende Randbedingungen beachtet werden:

- 8 • CV-Zertifikate müssen unterstützt werden.
- 9 • Die logische Struktur der Files auf der Chipkarte und die standardisierten Applikatio-
10 nen gemäß [HPC-Spec] müssen implementiert sein.

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

15 **5.1 Abweichende Bestimmungen für den Testzeitraum**

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

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

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

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

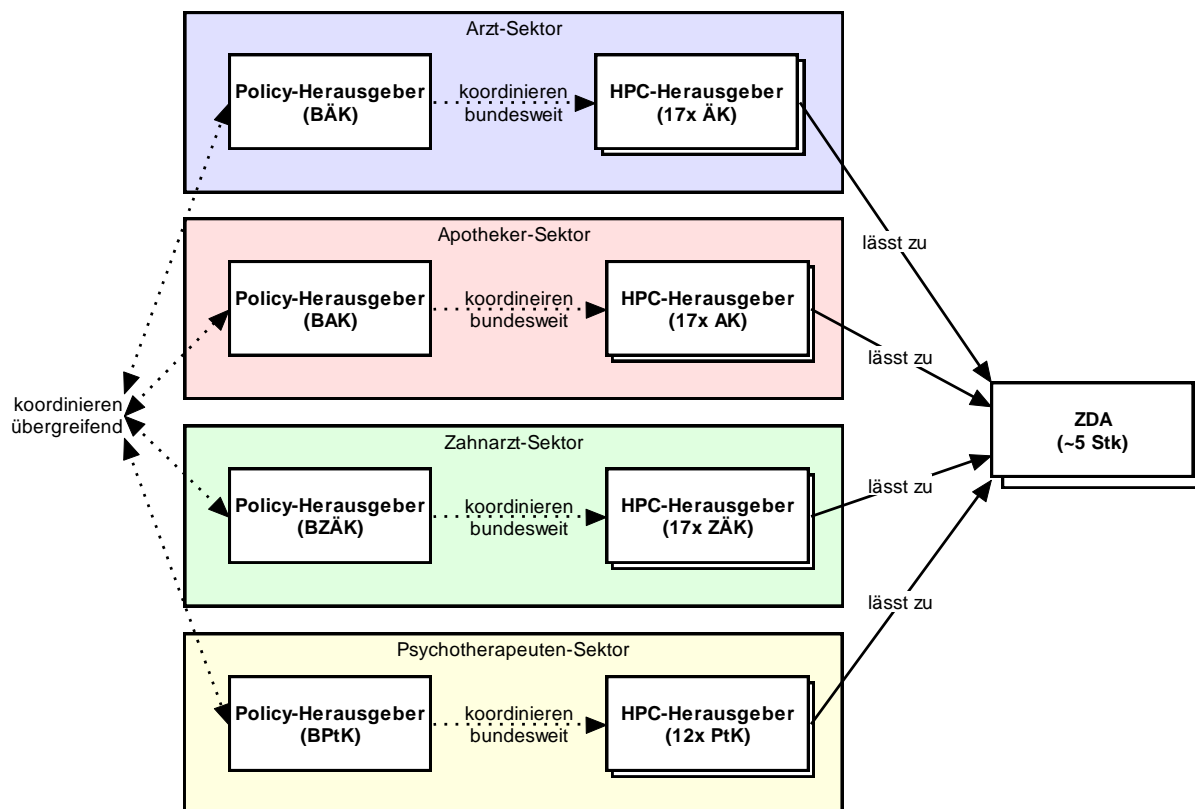
1 **5.2 Abweichende Bestimmungen für den Übergangszeitraum**

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

- 8 Das Ende des Übergangszeitraums wird öffentlich erklärt.

1 6 Anhang C – Verhältnis HPC- zu Policy-Herausgeber (informativ)

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



4
5 **Abbildung 1: Beziehungen zwischen Policy- und HPC-Herausgebern und den ZDA (informativ)**

6 Zur Zeit existieren fünf Policy-Herausgeber. Dies macht für den ärztlichen, den pharmazeuti-
7 schen, den psychotherapeutischen und den zahnärztlichen Bereich 63 (=3x17 + 1x12) ver-
8 schiedene HPC-Herausgeber.