# Konfigurationsdaten für die PKI der elektronischen Arztausweise, Version 2.3.8

## Bundesärztekammer, Berlin

| | Datum | Name, Abteilung, Firma |
|---|---|---|
| Autor, Ansprechpartner | | Dirk Schladweiler, Georgios Raptis |
| Status (Dezernat Telematik, BÄK) | 22.07.2014 | Freigegeben |

| **Versionshistorie** | | | | |
|---|---|---|---|---|
| **Version** | **Datum** | **Bearbeiter** | **Änderungen** | **Bemerkungen** |
| 0.1 | 14.07.05 | Georgios Raptis | | Initiale Version |
| 0.1 | 15.07.05 | Georgios Raptis | Einarbeitung Kommentare (Hr. Stachwitz) | QS |
| 0.2 | 01.08.05 | Dirk Schladweiler | Kap. 2 ergänzt, QS und Ergänzungen | |
| 0.3 | 29.09.05 | Dirk Schladweiler | Komplette Überarbeitung. | |
| 0.4 | 07.10.05 | Dirk Schladweiler | Differenzierung der Kartentypen | |
| 0.41 | 19.10.05 | Georgios Raptis | Definition: Zertifikatsanforderungen für die Tests | Kapitel 2.2, s. 9. Insb. Benennungskonzept für Zertifikate |
| 0.42 | 24.10.05 | Dirk Schladweiler | Löschen des alten Fahrplans und QS | |
| 0.43 | 25.10.05 | Georgios Raptis | QS | Präzisierung Namenskonzept |
| 0.44 | 27.10.05 | Georgios Raptis | WICHTIG: CV-CA-Kennungen | + Kennzeichnung Chipkarten |
| 0.45 | 06.12.05 | Dirk Schladweiler | -Aktualisierung<br><br>-Kartendifferenzierung und Tab. | |
| 0.46 | 06.12.05 | Georgios Raptis | -Korrekturen, QS | |
| 0.47 | 20.01.06 | Dirk Schladweiler | Hinweis auf „Laminierung der Kartenoberfläche *nach* der Personalisierung und Bedruckung der Aufschrift MUSTER“ angebracht. | |

| | | | | |
|---|---|---|---|---|
| 0.48 | 27.02.06 | Dirk Schladweiler | Umstellung und Ergänzung der Tabelleninhalte<br><br>Zeitliche Abbildung der Liefergegenstände auf die gematik-Meilensteinplanung<br><br>Kap. Bereitstellung von Entwicklerkarten[ARZT] für Entwickler<br><br>Differenzierung *[Arzt] hinzugefügt<br><br>Vorgehen für die Sicherstellung der Versorgung der Testung mit Komponenten | |
| 0.4.8 | 27.02.06 | Esther Freese | QS | |
| 0.5 | 01.03.06 | Dirk Schladweiler | Finalisierung, QS | |
| 0.5.1 | 01.03.06 | Georgios Raptis | Kap. 5 angepasst, ergänzt | |
| 0.5.2 | 01.03.06 | Schladweiler | Finalisierung, QS | |
| 0.5.3 | 02.03.06 | Esther Freese | QS | |
| 0.5.4 | 17.03.06 | Schladweiler | Fertigstellungszustand und Konfigurations-Data eingefügt | |
| 0.5.5 | 02.05.06 | Dirk Schladweiler | OID eingefügt | |
| 0.5.6 | 22.06.06 | Dirk Schladweiler | Kap. Sizing eingefügt | |
| 0.5.7 | 23.06.06 | Dirk Schladweiler | Kap. Nummerräume und ZDA-Spezifika eingefügt | |
| 0.5.8 | 26.06.06 | Georgios Raptis | QS, Klarstellungen im Kapitel 8 | |
| 0.5.9 | 28.12.06 | Esther Freese | Änderungen opt. Designvorgaben | |
| 0.6.0 | 06.09.07 | Dirk Schladweiler | Aktualisierung, Überarbeitung | + „HPCqSIG“<br>+ medisign<br>- Kap. 6 Zeitplan |
| 0.7.0 | 02.11.07 | Georgios Raptis | Änderung des Namens, Ergänzungen | **Alter Name ist „Fahrplan für die Versorgung mit HBA für die Testmaßnahmen“** |
| 0.7.1 | 23.11.07 | Dirk Schladweiler | Final-QS zur Konsolidierung | |

| | | | | |
|---|---|---|---|---|
| 0.7.2 | 07.01.08 | Georgios Raptis | Ergänzung Policy-OID für Ausweise für Kammermitarbeiter | |
| 0.7.3 | 09.09.08 | Dirk Schladweiler | Änderung des Namens DGN in dgnservice | lt. Mail v. 28.09.07 |
| 0.8.0 | 06.11.08 | Dirk Schladweiler | Nummernkreise für ZDA-Webdienste etc | |
| 2.3.1 | 10.03.09<br><br>29.05.09 | Georgios Raptis | Konsolidierung zum Paket V2.3.1 | **NAMENSÄNDERUNG. Alter Name ist: Spezifikation von Kartentypen für Testmaßnahmen, URLs, Nummernräume und OIDs, Version 2.3.1**<br><br>Konfigurationsdaten für Zertifikate aufgenommen<br><br>TestOID TestFacharzt |
| 2.3.2 | 06.10.09 | Georgios Raptis | Testkarten[ARZT] ohne Attributzertifikat (gem. Beschluss der ÄK)<br><br>Getrennte CAs für ENC und AUT sind zulässig | |
| 2.3.3 | 17.06.10 | Georgios Raptis | | Ergänzung Verifikationschipkarte |
| 2.3.4 | 12.05.11 | Dirk Schladweiler | Aktualisierung der Referenzen | |
| 2.3.5 | 20.03.12 | Georgios Raptis | Seriennummer/ICCSN Präfixe für ÄK und Projekte | |
| 2.3.6 | 07.11.12 | Georgios Raptis<br><br>Dirk Schladweiler | Präfixe für BezÄK in Rheinland-Pfalz für die Ausweisnummer, Tab. 5-1, Policy-OID für die Zertifikate | |
| 2.3.7 | 13.03.14 | Dirk Schladweiler | Nummernkreise für Entwicklerkarten[ARZT] für die Test- und Erprobungsmaßnahmen eingeführt | |

| | | | | |
|---|---|---|---|---|
| 2.3.8 | 17.07.14 | Dirk Schladweiler | Änderung der Mailadresse für den Bezug von Entwicklerkarten (→telematik@baek.de)<br><br>Aufteilen der Tabelle für die ICCSN Nummernkreise der ZDA und der Seriennummer-Nummernkreise für die LÄKs für ein leichteres Verständnis<br><br>Referenzen aktualisiert<br><br>Erstellung eines gesonderten Kap. „ERPROBUNG: Nummernkreise für von den Ärztekammern generierte Vorgangsnummern<br><br>Tab9.1 Policy-OIDs für die qSIG, qATTR, QES eingefügt | |

| **Fertigstellungszustand** | | | | |
|---|---|---|---|---|
| **Lfd Nr.** | **Probleme / Offene Punkte / Defizite** | **Ursachen** | **Maßnahmen / Lösungen** | **Kapitel-verweis** |
| | | | | |

# Inhalt



# 1 Einleitung

## 1.1 Zielsetzung

Dieses Dokument enthält Konfigurationsdaten zur PKI der elektronischen Arztausweise. Die Version des Dokuments korrespondiert mit der Version der Dokumente ([baekCerts], [baekAttr]), welche spezifisch die Zertifikatsprofile definieren. Eine Versionierung dieses Dokumentes erfolgt deshalb über die Revisionsnummer und das Datum.

Konfigurationsdaten sind Daten in der PKI der eArztausweise, die geändert werden können, ohne die Spezifikationsdokumente anpassen zu müssen. Typischerweise gehören zu den Konfigurationsdaten Eigenschaften der Zertifikatsprofile, wie die Policy-OIDs und –URLs, Algorithmen, die Inhalte der Admission (OIDs und professionItem), sowie Eigenschaften von

CRL-, OCSP-Profilen und Verzeichnisdienst-Eigenschaften. Das Vorhandensein der Admission-Extension im Public-Key-Signaturzertifikat oder die Existenz und Attributwerte von Attributzertifikaten werden ebenfalls hier festgelegt. Werden in diesem Dokument keine Werte für Konfigurationsdaten definiert, gelten die Ausgangswerte in den Spezifikationen (Def. s. o.). Darüber hinaus können hier Übergangszeiträume für eine Änderung der Konfigurationsdaten definiert werden.

In diesem Dokument werden u. a. die von der Bundesärztekammer (BÄK) vergebenen OIDs definiert.

# 2 Kartentypen

Die folgenden Begriffe sind für Karten mit genannten Eigenschaften zu verwenden.

- Als „**elektronischer Arztausweis (G2)**“, „**Wirkbetriebs- oder Echtkarten der Generation 2**“ werden ausschließlich Chipkarten gemäß der aktuellen HPC-Spezifikation ab Version 3.0.0 und mit dem beschlossenen Design für den elektronischen Arztausweis angesehen. Diese Karten sind konform zur Gemeinsamen Policy Version 1.0.5. Die optische Personalisierung erfolgte in einem hochwertigen Druckverfahren. Diese Karten enthalten als Sicherheitsmerkmal ein Hologramm, sind mit CV- (G2) und X.509-Schlüsseln und Zertifikaten der Wirkbetriebsumgebung ausgestattet. Diese Karten sind realen Ärzten zugeordnet und über bestätigte Prozesse an diese ausgegeben. Darüber hinaus sind die Karten nach dem deutschen Signaturgesetz bestätigt. Unter diesem Begriff fallen auch sogenannte Ersatzausweise und Reserveausweise (siehe [baekGlossar]), soweit sie über qualifizierte Zertifikate verfügen.
- **„HPCqSIG“, „eArztausweis“ (G0)** sind nach SigG bestätigte Karten, die bereits vor Aufnahme des TI-Wirkbetriebs an Heilberufler (Ärzte) ausgegeben werden. Diese Karten unterstützen nicht die Authentifizierung gegenüber eGKs mit Hilfe von CV-Zertifikaten, sondern sollen zielrichtend nach bestätigten Prozessen ausgegeben werden und in sonstigen Telematikprojekten der Ärzteschaft für Authentifizierungen (ESIGN) und digitale Signatur (QES) jeweils mit mind. 2048bit RSA Einsatz finden. Die Karten werden nach dem beschlossenen Design des eArztausweises bedruckt und enthalten als Sicherheitsmerkmal ein Hologramm. Sie müssen konform zur HPC-Spezifikation 2.1.1 (insbesondere in Bezug auf die Nutzung der X.509-Zertifikate und Schlüssel) mit Ausnahme der Funktionalitäten, die für die Interaktion mit der eGK notwendig sind, sowie zur Gemeinsamen Policy Version 1.0.0. D. h. sie müssen nicht zwingend CV-Zertifikate enthalten, logische Kanäle unterstützen usw. Diese Karten unterliegen den Anforderungen an das optische Design der elektronischen Arztausweise und enthalten ebenso ein Hologramm.
- Als „**HBA-Musterkarten[ARZT]**“ werden alle weiteren Karten, auch solche ohne Chip, aber im optischen Design des elektronischen Arztausweises angesehen. Diese Karten sind klar mit einem Schriftzug „MUSTER“ als solche kenntlich zu machen. Vorgaben für das Druckverfahren bestehen nicht, außer es werden Musterkarten im Rahmen von Produktionstests erstellt. Das Kartenbetriebssystem ist nicht konform zu einer HPC-Spezifikation. Diese Karten haben grundsätzlich kein Hologramm, es sei denn, sie wurden zu dem Zweck der Begutachtung und erster Tests von Kartenkörpern mit Hologramm hergestellt.

- Als „**HBA-Entwicklerkarten[ARZT]**“ werden Chipkarten verstanden, welche nicht im Design des eArztausweises bedruckt sind, jedoch elektrisch konform mindestens zur HPC-Spezifikation 3.0.0 und bzgl. CV- und X.509-Zertifikaten beschlüsselt bzw. ableitbar aus den übergreifenden Test-Hierarchien personalisiert sind. Diese Karten werden zu Entwicklungszwecken zur Verfügung gestellt. Durch den ZDA erfolgt die Verwaltung der Information, an welche Entwickler (welche) „HBA-Entwicklerkarten[ARZT]“ geliefert wurden. Auf Verlangen ist diese Information der BÄK zur Verfügung zu stellen. Der ZDA soll diese Karten für die Verwaltung geeignet optisch personalisieren.
- Als „**HBA-Verifikationschipkarte[ARZT]**“ werden Chipkarten verstanden, die für technische Tests gegenüber eGKs oder weiteren Systemen verwendet werden. Sie werden NICHT im Design des eArztausweises bedruckt, sind mit dem Namen und die Organisation des Anforderers beschriftet und tragen den Schriftzug „Verifikationskarte“. Diese Karten werden mit CV- und X.509-Zertifikaten aus dem Vertrauensraum von Test-HBA[ARZT] oder „Wirkbetriebs- oder Echtkarten“ personalisiert, jedoch nicht an echte Ärzte ausgestellt. Als Bestätigende Stelle für das Arztattribut im Feld admissionAuthority muss „O=Verifikationschipkarte,C=DE“ enthalten sein. In den X.509-Zertifikaten müssen im CN die Zeichenkette „Verifikationschipkarte“ und der Name des Verantwortlichen enthalten sein. Verifikationschipkarten[ARZT] werden nach Genehmigung durch die BÄK von einem ZDA ausgestellt. Der Empfänger der Karte muss dafür erklären, dass er die Karte nur für Test- und Verifikationszwecken einsetzen wird, und dass er organisatorische und technische Maßnahmen treffen wird, damit kein missbräuchlicher Zugriff auf echte Patientendaten erfolgen kann.
- „**HPC-Prototypen**“ sind Karten, die nicht dem Design des eArztausweises unterliegen, konform zur jeweils aktuellen HPC-Spezifikation sind und nicht über die übergreifende CV-Root und BÄK-Root beschlüsselt sind. Diese Karten unterliegen der Hoheit und Verwaltung des jeweiligen Produzenten. Diese Karten dienen bspw. zur Erlangung des gematik-Vorab-Prüfsiegels für die Komponente „Karte“ und sind damit die Grundlage für eine spätere Zulassung als Basis für den eArztausweis.
- „**Arztausweise**“ sind alle sonstigen von Ärztekammern herausgegebenen Ausweise, die die Arzteigenschaft bestätigen. Diese Arztausweise können im Chipkartenformat – auch im Design der eArztausweise – oder auch als Papierausweis ausgegeben werden.

*Tabelle 2-1: Übersicht Kartendifferenzierung*

| | HPC-Prototypen | HBA-Entwicklerkarten [ARZT] | HBA-Musterkarten [ARZT] | HBA-Verifikations-chipkarte [ARZT] | HPCqSIG (eArz-tausweis G0) | e-Arztausweis (G2) |
|---|---|---|---|---|---|---|
| Konform zur Spezifikation der HPC/SMC | X | X | - | X | 2.1.1 mit Ein-schränkungen | 3.0.0 |
| Ableitbar zur Test- CVC-Root | - | X | - | - | - | - |
| Ableitbar zur Wirk-CVC-Root | - | - | - | X | - | X |
| Ableitbar zur Test-X.509-Root | - | X | - | (X) | - | - |
| Ableitbar zur Wirk-X.509-Root | - | - | - | (X) | (X[1]) | X |
| Ableitbar zur BNetzA für qSIG | - | - | - | (X) | X | X |
| PKI-Dienste | - | X | - | X | X | X |
| gematik Zulas-sung | X (ggf. be-schränkte | opt. | - | X | - | X |

[1] ggf. dedizierte Root und/oder Policy

| | HPC-Prototypen | HBA-Entwicklerkarten [ARZT] | HBA-Musterkarten [ARZT] | HBA-Verifikationschipkarte [ARZT] | HPCqSIG (eArztausweis G0) | e-Arztausweis (G2) |
|---|---|---|---|---|---|---|
| | Zulassung) | | | | | |
| Optische Identifizierung der Karten[2] | Geeignet für Verwaltung durch gematik | Geeignet für Verwaltung durch BÄK (Übernahme der gematik-Vorgaben für HPC- und eGK-Prototypen) | Schriftzug „MUSTER“ | Schriftzug „Verifikationschipkarte“ | Schriftzug „qSIG“[3] | - |
| Design eArztausweis | - | - | X[4] | - | X[2] | X[2] |
| Hologramm | - | - | opt. | - | X | X |
| Auf reale Ärzte | - | - | - | - | X | X |

[2] Die ZDA werden gebeten, im optischen Design – vorzugsweise in ZDA-spezifischen Feldern (ZDA-Logo, Magnetstreifenfeld) – eine geeignete selbstverwaltete Versionierung der Kartenserie vorzunehmen. Eine geeignete optische Identifizierung soll auch für HBA-Entwicklerkarten[ARZT] und HPC-Prototypen (durch Chipkartenhersteller [CKH]) vorgesehen werden. Hierfür gelten die gleichen Anforderungen wie für die eGK-Testkarten der gematik.

[3] der Schriftzug „qSIG“ kann als Teil der Versionierungs-Kennzeichnung der Karte aufgebracht werden, d.h. auf der Rückseite

[4] Für alle Kartentypen, die das beschlossene Design des Arztausweises tragen, gelten die Bestimmungen der optischen Personalisierung und ggf. Zusatzinformation zur Kennzeichnung des Kartentyps (Aufbringung der MUSTER- bzw. TEST-Kennzeichnung). Zum Schutz der Karten(-bedruckung) ist eine Laminierungsschicht aufzubringen.

| | HPC-Prototypen | HBA-Entwicklerkarten [ARZT] | HBA-Musterkarten [ARZT] | HBA-Verifikations-chipkarte [ARZT] | HPCqSIG (eArztausweis G0) | e-Arztausweis (G2) |
|---|---|---|---|---|---|---|
| bezogen | | | | | | |

# 3 Object Identifier und Issuer Identification Number

Der BÄK ist die OID 1.3.6.1.4.1.24796 von der IANA zugewiesen. Folgende OIDs werden im Kontext der elektronischen Arztausweise definiert.

*Tabelle 3-1: Object Identifier*

| OID | Name | Bemerkung |
|---|---|---|
| 1.3.6.1.4.1.24796 | id-baek | Bundesärztekammer / BÄK |
| 1.3.6.1.4.1.24796.1 | id-baek-cp | Certificate Policy |
| ------->>>> 1.3.6.1.4.1.24796.1.1 | id-baek-cp-hbaTestkarteArzt | alt: HBA-Testkarte[ARZT] (Inhaber ist Ärztin/Arzt) |
| ------->>>> 1.3.6.1.4.1.24796.1.2 | id-baek-cp-hbaEntwicklerkarteArzt | HBA-Entwicklerkarte[ARZT] (Inhaber ist KEIN Arzt) |
| ------->>>> 1.3.6.1.4.1.24796.1.10 | id-baek-cp-eArztausweisV1 | Policy (Version 1) für den elektronischen Arztausweis (G0, HPCqSIG) mit qualifizierter Signatur, konform zur Gemeinsamen Policy V1.0.0 |
| ------->>>> 1.3.6.1.4.1.24796.1.1001 | id-baek-cp-mitarbeiterAerztekammerV1 | Policy (Version 1) für Ausweise für Mitarbeiter der Ärztekammern, nach dem Dokument „Ausweise für Kammermitarbeiter“. Kein Heilberufsausweis |
| 1.3.6.1.4.1.24796.4 | id-baek-at | (BÄK Attribute) |

| OID | Name | Bemerkung |
|---|---|---|
| 1.3.6.1.4.1.24796.4.11 | id-baek-at-namingAuthorityÄrzteschaft | (gemeinsames Attribut für alle Ärztekammern) |
| ------->>>> 1.3.6.1.4.1.24796.4.11.1 | id-baek-at-namingAuthorityÄrzteschaft-Ärztin/Arzt | (OID für das Berufsgruppenattribut ÄRZTIN/ARZT) |
| ------->>>> 1.3.6.1.4.1.24796.4.11.10 | id-baek-at-namingAuthorityÄrzteschaft-TestFacharzt | (OID für Testzwecken, kennzeichnet ein fiktives Attribut „TestFacharzt„ |
| ------->>>> 1.3.6.1.4.1.24796.4.1 | hpcField | (Fachrichtung) |
| ------->>>> 1.3.6.1.4.1.24796.4.2 | hpc hpcEAInhaberID | (eaInhaberID (bundeseinheitliche Arztnummer, BAN)) |
| ------->>>> 1.3.6.1.4.1.24796.4.3 | hpcEncCertificateSerial-Number | (Seriennummer des Verschlüsselungszertifikats) |
| ------->>>> 1.3.6.1.4.1.24796.4.4 | hpcEncCertificateIssuer | (Aussteller des Verschlüsselungszertifikats) |
| 1.3.6.1.4.1.24796.6 | id-baek-oc | (BÄK Objektklassen) |
| ------->>>> 1.3.6.1.4.1.24796.6.1 | hpcPerson | (Objektklasse für Attribute der HPC) |
| 1.3.6.1.4.1.24796.15 | id-baek-nf | (BÄK Name Forms) |

Alle OIDs, die mit "------->>>>" gekennzeichnet sind, werden entweder in Zertifikaten oder im LDAP-Schema produktiv eingesetzt.

Eine Issuer Identification Number wird als Bestandteil einer ICC Serial Number nach EN1867 gemäß der jeweils aktuellen HPC-Spezifikation in sämtlichen elektronischen Arztausweisen sowie Test- und Entwicklerkarten eingesetzt.

Die BÄK hat folgende Issuer Identification Number: 00108

# 4 URLs im Kontext der elektronischen Arztausweise

URL für die Signaturpolicy (Version 1) des elektronischen Arztbriefes nach [extern1]

http://www.e-arztausweis.de/sigpolicies/earztbrief-1_0/sigpolicyv1.xml

URL für die Policy der Root-Zertifikate der BÄK

http://www.e-arztausweis.de/policies/root_policy.html

URL für die Policy der CA-, CROSS-, CRLSigner- und OCSPSigner-Zertifikate, die von der BÄK ausgestellt werden.

http://www.e-arztausweis.de/policies/ca_policy.html

URL für die Policy der Zertifikate der elektronischen Arztausweise

http://www.e-arztausweis.de/policies/EE_policy.html

URL für den LDAP-Server des Trustcenters der BÄK (nur G0-eArztausweise)

ldap://ldap.e-arztausweis.de:389

URL für den LDAP-Server des Trustcenters der BÄK für die Entwickler- und Test-eArztausweise (nur G0-eArztausweise)

ldap://testldap.e-arztausweis.de:389

URL für den OCSP-Responder des Trustcenters der BÄK (nur G0-eArztausweise)

http://ocsp.e-arztausweis.de:8080/ocsp-ocspresponder

URL für den OCSP-Responder des Trustcenters der BÄK für die Entwickler- und Test-eArztausweise (nur G0-eArztausweise)

http://testocsp.e-arztausweis.de:8080/ocsp-ocspresponder

# 5 ICCSN-Nummernräume der ZDAs

Es besteht die Anforderung nach ZDA-übergreifender Eindeutigkeit der ICCSNs aller eArztausweise. Diese soll durch eine für alle zugelassenen ZDA verbindliche Verwendung von Nummernräumen erfolgen.

- Für eArztausweise: Auf Kartenebene sind die Nummernräume (2 BCD-Stellen) in die ICCSN als führender Bestandteil der SerialNumber, direkt hinter dem Issuer Identifier der BÄK, zu integrieren.
- Auf Zertifikatsebene ist die ZDA-übergreifende Eindeutigkeit durch die Verwendung desselben Nummernraumes an führender Stelle des Attributes "serialNumber" in allen Zertifikaten sicherzustellen.

*Tabelle 5-1: ICCSN-Nummernräume*

| Lfd. Nr. bzw. Kammercode | Zertifizierungsdiensteanbieter | Nummernkreis |
|---|---|---|
| 0 | D-TRUST (Bundesdruckerei) | 10 |
| 1 | Signtrust | 11 |
| 2 | T-Systems Telesec | 12 |
| 3 | S-Trust | 13 |
| 4 | Cybertrust | 14 |
| 5 | DGNservice | 15 |
| 6 | medisign | 16 |
| 7 | Entwicklerkarten[ARZT]: D-TRUST (Bundesdruckerei) | 20 |
| 8 | Entwicklerkarten[ARZT]: T-Systems Telesec | 22 |
| 9 | Entwicklerkarten[ARZT]: DGNservice | 25 |
| 10 | Entwicklerkarten[ARZT]: medisign | 26 |
| 11 | eArztausweis light (ÄKNo & ÄKWL) | 80000 und 80001 |

Beispiel-ICCSN: (siehe auch Tabelle F.1 HPC-Part II)

'80' '276' '00108' '10 12345678' D-TRUST

'80' '276' '00108' '11 12345678' Signtrust

Die ICCSN wie auch das SubjectDN-Attribut „serialNumber“ werden vom ZDA durch Variation des Nummernteils nach dem Präfix vergeben und eindeutig gehalten.

Anmerkung: Sobald die Nummernräume erschöpft sind, wird die BÄK weitere Bereiche zuordnen.

# 6 Seriennummer der Kammern für Arztausweisen im ID-1 Format

Entsprechend der Präfixe für die ICCSNs der ZDA sollen die Arztausweise im ID-1-Format (Plastikkarten), die von den Kammern selbst produziert und ausgegeben werden, die Se-

riennummer analog bilden. Hierfür wurden u.g. Nummernkreise eingerichtet, die den verschiedenen Nummerncodes der Kammern zugeordnet sind.

Somit besteht die Anforderung nach Ärztekammer-übergreifender Eindeutigkeit der Seriennummer aller (nichtelektronischen) Arztausweise. Diese soll durch eine für alle Ärztekammern verbindliche Verwendung von Nummernräumen erfolgen:

- Für Arztausweise im ID-1 Format: die Eindeutigkeit der Seriennummer ist nach demselben Prinzip wie die ICCSN der eArztausweisen zu bilden

*Tabelle 6-1: Nummernräume der Seriennummer*

| Kammercode | Ärztekammer | Nummernkreis |
|---|---|---|
| 010 | ÄK Schleswig-Holstein | 50 |
| 020 | ÄK Hamburg | 51 |
| 030 | ÄK Niedersachsen | 52 |
| 040 | ÄK Bremen | 53 |
| 051 | ÄK Nordrhein | 54 |
| 055 | ÄK Westfalen-Lippe | 55 |
| 060 | LÄK Hessen | 56 |
| 070 | LÄK Rheinland-Pfalz | 57 |
| 080 | LÄK Baden-Württemberg | 58 |
| 090 | Bayerische LÄK | 59 |
| 100 | ÄK Saarland | 60 |
| 110 | ÄK Berlin | 61 |
| 120 | ÄK Mecklenburg-Vorpommern | 62 |
| 130 | LÄK Brandenburg | 63 |
| 140 | ÄK Sachsen-Anhalt | 64 |
| 150 | LÄK Thüringen | 65 |
| 160 | Sächsische LÄK | 66 |
| 067 | Bezirksärztekammer Rheinhessen | 67 |
| 068 | Bezirksärztekammer Pfalz | 68 |
| 069 | Bezirksärztekammer Trier | 69 |
| 066 | Bezirksärztekammer Koblenz | 70 |

Beispiel-Seriennummer:

'80' '276' '00108' '65 12345678' LÄK Thüringen

'80' '276' '00108' '55 12345678' ÄK Westfalen-Lippe

Anmerkung: Sobald die Nummernräume erschöpft sind, wird die BÄK weitere Bereiche zuordnen.

# 7 Nummernräume für Vorgangsnummern der ZDA-Webdienste

Es besteht die Anforderung nach Eindeutigkeit der Vorgangsnummern, die von den ZDA-Webdiensten oder den KammerClients (bei Vorbefüllung) erzeugt werden. Um dies zu erreichen, sind die u. g. Nummernräume eingerichtet, die an entsprechender Stelle in die Vorgangsnummer einzubinden sind.

Diese ZDA-spezifischen Nummernräume werden ebenso in eine spätere Version der Technischen Richtlinie der Ärztekammern übernommen.

Für die Kammerspezifischen Nummernräume werden die Nummern aus Kap. 4.1. der Technischen Richtlinie der Ärztekammern verwendet.

Falls in einer Ärztekammer mehrere KammerClient-Installationen betrieben werden, muss die betreibende Ärztekammer durch – sich an den Nummernkreis anschließende – unterschiedliche 2-stellige, alphanumerische Kammerclient-IDs eine Eindeutigkeit herstellen. Die vergebenen Kammerclient-IDs müssen nicht im Rahmen des Konfigurationsmanagements nachgehalten werden, da sie lediglich dafür dienen, die Eindeutigkeit der Vorgangsnummern bei mehreren KammerClient-Instanzen innerhalb einer Ärztekammer zu gewährleisten.

*Tabelle 7-1: Vorgangsnummernräume*

| Lfd. Nr. | Zertifizierungsdiensteanbieter | Nummernkreis |
|---|---|---|
| 0 | D-TRUST | 510 |
| 1 | Signtrust | 511 |
| 2 | T-Systems Telesec | 512 |
| 3 | S-Trust | 513 |
| 4 | Cybertrust | 514 |
| 5 | dgnservice | 515 |
| 6 | medisign | 516 |
| 7 | Erprobungsumgebung: D-TRUST (Bundesdruckerei | 610 |
| 8 | Erprobungsumgebung: T-Systems Telesec | 612 |
| 9 | Erprobungsumgebung: DGNservice | 615 |
| 10 | Erprobungsumgebung: medisign | 616 |

# 8 ERPROBUNG: Nummernkreise für von den Ärztekammern generierte Vorgangsnummern

Das folgende Kap. beschreibt die Bildungsregel für Vorgangsnummern im Rahmen der Erprobung der gematik. D.h. die an den Tests teilnehmenden Ärztekammern müssen ggü. den beauftragten Zertifizierungsdiensteanbietern aus den Losen 3&4 der G2-Ausschreibung die Vorgangsnummer für Vorbefüllungen wie u.g. bilden. Folgende Anforderungen sind zu berücksichtigen:

Wenn der Kartenherausgeber bei der Vorbefüllung eine Vorgangsnummer erzeugt und im Vorbefüllungsdatensatz mitliefert, dann MUSS diese Vorgangsnummer innerhalb des jeweiligen Kartenherausgebers eindeutig sein.

Wenn der Kartenherausgeber keine Vorgangsnummer mitliefert, dann MUSS der TSP eine losübergreifend einheitliche Vorgangsnummer erzeugen und an den Kartenherausgeber zurückliefern.

Die folgende Bildungsregel MUSS vom TSP und von den Kartenherausgebern bei der Erzeugung von Vorgangsnummern umgesetzt werden:

- Die Vorgangsnummer hat 18 Stellen.
- 10 Stellen als „Klartext-Referenz“ zum Antrag, die sich wiederum aus zwei Blöcken zusammen setzen:
    - 5 Stellen Kennung des Kartenherausgebers oder TSP:
        - Eindeutige Identifizierung des Kartenherausgebers im Fall der Erzeugung der Vorgangsnummer durch den Kartenherausgeber, welche sich aus dem einstelligen Präfix der TelematikID des Sektors, dem Kartentyp (HBA oder SMC-B, einstellig) und einem dreistelligen Kartenherausgeber-spezifischen Nummernraum zusammensetzt (z.B. Kammercode oder vergleichbare bereits vorhandene Kennungen)
        - ZDA-Kennung im Fall der Erzeugung der Vorgangsnummer durch den TSP.
    - 5 Stellen: eindeutiges Identifizierungsmerkmal des Kartenherausgebers oder des TSP für die Vorgangsnummer z.B. eine fortlaufende Nummer oder eine Zuordnungssnummer aus den Bestandssystemen oder eine sonstige Nummer
- 8 Stellen Zufallszahl, um einen gezielten Zugriff auf Vorbefüllungsdaten durch Unberechtigte auszuschließen. Die Erzeugung der Zufallszahlen obliegt dem jeweiligen Kartenherausgeber bzw. TSP.

Die folgende Abbildung illustriert die Bildungsregel (am Beispiel einer vom Kartenherausgeber gebildeten Vorgangsnummer):

| **Stelle** | 1 | 2 | 3-5 | 6-10 | 11-18 |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| **Wert** | Sektorkennzeichen: Präfix der Telematik-ID gemäß gemKPT_PKI_TIP#Tab_PKI_101 | Kartentyp: "1" für HBA, "2" für SMC-B | Kartenherausgeber-spezifischer Nummernraum, z.B. Kammercode oder vergleichbare ggf. bereits vergebene Kennungen | Identifizierungsmerkmal für den Vorgang | 8-stellige Zufallszahl |

Hinweis der gematik bzgl. Zufallszahl: Der 14stellige Crypto-Key als Teil des Webtokens wurde von der BÄK als Schlüssel für die Verschlüsselung der vorbefüllten Daten definiert. Zu diesem Zweck ist viel Entropie erforderlich, deshalb die 14 alphanumerische Stellen. In den jetzt definierten Prozessen werden die Vorbefüllungsdaten nicht mit einer PB-Encryption verschlüsselt, sondern über eine TLS-Transportverschlüsselung abgesichert. Die Zufallszahl dient nur noch der Authentisierung und hat die Qualität eines Passworts. 14 Stellen sind für diesen Zweck nicht erforderlich. Für ein gutes Passwort dürften 8 Stellen ausreichend sein. Die Länge der Zufallszahl ist auf das notwendige Maß (8 Stellen) reduziert worden.

Für den eArztausweis sind damit folgende Werte bei der Generierung der Vorgangsnummer durch die Ärztekammer vorgegeben:

1. Stelle: →1 (entspricht „Ärzteschaft“)

2. Stelle: →1 (entspricht HBA)

3-5 Stelle: → Kammercode gemäß TR, siehe auch ebenda Tabelle 6-1: Nummernräume der Seriennummer

6-10 Stelle: → eindeutige, bspw. fortlaufende Nummer für den Vorgang

11-18 Stelle: → 8-stellige Zufallszahl

Beispiel-Vorgangsnummer:

'1' '1' '150' '12345' '38747321' → LÄK Thüringen

# 9 Bereitstellung von HBA-Entwicklerkarten[ARZT] für Anwendungsentwickler außerhalb der Testmaßnahmen der gematik

Zur Akzeptanzherstellung und -erhöhung soll neben den durch die eGK bedingten Anforderungen an den eArztausweis parallel in ausgewählten Projekten eine Integration der Karten in weitere medizinische (und ggf. andere) Anwendungen erfolgen.

Aus diesem Grund sind Regelungen für die Bereitstellung von HBA-Entwicklerkarten[ARZT] für Projekte zu definieren, um Inkompatibilitäten – bspw. durch Nutzung unterschiedlicher CV-Root-Hierarchien – von vornherein zu umgehen.

Die Bedarfe werden zentral über die BÄK aufgenommen und an interessierte Zertifizierungsdiensteanbieter weitergereicht. Für die Bereitstellung von HBA-Entwicklerkarten[ARZT] durch die ZDA soll grundsätzlich eine Vergütung der Leistungen in angemessenem Umfang erfolgen. Die Kosten für HBA-Entwicklerkarten[ARZT] außerhalb der gematik-Testmaßnahmen müssen durch die anfragenden Entwickler / Firmen selbst getragen werden. Die Rechnungsstellung erfolgt durch die ZDA.

Interessierte Entwickler wenden sich bei Bedarf direkt an die Bundesärztekammer: telematik@baek.de.

**Die ZDA werden gebeten, auch bzgl. HBA-Entwicklerkarten[ARZT] Preis-Angebote abzugeben, damit das Dezernat Telematik der BÄK gegenüber interessierten Entwicklern aussagefähig ist.**

Auch HBA-Entwicklerkarten[ARZT] sollen ein geeignetes optisches Merkmal enthalten, um eine Verwaltung der Karten leicht zu ermöglichen. Bspw. kann die ICCSN der ausgelieferten Karten für die Verwaltung rückgemeldet werden.

Den Entwicklern sollten ggf. drei HBA-Entwicklerkarten[ARZT] zur Verfügung gestellt werden, die den unterschiedlichen Status-Antworten des OCSP ((unknown, good, revoked) bezogen einheitlich auf alle Zertifikatstypen) entsprechen. Die Karten sind zusätzlich mit Informationen zu den personalisierten Testdaten, PINs, PUKs und Adressen (URL) der Infrastrukturdienste zu liefern.

Folgende Anforderungen gelten für die technische Ausgestaltung der Zertifikatsinhalte. Für Anwendungsentwickler bereitzustellende Infrastrukturdienste (LDAP, OCSP) sollen gemäß der beschriebenen Anforderungen der BÄK betrieben werden.

# 10 Konfigurationsdaten der Zertifikatsprofile

## 10.1 Admission im Basis-Signaturzertifikat

Die Extension „Admission“ muss in Basis-Signaturzertifikaten von **Generation-2** Entwickler-HBA[Arzt], Test-HBA[Arzt] der **HPC-Spezifikationsversion 3.0.0** gesetzt werden. Sie muss das Arzt-Attribut enthalten und strukturell dem Admission-Attribut des Attributzertifikats entsprechen. Das bedeutet auch, dass die Extension die Telematik-ID NICHT enthalten darf.

Entwicklerkarten und Testkarten der Generation 0 (HPC-Spezifikationsversion 2.1.1) sind von dieser Regelung nicht betroffen, d. h. Signaturzertifikate dieser Karten enthalten weiterhin keine Admission-Extension.

Auch echte elektronische Arztausweise der Generation 2 enthalten die Admission-Extension im Basis-Signaturzertifikat mit dem „Ärztin/Arzt“-Attribut. Dies ist allerdings abhängig von der allgemeinen Unterstützung von Attributzertifikaten mit generischen Attributen durch den Konnektor (bei einer Signatur wählbar im Ermessen des Anwenders), die von der gematik zugesagt und derzeit auch realisiert worden ist.

## 10.2 Nicht-qualifizierte CA-Zertifikate

Es ist zulässig, jeweils unterschiedliche CA-Zertifikate für die Erstellung von ENC- und AUT-Zertifikaten für Entwicklerkarten[ARZT] sowie für eArztausweise einzusetzen. Diese sollen zur besseren Unterscheidung entsprechende Namen (z. B. CN="{ZDA} Test **ENC**-CA für Ärzte {x}:PN", O={ZDA}, C=DE) haben.

## 10.3 Policy-OIDs für elektronische Arztausweise der Generation 2 (HPC-Spezifikationsversion ab 3.0.0)

In [baekCerts] und [baekAttr] ist die Policy-OID für elektronische Arztausweise der Generation 2 (HPC-Spezifikationsversion ab 3.0.0) nicht definiert. Folgende Policy-OIDs gelten dafür:

*Tabelle 10-1: Policy-OIDs*

| Karte | Zertifikatstyp | PolicyOID |
|---|---|---|
| HPC Version ab 3.0.0 | AUT | 1.2.276.0.76.4.145: policy-hba-010005-cp<br>1.2.276.0.76.4.75: hba-aut |
| HPC Version ab 3.0.0 | ENC | 1.2.276.0.76.4.145: policy-hba-010005-cp<br>1.2.276.0.76.4.74: hba-enc |
| HPC Version ab 3.0.0 | SIG, ATTR | 1.2.276.0.76.4.145: policy-hba-010005-cp<br>1.2.276.0.76.4.73: hba-sig |
| HPC Version ab 3.0.0 | qSIG, qATTR, QES | 1.2.276.0.76.4.145: policy-hba-010005-cp<br>1.2.276.0.76.4.72: hba-qes |

Der OID 1.2.276.0.76.4.145: policy-hba-010005-cp kennzeichnet die Gemeinsame Policy ([leoGemPolicy], in der Version 1.0.5), deren Regelungen für diese Karten gelten. Für HPCqSIG gilt die Gemeinsame Policy in der Version 1.0.0, OIDs sind im Kap. 3 definiert.

Für elektronische Arztausweise der Generation 2 muss zudem in allen Zertifikatsklassen die OID 1.3.6.1.4.1.42675.1.1 der Europäischen eID-Policy für Ärzte "CPME European eID-Policy for Physicians" Version 1.0.0 vom 23.11.2013 aufgenommen werden.

## 10.4 CRLDistributionPoints und AuthorityInfoAccess

Die Felder "CRLDistributionPoints" und "AuthorityInfoAccess" in den jeweiligen Zertifikaten müssen durch die ZDA, gemäß dem vorgegebenen Zertifikatsprofil der BÄK, strukturiert und gefüllt werden. Werden die (optionalen) CRLs für eine Zertifikatsklasse vom ZDA nicht ausgestellt, darf der „CRLDistributionPoint" in den entsprechenden Zertifikaten nicht gesetzt sein.

Die Feld-Inhalte (bspw. URL) müssen in Übereinstimmung zu den entsprechenden Infrastrukturdiensten korrekt durch den Zertifizierungsdiensteanbieter gesetzt sein.

### 10.5 Weitere Spezifische Konfigurationsdaten der X.509-Zertifikate auf HBA-Entwicklerkarten[ARZT]

- X.509-Trustcenter-Zertifikate (Root-, CA, CRL-Signer, OCSP, ggf. TSS-Zertifikate) sowie Enduser-Zertifikate auf HBA-Entwicklerkarten[ARZT] sollen folgende Bezeichnungen und Inhalte haben:
  - Die Trustcenter-Zertifikate werden nach folgenden Schema benannt (das Wort „{ZDA}“ wird durch die jeweilige Bezeichnung des Trustcenters ersetzt, ein „{x}“ durch eine fortlaufende Ganzzahl):
    - CA-Zertifikate für HBA-Entwicklerkarten[ARZT]: CN=”{ZDA} Entwickler CA für Ärzte {x}:PN“, O={ZDA}, C=DE
    - CRL-Signer, OCSP-Signer, ggf. TSS-Signer: CN=”{ZDA} Test {OCSP|CRL|TSS}-Signer{x}“, O={ZDA}, C=DE
  - Enduser-Zertifikate dürfen keine QC-Statements enthalten, optionale Extensions dürfen fehlen. Die Policy cp-isismtt-accredited darf nicht gesetzt werden.
  - Als „admissionAuthority“ für HBA-Entwicklerkarten[ARZT] wird „O=Landesärztekammer Beispielland, C=DE“ verwendet werden.
  - Es dürfen beliebige E-Mail-Adressen ins Zertifikat aufgenommen werden. Die Haftung dafür liegt beim Aussteller (z. B. bei unautorisierter Benutzung eines fremden domain-Namens).
  - Alle HBA-Entwicklerkarten[ARZT] müssen in der Restriction-Extension den Text „Nur zu Testzwecken. Der Inhaber ist kein Arzt.“ enthalten.

## 11 Referenzen

[extern1] Erstellung von XML-Signaturen für Dokumente nach Clinical Documents Architecture – R2 (Elektronische Signatur von Arztbriefen), BÄK, ÄKNo, ÄKWL, Version 1.0

[baekGlossar] Abkürzungsverzeichnis und Glossar

[baekCerts] Zertifikatsprofile für X.509 Basiszertifikate

[baekAttr] Zertifikatsprofile für X.509 Attributzertifikate

[leoGemPolicy] Gemeinsame Policy für die Herausgabe der HPC