

SRQ-ID: 1204

Betrifft:

Themenkreis	PKI und Zertifikate
Schlagwort	Welche Auswirkungen haben notwendige Aktualisierungen auf die Spezifikation?
zu Dokument / Datei (evtl. ersetzt SRQ)	gemX.509_eGK, ersetzt SRQ 0905
Version	1.4.0
Bezug (Kap., Abschnitt, Tab., Abb.)	3, 5, 6, 7, 8, 9, 10, 11, 12, A

Stichwort: Notwendige Aktualisierungen der Spezifikation

Frage:

Welche Auswirkungen haben notwendige Aktualisierungen auf die Spezifikation?

Betrifft:

Gültig ab	07.04.2011	Verbindlichkeit	normativ
Zulassungsrelevanz	Die SRQ ist für alle Zulassungen zu beachten, die nach dem 07.04.2011 beantragt werden.		
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
Anmerkungen:			
Status	<input checked="" type="checkbox"/> erfasst <input checked="" type="checkbox"/> intern abgestimmt <input type="checkbox"/> extern abgestimmt <input type="checkbox"/> zurückgezogen <input checked="" type="checkbox"/> freigegeben <input type="checkbox"/> eingearbeitet in Folgeversion		

Antwort:

Es wurden folgenden Änderungen/Ergänzungen vorgenommen:

- Die Eingangsanforderungs-Tabelle wurde mit der Anforderung A_01209 aktualisiert.
(Abschnitt 3)
- In den Zertifikatdefinitionen wurden die Attribute in Bezug auf die Verwendungsoptionen (Optional oder Pflicht) angepasst.
(Abschnitt 5.2)
- Eine Klarstellung zur Interpretation der maximalen Stringlänge in den Tabellen zum SubjectDN wurde vorgenommen.
(Abschnitt 5.2)
- Die Verbindlichkeit der Kürzungsregeln von Namen wurde präzisiert („MUSS“).
(Abschnitt 5.4)
- Die Felddefinitionen wurden angepasst und verdeutlicht.
(Abschnitt 5.4.2)
- Um Konsistenz mit der Facharchitektur VSDM [gemFA_VSDM] herzustellen, wurde die maximale Feldlänge des Feldes „title“ im SubjectDN von 10 auf 20 angepasst.
(Abschnitt 5.4.2)
- Die Bildung und Unterscheidung der beiden OU-Felder wurden in Bezug auf den Aufbau der Krankenversichertennummer verdeutlicht.
(Abschnitt 5.6)
- Der Inhalt des Abschnitts 5.7 wurde gelöscht und durch einen Überblick über die möglichen Extensions, die in einem Zertifikat enthalten sein müssen (P) bzw. enthalten sein können (O), ersetzt.
(Abschnitt 5.7)
- Der neue Abschnitt 5.8 mit Hinweis auf Aufbau und Inhalte der Admission-Struktur wurde aufgrund einer entsprechenden Anforderung der Gesamtarchitektur aufgenommen (Kennzeichnung von Rollen).
(neuer Abschnitt 5.8)
- Der neue Abschnitt 5.9 mit der Beschreibung der Kodierung des Zertifikatstyps wurde aufgenommen. Die Kodierung des Zertifikatstyps war zuvor in Abschnitt 5.7 beschrieben und wurde dort gelöscht.
(neuer Abschnitt 5.9)
- Der neue Abschnitt 5.11 mit Vorgaben zur Gültigkeit von Zertifikaten, zu CA- und OCSP-Zertifikaten in Anlehnung an weitere PKI-Spezifikationen zu Zertifikaten der Komponenten und der SMC-B wurde aufgenommen.
(neuer Abschnitt 5.11)
- Die Vorgaben zur Umsetzung bezüglich der Bildung der Pseudonymisierten Versichertenidentität wurden nun wieder in das Dokument aufgenommen

und erweitert.
(Abschnitt 9.1)

- Alle angepassten Kennzeichnungen der Extensions wurden in den jeweiligen Zertifikatsprofilen der Zertifikate der eGK C.CH.AUT, C.CH.ENC, C.CH.QES C.CH.AUTN und C.CH.ENCV aufgenommen.
(Abschnitt 6, 7, 8, 10 und 11)
- Eine Verdeutlichung der Optionalität der URL zur Zertifikatsrichtlinie in der Extension CertificatePolicies, sowie eine Verdeutlichung der Optionalität der Extension CRLDistributionPoints wurden vorgenommen.
(Abschnitte 6, 7, 8, 10 und 11)
- Ein Abschnitt über die Betriebumgebungen und Vorgaben zu deren Trennung wurde hinzugefügt.
(neuer Abschnitt 12)
- Das Verzeichnis der dokumentspezifischen Abkürzungen wurde erweitert.
(Abschnitt A1)
- Die Referenzierung der Dokumente wurde angepasst.
(Abschnitt A5)

3. Anforderungen

[...]

Tabelle 1: Bereits erfasste Eingangsanforderungen

Quelle	Anfor- derungs- nummer	Anfor- derungs- level	Beschreibung
[gemGesArch]	A_01209	MUSS	Aufnahme der Rolle in die Zertifikate Zertifikate zur Authentisierung von Akteuren in der Telematikinfrastruktur (zum Beispiel: AUT von HBA, BA, Diensten und OSIG von SMC-B) MÜSSEN eine Kennung für die durch das Zertifikat bestätigte Rolle enthalten.
[gemSpec_Ticket]	A_01583	MUSS	Übereinstimmung der IssuerDomain der Zertifikate AUT.N und ENC.V sowie AUT und ENC Jedes auf einer eGK gespeicherte Zertifikat enthält eine Herausgeberkennung, die IssuerDomain. Die IssuerDomain des AUT.N Zertifikates MUSS mit der IssuerDomain des ENC.V Zertifikates der gleichen eGK identisch sein. Ebenso MUSS die Issuer Domain des AUT Zertifikates mit der IssuerDomain des ENC Zertifikates übereinstimmen, um so eine Korrelierbarkeit der jeweiligen Zertifikate zu ermöglichen
...			

5.2 Attribute im SubjectDN

Zur Kodierung der Attribute sind die Hinweise in Abschnitt 9.2 zu beachten. Hinweis zur maximalen String-Länge: Die folgenden Übersichtstabellen zum SubjectDN enthalten die maximal zulässigen Feldlängen nach [COMMON-PKI]. Normativ für Zertifikate der TI sind jedoch die in Abschnitt 5.4.2 im Einzelnen getroffenen Festlegungen zur Feldlänge.

5.2.1 SubjectDN bei AUT-, ENC- und QES-Zertifikaten allen Zertifikaten außer AUTN und ENCV

Attribut	OID	Kodierung	max. String-Länge	Art
commonName	{id-at 3}	UTF8	64	Pflicht
title	{id-at 12}	UTF8	64	Option
surname	{id-at 4}	UTF8	64	P
givenName	{id-at 42}	UTF8	64	O
organizationalUnitName	{id-at 11}	UTF8	64	P

organizationName	{id-at 10}	UTF8	64	P
countryName	{id-at 6}	PrintableString	2 (ISO 3166 Code)	P

5.2.2 SubjectDN bei AUTN- und ENCV Zertifikaten

Attribut	OID	Kodierung	max. String-Länge	Art
commonName	{id-at 3}	UTF8	64	Pflicht
organizationalUnitName	{id-at 11}	UTF8	64	P
organizationName	{id-at 10}	UTF8	64	P
countryName	{id-at 6}	PrintableString	2 (ISO 3166 Code)	P

...

5.4 Aufbau der einzelnen Felder im SubjectDN

[...]

Dabei sind entsprechende Kürzungsregeln anzuwenden. Da in diesem Feld insgesamt 64 Zeichen zur Verfügung stehen, wird eine Kürzung nur in seltenen Fällen nötig sein.

Besteht dennoch die Notwendigkeit dafür, so **gelten MUSS** folgende Regeln **angewendet werden**:

- Ein gegebenenfalls vorhandener dritter Familienname ist sinnvoll, gegebenenfalls bis auf den Anfangsbuchstaben, zu verkürzen und die Kürzung durch einen Punkt kenntlich zu machen. Ist die Kürzung nicht ausreichend, **gilt MUSS** zusätzlich **gelten**:
- Ein zweiter Familienname ist sinnvoll, gegebenenfalls bis auf den Anfangsbuchstaben, zu kürzen und die Kürzung durch einen Punkt kenntlich zu machen.

Durch diese Regeln ist gewährleistet, dass sich die gegebenenfalls vorhandene zweite Namenszeile auf der Karte auch durch Kürzung aus dem Attribut `surname` ergibt.

Der `givenName` wird aus folgenden Attributen gebildet:

Vorname Namenszusatz Vorsatzwort.

Dabei sind entsprechende Kürzungsregeln anzuwenden. Da in diesem Feld insgesamt 64 Zeichen zur Verfügung stehen, wird eine Kürzung nur in seltenen Fällen nötig sein.

Besteht dennoch die Notwendigkeit dafür, so **gelten MUSS** folgende Regeln **angewendet werden**:

- Ein gegebenenfalls vorhandener dritter Rufname ist auf den Anfangsbuchstaben zu verkürzen und die Kürzung durch Punkt kenntlich zu machen. Ist die Kürzung nicht ausreichend, **gilt MUSS** zusätzlich **gelten**:

- Ein zweiter Rufname ist sinnvoll, gegebenenfalls bis auf den Anfangsbuchstaben, zu kürzen und die Kürzung durch Punkt kenntlich zu machen.

[...]

5.4.2 Felddefinitionen

givenName

Datenfeld: Vorname des Versicherten

Feld	Länge	Kardinalität	Datentyp	Format
givenName (mehrere Vornamen sind durch Blank oder Bindestrich getrennt. Aufbau: Vorname Namenszusatz Vorsatzwort)	1-64	0..1	AN	UTF-8

surname

Datenfeld: Familienname des Versicherten

Feld	Länge	Kardinalität	Datentyp	Format
surname (mehrere Nachnamen sind durch Blank oder Bindestrich getrennt)	1-64	1..1	AN	UTF-8

title

Datenfeld: Titel des Versicherten

Feld	Länge	Kardinalität	Datentyp	Format
title (mehrere Titel sind durch Bindestrich oder Blank getrennt)	1-20 1-10	0..1	AN	UTF-8

commonName

Datenfeld: Aufgedruckte Namenszeilen der Karte

Feld	Länge	Kardinalität	Datentyp	Format
Erste Namenszeile Zweite Namenszeile (Beide Bestandteile sind durch Blank getrennt)	1-28 1-28	1..1	AN	UTF-8

organizationalUnitName

Datenfeld: s. Detailfestlegungen in Abschnitt 5.6

organizationName

Datenfeld: Name des verantwortlichen Herausgebers

Feld	Länge	Kardinalität	Datentyp	Format
Name des verantwortlichen Herausgebers (Sollte der Name größer als die maximale Länge sein, muss dieser zusätzlich in die X.509-Extension SubjectAltNames (GeneralDN) eingetragen werden.)	1-64	1..1	AN	UTF-8

countryName

Datenfeld: Land dessen Gesetzgebung der Herausgabeprozess der Karte unterliegt

Feld	Länge	Kardinalität	Datentyp	Format
countryName	2	1..1	AN	Printable String

5.6 Aufbau der Krankenversichertennummer

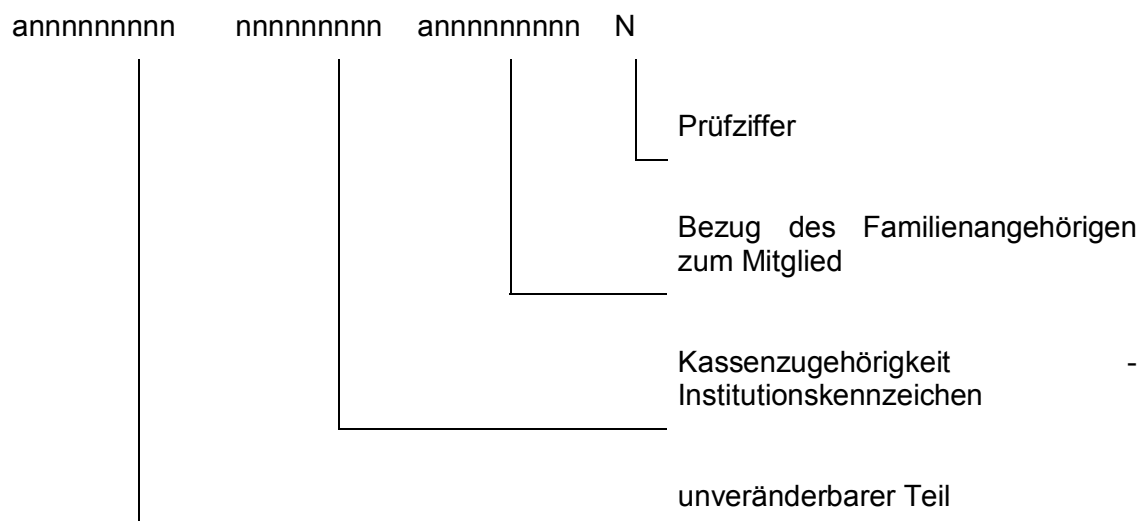


Abbildung 1: Aufbau der Krankenversichertennummer

Anmerkung/Begründung:

Gemäß § 290 definieren die Spitzenverbände der Krankenkassen die neue Struktur der Krankenversichertennummer, die aus einem unveränderbaren Teil zur Identifikation des

Versicherten und einem veränderbaren Teil, der bundeseinheitliche Angaben zur Kassenzugehörigkeit enthält und aus dem bei Vergabe der Nummer an Versicherte nach § 10 sichergestellt ist, dass der Bezug zu dem Angehörigen, der Mitglied ist, hergestellt werden kann.

organizationalUnitName

Datenfeld: unveränderbarer Teil

Feld	Länge	Kardinalität	Datentyp	Format
unveränderbarer Teil der KVNR	10	1..1	AN	annnnnnnnnn

organizationalUnitName

Datenfeld: ID des Kostenträgers

Feld	Länge	Kardinalität	Datentyp	Format
ID des Kostenträgers (hier: 9-stellige Institutionskennzeichen)	9	1..1	N	nnnnnnnnnn

Der unveränderbare Teil der Krankenversichertennummer und das Institutionskennzeichen werden im subjectDN im Feld „organizationalUnitName“ OU eingetragen.

Beide genannten Bestandteile stellen jeweils ein eigenes OU-Feld dar, eine Festlegung der Reihenfolge beider OUs erfolgt nicht! Ein Algorithmus bei der Zertifikatsauswertung kann beide Felder beispielsweise anhand der unterschiedlichen Länge differenzieren.

5.7 Notwendige Zertifikatsfelder Kennzeichnung von Zertifikatstypen

Zur Unterscheidung von Zertifikaten wird das jeweilige Kennzeichen in die Extension `additionalInformation` gespeichert.

Die genaue Festlegung der OID erfolgt im Prozess der Strukturierung der OIDs durch die gematik und das DIMDI.

ASN.1 Struktur nach [ISIS-MTT]

```

id-isismtt-at-additionalInformation OBJECT IDENTIFIER ::=
    {id-isismtt-at-15}

AdditionalInformationSyntax ::=
    DirectoryString (SIZE(1..2048))
  
```

Tabelle 3: Gültige Werte für Zertifikatstypen

Die folgende Tabelle gibt einen Überblick über die möglichen Extensions, die in einem Zertifikat enthalten sein müssen (P) bzw. enthalten sein können (O).

Tabelle 3: Mögliche Extensions in den Zertifikaten

	Versicherte n-zertifikat AUT/AUTN	Versicherte n-zertifikat ENC/ENCV	Versicherte n-zertifikat QES	CA- Zertifikat	OCSP- Responder Zertifikat
SubjectKeyIdentifier	P	P	P	P	P
BasicConstraints	O	O	O	P	P
KeyUsage	P	P	P	P	P
SubjectAltNames	O	O	-	O	O
CertificatePolicy	P	P	P	P	P
CRLDistributionPoint	O	O	O	O	O
AuthorityInfoAccess	P	P	P	P	P
SubjectDirectoryAttributes	-	-	O	-	-
AuthorityKeyIdentifier	P	P	P	P ⁴	P
Admission	P	P	P	O	O
QCStatements	-	-	P	-	-
ExtendedKeyUsage	P	O	O	O	P

Die Extension BasicConstraints MUSS für das CA-Zertifikat den Wert CA:true enthalten und für das Zertifikat des OCSP-Responders den Wert CA:false. Wird es bei den Versicherten-zertifikaten eingesetzt, MUSS der Wert ebenfalls CA:false sein.

Die Extension KeyUsage MUSS für das Versicherten-zertifikat je nach tatsächlichem Verwendungszweck den Wert „digitalSignature“ enthalten (AUT und AUTN), für die ENC- und ENCV-Zertifikate die Werte „keyEncipherment“ und „dataEncipherment“, für die QES-Zertifikate den Wert „nonRepudiation“, für das CA-Zertifikat die Werte „keyCertSign“ und „crlSign“, sowie für das Zertifikat des OCSP-Responders den Wert „nonRepudiation“. Normativ für die Umsetzung der KeyUsage sind die jeweiligen Zertifikatsprofile in den nachfolgenden Kapiteln.

In der Extension AuthorityInfoAccess MUSS die Adresse des OCSP-Services des TSP enthalten sein. Der Eintrag an dieser Stelle erfolgt aus Gründen der Kompatibilität. Die Feststellung zur Ermittlung der OCSP-Adresse in der TI ist in [gemVerw_Zert_TI#9.7] beschrieben.

⁴ Im Falle eines Root- bzw. self-signed CA-Zertifikats KANN diese Extension entfallen.

Die Extension ExtendedKeyUsage MUSS für ein Versichertenzertifikat für AUT und AUTN den Wert „clientAuth“ enthalten. Bei dem Zertifikat des OCSP-Responders MUSS diese Extension den Wert „OCSPSigning“ enthalten.

Siehe [COMMON-PKI] für die OIDs der anzugebenden Werte.

In allen Versichertenzertifikaten MUSS in der Extension Admission die Rolle des Zertifikatsinhabers (hier „Versicherter“) angegeben werden, weitere Details sind in Abschnitt 5.8 zu finden.

Zur Unterscheidung von Endnutzerzertifikaten MUSS neben den Referenzen auf die Policies auch der jeweilige Zertifikatstyp (OID) in der Extension CertificatePolicies gespeichert werden. Die genaue Festlegung der OID erfolgt verbindlich im Dokument [gemSpec_OID]. Nähere Vorgaben dazu finden sich im folgenden Abschnitt 5.9.

Bis auf die Extension „KeyUsage“ und „BasicConstraints“ werden alle Extensions auf „nicht kritisch“ gesetzt. Dieses ermöglicht den Einsatz der Zertifikate auch außerhalb der TI und innerhalb von ggf. zum Einsatz kommender Standardsoftware. Falls der Wert einer Extension für die Ablaufsteuerung einer Komponente der TI benötigt wird, MUSS diese Komponente der TI jedoch die Extension korrekt auswerten. Dieses MUSS durch die Ablaufsteuerung dieser Komponenten sichergestellt werden.

5.8 Kennzeichnung von Rollen in Extension Admission

Nach [gemGesArch#AnhB1] müssen zur Authentisierung und Autorisierung der technischen Identitäten in der TI technische Akteure und die ihnen zugeordneten technischen Rollen verwendet werden. Ebenso sind in [gemSiko#AnhD] fachliche Akteure und deren fachliche Berechtigungen beschrieben, sowie die zugeordnete Rollenhierarchie [gemSiko#AnhD3]. Somit MUSS auch in den Versichertenzertifikaten diese Rolle hinterlegt werden.

Die Extension Admission beinhaltet diese Rolle sowohl als Text als auch in Form einer maschinenlesbaren OID. Das Format und in welchem Feld diese Angaben gespeichert werden, findet sich am Ende des Abschnitts im Bereich „Gültige Werte“, die konkreten Inhalte werden in [gemSpec_OID] festgelegt.

Es MUSS genau eine Admission-Struktur aufgenommen werden, die genau ein Feld „ProfessionInfo“ enthalten MUSS. Die Admission-Extension MUSS in allen fünf Zertifikaten identisch enthalten sein.

ASN.1-Struktur nach [COMMON-PKI]:

```
id-isismtt-at-admission OBJECT IDENTIFIER ::= { isismtt-at 3 }  
id-isismtt-at-namingAuthorities OBJECT IDENTIFIER ::= { isismtt-at 11 }  
AdmissionSyntax ::= SEQUENCE {  
    admissionAuthority GeneralName OPTIONAL,  
    contentsOfAdmissions SEQUENCE OF Admissions}
```

```

Admissions ::= SEQUENCE {
    admissionAuthority [0] EXPLICIT GeneralName OPTIONAL,
    namingAuthority [1] EXPLICIT NamingAuthority OPTIONAL,
    professionInfos SEQUENCE OF ProfessionInfo}
NamingAuthority ::= SEQUENCE {
    namingAuthorityId OBJECT IDENTIFIER OPTIONAL,
    namingAuthorityUrl IA5String OPTIONAL,
    namingAuthorityText DirectoryString (SIZE(1..128)) OPTIONAL }
ProfessionInfo ::= SEQUENCE {
    namingAuthority [0] EXPLICIT NamingAuthority OPTIONAL,
    professionItems SEQUENCE OF DirectoryString (SIZE(1..128)),
    professionOIDs SEQUENCE OF OBJECT IDENTIFIER OPTIONAL,
    registrationNumber PrintableString (SIZE(1..128)) OPTIONAL,
    addProfessionInfo OCTET STRING OPTIONAL }

```

Tabelle 4: Gültige Werte der Kennzeichnung

Art der Kennzeichnung	Ort	Bezeichnung	Format	Inhalt
Rolle der jeweiligen Identität (s. [gemGesArch#AnhB1] und [gemSiKo#AnhD3])	Admission	ProfessionItem	Text	oid_versicherter
		ProfessionOID	OID	oid_versicherter

Entgegen der Optionalität aus [COMMON-PKI] MUSS das Feld „ProfessionOID“ gefüllt werden. In „ProfessionOID“ wird die OID der technischen Rolle gemäß [gemSpec_OID] in das Zertifikat aufgenommen.

Das vorliegende Dokument trifft nicht die Festlegungen zu den tatsächlich einzutragenden OIDs und Texten, sondern verwendet stattdessen eine OID-Referenz, die in der Spalte "Inhalt" der Tabelle „Gültige Werte“ genannt ist. Die normative Festlegung der OIDs und der Texte trifft das Dokument [gemSpec_OID], dort ist die Zuordnung zur OID-Referenz ersichtlich.

5.9 Angaben zum Zertifikatstyp in der Extension CertificatePolicies

Die Extension MUSS neben den Referenzen auf die zugrunde liegenden Policies für die Zertifikate auch die Angaben zum Zertifikatstyp enthalten. Die Extension ist „non-critical“.

ASN.1-Struktur nach [COMMON-PKI] (nur relevanter Teil):

```

CertificatePolicies ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation
PolicyInformation ::= SEQUENCE

```

```

    {policyIdentifier CertPolicyId,

      policyQualifiers SEQUENCE SIZE(1..MAX) OF PolicyQualifierInfo
    OPTIONAL
  }

  CertPolicyId ::= OBJECT IDENTIFIER

```

Es ist möglich, mehrere Zertifikats-Policies aufzunehmen. Wenn Anforderungen (z. B. Sicherheitsanforderungen) einer aufgeführten Policy durch eine andere aufgeführte Policy im selben Zertifikat vermindert werden, dann gelten stets die jeweiligen schärferen Anforderungen.

Für die Angabe des Zertifikatstyps MUSS ein Element `PolicyInformation` eingefügt werden, das die OID für den Zertifikatstyp als Wert des Unterelements `policyIdentifier` enthält. Dieses Element `PolicyInformation` enthält kein Unterelement `policyQualifier`.

Tabelle 5: Gültige Werte der Zertifikatskennzeichner

Zertifikat	Ort	Bezeichnung	Format	Inhalt
AUT	CertificatePolicies	C.CH.AUT	OID	oid_egk_aut
ENC		C.CH.ENC	OID	oid_egk_enc
QES		C.CH.QES	OID	oid_egk_qes
AUTN		C.CH.AUTN	OID	oid_egk_autn
ENCV		C.CH.ENCV	OID	oid_egk_encv

Das vorliegende Dokument trifft nicht die Festlegungen zu den tatsächlich einzutragenden OIDs, sondern verwendet stattdessen eine OID-Referenz, die in der Spalte "Inhalt" der Tabelle „Gültige Werte“ genannt ist. Die normative Festlegung der OIDs trifft das Dokument [gemSpec_OID], dort ist die Zuordnung zur OID-Referenz ersichtlich.

5.10 (leer)

Abschnitt entfällt. Um die Nummerierung der nachfolgenden Abschnitte zu erhalten, bleibt der Platzhalter Bestehen.

5.11 Zertifikatsprofil

Im Folgenden werden die Profile für die Versichertenzertifikate für AUT, ENC, QES, AUTN und ENCV beschrieben.

Die Unterscheidung der Zertifikate nach Test- und Produktivbetrieb wird anhand des Issuer-Eintrags im Zertifikat vorgenommen. Es werden jeweils unterschiedliche CAs für

den Test- und Produktivbetrieb erstellt. Im jeweiligen commonName der CA muss die Art des Betriebes hinterlegt werden, s. a. Abschnitt 12.

Die Gültigkeitsdauer der Zertifikate wird durch dieses Dokument nicht fest vorgegeben.

Die Gültigkeit der CA-Zertifikate und der OCSP-Responder-Zertifikate kann durch den TSP festgelegt werden.

Bei der Festlegung der Gültigkeit der Zertifikate und Schlüssel MÜSSEN die Vorgaben aus [gemSiKo#AnhF5] und [gemSpec_Krypt#5.1.1.2, #5.1.1.3 sowie #5.1.1.7] berücksichtigt werden.

Für den Aufbau des *SubjectDN* in einem Versichertenzertifikat MÜSSEN die Vorgaben aus Abschnitt 5.2 umgesetzt werden.

Für den Aufbau des *SubjectDN* in einem CA-Zertifikat MÜSSEN die folgenden Vorgaben umgesetzt werden:

- Der subjectDN einer CA MUSS diese eindeutig innerhalb der TI identifizieren.
- Das Attribut commonName MUSS enthalten sein. Es MUSS den Namen (maximal 64 Zeichen) der CA enthalten, mit der der TSP die Versichertenzertifikate ausstellt.
- Das Attribut organizationName MUSS enthalten sein. Es MUSS den Namen (maximal 64 Zeichen) des TSP enthalten.
- Das Attribut countryName MUSS enthalten sein und das Land des TSP (2 Zeichen, ISO 3166 Code) enthalten.
- Die Attribute serialNumber und organizationalUnitName KÖNNEN enthalten sein. Sie SOLLEN jedoch nur dann verwendet werden, falls sie für die Eindeutigkeit des subjectDN der CA notwendig sind.
- Weitere Attribute SOLLEN NICHT enthalten sein.

Für den Aufbau des *SubjectDN* in einem OCSP-Responder-Zertifikat MÜSSEN die folgenden Vorgaben umgesetzt werden:

- Der *subjectDN* eines OCSP-Responders MUSS diesen eindeutig innerhalb der TI identifizieren.
- Das Attribut commonName MUSS enthalten sein. Es MUSS den Namen (maximal 64 Zeichen) des OCSP-Responders enthalten, mit der der TSP die OCSP-Statusinformationen für die Versichertenzertifikate signiert.
- Das Attribut organizationName MUSS enthalten sein. Es MUSS den Namen (maximal 64 Zeichen) des TSP enthalten.
- Das Attribut countryName MUSS enthalten sein und das Land des TSP (2 Zeichen, ISO 3166 Code) enthalten.
- Das Attribut organizationalUnitName KANN enthalten sein. Es SOLL jedoch nur dann verwendet werden, falls es für die Eindeutigkeit des *subjectDN* des OCSP-Responders notwendig ist.

- Weitere Attribute SOLLEN NICHT enthalten sein.

5.11.1 Benennung der Zertifikate

Mit den eigentlichen Zertifikatsprofilen sind in den folgenden Kapiteln 6 bis 8 sowie 10 und 11 auch einheitliche Namen für die Zertifikate genannt.

Aus den folgenden Benennungen leiten sich auch die OID-Referenzen für den Zertifikatsbezeichner im Feld „CertificatePolicies“ ab.

Das Benennungsschema ist in [gemPKI_Nota] beschrieben. Dort sind die zulässigen Werte vorgegeben. Für die Benennung der Zertifikate wird dabei wie folgt vorgegangen:

Zertifikatsname ::= <Objekttyp>.<Service-Typ>.< Verwendungszweck >

6 Authentisierungszertifikat der eGk (C.CH.AUT)

Element		Bemerkungen
certificate		Authentisierungszertifikat
	tbsCertificate	Zertifikatsdaten
	version	Version der Spezifikation: Version 3
	serialNumber	Eindeutige Nummer des Zertifikats im Rahmen der ausstellenden CA (ganze Zahl, $1 \leq \text{serialNumber} \leq 2^{159}$)
	signature	Zur Signatur des Zertifikats verwendeter Algorithmus: Die konkrete Festlegung erfolgt gemäß [gemSpec_Krypt#5.1.1.2]
	issuer	Name der ausstellenden CA als Distinguished Name (DN); Codierung der Namen in UTF8, Subset ISO 8859-1
	validity	Gültigkeit des Zertifikats (von - bis); Codierung als UTCTime
	subject	Codierung der Namen in UTF8, Subset ISO 8859-1, Name des Zertifikatsinhabers als DN:
	CommonName	CN = Aufgedruckte Namenszeilen der Karte
	title	Titel des Versicherten (optional)
	givenName	Vorname des Inhabers (optional)
	surname	Nachname des Inhabers
	organizationalUnitName	OU = unveränderbarer Teil der KV-Nummer
	organizationalUnitName	OU = Institutionskennzeichen
	organizationalUnitName	O = Herausgeber
	countryName	C = DE
	subjectPublicKeyInfo	Algorithmus und tatsächlicher Wert des öffentlichen Schlüssels des Zertifikatsbesitzers: Die konkrete Festlegung erfolgt gemäß [gemSpec_Krypt#5.1.1.2] mit individuellem Wert
	extensions	Erweiterungen
	SubjectKeyIdentifier (2.5.29.14)	nicht kritisch ID für den öffentlichen Schlüssel des Zertifikatsinhabers in der Ausprägung 'keyIdentifier'
	KeyUsage (2.5.29.15)	kritisch Schlüsselverwendung mit dem Wert 'digitalSignature'
	SubjectAltNames (2.5.29.17)	nicht kritisch optional, wenn vorhanden wird die Komponente rfc822Name benutzt
	BasicConstraints (2.5.29.19)	kritisch Kennzeichnung, ob CA- oder End-Entity-Zertifikat (optional)

	CertificatePolicies (2.5.29.32)	nicht kritisch URL (optional) und OID mit der Zertifikatsrichtlinie sowie Angabe der OID des Zertifikatstyps
	CRLDistributionPoints (2.5.29.31)	nicht kritisch Verteilungspunkt für Sperrlisten (nach ISIS-MIT V1.4) (nach COMMON-PKI V1.1) (optional)
	AuthorityInfoAccess (1.3.6.1.5.5.7.1.1)	nicht kritisch Verteilungspunkt für Statusinformationen des Zertifikats (OCSP) (nach ISIS-MIT V1.4) (nach COMMON-PKI V1.1)
	AuthorityKeyIdentifier (2.5.29.35)	nicht kritisch ID für den öffentlichen Schlüssel der ausstellenden CA
	Admission (1.3.36.8.3.3)	nicht kritisch Rolle des Zertifikatsinhabers
	AdditionalInformation (1.3.36.8.3.15)	nicht kritisch Kennzeichen des Zertifikatstyps
	ExtendedKeyUsage (2.5.29.37)	nicht kritisch Schlüsselverwendung mit dem Wert 'clientAuth'
	signatureAlgorithm	Zur Signatur des Zertifikats verwendeter Algorithmus: Die konkrete Festlegung erfolgt gemäß [gemSpec_Krypt#5.1.1.2]
	signature	Wert der Signatur

7 Verschlüsselungszertifikat der eGk (C.CH.ENC)

Element		Bemerkungen
certificate		Verschlüsselungszertifikat
	tbsCertificate	Zertifikatsdaten
	version	Version der Spezifikation: Version 3
	serialNumber	Eindeutige Nummer des Zertifikats im Rahmen der ausstellenden CA (ganze Zahl, $1 \leq \text{serialNumber} \leq 2^{159}$)
	signature	Zur Signatur des Zertifikats verwendeter Algorithmus: Die konkrete Festlegung erfolgt gemäß [gemSpec_Krypt#5.1.1.2] [gemSpec_Krypt#5.1.1.7]
	issuer	Name der ausstellenden CA als Distinguished Name (DN); Codierung der Namen in UTF8, Subset ISO 8859-1
	validity	Gültigkeit des Zertifikats (von - bis); Codierung als UTCtime
	subject	Codierung der Namen in UTF8, Subset ISO 8859-1, Name des Zertifikatsinhabers als DN:
	commonName	CN = Aufgedruckte Namenszeilen der Karte
	title	Titel des Versicherten (optional)
	givenName	Vorname des Inhabers (optional)
	surname	Nachname des Inhabers
	organizationalUnitName	OU = unveränderbarer Teil der KV-Nummer
	organizationalUnitName	OU = Institutionskennzeichen
	organizationName	O = Herausgeber
	countryName	C = DE
	subjectPublicKeyInfo	Algorithmus und tatsächlicher Wert des öffentlichen Schlüssels des Zertifikatsbesitzers: Die konkrete Festlegung erfolgt gemäß [gemSpec_Krypt#5.1.1.2] [gemSpec_Krypt#5.1.1.7] mit individuellem Wert
	extensions	Erweiterungen
	SubjectKeyIdentifier (2.5.29.14)	nicht kritisch ID für den öffentlichen Schlüssel des Zertifikatsinhabers in der Ausprägung 'keyIdentifier'
	SubjectAltNames (2.5.29.17)	nicht kritisch optional, wenn vorhanden wird die Komponente rfc822Name benutzt

		BasicConstraints (2.5.29.19)	kritisch Kennzeichnung, ob CA- oder End-Entity-Zertifikat (optional)
		KeyUsage (2.5.29.15)	kritisch Schlüsselverwendung mit dem Wert 'keyEncipherment' und 'dataEncipherment'
		CertificatePolicies (2.5.29.32)	nicht kritisch URL (optional) und OID mit der Zertifikatsrichtlinie sowie Angabe der OID des Zertifikatstyps
		CRLDistributionPoints (2.5.29.31)	nicht kritisch Verteilungspunkt für Sperrlisten (nach ISIS-MTT V1.4) (nach COMMON-PKI V1.1) (optional)
		AuthorityInfoAccess (1.3.6.1.5.5.7.1.1)	nicht kritisch Verteilungspunkt für Statusinformationen des Zertifikats (OCSP) (nach ISIS-MTT V1.4) (nach COMMON-PKI V1.1)
		AuthorityKeyIdentifier (2.5.29.35)	nicht kritisch ID für den öffentlichen Schlüssel der ausstellenden CA
		Admission (1.3.36.8.3.3)	nicht kritisch Rolle des Zertifikatsinhabers
		AdditionalInformation (1.3.36.8.3.15)	nicht kritisch Kennzeichen des Zertifikatstyps
	signatureAlgorithm		Zur Signatur des Zertifikats verwendeter Algorithmus: Die konkrete Festlegung erfolgt gemäß [gemSpec_Krypt#5.1.1.2] [gemSpec_Krypt#5.1.1.7]
	signature		Wert der Signatur

8 Optionales Qualifiziertes Signaturzertifikat der eGk (C.CH.QES)

Element		Bemerkungen
certificate		Qualifiziertes Signaturzertifikat für QES (Willenserklärung)
tbsCertificate		Zertifikatsdaten
	version	Version der Spezifikation: Version 3
	serialNumber	Eindeutige Nummer des Zertifikats im Rahmen der ausstellenden CA (ganze Zahl, $1 \leq \text{serialNumber} \leq 2^{159}$)
	signature	Zur Signatur des Zertifikats verwendeter Algorithmus: Die konkrete Festlegung erfolgt gemäß [gemSpec_Krypt#5.1.1.3]
	issuer	Name der ausstellenden CA als Distinguished Name (DN); Codierung der Namen in UTF8, Subset ISO 8859-1
	validity	Gültigkeit des Zertifikats (von - bis); Codierung als UTCTime
	subject	Codierung der Namen in UTF8, Subset ISO 8859-1, Name des Zertifikatsinhabers als DN:
	CommonName	CN = Aufgedruckte Namenszeilen der Karte
	title	Titel des Versicherten (optional)
	givenName	Vorname des Inhabers (optional)
	surname	Nachname des Inhabers
	organizationalUnitName	OU = unveränderbarer Teil der KV-Nummer
	organizationalUnitName	OU = Institutionskennzeichen
	organizationName	O = Herausgeber
	countryName	C = DE
	subjectPublicKeyInfo	Algorithmus und tatsächlicher Wert des öffentlichen Schlüssels des Zertifikatsbesitzers: Die konkrete Festlegung erfolgt gemäß [gemSpec_Krypt#5.1.1.3] mit individuellem Wert
	extensions	Erweiterungen
	SubjectKeyIdentifier (2.5.29.14)	nicht kritisch ID für den öffentlichen Schlüssel des Zertifikatsinhabers in der Ausprägung 'keyIdentifier'

KeyUsage (2.5.29.15)	kritisch Schlüsselverwendung mit dem Wert 'nonRepudiation'
BasicConstraints (2.5.29.19)	kritisch Kennzeichnung, ob CA- oder End-Entity-Zertifikat (optional)
Certificate Policies (2.5.29.32)	nicht kritisch URL (optional) und OID mit der Zertifikatsrichtlinie sowie Angabe der OID des Zertifikatstyps
CRLDistributionPoints (2.5.29.31)	nicht kritisch Verteilungspunkt für Sperrlisten (nach ISIS-MTT V1.1) (nach COMMON-PKI V1.1) (optional)
AuthorityInfoAccess (1.3.6.1.5.5.7.1.1)	nicht kritisch Verteilungspunkt für Statusinformationen des Zertifikats (OCSP) (nach ISIS-MTT V1.1) (nach COMMON-PKI V1.1)
SubjectDirectory- Attributes (2.5.29.9)	optional, nicht kritisch Angaben, die den Zertifikatsinhaber zusätzlich zu den Angaben unter 'subject' eindeutig identifizieren: Titel (optional), Geburtstag (optional), Geburtsort (optional), Geburtsname (optional)
AuthorityKeyIdentifier (2.5.29.35)	nicht kritisch ID für den öffentlichen Schlüssel der ausstellenden CA
Admission (1.3.36.8.3.3)	nicht kritisch Rolle des Zertifikatsinhabers
AdditionalInformation (1.3.36.8.3.15)	nicht kritisch Kennzeichen des Zertifikatstyps
QCStatements (1.3.6.1.5.5.7.1.3)	id-qcs-pkixQCSyntax-v1 (1.3.6.1.5.5.7.11.1) Konformität zu Syntax und Semantik nach RFC 3039 id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) Ausgabe des Zertifikats erfolgte konform zur Europäischen Richtlinie 1999/93/EG und nach dem Recht des Landes, nach dem die CA arbeitet.
signatureAlgorithm	Zur Signatur des Zertifikats verwendeter Algorithmus: Die konkrete Festlegung erfolgt gemäß [gemSpec_Krypt#5.1.1.3]
signature	Wert der Signatur

9.1 Bildung der pseudonymisierten Versichertenidentität

Jeder Versicherte bekommt bei der Produktion seiner eGK ein Pseudonym. Das Pseudonym wird gemäß folgender Vorschrift aus dem Nachnamen des Karteninhabers, dem unveränderbaren Teil der KVNR und einer vom Herausgeber (Kostenträger) verwendeten Zusatzinformation (herausgeberspezifischer Zufallswert) mit einer geeigneten kryptographischen Hash-Funktion (SHA-256) gebildet.

Es wird der `subjectDN` des Versicherten im Zertifikat abgebildet, hierbei wird der `commonName` aus dem Hashwert der Konkatination der folgenden Attribute gebildet:

Hash der Datenfelder:
- Inhaber (Nachname)
- unveränderbarer Teil der KVNR
- herausgeberspezifischer Zufallswert (hs-ZW)

Der durch den Herausgeber (hier der Kostenträger) festzulegende Wert (hs-ZW) muss zufällig ausgewählt werden und eine ausreichende Entropie enthalten, hierfür muss ein Zufallswert aus mindestens 16 Hexadezimal-Zahlen (64 Bit) bestehen.

Dieser Wert bleibt für alle Versichertenkarten für einen bestimmten Zeitraum identisch und MUSS jährlich gewechselt werden. Nicht mehr benutzte Zufallswerte MÜSSEN beim Herausgeber sicher langfristig (mindestens für 10 Jahre) gespeichert werden. Es MUSS sichergestellt werden, dass bereits verwendete Zufallswerte nicht erneut eingesetzt werden. Die Zufallswerte MÜSSEN entsprechend der Schutzbedarfsanalyse (Methodik der Schutzbedarfsfeststellung, siehe [gemSiKo#C1.3]) eingeordnet und behandelt werden.

Durch die Verwendung dieses Verfahrens kann vermieden werden, dass die KVN in einem (öffentlichen) Zertifikats-Verzeichnis gespeichert werden muss. Eine Kontrolle, ob eine bestimmte KVN zu einem bestimmten Inhaber und dem entsprechenden Zertifikatsausgeber gehört, bleibt trotzdem gewährleistet, wenn sich der `commonName` aus den kodierten Zeichen des Hashwertes der oben genannten Felder ergibt.

Zum Beispiel könnte der SHA256-Hashwert der oben genannten Daten folgenden Wert ergeben:

A9E2FF93C69A32C463603146C077F592E85821A345F0DB3E5AA977772D8C97DF

Für den `commonName` werden die ersten 20 Zeichen

A9E2FF93C69A32C46360

der Bestandteile des Hashwertes verwendet. Da man diese „Seriennummer“ nur als Prüfkriterium verwendet, sind an dieser Stelle auch etwaige Kollisionen ohne Bedeutung.

Die Anzahl der Zeichen (20 Hexadezimalzahlen), die aus dem Hashwert in den `commonName` übernommen werden, hat eine Variationsbreite von 80 Bit.

Die Länge des `commonName` im SubjectDN MUSS 20 Zeichen betragen.

Beispiel:

Nachname = „Mustername1“

KVN (unveränderlicher Teil) = „M331784849“

herausgeberspezifischer Zufallswert = „MUKA124DKD9383KJ“

Konkatenation = „Mustername1M331784849MUKA124DKD9383KJ“

SHA-256- Hashwert = “E3F3555165491A7FB902BFAF254518C469E584A793...”

`commonName` = “E3F3555165491A7FB902”

geänderter herausgeberspezifischer Zufallswert = „3C463603146C077“

Konkatenation = „Mustername1M3317848493C463603146C077“

SHA-256- Hashwert = “868BF4FD1A8D8E14092239F9B2E1E138A76CA86346...”

`commonName` = “868BF4FD1A8D8E140922”

Nach Erzeugung des Pseudonyms MUSS geprüft werden, ob dieses Pseudonym vom Kartenherausgeber bereits vergeben wurde. Ist dies der Fall, DARF dieses Pseudonym NICHT verwendet werden und muss neu erzeugt werden. Dazu MUSS die Pseudonymbildung mit inkrementiertem hs-ZW wiederholt werden und erneut auf Eindeutigkeit geprüft werden. Die Pseudonyme bei einem Kartenherausgeber MÜSSEN eindeutig sein und es DARF NICHT zu Kollisionen gegen aktuell verwendete Pseudonyme des Herausgebers kommen. Dem Versicherten MUSS daher auch bei einem Kartenwechsel ein neues Pseudonym zugewiesen werden. Die maximale Lebensdauer eines Pseudonyms entspricht damit der Laufzeit der Karte bzw. wenn die letzten einem Pseudonym zugeordneten Daten in der TI gelöscht worden sind.

Weiterhin wird auf die Anforderungen aus Abschnitt 3 verwiesen, insbesondere A_01584.

10 Technisches Authentisierungszertifikat der eGk (C.CH.AUTN)

Element		Bemerkungen
certificate		Authentisierungszertifikat
tbsCertificate		Zertifikatsdaten
	version	Version der Spezifikation: Version 3
	serialNumber	Eindeutige Nummer des Zertifikats im Rahmen der ausstellenden CA (ganze Zahl, $1 \leq \text{serialNumber} \leq 2^{159}$)
	signature	Zur Signatur des Zertifikats verwendeter Algorithmus: Die konkrete Festlegung erfolgt gemäß [gemSpec_Krypt#5.1.1.2]
	issuer	Name der ausstellenden CA als Distinguished Name (DN); Codierung der Namen in UTF8, Subset ISO 8859-1
	validity	Gültigkeit des Zertifikats (von - bis); Codierung als UTCTime
	subject	Codierung der Namen in UTF8, Subset ISO 8859-1, Name des Zertifikatsinhabers als DN: CN = Hashwert des unveränderbaren Teils der KV-Nummer, des Nachnamens des Versicherten und eines herausgeberspezifischen Zufallswert. OU = Institutionskennzeichen O = Herausgeber C = DE
	subjectPublicKeyInfo	Algorithmus und tatsächlicher Wert des öffentlichen Schlüssels des Zertifikatsbesitzers: Die konkrete Festlegung erfolgt gemäß [gemSpec_Krypt#5.1.1.2] mit individuellem Wert
	extensions	Erweiterungen
	SubjectKeyIdentifier (2.5.29.14)	nicht kritisch ID für den öffentlichen Schlüssel des Zertifikatsinhabers in der Ausprägung ‚keyIdentifier‘
	KeyUsage (2.5.29.15)	kritisch Schlüsselverwendung mit dem Wert ‚digitalSignature‘
	SubjectAltNames (2.5.29.17)	nicht kritisch optional, wenn vorhanden wird die Komponente rfc822Name benutzt
	BasicConstraints (2.5.29.19)	kritisch Kennzeichnung, ob CA- oder End-Entity-Zertifikat (optional)
	CertificatePolicies (2.5.29.32)	nicht kritisch URL (optional) und OID mit der Zertifikatsrichtlinie sowie Angabe der OID des Zertifikatstyps
	CRLDistributionPoints (2.5.29.31)	nicht kritisch Verteilungspunkt für Sperrlisten (nach ISIS-MTT V4.1) (nach COMMON-PKI V1.1) (optional)

	AuthorityInfoAccess (1.3.6.1.5.5.7.1.1)	nicht kritisch Verteilungspunkt für Statusinformationen des Zertifikats (OCSP) (nach ISIS-MTT V1.4) (nach COMMON-PKI V1.1)
	AuthorityKeyIdentifier (2.5.29.35)	nicht kritisch ID für den öffentlichen Schlüssel der ausstellenden CA
	Admission (1.3.36.8.3.3)	nicht kritisch Rolle des Zertifikatsinhabers
	AdditionalInformation (1.3.36.8.3.15)	nicht kritisch Kennzeichen des Zertifikatstyps
	ExtendedKeyUsage (2.5.29.37)	nicht kritisch Schlüsselverwendung mit dem Wert ‚clientAuth‘
	signatureAlgorithm	Zur Signatur des Zertifikats verwendeter Algorithmus: Die konkrete Festlegung erfolgt gemäß [gemSpec_Krypt#5.1.1.2]
	signature	Wert der Signatur

11 Technisches Verschlüsselungszertifikat der eGK (C.CH.ENCV)

Element	Bemerkungen
certificate	Verschlüsselungszertifikat
tbsCertificate	Zertifikatsdaten
version	Version der Spezifikation: Version 3
serialNumber	Eindeutige Nummer des Zertifikats im Rahmen der ausstellenden CA (ganze Zahl, $1 \leq \text{serialNumber} \leq 2^{159}$)
signature	Zur Signatur des Zertifikats verwendeter Algorithmus: Die konkrete Festlegung erfolgt gemäß [gemSpec_Krypt#5.1.1.2] [gemSpec_Krypt#5.1.1.7]
issuer	Name der ausstellenden CA als Distinguished Name (DN); Codierung der Namen in UTF8, Subset ISO 8859-1
validity	Gültigkeit des Zertifikats (von – bis); Codierung als UTCTime
subject	Codierung der Namen in UTF8, Subset ISO 8859-1, Name des Zertifikatsinhabers als DN:
commonName	CN = Hashwert des unveränderbaren Teils der KV-Nummer, des Nachnamens des Versicherten und eines herausgeberspezifischen Zufallswert.
organizationalUnitName	OU = Institutionskennzeichen
organizationName	O = Herausgeber
countryName	C = DE
subjectPublicKeyInfo	Algorithmus und tatsächlicher Wert des öffentlichen Schlüssels des Zertifikatsbesitzers: Die konkrete Festlegung erfolgt gemäß [gemSpec_Krypt#5.1.1.2] [gemSpec_Krypt#5.1.1.7] mit individuellem Wert
extensions	Erweiterungen
SubjectKeyIdentifier (2.5.29.14)	nicht kritisch ID für den öffentlichen Schlüssel des Zertifikatsinhabers in der Ausprägung ‚keyIdentifier‘
KeyUsage (2.5.29.15)	kritisch Schlüsselverwendung mit dem Wert ‚keyEncipherment‘ und ‚dataEncipherment‘
SubjectAltNames (2.5.29.17)	nicht kritisch optional, wenn vorhanden wird die Komponente rfc822Name benutzt
BasicConstraints (2.5.29.19)	kritisch Kennzeichnung, ob CA- oder End-Entity-Zertifikat (optional)

		CertificatePolicies (2.5.29.32)	nicht kritisch URL (optional) und OID mit der Zertifikatsrichtlinie sowie Angabe der OID des Zertifikatstyps
		CRLDistributionPoints (2.5.29.31)	nicht kritisch Verteilungspunkt für Sperrlisten (nach ISIS MTT V1.1) (nach COMMON-PKI V1.1) (optional)
		AuthorityInfoAccess (1.3.6.1.5.5.7.1.1)	nicht kritisch Verteilungspunkt für Statusinformationen des Zertifikats (OCSP) (nach ISIS MTT V1.1) (nach COMMON-PKI V1.1)
		AuthorityKeyIdentifier (2.5.29.35)	nicht kritisch ID für den öffentlichen Schlüssel der ausstellenden CA
		Admission (1.3.36.8.3.3)	nicht kritisch Rolle des Zertifikatsinhabers
		AdditionalInformation (1.3.36.8.3.15)	nicht kritisch Kennzeichen des Zertifikatstyps
	signatureAlgorithm	Zur Signatur des Zertifikats verwendeter Algorithmus: Die konkrete Festlegung erfolgt gemäß [gemSpec_Krypt#5.1.1.2] [gemSpec_Krypt#5.1.1.7]	
	signature	Wert der Signatur	

12 Produktiv- / Test-Umgebungen

Bei X.509-Zertifikaten in der TI wird unterschieden, in welchen Einsatzumgebungen diese verwendet werden. Eine grundsätzliche Trennung erfolgt nach Produktiv- und Testumgebung, wobei die produktive Umgebung selbst wiederum aus drei Umgebungen besteht, wie im Folgenden näher erläutert wird. Somit MUSS der TSP für jede Umgebung eine eigene CA betreiben. Diese Systeme MÜSSEN technisch und organisatorisch getrennt werden. Die sich aus dieser Trennung der Umgebungen ergebenden Sicherheitsanforderungen an den TSP sind in [gemSiKo#AnhG3.2.4 und 3.2.8] zu finden und MÜSSEN umgesetzt werden.

Die Produktivumgebung wird gemäß [gem_Betr_BK_R2FT] in die verschiedenen Umgebungen Produktionsumgebung (PU), Produktionsreferenzumgebung (PRU) und eine Produktionstestumgebung (PTU) unterschieden. Um den Betrieb dieser Umgebungen sauber trennen zu können, MÜSSEN die dabei in einer PU, PRU bzw. PTU zum Einsatz kommenden Zertifikate aus unterschiedlichen Vertrauensräumen kommen. Entsprechend wird auch bei der TSL zwischen PU-TSL, PRU-TSL und PTU-TSL unterschieden. Die zertifikatsprüfenden Komponenten MÜSSEN daher mit der jeweils für sie anhand der Betriebsumgebung relevanten TSL ausgestattet sein. Für die Produktiv-CA(s) des TSP ergibt sich daraus, dass für diese ebenfalls getrennt eine PU, eine PRU und eine PTU betrieben werden MÜSSEN.

- Das CA-Zertifikat der CA der Produktionsumgebung wird durch die gematik in die PU-TSL eingetragen.
- Das CA-Zertifikat der CA der Produktionsreferenzumgebung wird durch die gematik in die PRU-TSL eingetragen.
- Das CA-Zertifikat der CA der Produktionstestumgebung wird durch die gematik in die PTU-TSL eingetragen.
- Das CA-Zertifikat der CA der Testumgebung wird durch die gematik in die TU-TSL eingetragen.

Die folgende Abbildung verdeutlicht die Unterscheidung dieser Betriebsumgebungen:

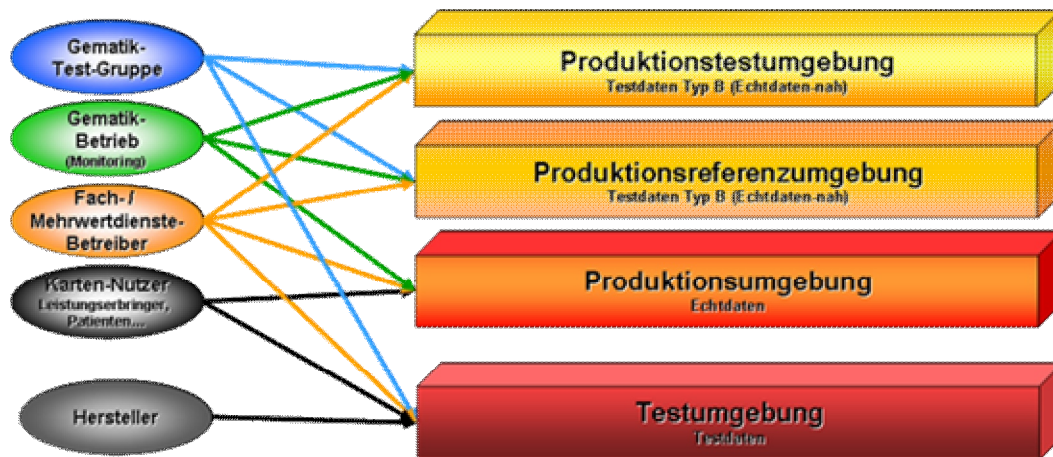


Abbildung 3: Unterscheidung der Betriebsumgebungen

A1 - Abkürzungen

Kürzel	Erläuterung
AN	alphanumerisch
AUT	Authentication
AUTN	Technisches Authentisierungszertifikat für Nachrichten
C2C	card to card
CA	certification authority
CRL	Certificate Revocation List
CVC	Card Verifiable Certificate
DN	Distinguished Name
EE	End Entity
eGK	Elektronische Gesundheitskarte
ENC	Encryption
ENCV	Technisches Verschlüsselungszertifikat für Verordnungen
ETSI	Europäisches Institut für Telekommunikationsnormen
HBA	Heilberufsausweis
KVNR	Krankenversichertennummer
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OSig	Organizational Signature

PIN	Personal Identification Number
PKI	Public Key Infrastructure
PRU	Produktionsreferenzumgebung
PTU	Produktionstestumgebung
PU	Produktionsumgebung
QES	Qualifizierte elektronische Signatur
SigG	Signaturgesetz
SigV	Signaturverordnung
SMC	Security Module Card
TSL	Trust-service Status List nach ETSI TS 102 231 V2.1.1 (2006-03)
TSP	Trust Service Provider
XML	Extensible Markup Language
ZW	Zufallswert

A5 - Referenzierte Dokumente

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik. Der mit dem vorliegenden Dokument korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen, die im Rahmen des Vorhabens zur Einführung der Gesundheitskarte veröffentlicht werden, wird pro Release in einer Dokumentenlandkarte definiert. Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Die jeweils gültige Version und das Freigabedatum der aufgeführten gematik-Dokumente entnehmen Sie bitte der von der gematik veröffentlichten Dokumentenlandkarte, wobei jeweils der aktuellste Releasestand maßgeblich ist, in dem die vorliegende Version aufgeführt wird. Zur Unterstützung der Zuordnung wird in der Dokumentenlandkarte im Kapitel 4 eine Übersicht über die Dokumentenversionen und deren Zuordnung zu den verschiedenen Releases bereitgestellt.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gem_Betr_BK_R2FT]	gematik: Einführung der Gesundheitskarte Betriebskonzept Leitstand Gesundheitstelematik <u>Gültig für</u> Release: 2 Teststufe: 03_Feldtest
[gemFK_VSDM]	gematik: Einführung der Gesundheitskarte Fachkonzept Versichertenstammdatenmanagement,
[gemFK_X.509]	gematik: Einführung der Gesundheitskarte - PKI für die X.509-Zertifikate Grobkonzept
[gemGesArch]	gematik: Einführung der Gesundheitskarte -

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	Gesamtarchitektur
[gemPKI_Nota]	gematik: Einführung der Gesundheitskarte - Festlegungen zu den Notationen von Schlüsseln und Zertifikaten kryptographischer Objekte in der TI
[gemSiKo]	gematik: Einführung der Gesundheitskarte – Übergreifendes Sicherheitskonzept der Telematikinfrastruktur
[gemSiKo#7.9.1]	Pseudonymisierung bei Pflichtanwendungen
[gemSiKo#AnhF5]	Lebenszyklus des eingesetzten Schlüsselmaterials
[gemSiKo#AnhG3.2]	Sicherheitsanforderungen Betrieb – Definieren und Schützen von Assets
[gemSpec_Krypt]	gematik: Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur,
[gemSpec_Krypt#5.1.1]	Kap 5.1.1 - X.509-Identitäten
[gemSpec_OID]	gematik: Einführung der Gesundheitskarte - Spezifikation: Festlegung von OIDs
[gemTSL_SP_CP]	gematik: Einführung der Gesundheitskarte - Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL zur Herausgabe von X.509-ENC/AUT/OSIG- Zertifikaten
[gemSpec_Ticket]	gematik: Einführung der Gesundheitskarte - Spezifikation TicketService
[gemSpec_TTD]	gematik: Einführung der Gesundheitskarte - Spezifikation TelematikTransport-Details
[gemVerw_Zert_TI]	gematik: Einführung der Gesundheitskarte - Verwendung von Zertifikaten in der Telematikinfrastruktur

weitere Referenzierungen:

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ALGCAT]	Bundesanzeiger Nr. 59, S. 4695-4696 (30. März 2005): Suitable Cryptographic Algorithms Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001, http://www.bundesnetzagentur.de/media/archive/1507.pdf (zuletzt geprüft am 13.12.2006)
[BSI-TR03116]	BSI TR-03116 (23.03.2007): Technische Richtlinie für die eCard-Projekte der Bundesregierung Version: 1.0 http://www.bsi.de/literat/tr/tr03116/BSI-TR-03116.pdf
[COMMON-PKI]	PKI- Interoperabilitätsspezifikation

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	Aktuelle Quelle http://www.common-pki.org/index.php?id=567 (zuletzt geprüft am 21.05.2008)
[ISIS-MTT]	PKI-Interoperabilitätsspezifikation Aktuelle Quelle http://www.isis-mtt.org/uploads/media/ISIS-MTT-Core-Specification-v1.1-03.pdf (zuletzt geprüft am 14.12.2006)
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://www.ietf.org/rfc/rfc2119.txt (zuletzt geprüft am 14.12.2006)