Einführung der Gesundheitskarte

Festlegungen zu den X.509 Zertifikaten der Versicherten

Version:	1.4.0
Stand:	26.11.2007
Status:	freigegeben

Dokumentinformationen

Änderungen zur Vorversion

Zwei bisher als SRQ veröffentlichte Ergänzungen / Korrekturen wurden eingearbeitet:

- SRQ 0502: Der Vorname in den Zertifikaten wurde (in Übereinstimmung mit [gemFK_VSDM] als optional gekennzeichnet.
- SRQ 0574: Festlegungen zur Übereinstimmung der Issuer Domains der unterschiedlichen Zertifikate wurden getroffen.

Weiterhin wurde die Reihenfolge von Vorsatzwort und Namenszusatz korrigiert.

Vorgaben zur Umsetzung bzgl. der Bildung der pseudonymisierten Versichertenidentität wurden aus dem Dokument entfernt, stattdessen wird auf die Vorgaben im Sicherheitskonzept [gemSiKo#7.9.1] verwiesen.

Hinsichtlich der kryptographischen Algorithmen wurde auch in den Zertifikatsprofilen anstelle konkreter Festlegungen der Verweis auf das jeweilige Unterkapitel des Dokuments „Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur“, Abschnitt 5.1.1 [gemSpec_Krypt#5.1.1] eingefügt.

Aufgrund der Anforderung der Gesamtarchitektur „Zertifikate zur Authentisierung von Akteuren in der Telematikinfrastruktur MÜSSEN eine Kennung für die durch das Zertifikat bestätigte Rolle enthalten“ (A_01209) wurde entschieden, die dazu notwendige Zertifikatskennzeichnung wie bei den Zertifikaten der SMC-B in die Extension „AdditionalInformation“ einzutragen.

Inhaltliche Änderungen gegenüber der letzten freigegebenen Version sind gelb markiert. Sofern ganze Kapitel eingefügt wurden, wurde zur besseren Lesbarkeit lediglich die Überschrift durch gelbe Markierung hervorgehoben.

Referenzierung

Die Referenzierung in weiteren Dokumenten der gematik erfolgt unter:

[gemX.509_eGK]	gematik (26.11.2007): Einführung der Gesundheitskarte - Festlegungen zu den X.509-Zertifikaten der Versicherten Version 1.4.0

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.1	29.05.05		Neuerstellung	gematik, AG3
0.2	01.08.05		Überarbeitung aufgrund der Kommentierungen , Einführung von Kommata (CSV) als Trenner zwischen	gematik, AG3

Versi-on	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
			Namensbestandteilen.	
0.3	24.08.05		Präzisierung des Common Name	gematik, AG3
0.4.1	07.12.05		Berücksichtigung von SHA-256 Einfügen des „SubjectKeyIdentifier“ bei C.CH.AUT	gematik, AG3
1.0.0	12.12.05		Qualitätssicherung, Freigabe und Veröffentlichung	gematik, AG3
1.0.1	07.06.06	7	Einfügen einer Erläuterung bei Nichtverwendung von Namensfeldern. Korrektur der OID des AuthorityKey-Identifier (2.5.29.35). Sicherstellung der ISIS-MTT Konformität. Überarbeitung SubjectDN, Profile	gematik, AG3
1.1.0	07.09.06		freigegeben	gematik
1.0.1	07.06.06		Korrektur der OID des AuthorityKeyIdentifier (2.5.29.35)	gematik, AG3
1.1a	14.06.06		Sicherstellung der ISIS-MTT Konformität	gematik, AG3
1.1.1	06.09.06		Überarbeitung SubjectDN, Profile	gematik, AG3
1.1.2	28.09.06		Zusammenführung mit den Zusatz-Zertifikaten AUTN und ENCV	gematik, AG3
1.2.0	02.10.06		freigegeben	gematik
1.2.1	14.05.07		Subject.CommonName des ENCV-Zertifikats erhält statt des Klarnamens ebenfall das Pseudonymzertifi-kat; Klarstellung zur Kodierung der Daten	gematik, AG3
1.3.0	05.06.07		freigegeben	gematik
1.3.1	19.10.07	4-10	Einarbeitung SRQs zu optionalem Vornamen, Vor-gaben zu Issuer Domain Korrektur Reihenfolge Vorsatzwort Namenszusatz Konkrete Verweise auf [gemSpec_Krypt]	gematik, AG8
1.3.2	09.11.07	Alle	Einarbeitung Review-Ergebnisse	gematik, AG8
1.3.3	15.11.07	2.5 8.1	Präzisierung bzgl. Abgrenzung zum SiKo Verweis auf SiKo bzgl. Bildung pseudonymisierter Versichertenidentität	gematik, AG8
1.4.0	26.11.07		freigegeben	gematik

Inhaltsverzeichnis

1 Zusammenfassung

Im Rahmen der Einführung der elektronischen Gesundheitskarte (eGK) wurde festgestellt, dass X.509-Zertifikate zu Authentisierung, Verschlüsselung und zur Erstellung elektronischer Signaturen (Willenserklärung) als Bestandteil der eGK Spezifikation standardisiert festgelegt werden müssen. Diese Zertifikate sind vor unberechtigter Nutzung durch die Erfordernis der PIN-Eingabe durch den Versicherten geschützt und werden im folgenden auch „Klar-Zertifikate“ genannt.

Es wurde der Bedarf für zwei zusätzliche Zertifikate erkannt, welche zu technischen Zwecken auch ohne PIN-Eingabe verwendet werden können. Aus Gründen des Datenschutzes, insbesondere zur Vermeidung der unnötigen Verwendung der „Klarnamen“ der Versicherten, wird bei den Zertifikaten (AUTN und ENCV) im „CommonName“ eine pseudonyme Identität des Versicherten gewählt. Diese beiden Zertifikatstypen werden im Folgenden auch „Zusatz-Zertifikate“ genannt.

Im Projekt [ISIS-MTT] wurde eine auf internationalen Standards beruhende Spezifikation für PKI-gestützte Anwendungen und ein Testbed. für den Nachweis der Interoperabilität von Produkten und Lösungen für elektronische Signaturen, Authentisierung und Verschlüsselung erarbeitet.

Alle erforderlichen Komponenten für E-Mail-, Daten- und XML-Signaturen bzw. Verschlüsselung und für Zertifikats- und Schlüsselmanagement, Sperrlisten, Verzeichnisdienste und PC-Schnittstellen sind dort detailliert beschrieben (siehe www.isis-mtt.org).

Diese Spezifikation dient als Vorlage für die hier erfolgten Festlegungen und sichert so die Interoperabilität und die Erstellung, Nutzung und Prüfung aller Zertifikate auch in heterogenen Public-Key-Infrastrukturen.

2 Einführung

2.1 Zielsetzung und Einordnung des Dokumentes

2.1.1 Zertifikatsprofil für Klar-Zertifikate

In diesem Dokument wird ein Zertifikatsprofil zur Festlegung der Versicherten-Identität im Umfeld von X.509-basierenden Public-Key-Infrastrukturen beschrieben. Hierbei ist eine detaillierte Festlegung für die Felder „Subject“ und „SubjectDirectoryAttribute“ getroffen worden, welche den Versicherten ein-(ein)-deutig bestimmt und welche den Anforderungen des Datenschutzes nach „Datensparsamkeit“ genügen soll. Daraus werden die entsprechenden Vorgaben für das Verschlüsselungszertifikat und das Authentisierungszertifikat abgeleitet. Zusätzlich ist das optionale qualifizierte Signatur-Zertifikat beschrieben, welches es den Versicherten erlaubt, rechtsverbindliche Willenserklärungen nach SigG/SigV zu leisten.

2.1.2 Zertifikatsprofil für Zusatz-Zertifikate

Des Weiteren wird ein Zertifikatsprofil zur Festlegung der pseudonymisierten Versicherten-Identität im Umfeld von X.509-basierenden Public-Key-Infrastrukturen beschrieben. Diese Zertifikate dienen z. B. dem Nachweis, dass bei einer Verordnung die eGK eines Versicherten vorgelegen hat. Hinsichtlich der Bildung des Pseudonyms werden aus Gründen der Datensparsamkeit personenbezogene Datenfelder verwendet, die bereits offensichtlich vorliegen. Auf den Einsatz eines komplexen Hintergrundsystems, welches einen Treuhänder zur Verwaltung der Zuordnung von pseudonymen zur Klaridentitäten erfordert, wird bewusst verzichtet. Ein solches Hintergrundsystem hätte wiederum umfangreiche Anforderungen an die datenschutzgerechte Verwaltung der Daten, da dort ein Zugriff auf alle Klaridentitäten aller Versicherten erforderlich wäre.

Bei Kenntnis des Nachnamens des Versicherten, seiner KVNR und einer vom Herausgeber (Kostenträger) verwendeten Zusatzinformation (herausgeberspezifischer Zufallswert) kann das Pseudonym auch durch berechtigte Dritte errechnet werden. Der Vergleich des so nachträglich errechneten Pseudonymwerts mit dem im Zertifikat enthaltenen signierten Pseudonym dient erforderlichenfalls dem Nachweis des Vorliegens der eGK zu einem bestimmten Vorgang, z. B. der Erstellung einer Verordnung. Dieses wird dann angewendet, wenn durch den Versicherten oder andere das Vorliegen der eGK bei einer bestimmten Transaktion abgestritten wird. Das Standard-Authentisierungszertifikat des Versicherten soll hierfür nicht verwendet werden, da zur Freischaltung eine Eingabe der PIN durch den Versicherten erforderlich wäre.

Weiterhin wird ein ENCV Zertifikat definiert, welches dazu dient, eine zu speichernde Verordnung patientenbezogen zu verschlüsseln. Der private ENCV-Schlüssel zur Entschlüsselung kann nur nach vorheriger C2C Authentisierung mit entsprechendem Profil benutzt werden, ohne dass hierfür eine PIN-Eingabe durch den Versicherten erforderlich ist.

Auf Grundlage der Anforderung: „Der Inhalt des ENCV-Zertifikats, (nach bisheriger Festlegung der Klarname des Versicherten), soll außerhalb der eGK nicht mit dem Pseudonym im AUTN-Zertifikat verknüpft werden können“, wurde entschieden, dass auch im ENCV-Zertifikat statt des Klarnamens das Pseudonym analog zum AUTN-Zertifikat ver-

wendet wird. Dies ist bei Service-Tickets relevant, da zur Authentisierung das AUTN-Zertifikat verwendet wird, d.h. das Service-Ticket enthält sowohl das AUTN- wie auch das ENCV-Zertifikat und würde damit die o.g. Anforderung verletzen.

2.2 Zielgruppe

Das Dokument wendet sich an die technischen Spezialisten der Betreiber von Kartenmanagementsystemen und die Administratoren der Zertifizierungsdiensteanbieter.

2.3 Geltungsbereich

Die getroffenen Festlegungen zu den Klar- und pseudonymisierten X.509-Identitäten sind für alle Betreiber von Kartenmanagementsystemen und Zertifizierungsdiensteanbieter, die innerhalb der Gesundheitstelematik tätig sind, verbindlich.

2.4 Arbeitsgrundlagen

Das Dokument präzisiert die allgemeinen Aussagen bzgl. der X.509-Zertifikate aus dem PKI-Grobkonzept [gemFK_X.509] hinsichtlich der Zertifikate des Versicherten in der eGK. Dabei wird auf die Struktur der Daten des Versicherten aus dem Fachkonzept Versichertenstammdatenmanagement [gemFK_VSDM] zurückgegriffen.

2.5 Abgrenzung des Dokumentes

Die langfristige Bestimmung der Hash-Algorithmen, der Schlüssellängen und der Signaturalgorithmen ist nicht Gegenstand der Betrachtung, hier werden jeweils aktuell die Empfehlungen der international relevanten Gremien und die Anforderungen von SigG/SigV [ALGCAT] berücksichtigt. Die Festlegungen zum „Aktivieren qualifizierter Zertifikate“ [gemQES] und die Vorgaben für die Vereinheitlichung der Public-Key-Infrastrukturen, insbesondere hinsichtlich der „Policy-Aspekte“ [gemTSL_SP_CP], werden in gesonderten Dokumenten getroffen.

Im vorliegenden Dokument werden ebenfalls keine Aussagen zum Management der kryptographischen Schlüssel getroffen. Diesbezüglich wird auf das übergreifende Sicherheitskonzept der gematik [gemSiKo] verwiesen, insbesondere auf Abschnitt F5 [gemSiKo#AnhF5].

Die für die Verwendung in der TI zulässigen Algorithmen, Schlüssellängen und maximalen Gültigkeitsdauern von Schlüsseln und Zertifikaten werden in [gemSiKo] sowie entsprechend der Technischen Richtlinie für eCard-Projekte der Bundesregierung [BSI-TR03116] normativ vorgegeben. Die freie Auswahl aus den hier zugelassenen Algorithmen durch die Hersteller könnte zu Interoperabilitätsproblemen führen, während die Implementierung aller zulässigen Algorithmen erheblichen Aufwand verursacht. Dieser Konflikt wird durch [gemSpec_Krypt] adressiert. Ziel des Dokumentes „Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur“ [gemSpec_Krypt] ist es, das Spektrum der zulässigen kryptographischen Algorithmen, sofern sie betreiberübergreifend verwendet werden,

einzuschränken, um so mit einer minimalen Anzahl von Algorithmen kryptographische Interoperabilität herzustellen.

Deshalb wird als Basis zur Referenzierung der kryptographischen Algorithmen auf o. g. Dokument, Abschnitt 5.1.1 [gemSpec_Krypt#5.1.1] verwiesen.

2.6 Methodik

2.6.1 Verwendung von Schüsselworten

Für die genauere Unterscheidung zwischen normativen und informativen Inhalten werden die dem RFC 2119 [RFC2119] entsprechenden in Großbuchstaben geschriebenen, deutschen Schlüsselworte verwendet:

- **MUSS** bedeutet, dass es sich um eine absolutgültige und normative Festlegung bzw. Anforderung handelt.
- **DARF NICHT** bezeichnet den absolutgültigen und normativen Ausschluss einer Eigenschaft.
- **SOLL** beschreibt eine dringende Empfehlung. Abweichungen zu diesen Festlegungen sind in begründeten Fällen möglich. Wird die Anforderung nicht umgesetzt, müssen die Folgen analysiert und abgewogen werden.
- **SOLL NICHT** kennzeichnet die dringende Empfehlung, eine Eigenschaft auszuschließen. Abweichungen sind in begründeten Fällen möglich. Wird die Anforderung nicht umgesetzt, müssen die Folgen analysiert und abgewogen werden.
- **KANN** bedeutet, dass die Eigenschaften fakultativ oder optional sind. Diese Festlegungen haben keinen Normierungs- und keinen allgemeingültigen Empfehlungscharakter.

2.6.2 Hinweis auf offene Punkte

Offene Punkte, die bis zur nächsten Dokumentversion bearbeitet werden, sind mit den folgenden Konventionen gekennzeichnet:

Beschreibung der Aufgabe

3 Anforderungen

Die Anforderungen müssen noch mit dem Anforderungsmanagement abgestimmt werden. Das Kapitel wird in einer späteren Version des Dokumentes entsprechend überarbeitet.

Die Notwendigkeit für normative Vorgaben bzgl. der Zertifikatsprofile der Versichertenzertifikate ergibt sich aus mehreren Anforderungen zur Sicherstellung der Interoperabilität der PKI durch die gematik.

Die folgende Tabelle enthält die entsprechenden Eingangsanforderungen, wie sie aktuell bereits identifiziert werden können.

Tabelle 1: Bereits erfasste Eingangsanforderungen

Quelle	Anforderungsnummer	Anforderungslevel	Beschreibung
[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
[gemSpec_Ticket]	A_01584	MUSS	**Eindeutigkeit des Versichertenpseudonyms** Das im AUT.N und ENC.V Zertifikat des Versicherten gespeicherte Pseudonym MUSS innerhalb der Herausgeber Domäne (IssuerDomain) des Zertifikatherausgebers eindeutig sein und somit als eindeutiges Ordnungskriterium für die Ablage von medizinischen Objekten und die Erteilung von Berechtigungen verwendet werden können.
[gemSpec_TTD]	A_01591	MUSS	**Meldung von neuen Rollen OIDs an die gematik** Kartenherausgeber MÜSSEN Rollen-OIDs, die in ihren Zertifikaten Verwendung finden, an die gematik melden.
[gemSpec_TTD]	A_01592	MUSS	**Policy zur Zuordnung von Rollen-OIDs zu Personen** Kartenherausgeber MÜSSEN für jede Rollen-OID eindeutig spezifizieren, welche Personen und somit fachlichen Akteure Zertifikate mit dieser Rolle erhalten und die Einhaltung dieser Regeln als Basis für die rollenbasierte Autorisierung zusichern.

Quelle	Anforderungsnummer	Anforderungslevel	Beschreibung
[gemSpec_TTD]	A_01593	MUSS	**Zuordnung der Rollen OIDs aus X.509 Zertifikaten auf gesetztliche Rollen** Die Betriebsorganisation der gematik MUSS jede durch einen Kartenherausgeber gemeldeten Rollen-OID eindeutig auf einen fachlichen Akteur abbilden und diese Abbildungstabellen den Betreibern von Diensten zur Verfügung stellen.
[gemSpec_TTD]	A_01594	MUSS	**Spezifikation der Zugrifsrechte gesetzlicher Rollen auf Fachdienstoperationen** Alle Facharchitekturen MÜSSEN für jede Kombination aus fachlichem Akteur und Fachdienstoperation spezifizieren, ob die gesetzliche Rolle zur Durchführung dieser Operation berechtigt ist oder nicht.

4 Sicherheitsanforderungen hinsichtlich der Zertifikatsdefinitionen

Auf Basis eines genauen X.509-Zertifikatsprofils mit eindeutiger und datenschutzkonformer Beschreibung der Versichertenidentität kann ein verlässlicher Zugriff auf die Dienste zur Bereitstellung der relevanten Daten der Versicherten realisiert werden.

Um eine Bildung von Profilen zu vermeiden wird bei den beiden pseudonymisierten Zertifikaten die KV-Nummer zusammen mit weiteren Feldern „gehasht“. Hierbei sind vom Herausgeber folgende Sicherheitsanforderungen zwingend zu erfüllen:

Es muss eine sichere Erzeugung eines vertraulichen herausgeberspezifischen Zufallswerts von mindestens 64 Bit erfolgen.

Die sichere Weitergabe und Speicherung des vertraulichen herausgeberspezifischen Zufallswerts ist durch die Umsetzung einer einheitlichen Sicherheitspolicy zu gewährleisten.

Da der herausgeberspezifische Zufallswert für alle Versicherten eines Herausgebers identisch ist, muss dieser periodisch, z. B. jährlich gewechselt werden.

Tabelle 2: Zugriffsmatrix der X.509 Zertifikate der eGK

	Authentisierungszertifikat (C.CH.AUT)	Verschlüsselungszertifikat (C.CH.ENC)	Optionales Qualifiziertes Signaturzertifikat (C.CH.QES)	Technisches Authentisierungszertifikat (C.CH.AUTN)	Technisches Verschlüsselungszertifikat (C.CH.ENCV)
Typ der Versicherten-identität	Klar	Klar	Klar	Pseudonym	Pseudonym
Verwendbarkeit des „Private Key“	PIN	PIN	PIN (-SigG)	CVC	CVC

5 Fachlicher Teil

5.1 Zielbeschreibung hinsichtlich der Zertifikatsdefinitionen

Auf Basis eines genauen X.509 Zertifikatsprofils mit eindeutiger und datenschutzkonformer Beschreibung der Versichertenidentität kann ein verlässlicher Zugriff auf die Dienste zur Bereitstellung der relevanten Daten der Versicherten realisiert werden. Dieses erfolgt ereignisbezogen zum Zwecke der Client-Server-basierten Authentifizierung der beteiligten Personen, zur Nutzung einer „starken“ Verschlüsselung patientenbezogener Daten oder zu Willenserklärungen in elektronischer Form.

5.2 Attribute im SubjectDN

Zur Kodierung der Attribute sind die Hinweise in Abschnitt 9.2 zu beachten.

5.2.1 SubjectDN bei allen Zertifikaten außer AUTN und ENCV

Attribut	OID	Kodierung	max. String-Länge
commonName	{id-at 3}	UTF8	64
title	{id-at 12}	UTF8	64
surname	{id-at 4}	UTF8	64
givenName	{id-at 42}	UTF8	64
organizationalUnitName	{id-at 11}	UTF8	64
organizationName	{id-at 10}	UTF8	64
countryName	{id-at 6}	PrintableString	2 (ISO 3166 Code)

5.2.2 SubjectDN bei AUTN- und ENCV Zertifikaten

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

5.3 Festlegungen zur Definition der Versichertenidentität

Die Daten des Versicherten werden in [gemFK_VSDM] beschrieben. Folgende Datenfelder sind demnach Grundlage und bilden die Namensidentität des Versicherten in den Zertifikaten.

(a) Vorname des Versicherten

(b) Familienname des Versicherten

(c) Titel des Versicherten

(d) Namenszusatz

(e) Vorsatzwort

Diese Daten werden in den folgenden Feldern des `SubjectDN` des Versicherten im Zertifikat abgebildet:

- commonName
- title
- surname
- givenName

5.4 Aufbau der einzelnen Felder im SubjectDN

Die beiden Namenszeilen, die auf die Karte gedruckt werden, bestehen aus jeweils 28 Zeichen, die beide zusammen mit einem zusätzlichen Trennzeichen den `commonName` des Versicherten bilden. Die Begrenzung auf 64 Zeichen wird erfüllt.

Für die Bildung der anderen Felder wird im Folgenden der Name des Versicherten in der natürlichen Schreibweise und Reihenfolge betrachtet.

Titel Vorname Namenszusatz Vorsatzwort Familienname

Der `surname` wird aus dem folgenden Attribut gebildet:

Familienname.

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 folgende Regeln:

- 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 zusätzlich:

- 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 folgende Regeln:

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

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

Der `title` wird aus folgenden Attributen gebildet:

Titel

Hier ist nicht mit Kürzungen zu rechnen.

5.4.1 Beispielsatz der Feldinhalte

Name: Dr.-Ing. Peter-Wilhelm Markgraf von Meckelburg-Vorpommeln

Erste Namenszeile auf der Karte:

Peter-W. Markgraf von

Zweite Namenszeile auf der Karte:

Meckelburg-Vorpommeln

Bei durchaus akzeptabler Titelkürzung wäre auch eventuell

Dr. Peter-W. Markgraf von

in der ersten Zeile denkbar.

Im Zertifikat wären folgende Attribute zu verwenden:

Feld	Inhalt
title	**Dr.-Ing.** oder bei gekürztem Titel nur **Dr.**
givenName	**Peter-Wilhelm Markgraf von**
surname	**Meckelburg-Vorpommeln**
commonName	**Dr. Peter-W. Markgraf von Meckelburg-Vorpommeln**

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	

surname

Datenfeld: Familienname des Versicherten

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

title

Datenfeld: Titel des Versicherten

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

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	

5.5 Festlegungen zur Issuer Domain (Zertifikatsherausgeber)

Jedes auf einer eGK gespeicherte Zertifikat enthält eine Herausgeberkennung, die Issuer Domain. Folgende Anforderung (A_01583) MUSS dabei erfüllt werden:

Die Issuer Domain des AUT.N Zertifikates MUSS mindestens mit der Issuer Domain des ENC.V Zertifikates der gleichen eGK Identisch sein. Ebenso MUSS mindestens die Issuer Domain des AUT Zertifikates mit der Issuer Domain des ENC Zertifikates übereinstimmen um so eine Korrelierbarkeit der jeweiligen Zertifikate zu ermöglichen. Alle 4 Zertifikatsprofile KÖNNEN aus einer Issuer Domain stammen.

5.6 Aufbau der Krankenversichertennummer

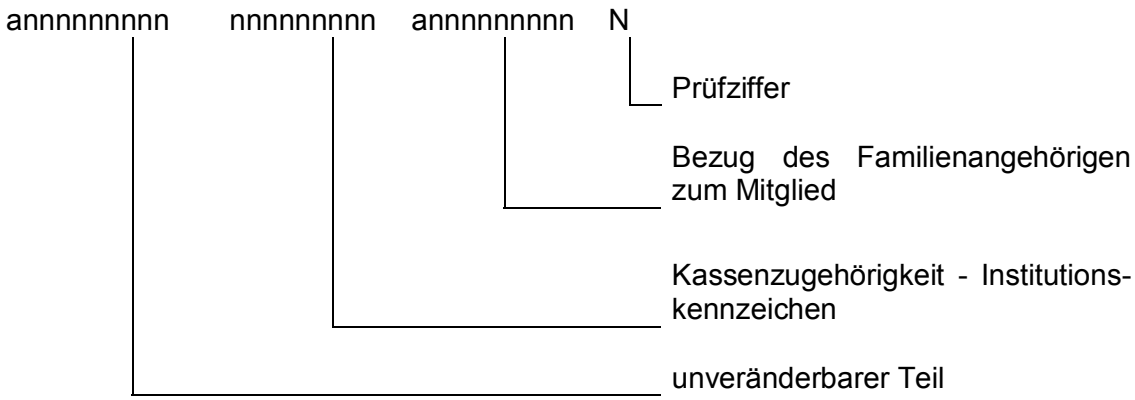

Abbildung 1: Aufbau der Krankenversichertennummer

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.

Datenfeld: unveränderbarer Teil

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

Datenfeld: ID des Kostenträgers

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

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

5.7 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

Zertifikat	Ort	Bezeichnung	Format
AUT	Additional Information	C.CH.AUT	OID
ENC		C.CH.ENC	OID
QES		C.CH.QES	OID
AUTN		C.CH.AUTN	OID
ENCV		C.CH.ENCV	OID

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<=serialNumber<= 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
givenName	Vorname des Inhabers
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] 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
CertificatePolicies (2.5.29.32)	nicht kritisch URL und OID mit der Zertifikatsrichtlinie
CRLDistributionPoints (2.5.29.31)	nicht kritisch Verteilungspunkt für Sperrlisten (nach ISIS-MTT V1.1)
AuthorityInfoAccess (1.3.6.1.5.5.7.1.1)	nicht kritisch Verteilungspunkt für Statusinformationen des Zertifikats (OCSP) (nach ISIS-MTT V1.1)
AuthorityKeyIdentifier (2.5.29.35)	nicht kritisch ID für den öffentlichen Schlüssel der ausstellenden CA
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<=serialNumber<= 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
givenName	Vorname des Inhabers
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] 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'
CertificatePolicies (2.5.29.32)	nicht kritisch URL und OID mit der Zertifikatsrichtlinie
CRLDistributionPoints (2.5.29.31)	nicht kritisch Verteilungspunkt für Sperrlisten (nach ISIS-MTT V1.1)
AuthorityInfoAccess (1.3.6.1.5.5.7.1.1)	nicht kritisch Verteilungspunkt für Statusinformationen des Zertifikats (OCSP) (nach ISIS-MTT V1.1)
AuthorityKeyIdentifier (2.5.29.35)	nicht kritisch ID für den öffentlichen Schlüssel der ausstellenden CA
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]
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<=serialNumber<= 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
	givenName		Vorname des Inhabers
	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'
	Certificate Policies (2.5.29.32)		nicht kritisch URL und OID mit der Zertifikatsrichtlinie
	CRLDistributionPoints (2.5.29.31)		nicht kritisch Verteilungspunkt für Sperrlisten (nach ISIS-MTT V1.1)
	AuthorityInfoAccess (1.3.6.1.5.5.7.1.1)		nicht kritisch Verteilungspunkt für Statusinformationen des Zertifikats (OCSP) (nach ISIS-MTT 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
	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 Festlegung der pseudonymisierten Versichertenidentität

9.1 Bildung der pseudonymisierten Versichertenidentität

Vorgaben sowie Beispiele zur Umsetzung bzgl. der Bildung der pseudonymisierten Versichertenidentität sind in [gemSiKo#7.9.1] zu finden.

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

9.2 Kodierung der pseudonymisierten Versichertenidentität

Alle Daten in der Telematikinfrastruktur, die den Primärsystemen bereitgestellt werden, sind ISO 8859-15 kodiert. Daraus leitet sich dann ab, dass die Daten, die zur Bildung des Pseudonyms herangezogen werden (s. [gemSiKo#7.9.1]), ISO 8859-15 kodiert sind. Das Pseudonym ist dann natürlich auch ISO 8859-15 kodiert.

Des Weiteren unterscheidet sich die Kodierung der Fachdaten in den X.509 Zertifikaten des Versicherten. Im SubjectDN liegen die Daten UTF-8 kodiert vor. Dies ist im Standard festgelegt. Daraus ergibt sich, dass alle Fachdaten in den Zertifikaten (und auch nur dort) von ISO nach UTF-8 transformiert werden müssen.

Die folgende Grafik verdeutlicht diesen Umgang, der analog auch für die Kodierung bei den Klarzertifikaten gilt:

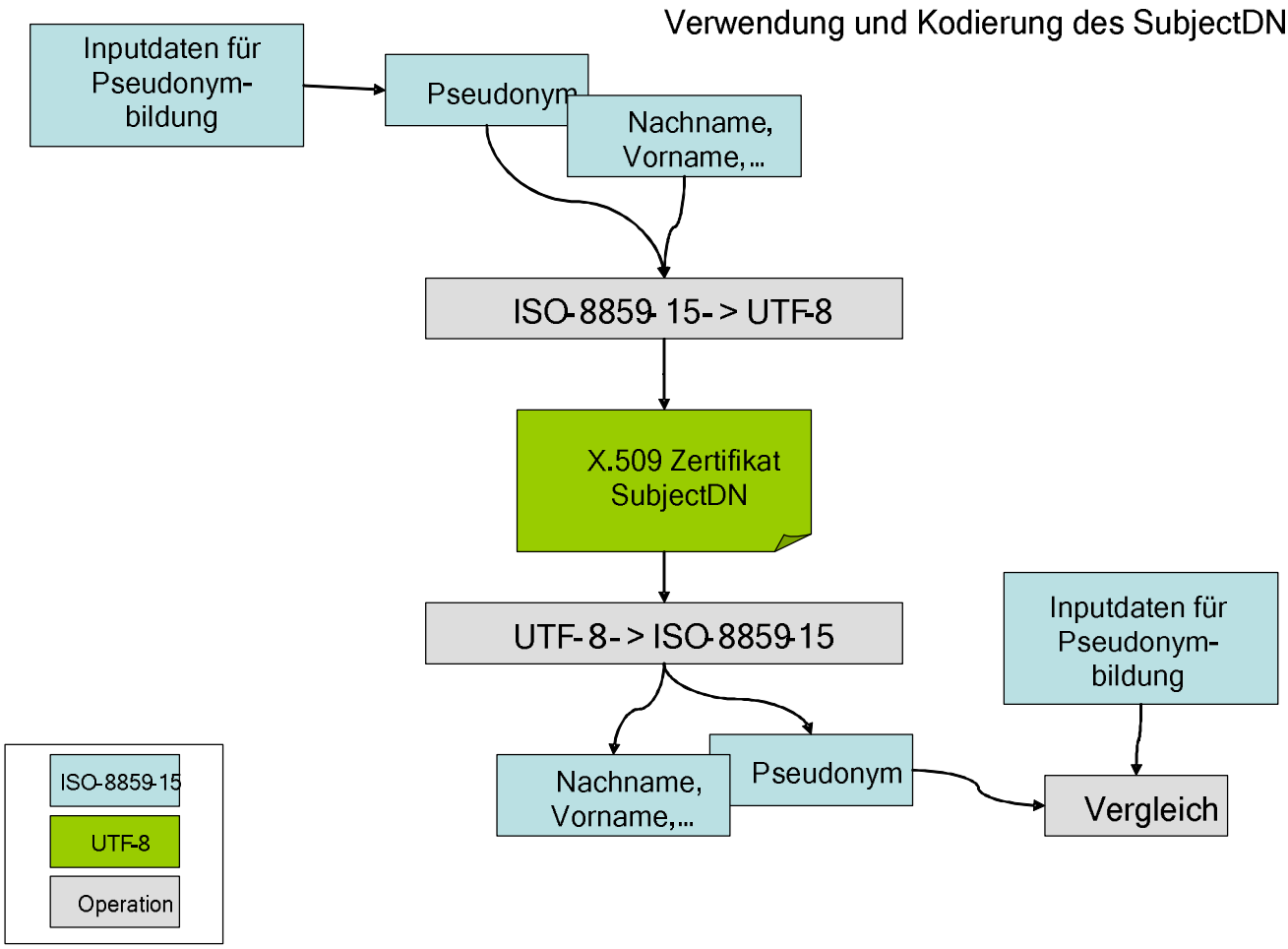

Abbildung 2: Verwendung und Kodierung des SubjectDN

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<=serialNumber<= 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
		CertificatePolicies (2.5.29.32)	nicht kritisch URL und OID mit der Zertifikatsrichtlinie
		CRLDistributionPoints (2.5.29.31)	nicht kritisch Verteilungspunkt für Sperrlisten nach ISIS-MTT V1.1
		AuthorityInfoAccess (1.3.6.1.5.5.7.1.1)	nicht kritisch Verteilungspunkt für Statusinformationen des Zertifikats (OCSP) (nach ISIS-MTT V1.1)
		AuthorityKeyIdentifier (2.5.29.35)	nicht kritisch ID für den öffentlichen Schlüssel der ausstellenden CA
		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<=serialNumber<= 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
commonName organizationalUnitName organizationName countryName	
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 ‚keyEncipherment' und ‚dataEncipherment'
CertificatePolicies (2.5.29.32)	nicht kritisch URL und OID mit der Zertifikatsrichtlinie
CRLDistributionPoints (2.5.29.31)	nicht kritisch Verteilungspunkt für Sperrlisten (nach ISIS-MTT V1.1)
AuthorityInfoAccess (1.3.6.1.5.5.7.1.1)	nicht kritisch Verteilungspunkt für Statusinformationen des Zertifikats (OCSP) (nach ISIS-MTT V1.1)
AuthorityKeyIdentifier (2.5.29.35)	nicht kritisch ID für den öffentlichen Schlüssel der ausstellenden CA
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]
signature	Wert der Signatur

Anhang

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
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
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

A2 - Glossar

Begriff	Englisch, (Abk.)	Definition (Synonym)
Klar-Zertifikat		Zusammenfassender Begriff für die eGK-Zertifikate mit dem „Klar-Namen“, d.h. nicht pseudonymisiert, im Subject (AUT, ENC, QES).
Zusatz-Zertifikat		Zusammenfassender Begriff für die eGK-Zertifikate mit pseudonymisierter Identität im Subject (AUTN und ENCV).

Das übergreifende Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A3 - Abbildungsverzeichnis

A4 - Tabellenverzeichnis

A5 - Referenzierte Dokumente

[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
[gemFK_VSDM]	gematik (20.12.2007): Einführung der Gesundheitskarte Fachkonzept Versichertenstammdatenmanagement, Version 2.6.0
[gemFK_X.509]	gematik (04.05.2007): Einführung der Gesundheitskarte -

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	PKI für die X.509-Zertifikate Grobkonzept Version 1.2.0, www.gematik.de
[gemQES]	gematik (15.12.2005): Einführung der Gesundheitskarte - Aktivierung der qualifizierten elektronischen Signatur Version 1.0.0, www.gematik.de
[gemSiKo]	gematik (10.12.2007): Einführung der Gesundheitskarte – Übergreifendes Sicherheitskonzept der Telematikinfrastruktur Version 2.1.0
[gemSiKo#7.9.1]	Pseudonymisierung bei Pflichtanwendungen
[gemSiKo#AnhF5]	Lebenszyklus des eingesetzten Schlüsselmaterials
[gemSpec_Krypt]	gematik (18.12.2007): Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 1.1.0
[gemSpec_Krypt# 5.1.1]	Kap 5.1.1 - X.509-Identitäten
[gemTSL_SP_CP]	gematik (29.11.2007): Einführung der Gesundheitskarte - Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL zur Herausgabe von X.509-ENC/AUT/OSIG-Zertifikaten Version 1.2.0, www.gematik.de
[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)