

## Änderung in gemSpec\_PKI

### 1.1.1.1 Kapitel 4.8.3.1 serialNumber

(...)

#### GS-A\_4726-01 - Verwendung von serialNumber zur Schaffung eindeutiger SubjectDNs

TSP-X.509 nonQES MÜSSEN bei Verwendung des Attributs serialNumber in X.509-Zertifikaten für Zentrale Dienste und Fachanwendungsspezifische Dienste den Inhalt entsprechend dem folgenden Format aufbauen: Instanz (fünfstellige Dezimalzahl) + "-" + Unterscheidung Zertifikat (alphanumerischer Wert erlaubt sind Zeichen aus {a,...,z, A,...,Z, 0,...,9} ohne Umlaute und Sonderzeichen).

[<=]

(...)

Tabelle 13: Tab\_PKI\_223-01 Aufbau der Telematik-ID

Bestandteil	Inhalt	Länge	Format
Präfix	Nummernkreis der jeweiligen Organisation (Unterscheidung der Sektoren)	nicht festgelegt 1 oder 2, siehe GS-A_4710	N
Separator	Trennzeichen zwischen Präfix und Fortsatz: „-“	N	
Fortsatz	eindeutige Nummer, sektorspezifisch (z. B. Betriebsstätten-Nr. o. ä.)	nicht festgelegt-Begrenzung durch GS-A_4587	AN

Anmerkung zur Darstellung des Formats: N=numerisch, AN=alphanumerisch

### 1.1.1.2 Kapitel 4.8.3.2 Admission

(...)

#### GS-A\_4717-02 - TI-spezifische Vorgabe zur Nutzung der Extension Admission

TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN bei Verwendung der Extension Admission {1 3 36 8 3 3} die Struktur in X.509-Zertifikaten entsprechend Tab\_PKI\_226-\* erstellen

Tabelle 1: Tab\_PKI\_226-\* Struktur Admission

#	ASN.1 definition	TI-spezifische Vorgaben
1	<pre>id-isismtt-at-admission OBJECT IDENTIFIER ::= {1 3 36 8 3 3}</pre>	Identifizierung des Objekts über die OID

2	<b>id-isismtt-at-namingAuthorities</b> OBJECT IDENTIFIER ::= {1 3 36 8 3 11}	Identifizierung des Objekts über die OID
3	<b>AdmissionSyntax</b> ::= SEQUENCE {	
4	admissionAuthority GeneralName OPTIONAL,	Angabe (optional) der admissionAuthority auf der obersten Ebene der Extension in Form eines Distinguished Name (directoryName). In den jeweiligen Zertifikatsprofilen und -ausprägungen wird dieser Distinguished Name in Textform gemäß [RFC4514] dargestellt.
5	contentsOfAdmissions SEQUENCE OF Admissions }	Diese Sequenz MUSS genau ein Element vom Typ Admissions enthalten.
6	<b>Admissions</b> ::= SEQUENCE {	
7	admissionAuthority [0] EXPLICIT GeneralName OPTIONAL,	
8	namingAuthority [1] EXPLICIT NamingAuthority OPTIONAL,	
9	professionInfos SEQUENCE OF ProfessionInfo }	Diese Sequenz MUSS ein Element vom Typ ProfessionInfo enthalten.
-		
14	<b>ProfessionInfo</b> ::= SEQUENCE {	
15	namingAuthority [0] EXPLICIT NamingAuthority OPTIONAL,	
16	professionItems SEQUENCE OF DirectoryString (SIZE(1..128)),	professionItems enthält ein Element von Typ DirectoryString (Hinweis: Neben „PrintableString“ werden auch andere Formate zugelassen, etwa UTF8String). Für DirectoryString MUSS die Kodierung UTF8String verwendet werden.
17	professionOIDs SEQUENCE OF OBJECT IDENTIFIER OPTIONAL,	Dieses Element MUSS eine OID enthalten.
18	registrationNumber PrintableString(SIZE(1..128)) OPTIONAL,	Wenn dieses optionale Feld enthalten ist, enthält es die Telematik-ID. In QES-HBA-Zertifikaten für Ärzte wird das Feld registrationNumber nicht gesetzt.

19	<pre> addProfessionInfo   OCTET STRING OPTIONAL } </pre>	
----	--	--

[&lt;=]

## 1.2 Kapitel 11.1 Abkürzungen

Kürzel	Erläuterung
AES	Advanced Encryption Standard
AK	Anwendungskonnektor
AN	alphanumerisch
...	...
ZOD	Zahnärzte Online Deutschland

## Änderung in gemKPT\_PKI\_TIP

## 1.3 Kapitel 8.1 Abkürzungen

Kürzel	Erläuterung
AES	Advanced Encryption Standard
AK	Anwendungskonnektor
AN	alphanumerisch
...	...
ZOD	Zahnärzte Online Deutschland

## Änderungen in gemProdT\_...\_PTVx.y.z-n

*Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT...]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.*

**Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4726-01	Verwendung von serialNumber zur Schaffung eindeutiger SubjectDNs	gemProdT_X509_TSP_nonQES_Komp
GS-A_4717-02	TI-spezifische Vorgabe zur Nutzung der Extension Admission	gemProdT_X509_TSP_nonQES_Komp gemProdT_X509_TSP_nonQES_HBA gemProdT_X509_TSP_nonQES_eGK gemProdT_X509_TSP_QES gemProdT_X509_TSP_nonQES_SMC-B