SRQ - Specification Related Question

SRQ-ID: 0913

Betrifft (wird vom FLS (optional vom Erfasser) ausgefüllt):

Themenkreis	PKI und Zertifikate
Schlagwort	Anpassungen an die Codierung des Zertifikattyps
zu Dokument / Datei	[gemTSL_SP_CP]
Version	1.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	5.1.4.1,5.1.5 und 5.1.6

Stichwort: Anpassungen an die Codierung des Zertifikattyps

Frage:

Welche Änderungen der Dokumentversion 1.2.0 ergeben sich durch an die Codierung des Zertifikattyps?

Betrifft (wird vom PB ausgefüllt):

Gültig ab Release	0.5.2	Verbindlichkeit	ja
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
Anmerkungen:			
Status	☐ erfasst ☐ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☐ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Im Zuge der Anpassung des Release 0.5.2 an das R 2.3.4 wurden die folgenden Änderungen im [gemPKI_SP_CP] gegenüber der Dokumentversion 1.2.0 vorgenommen. Die Änderungen sind verbindlich und wurden in der Dokumentversion 1.3.0 umgesetzt. Die vorliegende SRQ beschreibt die funktionalen Änderungen.

Die OID für diese Polycy wurde nun im Zuge der OID-Vereinheitlichung mit dem DIMDI festgelegt und im Dokument entsprechend angepasst.

Einführung der Gesundheitskarte

- Certificate Policy -

Gemeinsame Zertifizierungs-Richtlinie für Teilnehmer der gematik-TSL zur Herausgabe von X.509-ENC/AUT/OSIG-Zertifikaten

Version:	n.m.p
Revision:	
Stand:	TT.MM.JJJJ
Status:	in Bearbeitung
OID:	1.2.276.0.76.4.61

Referenzierung

Die Referenzierung in weiteren Dokumenten der gematik erfolgt unter:

[gemTSL_SP_CP]	gematik: Einführung der Gesundheitskarte - Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL zur Herausgabe von X.509-ENC/AUTH/OSIG-Zertifikaten

Diese spezifische Version wird unter dem Object Identifier (OID) definiert:

1.2.276.0.76.4.61

Soll die OID in anderen Dokumenten versionsunabhängig referenziert werden, so ist die Kennung

[gemSpec_OID#oid_policy_gem_cp]

zu verwenden. Die Ermittlung der relevanten OID ist dann über das Dokument [gemSpec_OID] möglich.

Die Hinweise zur Kodierung des Zertifikatstyps wurden aufgrund der Änderungen angepasst. (Abschnitt 5.1.4).

5.1.4 Notwendigkeit für aussagefähige und eindeutige Namen

Bei der Vergabe von Namen (Nutzer- oder PKI-Zertifikate) **muss** sichergestellt sein, dass der gewählte distinguishedName des Zertifikatsnehmers innerhalb des ausstellenden TSP eindeutig ist. Durch die Verwendung der Namensform in Kapitel 5.1.2 wird die Eindeutigkeit sichergestellt. Der ausstellende TSP **MUSS** sicherstellen, dass die Daten in dieser Form aufbereitet werden. Die Integrität und Vollständigkeit der Daten liegt in der Hoheit der jeweiligen Registrierungsstellen (bei Versicherten ist dies der Kostenträger).

Personen- bzw. organisationsbezogene Zertifikate **MÜSSEN** eindeutig als solche kenntlich sein (Einhaltung der entsprechenden Zertifikatsprofile).

Maschinen-, Rollen- oder pseudonymisierte (nicht personenbezogene) Zertifikate **MÜSSEN**, um Verwechslungsfreiheit zu garantieren, ebenfalls als solche kenntlich sein.

Zur Unterscheidung von Zertifikaten wird das jeweilige Kennzeichen in Form einer OID in die Extension ~~additionalInformation~~ certificatePolicies gespeichert z. B. C.CH.AUT (C=Certificate, CH=Cardholder, AUT=Authentication).

5.1.6 Regeln für die Interpretation verschiedener Namensformen

Maschinen-, Rollen- oder pseudonymisierte (nicht personenbezogene) Zertifikate **MÜSSEN**, um Verwechslungsfreiheit zu garantieren, als solche kenntlich sein. Zur Unterscheidung von Zertifikaten wird das jeweilige Kennzeichen in die Extension ~~additionalInformation~~ certificatePolicies gespeichert. Details dazu sind in den jeweiligen Zertifikatsspezifikationen zur SMC-B und eGK zu finden [gemX.509_eGK], [gemX.509_SMCB].

Hinsichtlich der Pseudonymbildung die den Versichertenzertifikaten wird ncht mehr auf dem [gemSiKo] verwiesen, da die konkreten Festlegungen nun wieder im Dokument [gemX.509_eGK] getroffen werden (Abschnitt 5.1.5).

5.1.5 Anonymität oder Pseudonyme von Zertifikatsnehmern
Pseudonyme-Zertifikate **MÜSSEN** pro ~~TSPs~~ Kartenherausgeber eindeutig sein. Vorgaben sowie Beispiele zur Umsetzung bzgl. der Bildung der pseudonymisierten Versichertenidentität sind in ~~[gemSiKo#7.9.1]~~ [gemX.509_eGK] zu finden.