Einführung der Gesundheitskarte

Errata zu Release 1.5.4 Online-Rollout (Stufe 1) Erprobung und Produktivbetrieb

führt zu

Release 1.5.5

Version:	1.0.0
Stand:	06.12.2016
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemErrata_1.5.5]

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_5552	gemSpec_PKI	Tab_PKI_243 Tab_PKI_228	Der Standard HTTPS schreibt vor, dass der Host-Name eines Servers durch den Client geprüft werden soll. Dieser Host-Name soll dabei im Format 'dNSName' in der Zertifikats-Erweiterung SubjectAltName (SAN) eingetragen sein. Siehe RFC2818, Kap. 3.1 für HTTP über TLS. Es ist vorgesehen das Zertifikat C.AK.AUT als Authentisierungszertifikat des Konnektor für HTTPS-Verbindungen zu nutzen. Daher wird zukünftig der definierte Host-Name des Konnektors in dieses Zertifikat eingetragen. Das Zertifikatsprofil f. C.AK.AUT muss deshalb um den entsprechenden 'dNSName'-Eintrag im SAN ergänzt werden. Auch die Vorgaben für erlaubte Werte in der SAN-Erweiterung in Kap. 4.8.3.5 "SubjectAltNames" müssen um 'dNSName' erweitert werden.	Geänderte Anforderung: GS-A_4610 Umsetzung Zertifikatsprofil C.AK.AUT Tab_PKI_243 ALT […] SubjectAltNames {2 5 29 17}; bei überlangem organizationName: Langname des Konnektor-Herstellers (Kar.: 0-1); […] Tab_PKI_243 NEU: […] SubjectAltNames {2 5 29 17}; dNSName = „konnektor.konlan“ (Kar.: 1); bei überlangem organizationName: Langname des Konnektor-Herstellers (Kar.: 0-1); […] Geänderte Anforderung: GS-A_4719 TI-spezifische Vorgabe zur Nutzung der Extension SubjectAltNa-mes Tab_PKI_228 ALT: #; ASN.1 DEFINITION; TI-SPEZIFISCHE VORGABEN; 1; SubjectAltNames ::= GeneralNames; Der GeneralName KANN in der Form rfc822Name angegeben werden.; [...] Tab_PKI_228 NEU: #; ASN.1 DEFINITION; TI-SPEZIFISCHE VORGABEN; 1; SubjectAltNames ::= GeneralNames; Ein GeneralNames-Feld enthält eine Sequenz von GeneralName-Elementen. Die Typ-Ausprägungen in den folgenden Zeilen sind für GeneralName zulässig.; 2; rfc822Name [1] IMPLICIT IA5String,; E-Mail-Adresse in der Form rfc822Name; 3; dNSName [2] IMPLICIT IA5String,; “Domain Name Label” wie in [RFC5280], Kap. 4.2.1.6. beschrieben.; [...]	gemSpec_PKI gemProdT_X.509_TSP_nonQES_Komp