SRQ - Specification Related Question

SRQ-ID: 1154

Betrifft:

Themenkreis	Elektronische Gesundheitskarte
Schlagwort	zueinander passende OID und algID
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSpec_eGK_P1], ergänzt SRQ_1047
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	10.2.4

Stichwort: zueinander passende OID und algID

Frage:

Wann passen OID und algID zueinander?

Betrifft:

Gültig ab	01.04.2011	Verbindlichkeit	normativ
Zulassungsrelevanz	Keine Zulassungsrelevanz		
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version	2.2.1	voraussichtl. Zeitpunkt	
Anmerkungen:			
Status	☒ erfasst ☒ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☐ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Diese SRQ ist nicht zulassungsrelevant, da die normativen Vorgaben bereits implizit im Basisdokument angelegt waren.

Diese SRQ wirkt sich auf die Versionsnummern in EF.Version nicht aus, weil bereits alle zugelassenen eGK diesen Sachverhalt berücksichtigen.

Bereits im SRQ_1047 wurden die normativen Vorgaben im Kapitel 10.2.4 „Suche nach einem öffentlichen Schlüsselobjekt“ geändert. Dabei wurde allerdings nicht explizit verdeutlicht, wann ein Attribut *oid* zu einer vorgegebenen *algID* passt. Neben impliziten Festlegungen (siehe Hinweise weiter unten) ist es erstrebenswert, diese Festlegung auch explizit zu treffen. Dazu wird nach dem Punkt (N216,05) (siehe SRQ_1047) folgendes eingefügt:

(N216,10) K_eGK
Zum OID

a. sigS_ISO9796-2Withrsa_sha256 (siehe Tabelle 6) MUSS genau *algID* gleich verifyCertificate (siehe Tabelle 169) passen.

b. authS_ISO9796-2Withrsa_sha256_mutual (siehe Tabelle 6) MÜSSEN genau die *algID* aus folgender Menge passen: {rsaRoleCheck, rsaSessionkey4SM}.

Hinweis (1): Gemäß Kapitel 8.1.1.5, Tabelle 6, (N192) und (N196) sind für dieses Dokument nur OIDs aus folgender Menge relevant: {sigS_ISO9796-2Withrsa_sha256, authS_ISO9796-2Withrsa_sha256_mutual}.

Hinweis (2): Gemäß (N842)b und (N869)f.v.2 in Verbindung mit (N1018) sowie (N958)b sind für dieses Dokument nur algIDs aus folgender Menge relevant: {rsaRoleCheck, rsaSessionkey4SM, verifyCertificate}.