

SRQ-ID: 1047

Betrifft:

Themenkreis	Elektronische Gesundheitskarte
Schlagwort	Suche nach öffentlichen Schlüsseln
zu Dokument / Datei	[gemSpec_eGK_P1]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	(N216)

Stichwort: Suche nach öffentlichen Schlüsseln

Frage:

Es gibt eine Diskrepanz zwischen der Suche nach öffentlichen Schlüsseln und der Suche nach geheimen Schlüsseln. Ist dies beabsichtigt?

Betrifft:

Gültig ab Release	0.5.2	Verbindlichkeit	
zusätzlicher Download-Link zu Datei:			
Herstellerebefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
Anmerkungen:			
Status	<input checked="" type="checkbox"/> erfasst <input checked="" type="checkbox"/> intern abgestimmt <input type="checkbox"/> extern abgestimmt <input type="checkbox"/> zurückgezogen <input checked="" type="checkbox"/> freigegeben <input type="checkbox"/> eingearbeitet in Folgeversion		

Diese SRQ ist zulassungsrelevant, weil sich das spezifizierte Verhalten an der Schnittstelle zur Karte durch diese SRQ ändert. Auf bereits zugelassene Betriebssysteme hat diese SRQ keinerlei Einfluss.

Obwohl diese SRQ schnittstellenrelevant ist, hat diese SRQ keinen Einfluss auf den Inhalt von EF.Version, weil bereits alle zugelassenen Betriebssysteme diese SRQ berücksichtigen.

Antwort:

In der Tat besteht eine Diskrepanz zwischen der Suche nach öffentlichen Schlüsseln und der Suche nach geheimen Schlüsseln. Während die Suche nach geheimen Schlüsseln gemäß [gemSpec_eGK_P1#10.2.3] zunächst nach einem Schlüssel mit passendem Identifier sucht und dann überprüft, ob der gefundene Schlüssel den gewünschten Algorithmus unterstützt, wird bei der Suche nach öffentlichen Schlüsseln gemäß [gemSpec_eGK_P1#10.2.4] schon bei der Suche nach passendem Identifier und gleichzeitig nach passendem Algorithmus gesucht.

Als Konsequenz sind derzeit bei der Suche nach geheimen Schlüsseln zwei Fehler zu unterscheiden: "*keyNotFound*" und "*notSupported*". Die Suche nach einem öffentlichen Schlüssel kennt derzeit nur den Fehler "*keyNotFound*".

Diese SRQ behebt die Diskrepanz und gleicht die Suche nach einem öffentlichen Schlüssel der Suche nach einem geheimen Schlüssel an.

Änderung 1

In der Tabelle vor [gemSpec_eGK_P1#(N216)] wird zusätzlich zum Fehler "*keyNotFound*" der Fehler "*notSupported*" ergänzt. Damit sieht die Tabellenzeile insgesamt wie folgt aus:

Errors:	<i>keyNotFound</i>	Zu den gegebenen Inputparametern wurde kein passendes Schlüsselobjekt gefunden.
	<i>notSupported</i>	Der Schlüssel unterstützt den von <i>algID</i> geforderten Algorithmus nicht.

Änderung 2

Die Anforderung [gemSpec_eGK_P1#(N216)a Spiegelstrich 2] wird ersatzlos gestrichen.

Änderung 3

Nach der Anforderung [gemSpec_eGK_P1#(N216)] wird folgende Anforderung ergänzt:

(N216,05) K_eGK

Wenn das Attribut *oid* des Output-Parameters *key* nicht zur vorgegebenen *algID* passt, genau dann MUSS der Fehler *notSupported* zurückgemeldet werden.