

SRQ-ID: 1153

Betrifft:

Themenkreis	Elektronische Gesundheitskarte
Schlagwort	Schlüsselverwendung SE-spezifisch
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSpec_eGK_P1], ersetzt SRQ_0839
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	(N174), (N215)b

Stichwort: Schlüsselverwendung SE-spezifisch

Frage:

Der Verwendungszweck eines Schlüssels lässt sich SE-spezifisch angeben und wurde in Teil 2 auch so genutzt. Warum ist dies in Teil 1 nicht explizit erwähnt?

Betrifft:

Gültig ab	01.04.2011	Verbindlichkeit	normativ
Zulassungsrelevanz	Diese SRQ ist zulassungsrelevant, aber die normativen Vorgaben waren bereits in der SRQ_0839 festgelegt.		
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version	2.2.1	voraussichtl. Zeitpunkt	
Anmerkungen:	Alle vor dem 01.04.2011 zugelassenen eGKs und Testsuites enthalten diese Änderungen bereits.		
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		

Antwort:

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

Änderung 1:

Der Punkt (N174) wird inklusive aller Unterpunkte durch folgenden ersetzt:

(N174) K_Anwendungsspezifikation {K_eGK}

Ein *privates* Schlüsselobjekt MUSS genau ein Attribut *listAlgorithmIdentifier* besitzen, welches angibt, für welche Zwecke das *private* Schlüsselobjekt verwendbar ist.

- a. Für die Länge der Liste gilt: Die Liste MUSS mindestens ein Element und DARF NICHT mehr als vier Elemente enthalten.
- b. Jedes Listenelement MUSS
 1. genau einen *seldentifier* gemäß (N79) und
 2. genau eine Menge *setAlgorithmIdentifier* mit Elementen des Typs *algorithmIdentifier* enthalten.
 3. Die Werte von *algorithmIdentifier* MÜSSEN aus den in (N176), (N179) und (N183) genannten Mengen gewählt werden.
- c. Die Menge *setAlgorithmIdentifier* DARF NICHT mehr als sechs Elemente enthalten.
- d. Das COS KANN Mengen des Typs *setAlgorithmIdentifier*, welche mehr Elemente enthalten als nach (N174)c gefordert
 1. unterstützen, oder
 2. ablehnen.

Änderung 2:

Der Unterpunkt (N215)b wird durch folgenden ersetzt:

[Wenn der Output-Parameter *key* ein ...]

- b. *privater* Schlüssel ist, dann wird in den Elementen von *listAlgorithmIdentifier* nach einem Element gesucht, dessen *seldentifier* (siehe (N174)b.1) identisch zum Attribut *seldentifier* (siehe (N300)a) des Ordners ist, in welchem *key* als *child* enthalten ist. Es wird der Fehler "notSupported" zurückgemeldet, wenn ein solches Element
 1. nicht existiert, oder
 2. existiert, aber die Menge *setAlgorithmIdentifier* (siehe (N174)b.2) das Element *algId* nicht enthält.