SRQ - Specification Related Question

SRQ-ID: 1157

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	Informativen Charakter der Tabelle der Prozesschritte klarstellen und PUK in Anforderungen der PIN/PUK-Policy ergänzen.
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSiKo]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Anh E 2.1, 2.1.8

Stichwort: PIN/PUK

Frage:

Sind die Maßnahmen der Prozesschritte in der Tabelle auf S.477 normativ und sind in den Anforderungen A_03037, A_03052 und A_03072 die PUKs vollständig berücksichtigt?

Betrifft:

Gültig ab	07.04.2011	Verbindlichkeit	normativ
Zulassungsrelevanz	SRQ ist für alle Zulassungen zu beachten, die nach dem 07.04.2011 beantragt werden.		
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:

Die Maßnahmen in der Tabelle auf S.477 sind nicht normativ. Die Tabelle auf S. 477 zeigt eine informative, überblicksartige, nicht vollständige Darstellung optional möglicher einzelner Prozessschritte. Entsprechende Hinweise werden der Tabelle zugefügt.

In den Anforderungen A_03037, A_03052 und A_03072 sind die PUKs nicht vollständig berücksichtigt worden. In den Anforderungen werden Änderungen aufgenommen, die auch die PUKs berücksichtigen.

Das Ergebnis der Änderungen in [gemSiKo#Anhang E]:

1) Änderung der Tabelle auf S. 477:

Die nachfolgende Tabelle enthält informativ eine überblicksartige, nicht vollständige Darstellung optional möglicher einzelner Prozessschritte und eine exemplarische Zuordnung.

Tabelle AnhE-2.1: Informative, überblicksartige, nicht vollständige Darstellung optional möglicher einzelner Prozessschritte

	exemplarische, informelle Bewertung	
	Erstausgabe der eGK[4] Maßnahmenstärke: mittel	Folgekarten eGK HBA/SMC-B/BA Maßnahmenstärke: hoch
Nachweis der Identität des Karteninhabers	Bestätigung der Identität durch eine vom Benutzer unabhängige Instanz notwendig, z. B. Vorlage eines persönlichen Dokumentes	Belastbare Bestätigung der Identität durch eine vom Benutzer unabhängige Instanz notwendig, z. B. persönlich (sicher) bekannt (persönlich identifiziert)
Vertrauenswürdigkeit der Registrierungsinstanz	Mitarbeiter der Registrierungsinstanz sind nach der Schutzbedarfsklasse „mittel“ identifiziert worden und vertrauenswürdig.	Mitarbeiter der Registrierungsinstanz sind nach der Schutzbedarfsklasse „hoch“ identifiziert worden, vertrauenswürdig, geschult und arbeiten nach festgelegter Policy.
Aushändigung der Authentifizierungsinformationen (PIN/PUK-Brief, Karte)	Postweg	Postweg + Rückmeldung (Postzustellungsurkunde) oder gleichwertige Ersatzverfahren
Konformität	Standards oder Best Practices, Herstellererklärung	Offizielle Standards mit unabhängiger Evaluierung und Zulassung für das Gesundheitswesen
Aufbewahrung, Speicherung	Authentifizierungsdaten unterliegen SW-Kontrolle	Authentifizierungsdaten unterliegen HW-Kontrolle

[4] Dieser verringerte Schutzbedarf ist nur bei der Erstausgabe der eGK für die PIN.CH möglich, da damit alleine noch kein Zugriff auf personenbezogene medizinische Daten möglich ist. Die auf der eGK ggf. vorhandenen geschützten Versichertendaten sind nur von berechtigten Leistungserbringern nach Eingabe der PIN.CH mit dem HBA/SMC/BA einsehbar. Es ist daher bei der Ausgabe der HBA/SMC/BA besonders auf die persönliche Übergabe der PIN.CH bzw. der zugehörigen Karte an den berechtigten Leistungserbringer zu achten. Daher sind die Mindestanforderungen an die Maßnahmenstärke bei der Erstausgabe der Heilberufsausweise und der entsprechenden PIN.CH als „hoch“ einzustufen.

	exemplarische, informelle Bewertung	
	Erstausgabe der eGK[4] Maßnahmenstärke: mittel	Folgekarten eGK HBA/SMC-B/BA Maßnahmenstärke: hoch
Übertragung	Authentifizierungsdaten werden in Software ver- bzw. umgeschlüsselt	Authentifizierungsdaten werden von der Eingabe bis zur Prüfung verschlüsselt übertragen und in physikalisch geschützter Hardware geprüft
Adressierbarkeit und Zustellbarkeit	Bestätigung der Adresse durch eine vom Benutzer unabhängige Instanz ist notwendig	belastbare Bestätigung der Adresse durch eine vom Benutzer unabhängige Instanz ist notwendig
Protokollierbarkeit	innerhalb existierender Vertragsbeziehungen gegen Dritte als Beweis verwertbar	gegen (beliebige) Dritte als Beweis verwertbar
Rückführbarkeit	auf genau ein Unternehmen/Partner rückführbar	auf genau eine Person rückführbar

2) Änderung der Anforderungen A_03037, A_03052 und A_03072 in Tabelle E2.1.8:

Afo-ID	Anfo	Art	Titel	Beschreibung		Quelle
[...]	[...]		[...]	[...]		[...]
A_03037	SP_PIN_CRE_2	S	PIN_PUK_Erzeugung_02: Mögliche Arten von PINs/PUKs.	Die PIN/PUK-Auswahl MUSS gemäß einer der folgenden Techniken erfolgen: o zugewiesene echt zufällige oder pseudozufällige PIN, PUK o zugewiesene abgeleitete PIN, PUK o durch Kunden gewählte PIN.		Anhang E.2.1
A_03052	SP_PIN_TRA_1	S	PIN_PUK_Transport_1: Vetraulich-keit bei Transport /Verteilung.	Die PIN/PUK MUSS nur dem Karteninhaber bekannt sein. Daher ist die Vertraulichkeit der PIN/PUK in Transport, Speicherung und Gebrauch vor nicht autorisierter Aufdeckung und Weitergabe der PIN/PUK zu schützen, dies betrifft: PINs, PUKs DÜRFEN außerhalb geschützter Hardware NICHT unverschlüsselt auftreten. Ausnahme ist der einmalige Ausdruck des PIN/PUK-Briefes, der durch gesonderte		Anhang E.2.1

Afo-ID	Anfo	Art	Titel	Beschreibung		Quelle
				organisatorische Maßnahmen gesichert ist. Die Verteilung der PINs/PUKs MUSS auf das absolut notwendige Maß eingeschränkt werden, um die Möglichkeiten zur Kompromittierung der PIN/PUK zu minimieren und potentielle Schäden zu beschränken. Eine PIN/PUK DARF NICHT mehr als einmal erstellt werden und MUSS dem Karteninhaber übermittelt werden.		
A_03072	SP_PIN_DEL_2	S	PIN_PUK_Löschung_2: Zerstörung nicht mehr benötigter Klartext-PINs/Trägermedien.	Es MÜSSEN Vorkehrungen getroffen werden, um die nicht mehr benötigten Klartext-PINs/PUKs so zerstören zu können, dass es nicht mehr möglich ist, die PINs/PUKs ganz oder teilweise zu rekonstruieren. Insbesondere MÜSSEN die Kartenherausgeber geeignete Sicherheitsmaßnahmen treffen in Bezug auf die interne Handhabung und Beseitigung von zurückgesendeten PIN/PUK-Briefen und Material, das mit dem ursprünglichen Druck der PIN/PUK-Briefe verbunden ist. Dabei ist darauf zu achten, dass die Behandlung zurückgesandter PIN/PUK-Briefe von der Behandlung der zurückgesandten Karten organisatorisch getrennt sein MUSS.		Anhang E.2.1
[...]	[...]		[...]	[...]		[...]