SRQ-ID: 1156

Betrifft:

Themenkreis	Fachanwendungen
Schlagwort	Schutzbedarfsfeststellung
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemSiKo#AnhC]
Version	2.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Anh C 2.47, 2.88, 2.90, 2.111, 2.112, 2.113, 2.114, 2.115, 2.117

Stichwort: Schutzbedarfsfeststellung

Frage:

Haben sich für den Basis-Rollout relevante Korrekturen bzw. Ergänzungen der Schutzbedarfsfeststellungen (Anhang C im Übergreifenden Sicherheitskonzept der Telematikinfrastruktur) ergeben?

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:

Ja. Konkret bedeutet dies:

Änderungen der Einstufung beim Schutzbedarf gab es bei den folgenden Informationsobjekten: Io072, Io123, Io125. Die Änderungen gegenüber dem ursprünglichen Inhalt des [gemSiKo] sind an den gelben Markierungen erkennbar.

Die folgenden Informationsobjekte wurden neu erstellt bzw. der Schutzbedarf wurde erstmalig bewertet: Io151, Io152, Io157, Io158, Io234, Io252.

Die detaillierte Darstellung der Schutzbedarfsfeststellung dieser Informationsobjekte folgt auf den nächsten Seiten des vorliegenden SRQ.

Hinweis: Folgeversionen von [gemSiKo] enthalten bereits die hier aufgeführten Schutzbedarfsfeststellungen.

C2.47 - Io072 – Verwendete Software (TI)

Typ des Schutzobjektes: Informationsobjekt		ID: Io072
Grundwert	**Schutzbedarf**	**Begründung**
Vertraulichkeit	**r** niedrig **ü** mittel **r** hoch **r** sehr hoch	„Security by Obscurity“ wird im technischen Bereich als eine nicht zielführende Vorgehensweise angesehen. Da es sich bei der Software aber zum Teil um Firmengeheimnisse handelt, wird hier ein ~~hoher~~ mittlerer Schutzbedarf angesetzt.
Integrität	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Bei Integritätsverletzung von sicherheitsrelevantem Programmcode besteht das Risiko von Vertrauensverletzungen. Auch Gefahr für Leib- und Leben kann nicht ausgeschlossen werden.
Verfügbarkeit	irrelevant	-
Authentizität	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Der Schaden beim Einsatz von Programmcode dessen Herkunft nicht nachvollziehbar ist, bietet dasselbe Schadenspotential wie bei Integritätsverletzungen.
Nichtabstreitbarkeit	irrelevant	-

C2.88 - Io123 – Public-Key und dazugehöriges Zertifikat der CV-Root

Typ des Schutzobjektes: Informationsobjekt		ID: Io123
Grundwert	**Schutzbedarf**	**Begründung**
Vertraulichkeit	**r** niedrig **ü** mittel **r** hoch **r** sehr hoch	~~Die Public-Keys und die dazugehörigen Zertifikate haben nur einen niedrigen bis mittleren Schutzbedarf, denn sie sind sowieso bekannt und ggf. öffentlich verfügbar (Verzeichnisdienst).~~ Der Öffentliche Schlüssel ist innerhalb des Gesamtsystems nur den an der Kartenproduktion Beteiligten bekannt. Es gibt keinen technischen Grund ihn außerhalb dieses Workflows bekannt zu machen. Wird anhand des Öffentlichen Schlüssels eine Schwäche des korrespondierenden Privaten Schlüssels erkannt, sind alle Karten auszutauschen.
Integrität	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Die Integrität des Public-Key der CV-Root hat einen sehr hohen Schutzbedarf, denn eine Manipulation, das Unterschieben eines falschen Schlüssels, kann die CV-Authentifikation unterlaufen.
Verfügbarkeit (1)	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Wird als hoch angesehen, denn nur Mithilfe des Public-Key der CV-Root können sich eGK und HBA gegenseitig authentisieren.
Authentizität	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Der Erzeuger eines CVC-Zertifikats der CV-Root muss aus Gründen der Revisionsfähigkeit und Rechtssicherheit bestimmbar sein.
Nichtabstreitbarkeit	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Aus Gründen der Revisionsfähigkeit und Rechtssicherheit darf die Erstellung eines korrekten CVC-Zertifikats der CV-Root vom Ersteller nicht abgestritten werden können.

C2.90 - Io125 – Public-Keys und dazugehörige Zertifikate der CV-SUB-CA

Typ des Schutzobjektes: Informationsobjekt		ID: Io125
Grundwert	**Schutzbedarf**	**Begründung**
Vertraulichkeit	**ü** niedrig **r** mittel **r** hoch **r** sehr hoch	~~Das Zertifikat ist innerhalb des Gesamtsystems „öffentlich“, sollte aber nicht unbedingt hinausgelangen.~~ Zertifikate sind innerhalb des Gesamtsystems „öffentlich“, sollten aber nicht unbedingt hinausgelangen (Mittel). Zertifikate in Verzeichnissen und CVZertifikate (da vor der Authentifikation präsentiert) sind leicht zu erfahren. Dieses CVZertifikat wird vor der Prüfung präsentiert, daher niedriger Schutzbedarf.
Integrität	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Die Integrität Public-Key und des Zertifikats der CV-SUB-CA hat einen sehr hohen Schutzbedarf, denn eine Manipulation, das Unterschieben eines falschen Schlüssels, kann die CV-Authentikation unterlaufen.
Verfügbarkeit (1)	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Wird als hoch angesehen, denn nur Mithilfe des CVC-Zertifikats der CV-SUB-CA können sich eGK und HBA gegenseitig authentisieren.
Authentizität	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Der Erzeuger eines CVC-Zertifikats der CV-SUB-CA muss aus Gründen der Revisionsfähigkeit und Rechtssicherheit bestimmbar sein.
Nichtabstreitbarkeit	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Aus Gründen der Revisionsfähigkeit und Rechtssicherheit darf die Erstellung eines korrekten CVC-Zertifikats der CV-SUB-CA vom Ersteller nicht abgestritten werden können.

C2.111 – Io151 – Privater Schlüssel PrK.CH.ENCV der eGK

Typ des Schutzobjektes: Informationsobjekt		ID: Io151
Grundwert	**Schutzbedarf**	**Begründung**
Vertraulichkeit	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Der Private Schlüssel besitzt einen sehr hohen Schutzbedarf, denn sollten er kompromittiert werden, ist das unberechtigte Lesen von personenbezogenen medizinischen Daten möglich.
Integrität	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Die Integrität der Privaten Schlüssel hat einen hohen Schutzbedarf, denn der Verlust der Integrität der Privaten Schlüssel führt dazu, dass die eGK keine eVerordnung mehr entschlüsseln kann.
Verfügbarkeit (1)	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Wenn eGK vorhanden „hoch“ (d.h. in mindestens 99,3 % der Fälle verfügbar), denn nur wenn der Private Schlüssel vorhanden ist, kann eine Verordnung entschlüsselt werden).
Authentizität	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Der Erzeuger eines Privaten Schlüssels muss aus Gründen der Revisionsfähigkeit und Rechtssicherheit eineindeutig und nachweisbar bestimmbar sein.
Nichtabstreit-barkeit	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Aus Gründen der Revisionsfähigkeit und Rechtssicherheit darf die Erstellung eines Privaten Schlüssels vom Ersteller nicht abgestritten werden können.

C2.112 – Io152 – Privater Schlüssel PrK.CH.AUTN der eGK

Typ des Schutzobjektes: Informationsobjekt		ID: Io152
Grundwert	**Schutzbedarf**	**Begründung**
Vertraulichkeit	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Der Private Schlüssel besitzt einen sehr hohen Schutzbedarf, denn sollte er kompromittiert werden, ist ggf. ein Zugriff auf vertrauliche Daten möglich.
Integrität	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Die Integrität des Privaten Schlüssels hat einen hohen Schutzbedarf, denn eine Manipulation des Privaten Schlüssels führt entweder dazu, dass eine Authentifikation oder Ent- bzw. Verschlüsselung vertraulicher Daten nicht mehr möglich ist. Anm.: Dieser Fall ist aber von der Auswirkung mit einem physischen Defekt der Karte vergleichbar.
Verfügbarkeit (1)	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Wenn eGK vorhanden „hoch“ (d.h. in mindestens 99,3 % der Fälle verfügbar), denn nur bei Vorhandensein des Privaten Schlüssels kann sich der Versicherte authentifizieren).
Authentizität	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Der Erzeuger eines Privaten Schlüssels muss aus Gründen der Revisionsfähigkeit und Rechtssicherheit eineindeutig und nachweisbar bestimmbar sein.
Nichtabstreit-barkeit	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Aus Gründen der Revisionsfähigkeit und Rechtssicherheit darf die Erstellung eines Privaten Schlüssels vom Ersteller nicht abgestritten werden können.

C2.113 – Io157 – Datensatz der Einwilligung zur Nutzung von freiwilligen Anwendungen auf der eGK

Typ des Schutzobjektes: Informationsobjekt		ID: Io157
Grundwert	**Schutzbedarf**	**Begründung**
Vertraulichkeit	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Auch die Information, dass freiwillige Anwendungen genutzt werden ist eine hoch vertrauliche Information (fällt unter Schweigepflicht).
Integrität	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Bei Verlust (z. B. unbeabsichtigte Löschung, Manipulation) des Eintrags kann der Versicherte nicht mehr auf die freiwilligen Anwendungen zugreifen.
Verfügbarkeit (1)	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Wenn eGK vorhanden „hoch“ (d.h. in mindestens 99,3 % der Fälle verfügbar), denn nur wenn der Datensatz vorhanden ist, kann der Versicherte auf seine freiwilligen Anwendungen zugreifen.
Authentizität	**r** niedrig **ü** mittel **r** hoch **r** sehr hoch	Die Einträge dürfen nur von einer natürlichen Person der Gruppe der Leistungserbringer erstellt werden. Der Ersteller des letzten Eintrages ist namentlich bekannt.
Nichtabstreit-barkeit	**r** niedrig **ü** mittel **r** hoch **r** sehr hoch	Die Einträge dürfen nur von einer natürlichen Person der Gruppe der Leistungserbringer erstellt werden. Der Ersteller des letzten Eintrages ist namentlich bekannt.

C2.114 – Io158 – Datensatz der Links zur Nutzung von freiwilligen Anwendungen

Typ des Schutzobjektes: Informationsobjekt		ID: Io158
Grundwert	**Schutzbedarf**	**Begründung**
Vertraulichkeit	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Auch die Information, dass freiwillige Anwendungen genutzt werden ist eine hoch vertrauliche Information (fällt unter Schweigepflicht).
Integrität	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Bei Verlust (z. B. unbeabsichtigte Löschung, Manipulation) des Links kann der Versicherte nicht mehr automatisch auf die freiwilligen Anwendungen zugreifen.
Verfügbarkeit (1)	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Wenn eGK vorhanden „hoch“ (d.h. in mindestens 99,3 % der Fälle verfügbar), denn nur wenn die Links vorhanden sind, kann der Versicherte auf seine freiwilligen Anwendungen zugreifen.
Authentizität	**r** niedrig **ü** mittel **r** hoch **r** sehr hoch	Die Links dürfen nur von einer natürlichen Person der Gruppe der Leistungserbringer erstellt werden. Der Ersteller des letzten Eintrages ist namentlich bekannt.
Nichtabstreit-barkeit	**r** niedrig **ü** mittel **r** hoch **r** sehr hoch	Die Einträge dürfen nur von einer natürlichen Person der Gruppe der Leistungserbringer erstellt werden. Der Ersteller des letzten Eintrages ist namentlich bekannt.

C2.115 – Io234 – Privater Schlüssel zum X.509 AUT-Zertifikat der eGK

Typ des Schutzobjektes: Informationsobjekt		ID: Io234
Grundwert	**Schutzbedarf**	**Begründung**
Vertraulichkeit	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Der Private Schlüssel besitzt einen sehr hohen Schutzbedarf, denn sollte er kompromittiert werden, ist der Zugriff auf vertrauliche Daten möglich.
Integrität	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Die Integrität der Privaten Schlüssel hat einen sehr hohen Schutzbedarf, denn der Verlust der Integrität des Privaten Schlüssels führt dazu, dass eine Authentifikation und eine Rechteverwaltung nicht mehr möglich sind.
Verfügbarkeit (1)	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Wenn eGK vorhanden „hoch“ (d.h. bei Vorhandensein der Karte in mindestens 99,3 % der Fälle verfügbar), denn nur bei Verfügbarkeit des Privaten Schlüssels kann der Versicherte seine Rechte verwalten.
Authentizität	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Der Erzeuger eines Privaten Schlüssels muss aus Gründen der Revisionsfähigkeit und Rechtssicherheit eineindeutig und nachweisbar bestimmbar sein.
Nichtabstreit-barkeit	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Aus Gründen der Revisionsfähigkeit und Rechtssicherheit darf die Erstellung eines Privaten Schlüssels vom Ersteller nicht abgestritten werden können.

C2.117 – Io252 – Privater Schlüssel zum X.509-ENC-Zertifikat der eGK

Typ des Schutzobjektes: Informationsobjekt		ID: Io252
Grundwert	**Schutzbedarf**	**Begründung**
Vertraulichkeit	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Der Private Schlüssel besitzt einen sehr hohen Schutzbedarf, denn sollte er kompromittiert werden, ist die Entschlüsselung von vertraulichen Daten möglich.
Integrität	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Die Integrität der Privaten Schlüssel hat einen sehr hohen Schutzbedarf, denn der Verlust der Integrität des Privaten Schlüssels führt dazu, dass die Entschlüsselung vertraulicher Daten nicht mehr möglich ist.
Verfügbarkeit (1)	**r** niedrig **r** mittel **ü** hoch **r** sehr hoch	Wenn eGK vorhanden „hoch“ (d.h. bei Vorhandensein der Karte in mindestens 99,3 % der Fälle verfügbar), denn nur bei Verfügbarkeit des Privaten Verschlüsselungsschlüssels kann der Versicherte seine Daten wieder entschlüsseln.
Authentizität	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Der Erzeuger eines Privaten Schlüssels muss aus Gründen der Revisionsfähigkeit und Rechtssicherheit eineindeutig und nachweisbar bestimmbar sein.
Nichtabstreit-barkeit	**r** niedrig **r** mittel **r** hoch **ü** sehr hoch	Aus Gründen der Revisionsfähigkeit und Rechtssicherheit darf die Erstellung eines Privaten Schlüssels vom Ersteller nicht abgestritten werden können.