# SRQ - Specification Related Question

**SRQ-ID: 1083**

**Betrifft:**

| | |
|---|---|
| Themenkreis | PKI und Zertifikate |
| Schlagwort | Zusätzliche Sicherheitsvorgaben |
| zu Dokument / Datei (evtl. ersetzt SRQ) | gemPers_Krypt, SRQ_0906 |
| Version | 1.0.0 |
| Bezug (Kap., Abschnitt, Tab., Abb.) | 4.2, 5.1.2, 5.1.6, 7.1 |

**Stichwort: Zusätzliche Sicherheitsvorgaben**

**Frage:**

Welche sicherheitstechnischen Anforderungen sind für die Personalisierungssschnittstelle zusätzlich zu beachten?

**Betrifft:**

| | | | |
|---|---|---|---|
| Gültig ab | 07.04.2011 | Verbindlichkeit | normativ |
| Zulassungsrelevanz | SRQ ist für alle Zulassungen zu beachten, die nach dem 01.04.2011 beantragt werden | | |
| zusätzlicher Download-Link zu Datei: | | | |
| Herstellerbefragung durchgeführt | | am | |
| Wird behoben mit Version | | voraussichtl. Zeitpunkt | |
| Anmerkungen: | Dieser SRQ enthält Maßnahmen, die sich aus dem Sicherheitsgutachten ergeben haben. | | |
| Status | ☒ erfasst ☒ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☒ freigegeben ☐ eingearbeitet in Folgeversion | | |

---

**Antwort**:

Folgende Änderungen ergeben sich an der Spezifikation. **Alle Änderungen beziehen sich dabei auf den Inhalt der SRQ_0906.**

## 4.2 Datenfluss bei der Kartenproduktion

…

Für das Zusammenspiel der Organisationen gibt es keine festen Vorgaben, diese müssen vielmehr bilateral zwischen den Beteiligten vereinbart werden. Der Datenfluss zwischen den einzelnen Organisationen muss ggf. verschlüsselt und integritätsgesichert sein. Ebenso ist die Authentizität der Personalisierungsdaten in jedem Prozessschritt sicherzustellen (gemSiko#A_02690). Für die Sicherstellung der Authentizität und Integrität wird als technische Lösung eine Signatur des kompletten Personalisierungsdatensatzes empfohlen. Die jeweilige Vereinbarung muss von der gematik zugelassen werden. In der Abbildung wird eine (logische) Organisation im Sinne einer Rolle betrachtet. Natürlich kann eine tatsächlich an der Kartenproduktion beteiligte Organisation mehrere der aufgezeigten Rollen übernehmen.

…

Kapitel 5.1 ist in den entsprechenden Unterkapiteln folgendermaßen zu ergänzen:

### 5.1.2 Sicherheit geheimer kryptographischer Schlüssel

…

Analoge Vorgaben gelten für die (kryptographisch abgesicherte) Speicherung von geheimen Schlüsseln einer eGK außerhalb eines HSMs:

- Ein geheimer Schlüssel einer eGK DARF außerhalb eines HSM NUR dann (kryptographisch abgesichert) gespeichert werden, falls dies für die Produktion einer eGK direkt notwendig ist.
- Ein außerhalb eines HSM (kryptographisch abgesichert) gespeicherter geheimer Schlüssel einer eGK MUSS unverzüglich gelöscht werden, sobald dieser durch das speichernde System nicht mehr benötigt wird. Ein typischer Anwendungsfall ist die Übergabe der privaten Schlüssel an den Personalisierer in der DÜS [gemPers].

Weiter ist bezüglich der vollständigen Kontrolle und Kenntnis bei geheimen und privaten kryptographischen Schlüsseln durchgängig das Vier-Augen-Prinzip umzusetzen (siehe (gemSiko#A_03228), sowie Abschnitt 7.1.1 und Abschnitt 7.1.2).

### 5.1.6 Anforderungen an ein HSM

…

- Bei der notwendigen Prüftiefe muss berücksichtigt werden, ob und wie weit unberechtigte physische Zugriffe auf das HSM während seiner gesamten Lebensdauer durch weitere organisatorische und bauliche Maßnahmen verhindert werden. Werden entsprechende Zugriffe nicht durch weitere Maßnahmen ausgeschlossen, muss die Prüftiefe mindestens FIPS 140 Level 3 oder CC EAL 4 (bzw. bei den anderen Evaluierungsschemata vergleichbar) umfassen. Mechanismenstärke (bzw. das angenommene Angriffspotential) müssen "hoch" sein.

Folgende Funktionen eines Produktions-HSM dürfen nur nach einer ~~ausreichend sicheren Authentikation~~ erfolgreichen Authentifikation und Autorisierung des aufrufenden Systems möglich sein:

- Generieren eines geheimen Schlüssels bzw. einer PIN oder PUK,
- (kryptographisch abgesicherter) Export eines geheimen Schlüssels bzw. einer PIN oder PUK,

- (kryptographisch abgesicherter) Import eines geheimen Schlüssels bzw. einer PIN oder PUK,
- Löschen eines geheimen Schlüssels bzw. einer PIN oder PUK (falls dies durch das HSM unterstützt wird),
- Sperren der Zugriffe auf einen geheimen Schlüssel bzw. einer PIN oder PUK (falls dies durch das HSM unterstützt wird)

Das genaue Vorgehen bei der ~~Authentikation~~ Authentifikation MUSS durch den Betreiber festgelegt werden. Sichergestellt werden muss dabei aber, dass das HSM nur nach erfolgter ~~Authentikation~~ Authentifikation genutzt werden kann [gemSiKo#AnhB4.5.4] A_02809.

Kapitel 7 ist folgendermaßen zu ergänzen:

### 7.1 Key-Management

Um die im letzten Kapitel eingeführte Erweiterung der Datenübergabeschnittstelle für die Übertragung kryptographischer Daten einer eGK nutzen zu können, werden zwei neue "Typen" kryptographischer Schlüssel benötigt:

- Transportschlüssel: Dieser wird für das symmetrische Ver- und Entschlüsseln der eigentlichen eGK-Daten verwendet. Die Länge des Transportschlüssels hängt von dem Verschlüsselungsverfahren ab, das gemäß [gemSpec_Krypt#6.1.5] gewählt werden MUSS.
- Key-Encryption-Key (KEK): Dies ist ein RSA-Schlüsselpaar. Der zugehörige öffentliche Schlüssel wird zum Verschlüsseln eines Transportschlüssels verwendet, der zugehörige private Schlüssel wird entsprechend zum Entschlüsseln des Transportschlüssels verwendet. Kartenherausgeber und Kartenpersonalisierer benötigen jeweils ein Paar.

Wird für die Sicherstellung der Authentizität und Integrität wie empfohlen die Signatur als technische Realisierung gewählt, wird zusätzlich ein Schlüsselpaar für die Signatur benötigt:

- ein RSA-Schlüsselpaar für die Signatur (K.Sign) (Sicherung Authentizität und Integrität): Der private Schlüssel dient als Signaturschlüssel für die Sicherung der Authentizität und Integrität der übermittelten kryptographischen Schlüssel. Wird in die Signatur der gesamte Personalisierungsdatensatz einbezogen, wird hierdurch eine kryptographisch feste Bindung zwischen einzelner eGK und dessen kryptographischer Identität (Schlüssel) erreicht. Ferner ist durch eine eindeutige Referenzierungs-ID (z. B. die Auftragsnummer, siehe [gemPers#3.2]) des Personalisierungsdatensatzes eine gesicherte Zuordnung von eGKs zu einer eindeutigen Auftragsnummer gegeben (mögliche Umsetzung von gemSiko#A_03033). Mit dem öffentlichen Schlüssel überprüft der Empfänger die entsprechende Signatur. Bei negativem Ergebnis der Prüfung ist der Auftrag abzulehnen. Kartenherausgeber und Kartenpersonalisierer benötigen jeweils ein Paar.

~~Der KEK ist gemäß den Vorgaben aus dem Kryptographiekonzept des Sicherheitskonzepts [gemSiKo#Anh.F5.1.2] sicher zu erzeugen und sicher aufzubewahren.~~

Für den Umgang mit dem Schlüsselmaterial sind die Vorgaben aus dem Kryptographiekonzept des Sicherheitskonzepts [gemSiKo#Anh.F5.1.2] zu beachten.

Zudem gelten für den Umgang mit diesen Schlüsseln ~~gelten~~ die gleichen Anforderungen aus Abschnitt 5.1 wie für die kryptographischen Daten einer eGK.

~~Für die Schlüssellänge gilt dabei folgende Konkretisierung:~~

- ~~Ein KEK MUSS eine Mindestlänge haben, die die Vorgaben aus [gemSpec_Krypt#5.1.1.7] erfüllt.~~

Für die RSA-Schlüssel gelten insbesondere bezüglich der kryptographischen Parameter die Vorgaben aus [gemSpec_Krypt#5.1.1.7].

Es muss sichergestellt werden, dass die entsprechenden Schlüssel nur genau für ihren Bestimmungszweck eingesetzt werden ([gemSiko#AnhF#SP_KEY_ALL_5] bzw. [gemSiKo#Anh.F5.1.13] „Prüfung der Schlüsselverwendung“). Maßnahmen, um dies sicherzustellen, sind in den Sicherheitskonzepten der Beteiligten zu dokumentieren und deren Wirksamkeit ist zu begründen.

Ein Transportschlüssel wird immer durch den Absender der mit ihm verschlüsselten Daten generiert. Die Gültigkeit des Transportschlüssels ist dabei maximal eine Nachricht (z.B. ein Personalisierungsauftrag). Ob für die Verschlüsselung der in einer Nachricht enthaltenen Daten ein oder mehrere Transportschlüssel zum Einsatz kommen, muss bilateral zwischen dem Absender und dem Empfänger geregelt werden.

Jedes CMS (bzw. jeder Kartenherausgeber) sowie jeder Personalisierer benötigt mindestens einen KEK. Für diesen gilt:

- Ein Schlüssel wird durch seinen "Besitzer" selber generiert.
- Die Gültigkeit eines Schlüssels beträgt maximal ein Jahr.
- Jedem Schlüssel wird durch seinen Besitzer ein Schlüsselname zugeordnet. Anhand dieses Namens muss der Besitzer den Schlüssel eindeutig bestimmen können. Ein Schlüsselname besteht dabei aus maximal 20 Zeichen.
- Will ein Kartenherausgeber eGKs mit einem Personalisierer bei der Produktion seiner eGKs zusammenarbeiten, müssen diese die öffentlichen Schlüssel und Schlüsselnamen ihrer Schlüssel austauschen. Dabei MUSS die Authentizität der ausgetauschten Schlüssel gewährleistet sein. Das genaue Vorgehen hierbei muss bilateral zwischen den Beteiligten abgestimmt werden. Die gematik lässt den verantwortlichen Kartenproduzenten zu und prüft das Verfahren. Es MUSS das Vier-Augen-Prinzip angewendet werden (siehe Abschnitt 7.1.2).

Abhängig von dem gewählten Modell für die Zusammenarbeit der beteiligten Organisationen (siehe Abschnitt 7.2) kann es notwendig sein, dass auch ein Zulieferer von kryptographischen Daten den öffentlichen Schlüssel des Personalisierers erhält (siehe Variante in Abschnitt 7.2.2). In diesem Fall muss das CMS den vom Personalisierer erhaltenen öffentlichen Schlüssel (inkl. Schlüsselnamen) an die vom Kartenherausgeber beauftragten Zulieferer übermitteln. Dabei MUSS wieder die Authentizität des öffentlichen Schlüssels unter Verwendung des Vier-Augen-Prinzips gewährleistet sein.

### 7.1.1 Vier-Augen-Prinzip private und geheime Schlüssel

Für geheime Schlüssel (bspw. symmetrische Transportschlüssel) und private Schlüssel ist durchgängig während ihres gesamten Lebenszyklus (siehe [gemSiKo#AnhF5]) das Vier-Augen-Prinzip anzuwenden. Zu keinem Zeitpunkt darf das Schlüsselmaterial unter der alleinigen Kontrolle nur einer Person stehen (siehe gemSiko#A_03228). Andernfalls könnte es ausgetauscht werden und Ziele der Sicherungsmaßnahmen, für die jene Schlüssel verwendet werden, nicht mehr erreicht werden.

### 7.1.2 Vier-Augen-Prinzip öffentliche Schlüssel

Beim gegenseitigen Austausch von öffentlichen Schlüsseln (bspw. bei KEK) zwischen Kartenherausgeber und Personalisierer muss das Vier-Augen-Prinzip angewendet werden. Es soll die Authentizität und Integrität schützen, jedoch hauptsächlich dafür sorgen, dass das Schlüsselmaterial zu keinem Zeitpunkt unter der alleinigen Kontrolle einer einzigen Person ist

(siehe gemSiko#A_03228). Andernfalls könnte es ausgetauscht werden und Ziele der Sicherungsmaßnahmen, für die jene Schlüssel verwendet werden, nicht mehr erreicht werden.

Sowohl Kartenherausgeber als auch Personalisierer müssen für ihre Schlüsselpaare das Vier-Augen-Prinzip von der Erzeugung, über die Übergabe der öffentlichen Schlüssel an den Kommunikationspartner, über die Verwendung der DÜS bis zur sicheren Löschung des Schlüsselpaares nach Ende seines Gültigkeitsdauer durchgängig in und zwischen allen Arbeitsschritten umsetzen.

Das Vier-Augen-Prinzip von Kartenherausgeber und Personalisierer muss bei der gegenseitigen Übergabe der jeweiligen öffentlichen Schlüssel so ineinandergreifen, dass die Durchgängigkeit des Vier-Augen-Prinzip bezogen auf den Gesamtprozess garantiert ist.

### 7.1.3 Notfallmaßnahme bei Schlüsselkompromittierung

Für den Fall einer Kompromittierung eines kryptographischen Schlüssels sind Notfallmaßnahmen zu definieren und im Eintrittsfalle einzuleiten (siehe (gemSiko#A_03116)). Im Notfallkonzept müssen zu ergreifende Maßnahmen und Ansprechpartner benannt werden.