SRQ-ID: 1220

SRQ	
Themenbereich:	Dezentrale Komponenten
Schlagwort:	Anforderungen Einsatzumgebung eHealth-Kartenterminals
Stand:	05.07.2012
Status:	freigegeben
Klassifizierung:	öffentlich
Zu Dokument	
Referenz:	[gemSpec_KT]
Version:	2.6.0
Bezug (Kap., Tab., Abb.):	3.6.8.2
Ersetzte SRQ:	

Gültig ab:	16.07.2012	Verbindlichkeit:	normativ
Zulassungsrelevanz[1]:	☒ SRQ ist nicht zulassungsrelevant.		
	☐ SRQ ist für zukünftige Zulassungsanträge ab dem „gültig ab"-Datum relevant. ☐ SRQ ist für laufende Zulassungsanträge, deren Testobjekte NACH dem „gültig ab"-Datum bei der gematik eingereicht werden, relevant. ☐ SRQ ist zusätzlich für laufende Zulassungsanträge, deren Testobjekte VOR dem „gültig ab"-Datum bei der gematik eingereicht werden, relevant. ☐ Vor dem „gültig ab"-Datum erteilte Zulassungen müssen erneuert werden.		
Bemerkung zur Zulassungsrelevanz:			
Betroffene Zulassungs-verfahren:	☐ elektronische Gesundheitskarte (eGK) ☐ Validierung Personalisierungsdaten eGK ☐ Heilberufausweis (HBA) ☐ Secure Module Card Typ A/B (SMC-A/B) ☐ eHealth-BCS-Kartenterminal ☐ mobiles Kartenterminal (mobKT) ☐ Bestätigung der Vorlage von Sicherheitsgutachten für die eGK-		

[1] Bei einer festgestellten Zulassungsrelevanz sind Mehrfachnennungen möglich.

	Herausgabeprozesse ☐ Weitere:
Versionierung Produkttyp:	☒ Die Versionierung von Produkttypen ist nicht betroffen. ☐ Die Versionierung von Produkttypen ist wie folgt betroffen:
Zusätzliche Anlagen:	
Anmerkungen:	

Frage:

Sind Anforderungen an Einsatzumgebungen in der Spezifikation oder dem Protection Profile führend?

Antwort:

Die Anforderungen an die Einsatzumgebungen von Kartenterminals werden durch die Annahmen im Schutzprofil des eHealth-Kartenterminals festgelegt. Daher wird das Kapitel 3.6.8.2 wie folgt geändert:

3.6.8.2 Umgebungsanforderungen für Kartenterminals

Die Anforderungen an die Einsatzumgebung der Kartenterminals werden im Kapitel der Annahmen des Schutzprofils [BSI-PP-0032] des BSI festgelegt und müssen vom Hersteller bei der Evaluierung berücksichtigt werden.

~~Nach aktuellen Spezifikationen ergeben sich aus Sicherheitssicht Anforderungen an die Sicherheit des Terminals (siehe SP_PIN_USE_2 in [gemSiKo#AnhE]):~~

~~Die Ausgestaltung der Kartenterminals bzw. der Umgebung MUSS so gestaltet sein, dass von der gematik nicht zugelassene oder möglicherweise kompromittierte Komponenten vom Karteninhaber erkannt werden können. Es DARF NICHT möglich sein,~~

- ~~die geheimen Daten, die im sicheren PIN-Eingabegerät gespeichert sind (Schlüssel und PINs), in Erfahrung zu bringen oder zu verändern, oder~~
- ~~eine Abhörvorrichtung innerhalb des Gerätes einzurichten oder~~
- ~~die Hard- oder Software des sicheren PIN-Eingabegerätes zu verändern.~~

~~Solche Angriffe MÜSSEN am Gerät physischen Schaden in der Art anrichten, dass er beim weiteren Betrieb, bzw. vor der Wiederinbetriebnahme des Gerätes mit hoher Wahrscheinlichkeit entdeckt wird. In der kontrollierten Einsatzumgebung (siehe Kapitel 3.6.8.2.1) ist Das Brechen von Gehäusesiegeln ist ebenfalls als eine derartige physische Beschädigung des Gerätes zu betrachten.~~

Diese übergreifende Sicherheitsanforderung resultiert aus dem Schutzbedarf der nachfolgenden Sicherheitsobjekte:

- Signatur-PIN und Qualifizierte Signatur des Leistungserbringers
  Die Qualifizierte Signatur des Leistungserbringers stellt sehr hohe Anforderungen an die Sicherheit der Signaturkomponenten (siehe [gemSiKo#AnhE]).
- PIN des Versicherten für Autorisierung des Zugriffs auf freiwillige Anwendungen. Der Schutzbedarf dieser Daten ist sehr hoch, u. a. bezüglich der Vertraulichkeit, und äquivalent zu der PIN für die qualifizierte Signatur (siehe [gemSiKo#AnhF5.11]). Der Versicherte muss die PIN an einem Gerät eingeben, das nicht in seiner Verantwortung ist.
- Session-Key oder Objekt-Schlüssel
  Der Session-Key, der den sicheren Kanal zwischen Konnektor und KT definiert, ist im KT im Klartext verfügbar. Dies gilt ebenso für Objektschlüssel zur Verschlüsselung langlebiger medizinischer Objekte.

Die Maßnahmen zum Schutz von diesen Informationsobjekten mit hohem und sehr hohem Schutzbedarf (z. B. PINs, Schlüssel, medizinische Daten) drücken sich im PP des Kartenterminals in organisatorischen Anforderungen der Einsatzumgebungen und sicherheitstechnischen Maßnahmen des Kartenterminals aus. Generell DÜRFEN Daten aus der Telematikinfrastruktur (TI) NICHT persistent im Kartenterminal gespeichert werden, außer (und dieses ist die einzige Ausnahme) Konfigurationsdaten zwischen Konnektor und Kartenterminal (inkl. Shared Secret für das Pairing, siehe Kapitel 3.7).

Folgende typische Einsatzumgebungen von Kartenterminals werden im Gesundheitswesen unterschieden:

- Kontrollierte Einsatzumgebung
- Nicht überwachte Einsatzumgebung

Für jede der beiden Einsatzumgebungen wird ein eigenes Schutzprofil definiert. Dies hat zur Folge, dass hinsichtlich ihres physischen Schutzes und der organisatorischen Verpflichtung des Leistungserbringers zwei unterschiedliche Typen von eHealth-Kartenterminals zur Ausgestaltung kommen können.

3.6.8.2.1 Anforderungen an kontrollierte Einsatzumgebung

Bestehende zum Signaturgesetz konforme Kartenterminals kommen derzeit ohne hohen physikalischen Schutz aus, da Anforderungen an eine sichere Umgebung in die Verantwortung des Signaturkarteninhabers gestellt werden (lokaler Anschluss an den PC, Verbindungskabel im Sichtbereich etc.) Der Signaturkarteninhaber hat dafür Sorge zu tragen, dass in der Arbeitsumgebung, in der eine sichere elektronische Signatur erstellt wird, die geforderten Rahmenbedingungen der nach [SigG01] bestätigten Komponenten und Verfahren eingehalten werden. Dazu hat der Leistungserbringer (siehe [BÄK_POL]) sowohl alle technischen als auch organisatorischen Maßnahmen zu ergreifen, welche nur einen befugten Zugriff auf diese Arbeitsumgebung ermöglicht.

Es wird als Umgebungsanforderung der Kartenterminals angenommen,

- dass sich der Nutzer vor der Inbetriebnahme durch die Kontrolle der Unversehrtheit der Siegel überzeugt, dass keine sicherheitstechnischen Veränderungen am Kartenterminal bzw. an den Kabelanschlüssen

vorgenommen wurden. Der Leistungserbringer MUSS sich daher, vor jeder Verwendung des Terminals von der Unversehrtheit des Siegels überzeugen, falls das Terminal seit der letzten Verwendung unbeaufsichtigt war. Ein manipuliertes Terminal wird durch Veränderungen am Gehäuse oder an Veränderungen an den Sicherheitssiegeln erkennbar (siehe [TR-03120#9]).

- dass dem Benutzer eine unbeobachtete Eingabe der Identifikationsdaten (PIN) gewährleistet wird.
- dass der Benutzer die PIN über den Nummernblock des Kartenterminals eingibt und während der PIN-Eingabe den Status des Kartenterminals dahingehend überprüfen kann, ob der Modus der sicheren PIN-Eingabe aktiv ist (s. Kap. 3.6.5).

Durch organisatorische Maßnahmen MUSS der Leistungserbringer die Möglichkeiten für einen Angriff verringern und die Sicherheitsrisiken vermindern. Dies beinhaltet beispielsweise, dass

- der unbeaufsichtigte Zugriff von unbefugten Personen auf das Terminal unterbunden ist (z. B. weil der Arzt bzw. vertrauenswürdiges Personal immer im Zimmer ist) und der Raum ansonsten verschlossen ist;
- ein unbeaufsichtigter Zugriff auf das Terminal für unbefugte Personen nicht lange genug möglich ist, um einen Angriff auszuführen;
- die Mitnahme von notwendigem Werkzeug oder manipulierter Nachbauten eines Kartenterminals in die kontrollierte Einsatzumgebung nicht möglich ist;
- das Praxispersonal mit den Sicherheitsvorkehrungen, die zum Schutz des Terminals notwendig sind, vertraut gemacht und geschult wird.

Bei Einhaltung dieser organisatorischen Maßnahmen stellt die Versiegelung des Terminals einen hinreichenden physischen Schutz dar. Weiterführende Anforderungen an die kontrollierte Einsatzumgebung sind dem Protection Profile [BSI-PP-0032] zu entnehmen.

3.6.8.2.2 Anforderungen an nicht-überwachte Einsatzumgebung

Da in einer nicht-überwachten Einsatzumgebung eine Einschränkung eines Angriffs durch organisatorische Maßnahmen nicht möglich ist, MUSS ein Angriff an dem Kartenterminal einen physischen Schaden in der Art anrichten, dass das Kartenterminal nicht mehr funktionsfähig ist. Eine reine Versiegelung eines Terminalgehäuses kann in einer solchen Umgebung nicht als geeignet erachtet werden.