SRQ - Specification Related Question

SRQ-ID: 0872

Betrifft (wird vom FLS (optional vom Erfasser) ausgefüllt):

Themenkreis	Dezentrale Komponenten
Schlagwort	Sicherung Managementschnittstelle
zu Dokument / Datei	gemSpec_KT
Version	2.6.0
Bezug (Kap., Abschnitt, Tab., Abb.)	3.5.14, 3.6.6

Stichwort: Sicherung Managementschnisttstelle

Frage:

Welche Änderungen haben sich an den Anforderungen zur Sicherung der Managementschnittstelle ergeben?

Betrifft (wird vom PB ausgefüllt):

Gültig ab Release	0.5.2	Verbindlichkeit	
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version	2.6.2	voraussichtl. Zeitpunkt	19.09.08
Anmerkungen:			
Status	☒ erfasst ☐ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☐ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort: Die überarbeiteten Anforderungen an die Managementschnittstelle sind in Kapitel 3.5.14 sowie 3.6.6 aufgenommen

3.5.14 Terminal Managementverfahren

Ein Kartenterminal MUSS über eine direkte Managementschnittstelle verfügen, welche zur Interaktion das Display sowie die Tastatur des Kartenterminals nutzt (siehe auch Kapitel 3.6.6.2). Es MUSS über die direkte Managementschnittstelle mindestens möglich sein weitere Managementschnittstellen (siehe unten), soweit vorhanden, zu aktivieren und zu deaktivieren. Das Aktivieren und Deaktivieren von Managementschnittstellen MUSS ausschließlich an der direkten Managementschnittstelle des Kartenterminals erfolgen. Die Administration des Kartenterminals MUSS ausschließlich über die direkte Managementschnittstelle oder aktivierte Managementschnittstellen erfolgen.

Neben der direkten Managementschnittstelle, KANN das Kartenterminal über weitere Managementschnittstellen verfügen, um über das Netzwerk administriert werden zu können. Diese Schnittstellen KÖNNEN sowohl vom Konnektor, von Administrationsprogrammen der Hersteller als auch über das Webinterface durch den Administrator bedient werden (siehe auch Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**). Die LAN Schnittstelle zur Administrierung MUSS mittels TLS gesichert sein. (siehe Kapitel 3.6.6.1).

Hinweis: Aus den Sicherheitsforderungen des PP kann es sich ergeben, dass einzelne Managementfunktionen als sicherheitsrelevant eingestuft werden und daher Interaktionen an der lokalen Managementschnittstelle des KTs erfordern. Näheres hierzu ergibt sich aus dem PP und ist herstellerspezifisch umzusetzen.

3.6.6 Terminal Managementverfahren

Die Managementschnittstellen zur Administrierung des eHealth-Kartenterminals erlauben das Abfragen und Ändern der sicherheitskritischen Konfiguration erst nach erfolgreicher Authentisierung.

Es MUSS sichergestellt sein, dass Änderungen nur von berechtigten Akteuren durchgeführt werden können. Vor der Anzeige von sicherheitsrelevanten Konfigurationsdaten MUSS eine Authentifizierung stattfinden. Es MUSS mindestens die Rolle Administrator umgesetzt sein und es MUSS sichergestellt sein, dass ausschließlich die Rolle Administrator Einstellungen zur Benutzerverwaltung, Netzwerkkonfiguration, den Terminal- und Slot-Namen gemäß Abschnitt **Fehler! Verweisquelle konnte nicht gefunden werden.** ändern, und Pairinginformation gemäß Abschnitt **Fehler! Verweisquelle konnte nicht gefunden werden.** löschen kann.

Falls die Rolle Benutzer umgesetzt ist, MUSS sichergestellt sein, dass der Benutzer nur berechtigt ist, die aktuellen Einstellungen anzuzeigen und sein eigenes Kennwort zu ändern.

~~Das Einsehen der aktuellen Konfiguration MUSS geschützt werden, da die Daten der Terminalkonfiguration Informationen enthalten können, die für DoS und ähnliche Attacken benutzt werden können.~~ Medizinische und personenbezogene Daten DÜRFEN NICHT über die Managementschnittstelle übertragen oder angezeigt werden.

3.6.6.1 Sicherung der administrativen TLS-Verbindung

~~*Die Anforderungen an die Passwörter zur Sicherung der Managementschnittstelle stehen noch aus.*~~

Die Verbindung zu den Netzwerk-basierten Managementschnittstellen MUSS immer mindestens mit TLS 1.0 gemäß [RFC2246] gesichert sein. Zusätzlich SOLL sie auch mittels TLS 1.1 gemäß [RFC4346] gesichert werden können. In TLS Extension [RFC3546] beschriebene funktionale Erweiterungen MÜSSEN umgesetzt werden[3]. Der Port des Administrationsservices DARF NICHT gleich dem SICCT Port sein. Als

[3]Ein mit dem Schlüsselwort „MUSS“ gekennzeichneter RFC ist verpflichtend in dem Sinne, dass die normativen Vorgaben dieses RFC gemäß RFC2119 Gültigkeit haben. Der [RFC3546] zu TLS-Extensions gibt nicht normativ vor, dass die TLS-Extensions unterstützt werden müssen, sondern nur, wie sie ggf. umzusetzen sind. Daher ist keine der Anforderungen des [RFC3546] verpflichtend umzusetzen, werden sie umgesetzt, sind sie jedoch RFC-konform umzusetzten.

Authentisierungsverfahren für diese administrative TLS-Verbindung MUSS mindestens einseitige Authentisierung eingesetzt werden[4]. Zur Sicherung der administrativen TLS-Verbindung KANN auch gegenseitige Authentisierung eingesetzt werden. Im Fall der einseitigen Authentisierung MUSS sich das Kartenterminal (Server) gegenüber dem Client (z. B. Webbrowser) authentisieren.

Das Kartenterminal MUSS für die administrative TLS-Verbindung die in [gemSpec_Krypt#6.4.4] angeführten (stärkeren) Algorithmen unterstützen. Sofern eine SM-KT vorhanden ist, SOLL für den TLS Aufbau das Schlüsselmaterial der SM-KT verwendet werden (ID.SMKT.AUT). Falls keine SM-KT vorhanden ist, MUSS das Kartenterminal Schlüsselmaterial sowie ein zugehöriges Zertifikat zur Verfügung stellen (z. B. in der Firmware). Private Schlüssel MÜSSEN ausreichend vor Veränderung und Auslesen geschützt gespeichert werden. Öffentliche Schlüssel und Zertifikate MÜSSEN ausreichend vor Veränderung geschützt gespeichert werden. Es sei darauf hingewiesen, dass die Nutzung desselben Zertifikats für alle Kartentermials einer Baureihe mit einem Risiko behaftet ist, da der zugehörige private Schlüssel auf allen Kartenterminals einer Baureihe verteilt ist. Details zu den Vorgaben an die Zertifikate sind Bestandteil der Sicherheitsevaluierung.

3.6.6.2 Anforderungen an Kennwörter zur Sicherung der Managementschnittstelle

Im Folgenden werden die Anforderungen an die Kennwörter zur Sicherung der Managementschnittstellen aufgeführt. Das Administrator-Kennwort, welches lokal, direkt an der Tastatur des Kartenterminals (im Folgenden direkte Managementschnittstelle siehe auch Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**) eingegeben wird, wird als Direkt-Kennwort bezeichnet.

Nach erstmaliger Eingabe des Direkt-Kennwortes (siehe Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**) MUSS die direkte Managementschnittstelle aktiviert werden. Beim Aktivieren einer weiteren Management-Schnittstelle an der direkten Management-Schnittstelle KANN für diese weitere Management-Schnittstelle ein neues Administrator-Kennwort an der direkten Management-Schnittstelle abgefragt werden. Dieses neue Administrator-Kennwort KANN für alle anderen verfügbaren Management-Schnittstellen als deren jeweiliges Administrator-Kennwort übernommen werden. Die Kennwörter MÜSSEN für jede Schnittstelle separat gesetzt werden können und für jede Schnittstelle MUSS ein eigener Fehlerzähler vorgehalten werden. Der Fehlerzähler DARF NICHT über externe Schnittstellen verändert werden können. Der Fehlerzähler KANN von einem Benutzer über die Managementschnittstelle abgefragt werden. Kennwörter MÜSSEN geschützt gespeichert werden, sodass sie nicht ausgelesen oder verändert werden können.

Der Zugang des jeweiligen Benutzers oder Administrators zur direkten Managementschnittstelle MUSS ab der dritten aufeinander folgenden ungültigen Kennworteingaben an dieser Schnittstelle gesperrt werden, wobei die Dauer der Sperrzeit von der Anzahl aufeinander folgender Fehlversuche abhängig ist und gilt (siehe Tabelle 1):

[4] Im Gegensatz zur SICCT-TLS-Verbindung, bei der nur gegenseitige Authentisierung erlaubt ist.

Tabelle 1 Mindestsperrzeiten in Abhängigkeit der Anzahl ungültiger Kennworteingaben

Anzahl der aufeinander folgenden ungültigen Kennworteingaben	Mindestsperrzeit für die Kennworteingabe
3-6	1 Minute
7-10	10 Minuten
11-20	1 Stunde
ab 21	1 Tag

Zudem MUSS das Kartenterminal Fehlerzähler im spannungslosen Zustand erhalten. Das Kartenterminal KANN die bereits verstrichene Wartezeit während einer Direkt-Kennwort Eingabe im spannungslosen Zustand erhalten und den Zugang nach Neustart nur für die verbleibende Zeit sperren. Falls das Kartenterminal die bereits verstrichene Zeit nicht im spannungslosen Zustand erhält, MUSS die Sperrzeit nach einem Neustart, unabhängig von der bereits verstrichenen Sperrzeit, wieder der dem Fehlerzähler entsprechenden Mindestsperrzeit entsprechen.

Mit Ausnahme der direkten Managementschnittstelle, MUSS der Zugang des jeweiligen Benutzers oder Administrators zu einer Managementschnittstelle nach maximal 3 aufeinander folgenden ungültigen Kennworteingaben an dieser Schnittstelle deaktiviert werden. Die Managementschnittstelle KANN an dieser Schnittstelle auch für alle Benützer deaktiviert werden.

Für alle Kennwörter zur Sicherung einer Managementschnittstelle gelten folgende Anforderungen.

- Kennwörter MÜSSEN mindestens 8 Zeichen lang sein und mindestens aus Ziffern (‚0' bis ‚9') bestehen. Kennwörter KÖNNEN auch aus einer Mischung aus Ziffern, Buchstaben und Sonderzeichen bestehen.

- Die Benutzer-ID DARF NICHT Bestandteil des Kennwortes sein. Beim Kennwortwechsel DARF das letzte genutzten Kennworte NICHT als gültiges neues Kennwort akzeptiert werden. Kennwörter DÜRFEN NICHT auf programmierbaren Funktionstasten gespeichert werden. Bei der Eingabe DARF das Kennwort NICHT im Klartext angezeigt werden.

Zusätzliche, nicht normative Informationen zur Handhabung von Kennwörtern sind im vom BSI herausgegebenen Maßnahmenkatalog Organisation (M 2) Abschnitt 11 „Regelungen des Passwortgebrauchs" [BSI-M2.11] beschrieben.