SRQ - Specification Related Question

SRQ-ID: 0984

Betrifft:

Themenkreis	Dezentrale Komponenten
Schlagwort	Authentifikationsmechanismus
zu Dokument / Datei	gemSpec_MobKT
Version	1.1.1
Bezug (Kap., Abschnitt, Tab., Abb.)	5.5.1

Stichwort: Authentifikationsmechanismus

Frage:

Welche Änderungen haben sich an den Anforderungen an den Authentifikationsmechanismus ergeben?

Betrifft:

Gültig ab Release	0.5.2	Verbindlichkeit	
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 Spezifikation wurde wie folgt überarbeitet:

5.5.1 Authentifikationsmechanismus

Der Authentifikationsstatus MUSS nach maximal 15 Minuten Benutzerinaktivität zurückgesetzt werden bzw. bei Abschalten des Gerätes zurückgesetzt werden [A_04401].

[…]

Migrationsfähige mobile Kartenterminals MÜSSEN die Rolle Administrator vorsehen [A_41566], es KÖNNEN weitere Rollen z. B. Benutzer existieren [A_41567].

Für migrationsfähige mobile Kartenterminals MUSS sichergestellt sein, dass ausschließlich die Rolle Administrator berechtigt ist Firmwareupdates einzuspielen, die Uhrzeit einzustellen, sowie das Gerät in den Auslieferungs- bzw. Werkszustand zurückzusetzen [A_41568]. Bei Rücksetzen des Gerätes in den Auslieferungszustand MÜSSEN alle Daten im Zwischenspeicher gelöscht werden [A_41569]. Ist ausschließlich die Rolle Administrator vorgesehen, MUSS diese auf die zwischengespeicherten Daten zugreifen können [A_41570] und bei der Authentifizierung KANN die Angabe des Usernamens entfallen [A_41571].

Kennwörter

Die Anforderungen dieses Kapitels MÜSSEN von Kartenterminals die von Ausbaustufe 1 zu Ausbaustufe 2 migrationsfähig sind umgesetzt werden. Nicht migrationsfähige Kartenterminals können die Anforderungen dieses Kapitels umsetzten.

Kennwörter MÜSSEN geschützt gespeichert werden, sodass sie nicht über externe Schnittstellen ausgelesen oder verändert werden können [A_41572]. Für alle Kennwörter zur Sicherung der Managementschnittstelle gelten folgende Anforderungen.

- Kennwörter MÜSSEN mindestens 4 Zeichen lang sein und mindestens aus Ziffern (‚0' bis ‚9') bestehen [A_41573]. Kennwörter KÖNNEN auch aus einer Mischung aus Ziffern, Buchstaben und Sonderzeichen bestehen [A_41574].
- Die Benutzer-ID DARF NICHT als Teilzeichenkette Bestandteil des Kennwortes sein [A_41575]. Kennwörter DÜRFEN NICHT auf programmierbaren Funktionstasten gespeichert werden können [A_41576]. Bei der Eingabe DARF das Kennwort NICHT im Klartext angezeigt werden [A_41577].

Es MUSS ein Fehlerzähler für die Fehlversuche bei der Kennworteingabe vorgehalten werden [A_41578]. Der Fehlerzähler DARF NICHT über externe Schnittstellen verändert werden können [A_41579]. Der Fehlerzähler KANN von einem Benutzer über die Managementschnittstelle abgefragt werden [A_41580]. Der Zugang des jeweiligen Benutzers oder Administrators zur Managementschnittstelle MUSS ab der dritten aufeinander folgenden ungültigen Kennworteingabe an gesperrt werden, wobei die Dauer der Sperrzeit von der Anzahl aufeinander folgender Fehlversuche abhängig ist und gilt (siehe Tabelle) [A_41581]:

Tabelle 3 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 der Fehlerzähler im spannungslosen Zustand erhalten werden [A_41582]. Die bereits verstrichene Wartezeit während einer Direkt-Kennwort Eingabe KANN im spannungslosen Zustand erhalten werden und der Zugang nach Neustart nur für die verbleibende Zeit gesperrt werden [A_41583]. Falls die bereits verstrichene Zeit nicht im spannungslosen Zustand erhalten bleibt, MUSS die Sperrzeit nach einem Neustart, unabhängig von der bereits verstrichenen Sperrzeit, wieder der dem Fehlerzähler entsprechenden Mindestsperrzeit entsprechen [A_41584].

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. Im Auslieferungs- bzw. Werkszustand MUSS der Anwender, ausgehend von einem initialen Passwort, bei der ersten Benutzung gezwungen werden das Passwort zu ändern [A_41585].

A6 - Verzeichnis der Ausgangsanforderungen

A_04401	S	Der Authentifikationsstatus am mobilen Kartenterminal der Ausbaustufe 1 MUSS nach maximal 15 Minuten Benutzerinaktivität zurückgesetzt werden bzw. bei Abschalten des Gerätes zurückgesetzt werden	5.5.1
A_41566	S	Migrationsfähige mobile Kartenterminals der Ausbaustufe 1 MÜSSEN die Rolle Administrator vorsehen, es KÖNNEN weitere Rollen z. B. Benutzer existieren.	5.5.1
A_41567	N	Mobile Kartenterminals der Ausbaustufe 1 KÖNNEN Rollen z. B. Benutzer implementieren.	5.5.1
A_41568	S	Für migrationsfähige mobile Kartenterminals MUSS sichergestellt sein, dass ausschließlich die Rolle Administrator berechtigt ist Firmwareupdates einzuspielen, die Uhrzeit einzustellen, sowie das Gerät in den Auslieferungs- bzw. Werkszustand zurückzusetzen.	5.5.1
A_41569	S	Bei Rücksetzen des mobilen Kartenterminal der Ausbaustufe 1 in den Auslieferungszustand MÜSSEN alle Daten im Zwischenspeicher gelöscht werden.	5.5.1
A_41570	S	Ist am mobilen Kartenterminal der Ausbaustufe 1 ausschließlich die Rolle Administrator vorgesehen, MUSS diese auf die zwischengespeicherten Daten zugreifen können und bei der Authentifizierung KANN die Angabe des Usernamens entfallen.	5.5.1
A_41571	S	Ist am mobilen Kartenterminal der Ausbaustufe 1 ausschließlich die Rolle Administrator vorgesehen, KANN die Angabe des Usernamens entfallen.	5.5.1
A_41572	S	Kennwörter MÜSSEN durch das mobile Kartenterminal der Ausbaustufe 1 geschützt gespeichert werden, sodass sie nicht über externe Schnittstellen ausgelesen oder verändert werden können.	5.5.1
A_41573	I	Die an einem migrationsfähigen mobilen Kartenterminal der Ausbaustufe 1 eingesetzten Kennwörter MÜSSEN mindestens 4 Zeichen lang sein und mindestens aus Ziffern (‚0’ bis ‚9’) bestehen.	5.5.1
A_41574	S	Die an einem migrationsfähigen mobilen Kartenterminal der Ausbaustufe 1 eingesetzten Kennwörter KÖNNEN auch aus einer Mischung aus Ziffern, Buchstaben und Sonderzeichen bestehen	5.5.1
A_41575	S	Die an einem migrationsfähigen mobilen Kartenterminal der Ausbaustufe 1 eingesetzten Kennwörter DÜRFEN die Benutzer-ID NICHT als Teilzeichenkette enthalten.	5.5.1
A_41576	S	Kennwörter DÜRFEN NICHT auf programmierbaren	5.5.1

		Funktionstasten eines migrationsfähigen mobilen Kartenterminals der Ausbaustufe 1 gespeichert werden können.	
A_41577	S	Bei der Eingabe einer Kennwortes am migrationsfähigen mobilen Kartenterminals der Ausbaustufe 1 DARF das Kennwort NICHT im Klartext angezeigt werden.	5.5.1
A_41578	S	Es MUSS bei migrationsfähigen mobilen Kartenterminal der Ausbaustufe 1 ein Fehlerzähler für die Fehlversuche bei der Kennworteingabe vorgehalten werden	5.5.1
A_41579	S	Der Fehlerzähler falscher Kennworteingaben des migrationsfähigen mobilen Kartenterminals der Ausbaustufe 1 DARF NICHT über externe Schnittstellen verändert werden können	5.5.1
A_41580	S	Der Fehlerzähler falscher Kennworteingaben KANN von einem Benutzer über die Managementschnittstelle des migrationsfähigen mobilen Kartenterminals der Ausbaustufe 1 abgefragt werden	5.5.1
A_41581	S	Der Zugang des jeweiligen Benutzers oder Administrators zur Managementschnittstelle des migrationsfähigen mobilen Kartenterminals der Ausbaustufe 1 MUSS ab der dritten aufeinander folgenden ungültigen Kennworteingabe an gesperrt werden, wobei die Dauer der Sperrzeit von der Anzahl aufeinander folgender Fehlversuche abhängig ist und gilt: Bei 3-6 Fehlversuchen beträgt die Sperrzeit 1 Minute Bei 7-10 Fehlversuchen beträgt die Sperrzeit 10 Minuten Bei 11-20 Fehlversuchen beträgt die Sperrzeit 1 Stunde ab 21 Fehlversuchen beträgt die Sperrzeit 1 Tag	5.5.1
A_41582	S	Zudem MUSS der Fehlerzähler falscher Kennworteingaben eines migrationsfähigen mobilen Kartenterminals der Ausbaustufe 1 im spannungslosen Zustand erhalten werden.	5.5.1
A_41583	S	Die bereits verstrichene Wartezeit während einer Direkt-Kennwort Eingabe KANN im spannungslosen Zustand erhalten werden und der Zugang nach Neustart nur für die verbleibende Zeit gesperrt werden	5.5.1
A_41584	S	Falls die bereits verstrichene Wartezeit auf die nächste Kennworteingabe vom migrationsfähigen mobilen Kartenterminal der Ausbaustufe 1 nicht im spannungslosen Zustand erhalten bleibt, MUSS die Sperrzeit nach einem Neustart, unabhängig von der bereits verstrichenen Sperrzeit, wieder der dem Fehlerzähler entsprechenden Mindestsperrzeit entsprechen.	5.5.1
A_41585	S	Im Auslieferungs- bzw. Werkszustand des migrationsfähigen mobilen Kartenterminals der Ausbaustufe 1 MUSS der Anwender, ausgehend von einem initialen Passwort, bei der ersten Benutzung gezwungen werden das Passwort zu ändern.	5.5.1

B5 – Referenzierte Dokumente

[BSI-M2.11]	BSI (Oktober 2007): IT-Grundschutzkataloge – Maßnahmenkatalog Organisation (9. Ergänzungslieferung) http://www.bsi.bund.de/gshb/deutsch/m/m02011.htm