
1 Änderungsbeschreibung

Ein PS sollte nicht EjectCard und RequestCard aufrufen müssen, falls ein HBA in erhöhtem Sicherheitszustand ist. Das kann der Konnektor mit Hoheit über die Karten selbst durchführen. Weiterhin sollte bei EjectCard in dem Zusammenhang kein Fehlerevent gemeldet werden.

Diese Thematik wird in der Änderung C_11840 angegangen, indem innerhalb ActivateComfortSignature im Fall eines HBA in erhöhtem Sicherheitszustand TUC_KON_024 aufgerufen wird. In dem Fall gibt die Operation zusätzlich ein Ereignis aus, damit das PS erkennen kann, dass ein Karten-Reset mit daraufhin erneuter HBA-PIN-Abfrage erfolgte.

2 Änderung in gemSpec_Kon

A_19107 wird durch A_10107-01 ersetzt:

A_19107-01 - Operation ActivateComfortSignature

Der Signatordienst des Konnektors MUSS an der Clientschnittstelle eine Operation ActivateComfortSignature anbieten.

Tabelle 1: TAB_KON_874 ActivateComfortSignature

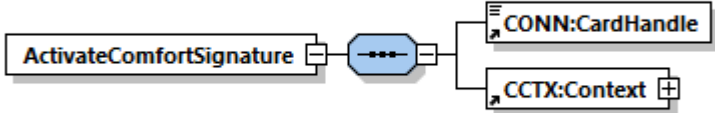
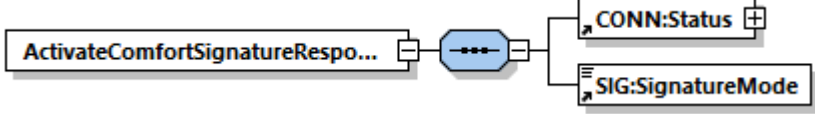
| | | |
|------------------------|---|---|
| Name | ActivateComfortSignature | |
| Beschreibung | Diese Operation aktiviert die Komfortsignatur für einen HBA bezogen auf einen Aufrufkontext. | |
| Aufrufparameter |  <pre> sequenceDiagram participant Client participant Service Client->>Service: ActivateComfortSignature activate Service Service->>Client: CONN:CardHandle Service->>Client: CCTX:Context deactivate Service </pre> | |
| | Name | Beschreibung |
| | CONN:CardHandle | Identifiziert die zu adressierende Karte. Es wird nur der HBA unterstützt. |
| | CCTX:Context | MandantId, ClientSystemId, WorkplaceId, UserId verpflichtend zu übergeben; MandantId, WorkplaceId nicht ausgewertet |
| Rückgabe |  <pre> sequenceDiagram participant Client participant Service Client->>Service: ActivateComfortSignature activate Service Service->>Client: CONN:Status Service->>Client: SIG:SignatureMode deactivate Service </pre> | |
| | CONN:Status | Enthält den Ausführungsstatus der Operation. |
| | SIG:SignatureMode | Signaturmodus des HBA Enthält bei erfolgreicher Ausführung der Operation den Wert „COMFORT“ |
| Vorbedingungen | Keine | |
| Nachbedingungen | Keine | |

Tabelle 2: TAB_KON_877 Ablauf ActivateComfortSignature

| Nr. | Aufruf Technischer Use Case oder Interne Operation | Beschreibung |
|-----|--|---|
| 1. | checkArguments | Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab. |
| 2. | TUC_KON_000 „Prüfe Zugriffsberechtigung“ | Die Prüfung erfolgt durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientsystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; userId = \$context.userId; cardHandle = \$cardHandle } Tritt dabei Fehler 4018 auf, setze CardNeedsReset = true, andernfalls false. Tritt bei der Prüfung ein anderer Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab. |
| 3. | TUC_KON_026 „Liefere CardSession“ | Ermittle CardSession über TUC_KON_026 { mandantId = \$context.mandantId; clientsystemId = \$context.clientsystemId; cardHandle = \$context.cardHandle; userId = \$context.userId } |
| 4. | TUC_KON_171 „Komfortsignatur einschalten“ | Der Komfortsignaturmodus wird für das Tupel (CardSession, CardNeedsReset) eingeschaltet. Tritt hierbei ein Fehler auf, bricht die Operation ab. |

Tabelle 3: TAB_KON_879 Fehlercodes ActivateComfortSignature

| Fehlercode | ErrorType | Severity | Fehlertext |
|---|-----------|----------|---|
| Neben den Fehlercodes der aufgerufenen TUCs können folgende weiteren Fehlercodes auftreten: | | | |
| 4000 | Technical | Error | Syntaxfehler |
| 4270 | Technical | Error | UserId wurde in den letzten 1.000 Vorgängen bereits verwendet |
| 4272 | Technical | Error | UserId nicht zulässig |

[<=, Konnektor Highspeed, Konnektor PTV5, Konnektor PTV5Plus, Konnektor PTV6, Konnektor PTV4Plus, funkt. Eignung: Test Produkt/FA]

[A_19104-04](#) wird durch [A_19104-05](#) ersetzt:

A_19104-05 - TUC_KON_171 „Komfortsignatur einschalten“

Der Konnektor MUSS den technischen Use Case TUC_KON_171 „Komfortsignatur einschalten“ umsetzen.

Tabelle 4: TAB_KON_883 – TUC_KON_171 „Komfortsignatur einschalten“

| Element | Beschreibung |
|----------------|--|
| Name | TUC_KON_171 „Komfortsignatur einschalten“ |
| Beschreibung | Zum Einschalten des Komfortsignaturmodus wird die PIN.QES verifiziert und der Signaturmodus „Comfort“ für die cardSession gesetzt. |
| Auslöser | <ul style="list-style-type: none">• Operation ActivateComfortSignature• Aufruf durch ein Fachmodul |
| Vorbedingungen | Der Karte muss gesteckt sein. |
| Eingangsdaten | <ul style="list-style-type: none">• cardSession - <i>verpflichtend</i> (nur HBA erlaubt)• cardNeedsReset - <i>verpflichtend</i> |
| Komponenten | Konnektor, Kartenterminal, Karte (HBA) |
| Ausgangsdaten | <ul style="list-style-type: none">• signatureMode |

| Element | Beschreibung |
|----------------|--|
| Standardablauf | <p>1. Prüfe <code>SAK_COMFORT_SIGNATURE = Enabled</code></p> <p>2. Die am Vorgang beteiligten Ressourcen (Karte sowie PIN-Pad und Display des PIN-Eingabe-Kartenterminals) werden für die exklusive Nutzung durch diesen Vorgang reserviert. Die Reservierung der Karte erfolgt durch Aufruf von <code>TUC_KON_023 „Karte reservieren“ { cardSession; doLock = true }</code></p> <p>3. Wenn <code>cardNeedsReset == true</code>:</p> <ul style="list-style-type: none"> • Rufe <code>TUC_KON_024 „Karte zurücksetzen“</code> auf: <code>TUC_KON_024 {cardSession}</code> • Tritt dabei ein Fehler auf, bricht die Operation mit Fehlercode aus <code>TUC_KON_024</code> ab. • Führe <code>TUC_KON_256 { topic = „CARD/RESET“; eventType = Op; severity = Info; parameters = ("description=„Karte wurde während einer Konnektoroperation zurückgesetzt“, CARD_SESSION=cardSession"); doLog=false; doDisp = true }</code> aus <p>Andernfalls wird Schritt 3 übersprungen.</p> <p>Der Zugriff auf die Karte im Schritt 4 muss im DF.QES erfolgen. Das DF.QES darf danach nicht verlassen werden, damit der PIN-Status der PIN.QES erhalten bleibt.</p> <p>4. Die Einschaltung der Komfortsignatur wird durch den Anwender autorisiert. Dies erfolgt durch Aufruf von <code>TUC_KON_012 „PIN verifizieren“ { cardSession; workplaceId; pinRef = PIN.QES; verificationType = Mandatorisch }</code> Für die Anzeige am Kartenterminal ist die Displaymessage für „Komfortsignatur aktivieren“ aus <code>TAB_KON_090</code> zu verwenden.</p> <p>5. Setze <code>CARDSESSION.SIGNMODE = Comfort</code></p> <p>6. Starte Komfortsignatur-Timer für die <code>cardSession</code> bei „0“</p> <p>7. Die reservierten Ressourcen (Karte sowie PIN-Pad und Display des PIN-Eingabe-Kartenterminals) werden wieder freigegeben. Zur Freigabe der Karte wird <code>TUC_KON_023 „Karte reservieren“ { cardSession; doLock = false }</code> aufgerufen.</p> |

| Element | Beschreibung |
|----------------------------|--|
| Varianten/ Alternativen | Keine |
| Fehlerfälle | <p>Fehler in den folgenden Schritten des Standardablaufs führen zum Abbruch mit den ausgewiesenen Fehlercodes:</p> <p>(->1) Komfortsignaturfunktion im Konnektor nicht aktiviert: Fehlercode 4263</p> <p>(->) Keine Komfortsignatursession für den HBA aktivierbar, da Maximalzahl an parallelen Komfortsignatursessions erschöpft: Fehlercode 4278</p> <p>(->2) Fehler bei der Reservierung von Ressourcen: Fehlercode 4060</p> <p>(->3) Karte ist kein HBA, sondern HBA-Vorläuferkarte: Fehlercode 4274</p> <p>(->3) pinResult = BLOCKED: Fehlercode 4275</p> <p>(->3) pinResult = REJECTED: Fehlercode 4276</p> <p>(->4) Fehler beim Setzen des Signaturmodus: Fehlercode 4267</p> <p>(->5) Fehler beim Starten des Komfortsignatur-Timers: Fehlercode 4267</p> <p>Im Fehlerfall, inklusive Timeout bei der PIN-Eingabe, oder bei Abbruch durch den Benutzer (Fehler 4049):</p> <ul style="list-style-type: none"> a) ... MUSS (ab Schritt 5) <code>CARDSESSION.SIGNMODE = PIN</code> gesetzt werden b) ... MUSS (ab Schritt 3) <code>DF.QES</code> verlassen werden c) ... MÜSSEN alle reservierten Ressourcen freigegeben werden d) ... MUSS der Fehler immer an das Clientsystem zurückgemeldet werden |

Tabelle 5: TAB_KON_886 Fehlercodes TUC_KON_171 „Komfortsignatur einschalten“

| Fehlercode | ErrorType | Severity | Fehlertext |
|---|-----------|----------|--|
| Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten: | | | |
| 4049 | Technical | Error | Abbruch durch den Benutzer |
| 4060 | Technical | Error | Ressource belegt |
| 4263 | Technical | Error | Komfortsignaturfunktion nicht aktiviert |
| 4267 | Technical | Error | Fehler beim Aktivieren des Komfortsignaturmodus <cardHandle> |
| 4274 | Technical | Error | Komfortsignaturen werden nur für den HBA unterstützt |
| 4275 | Technical | Error | Security Error PIN jetzt gesperrt (BLOCKED) |
| 4276 | Technical | Error | Security Error PIN falsch (REJECTED) |
| 4278 | Technical | Error | Keine Komfortsignatursession mehr verfügbar |

[<=, Konnektor Highspeed, Konnektor PTV5, Konnektor PTV5Plus, Konnektor PTV6, Sich.techn. Eignung: CC-Evaluierung, funkt. Eignung: Test Produkt/FA, Sich.techn. Eignung: Prüfung durch CC-Prüfstelle]

TIP1-A_4584 wird durch TIP1-A_4584-02 ersetzt (Achtung: gleiche Änderung wird auch in [F ML-154193 - PoPP über C2C zwischen eGK und PoPP-Service](#) vorgenommen):

TIP1-A_4584-02 - TUC_KON_024 „Karte zurücksetzen“

Der Konnektor MUSS den technischen Use Case „Karte zurücksetzen“ gemäß TUC_KON_024 umsetzen.

Tabelle 6: TAB_KON_737 – TUC_KON_024 „Karte zurücksetzen“

| Element | Beschreibung |
|----------------|---|
| Name | TUC_KON_024 „Karte zurücksetzen“ |
| Beschreibung | Der technische Use Case setzt die gewählte Karte zurück (alle erreichten Sicherheitszustände werden auf der Karte und in der Verwaltung des Konnektors zurückgesetzt; auf der Karte wird MF selektiert). Ein eventuell laufendes C2C wird dabei abgebrochen. |
| Auslöser | Aufruf durch: <ul style="list-style-type: none"> • Basisdienst • Fachmodul |
| Vorbedingungen | keine |
| Eingangsdaten | <ul style="list-style-type: none"> • ctId – <i>optional/verpflichtend, wenn keine cardSession angegeben ist</i> (Kartenterminalidentifikator) • slotId – <i>optional/verpflichtend, wenn keine cardSession angegeben ist</i> (Nummer des Slots, in dem die Karte steckt) • cardSession – <i>optional/verpflichtend, wenn ctId und slotId nicht angegeben sind</i> (Angabe der CardSession alternativ zur Angabe von ctId und slotId) |
| Komponenten | Karte, Kartenterminal, Konnektor |
| Ausgangsdaten | Keine |
| Standardablauf | <ol style="list-style-type: none"> 1. Wenn cardSession gegeben, dann ermittle ctId und slotId 2. Der Konnektor prüft, dass entweder die Karte nicht reserviert ist oder der Aufrufer im Besitz des Karten-Locks ist. 3. Brich eventuell parallel laufenden TUC_KON_005 ab 4. Sende SICCT RESET ICC für slotId an das Kartenterminal CtID, um einen Warm Reset auszulösen 5. Lösche alle Sicherheitszustände aus CARDSESSION.AUTHSTATE und den Inhalt von CARDSESSION.AUTHBY. |

| Element | Beschreibung |
|--------------------------------|--|
| Varianten/ Alternativen | Keine |
| Fehlerfälle | * Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→2) Der Aufrufer ist nicht im Besitz des Karten-Locks, Fehlercode 4232 (→4) Karte antwortet mit einer spezifischen Fehlermeldung, Fehlercode <Kartenfehlercode gemäß [gemSpec_COS]> |
| Nichtfunktionale Anforderungen | Keine |
| Zugehörige Diagramme | Keine |

Tabelle 7: TAB_KON_544 Fehlercodes TUC_KON_024 „Karte zurücksetzen“

| Fehlercode | ErrorType | Severity | Fehlertext |
|---|-----------|----------|---|
| Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten: | | | |
| 4094 | Technical | Error | Timeout beim Kartenzugriff aufgetreten |
| 4232 | Technical | Error | der Aufrufer ist nicht im Besitz des Karten-Locks |

[<=, Konnektor Highspeed, Konnektor PTV4, Konnektor PTV5, Konnektor PTV5Plus, Konnektor PTV6, Konnektor PTV4Plus, Konnektor eHealth, Sich.techn. Eignung: CC-Evaluierung, funkt. Eignung: Test Produkt/FA, Sich.techn. Eignung: Prüfung durch CC-Prüfstelle]

3 Änderung in gemILF_PS

In Kapitel 4.4.2.2 Verwalten der Komfortsignaturfunktion wird unter A_19259-02 der Freitext wie folgt geändert:

Da der Konnektor die UserID prüft, sobald der HBA einen erhöhten Sicherheitszustand hat, kann die Komfortsignatur nicht aktiviert werden, wenn die PIN.CH für eine Authentifizierungs- oder Entschlüsselungsfunktionen freigeschaltet ist. Aufrufe von `ActivateComfortSignature` mit einer neuen UserID ~~beantwortet der Konnektor mit Fehler 4018.~~ haben daher zur Folge, dass der Konnektor während der Ausführung der Operation den HBA zurücksetzt, um den erhöhten Sicherheitszustand der Karte zu entfernen. Das Primärsystem kann das Ereignis CARD/RESET abonnieren, um über durch den Konnektor zurückgesetzte Karten in Kenntnis gesetzt zu werden.

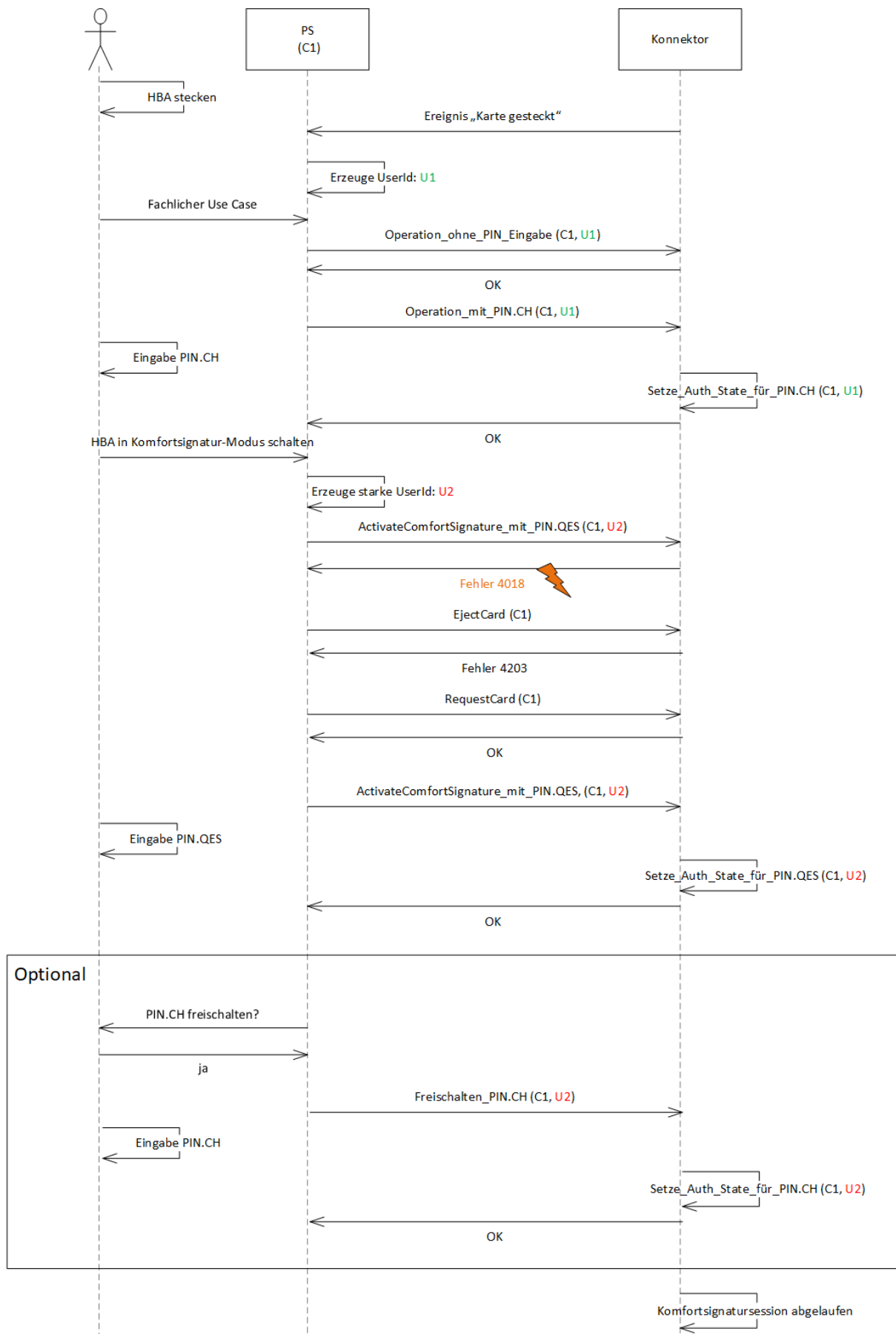
A_21528 wird entfernt:

A_21528 - PS: Zurücksetzen des HBA bei neuer UserID

Das Primärsystem MUSS den HBA vor dem Aufruf von `ActivateComfortSignature` mit den Operationen `EjectCard` und `RequestCard` zurücksetzen, wenn der HBA in einem erhöhten Sicherheitszustand ist oder Fehler 4018 empfangen wurde. [`<=`, PS, nicht prüfrelevant]

Abb. 31 wird angepasst, um Änderungen aus gemSpec_Kon zu entsprechen.

Alte Abbildung:





Neue Abbildung:



Der Hinweis als Freitext unter Abbildung 31 wird gestrichen:

~~Hinweis: Wenn das Verhalten der Konnektoren von dem dargestellten Ablauf abweicht, insbesondere wenn nach dem EjectCard und RequestCard das ActivateComfortSignature immer noch nicht erfolgreich durchgeführt wird, muss das Primärsystem den Anwender auffordern, die Karte zu ziehen und neu zu stecken.~~

3.1.1 Änderungen an api-telematik

3.1.1.1 SignatureService_V7_5_7.xsd und SignatureService_V7_5_7.wsdl

Die Schnittstellenbeschreibung aus [api-telematik] wird gemäß Pull Request <https://github.com/gematik/api-telematik/pull/24>

erweitert.

Die darin enthaltenen Änderungen müssen vom Konnektor umgesetzt werden.