Änderung in gemILF_PS

1.1.1 4.2.4 Kartensitzung HBAx

Im Folgenden bezeichnet „HBAx" den HBA sowie die HBA-Vorläuferkarten wie HBA-qSig und ZOD-2.0.

Die Anwendungsfälle Signieren und Verschlüsseln sind auf eine zuverlässige Identifikation des HBA bzw. seiner Vorläuferkarten angewiesen. Dabei muss die Nutzung der Signaturkarte durch die Person erfolgen, auf welche die Signaturkarte ausgestellt ist. Die HBAx-Kartensitzung, mit der eine Anwendungsschnittstelle (Signieren oder ~~Ver~~Entschlüsseln, siehe 4.4) aufgerufen wird, muss aus `Context`inklusive `UserId`, sowie dem `CardHandle` bestehen. Die Angabe der `UserId` stellt den Bezug zu einem konkreten Benutzer her und ist ~~ausschließlich~~ bei Signaturerstellung und Ent~~Ver~~schlüsselung verpflichtend. In einigen wenigen speziellen Anwendungsfällen, etwa beim Auslesen des AUT-Zertifikates des HBAx, ist es möglich, eine HBA-Kartensitzung ohne `UserId` zu verwenden.

Mittels Systeminformationsdienst `EventService.getCards` kann das Primärsystem direkt ein `CardHandle` anfordern. Dazu ist der entsprechende `Context` (insbesondere die Identifikation des Arbeitsplatzes) korrekt zusammenzustellen. Sofern ein bestimmtes Kartenterminal für den HBA vorgesehen ist, sollte die entsprechende `KartenterminalID` im Aufruf enthalten sein.

Im Ergebnis der Operation erhält das Clientsystem eine Liste der verfügbaren zugeordneten Karten (s. [gemSpec_Kon#4.1.6.5.2]). Gegebenenfalls muss unter den zurückgegebenen Karten anhand des Typs der HBAx (bzw. einer der verfügbaren HBAs) ausgewählt werden.

Darüber hinaus kann der Push-Mechanismus des Ereignisdienstes dazu verwendet werden, das `CardHandle` zu erhalten (siehe 4.1.4).

Zur Nutzung eines HBAxs muss eine Kartensitzung, bestehend aus `CardHandle` und `Context` inklusive `UserId` in den Schnittstellenaufrufen verwendet werden.

neue Anforderung:

A_24057 - Mandantenübergreifende Zuordnung von HBAx-Kartensitzungen
Das Primärsystem MUSS dem HBAx-Inhaber Aufrufkontexte (`Context`) mandantenübergreifend zuordnen. Das Primärsystem MUSS bei HBAx-relevanten Service Requests an den Konnektor Aufrufkontexte mandantenübergreifend so verwenden, dass eine gegebenenfalls im Konnektor bereits existierende Kartensitzung mit erhöhtem Sicherheitszustand nachgenutzt wird.
[<=]

Beispiel zur Komfortsignatur (siehe 4.4.2):

Eine HBA-Inhaberin arbeitet in einer Praxisgemeinschaft an einem Arbeitsplatz (A) mit einem Clientsystem (C) für drei verschiedene Mandaten (M1, M2, M3). Sie möchte in allen drei Mandatenkontexten Komfortsignaturen mit ihrem HBA, der in einem KT steckt, das allen Mandaten zugeordnet ist, ausführen. Am Beginn des Arbeitstages aktiviert sie in einem Mandantenkontext (bspw. M2) den Komfortsignaturmodus für ihren HBA. Das PS generiert die UserID U1 und verwendet den Aufrufkontext (M2, A, C, U1) beim ActivateComfortSignature-Request an den Konnektor. Nach erfolgreicher Verifikation der PIN.QES befindet sich die dem Aufrufkontext (M2, A, C, U1) zugeordnete Kartensitzung im Konnektor in einem erhöhten Sicherheitszustand. Wenn die HBA-Inhaberin nun

Komfortsignaturen in den Mandantenkontexten M1, M2, M3 ausführen möchte, verwendet das Primärsystem für die SignDocument-Requests in allen drei Mandantenkontexten den Aufrufkontext (M2, A, C, U1), um die im Konnektor beim ActivateComfortSignature im Mandantenkontext M2 etablierte Kartensitzung mit erhöhtem Sicherheitszustand nachzunutzen.