
C_12203_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Änderung in gemSpec_Kon.....	3
2.1 Änderung in api-telematik.....	10
3 Änderung in gemILF_PS.....	11

1 Änderungsbeschreibung

Um ein ggf. erhöhtes Auftreten von Fehlern beim Rollout von PTV6-Konnektoren zu vermeiden, werden die Operationen ReadCardCertificate und CheckCertificateExpiration, bzgl. deren Verhalten im Umgang mit dem Crypt-Parameter angepasst.

Bisher liefern diese Operationen ohne Angabe des Crypt-Parameters durch den Aufrufer immer mit Crypt=ECC die ECC-basierten Informationen zurück. Dieser ÄE ändert nun das Verhalten beim Crypt-Parameter als Default dahingehend, dass nun das Zertifikat entsprechend der vorhandenen Kartengeneration ausgewählt, und bei gesetztem CRYPT-Parameter das ausgewählte Zertifikat zurück geliefert wird, wenn vorhanden.

Weiterhin werden Inkonsistenzen im gemILF_PS im Zusammenhang Operationen ReadCardCertificate und CheckCertificateExpiration korrigiert.

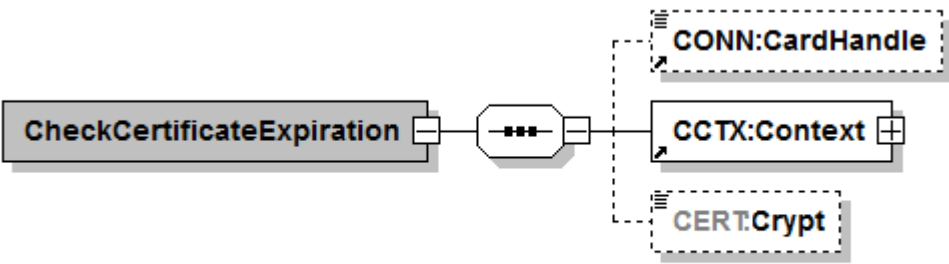
2 Änderung in gemSpec_Kon

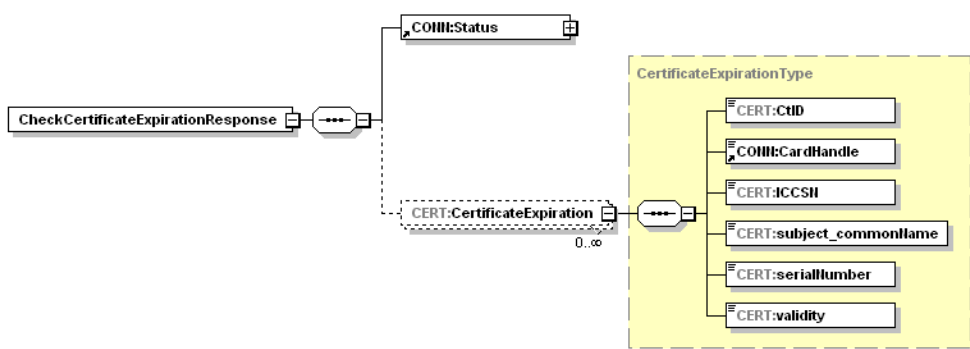
TIP1-A_4699-05 wird durch TIP1-A_4699-06 ersetzt:

TIP1-A_4699-06 - Operation CheckCertificateExpiration

Die Basisanwendung Zertifikatsdienst des Konnektors MUSS an der Clientschnittstelle eine Operation CheckCertificateExpiration anbieten.

Tabelle 1: TAB_KON_676 Operation CheckCertificateExpiration

Name	CheckCertificateExpiration	
Beschreibung	Gibt das Datum des Ablaufs eines bestimmten Zertifikats oder gesammelt des Zertifikats K, der gSMC-KT's sowie aller gesteckten HBAX und SM-B des Mandanten zurück.	
Aufrufparameter		
	Name	Beschreibung
	CardHandle	Optional. Identifiziert die Karte, deren Zertifikate geprüft werden. Wird der Parameter nicht angegeben, so werden alle für den Mandanten erreichbaren Karten (inkl. gSMC-K und aller gSMC-KT's), die dem Mandanten passen, berücksichtigt. Die Operation CheckCertificateExpiration DARF das Lesen von Zertifikaten der eGK NICHT unterstützen.
	Context	MandantId, Csid, WorkplacId verpflichtend; UserId optional
	Crypt	Optional; Default: ECC Defaultwert: <ul style="list-style-type: none"> Für eine Karte ab der Generation G2.1 setze den Defaultwert crypt Für eine Karte der Generation G2.0 setze den Defaultwert crypt Gibt den kryptographischen Algorithmus vor, für den das Zertifikat ermittelt werden soll. Wertebereich: RSA, ECC <ul style="list-style-type: none"> RSA: Zertifikat für RSA-2048 ECC: Zertifikat für ECC-256

Rückgabe		
	Status	Enthält den Ausführungsstatus der Operation.
	CertificateExpiration	Eine Liste von Tupeln aus (CtID, CardHandle, ICCSN, subject.CommonName, serialNumber, validity) der Zertifikate. Für die gSMC-K soll in CertificateExpiration/CtID und CertificateExpiration/CardHandle jeweils ein Leerstring zurückgegeben werden.
Vorbedingungen	Keine	
Nachbedingungen	Keine	

Der Ablauf der Operation CheckCertificateExpiration ist in Tabelle TAB_KON_677 beschrieben:

Tabelle 2: TAB_KON_677 Ablauf CheckCertificateExpiration

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. Wird die Operation für einen nicht unterstützten Kartentypen aufgerufen, so bricht die Operation mit Fehler 4058 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; allWorkplaces=true, wenn cardHandle nicht angegeben, ansonsten false } Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.

3.	enumerateCardHandles	Wenn der Parameter CardHandle übergeben wurde, wird dieser als einziges Element in eine Liste gepackt. Wenn der Parameter CardHandle leer war, wird eine Liste der CardHandles aller für den Konnektor erreichbaren Karten (inkl. gSMC-K und gSMC-KT's), die zum Mandanten passen, erstellt.
Für jedes CardHandle der in Schritt 3 erzeugten Liste werden folgende Schritte ausgeführt, für die gSMC-Ks die Schritte 5 und 6: Falls Schritt 5 der TUC_KON_033 die Warnung 4257 zurückgibt, wird Schritt 6 nicht ausgeführt und die Schritte für das CardHandle der in Schritt 3 erzeugten Liste weiter ausgeführt. Die Warnung 4257 wird mit dem <cardHandle> des aktuellen Schrittes für den Fehlertext erzeugt. Werden für mehrere CardHandle von TUC_KON_033 die Warnung 4257 zurückgegeben, so MUSS der Konnektor daher mehrere separate Warnungen 4257 ausgeben.		
4.	TUC_KON_026 „Liefere CardSession“	Ermittle CardSession über TUC_KON_026 { mandatId = MandantId; clientSystemId = ClientSystemId; cardHandle = CardHandle; userId = UserId }
5.	TUC_KON_033 „Zertifikatsablauf prüfen“	Das Gültigkeitsdatum des Zertifikats wird geprüft mit TUC_KON_033 { cardSession; doInformClients = false; Crypt; } bzw. TUC_KON_033 { checkSMCK = true; doInformClients = false; Crypt; }
6.	TUC_KON_034 „Zertifikatsinformationen extrahieren“	Beim Aufruf des TUC_KON_034 ist der Parameter qes = false zu setzen. Aus den jeweiligen Rückgabewerten entsteht eine Liste aus Tupeln (CtId, CardHandle, ICCSN, subject.CommonName, serialNumber, validity). Diese wird von der Operation zurückgegeben.

Tabelle 3: TAB_KON_603 Fehlercodes „CheckCertificateExpiration“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler

4058	Security	Error	Aufruf nicht zulässig
4257	Technical	Warning	<\$Crypt>Zertifikat nicht vorhanden auf Karte: <cardHandle>

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

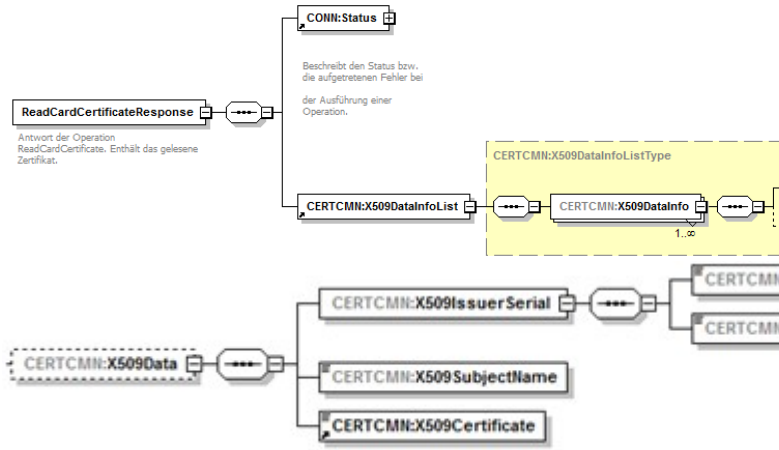
TIP1-A_4700-02 wird durch TIP1-A_4700-03 ersetzt:

TIP1-A_4700-03 - Operation ReadCardCertificate

Die Basisanwendung Zertifikatsdienst des Konnektors MUSS an der Clientschnittstelle eine Operation ReadCardCertificate wie in Tabelle TAB_KON_678 Operation ReadCardCertificate beschrieben anbieten.

Tabelle 4: TAB_KON_678 Operation ReadCardCertificate

Name	ReadCardCertificate	
Beschreibung	Liest X.509-Zertifikate von einer Karte.	
Aufrufparameter	<pre> sequenceDiagram participant R as ReadCardCertificate R->>...: ...->>CONN:CardHandle CONN:CardHandle->>CCTX:Context CCTX:Context->>CERT:CertRefList CERT:CertRefList->>...: ...->>CERT:Crypt style CERT:Crypt stroke-dasharray: 5 5 </pre>	
	Name	Beschreibung
	CardHandle	Gibt die Karte an, von der das Zertifikat gelesen werden soll. Es können Zertifikate von HBAX (HBA, HBA-VK), SM-B ausgelesen werden. Die Operation ReadCardCertificate DARF das Lesen von Zertifikaten der eGK NICHT unterstützen.

	Context	Aufrufkontext (Mandant)
	CertRefList	Gibt an, welche(s) Zertifikat(e) gelesen werden soll. Mögliche Werte für CertRef sind: C.AUT, C.ENC, C.SIG, C.QES
	Crypt	Optional; Default: ECC Defaultwert: <ul style="list-style-type: none"> Für eine Karte ab der Generation G2.1 setze den Defaultwert crypt=ECC. Für eine Karte der Generation G2.0 setze den Defaultwert crypt=RSA. Gibt den kryptographischen Algorithmus vor, für den das Zertifikat ermittelt werden soll. Wertebereich: RSA, ECC <ul style="list-style-type: none"> RSA: Zertifikat für RSA-2048 ECC: Zertifikat für ECC-256
Rückgabe 		
	Status	Enthält den Ausführungsstatus der Operation.
	CertRef	Dieses Element beinhaltet die Referenz des Zertifikats, welches bei der Anfrage übergeben wurde.

	X509Data	Inhalt des über die CertRef referenzierten Zertifikats. Ist das referenzierte Zertifikat nicht vorhanden, so wird dieses Element nicht vom Konnektor gefüllt.	
		X509Issuer Name	Enthält den Issuer-Name des Zertifikats. Bezüglich des Encodings sind die in [XMLDSig#4.4.4.4.1] angegebenen Regeln zu beachten (Escaping von Sonderzeichen etc.)
		X509Serial Number	Enthält die serialNumber des Zertifikats.
		X509Subject Name	Enthält das Feld subject.CommonName. Bezüglich des Encodings sind die in [XML DSig#4.4.4.4.1] angegebenen Regeln zu beachten (Escaping von Sonderzeichen etc.)
		X509 Certificate	Enthält das base64-codierte Zertifikat, dessen Binärstruktur wiederum ASN.1-codiert (gemäß [COMMON_PKI]) vorliegt.
Vorbedingungen	Keine		
Nachbedingungen	Keine		

Der Ablauf der Operation ReadCardCertificate ist in Tabelle TAB_KON_679 Ablauf ReadCardCertificate beschrieben:

Tabelle 5: TAB_KON_679 Ablauf ReadCardCertificate

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. Wurde als Zielkarte eine eGK adressiert, wird Fehlercode 4090 zurückgeliefert.
2.	TUC_KON_000 „Prüfe Zugriffs- berechtigung“	Die Prüfung erfolgt durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientsystemId = \$context.clientsystemId; workplaceld = \$context.workplaceld; userId = \$context.userId; cardHandle = \$cardHandle } Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_026 „Liefere CardSession“	Ermittle CardSession über TUC_KON_026 { mandatId = \$context.mandantId; clientsystemId = \$context.clientsystemId; cardHandle = \$context.cardHandle; userId = \$context.userId } }
4.	getEF	Für jedes Paar von CertRef und CardHandle wird in Abhängigkeit des Parameters Crypt gemäß Tabelle TAB_KON_858 das zu lesende File (EF) bestimmt: Ist die übergebene Zertifikatsreferenz ungültig, wird Fehlercode 4149 zurückgegeben. Das Lesen von Zertifikaten der eGK ist aus Sicherheitsgründen für Clientsysteme nicht zulässig.
	TUC_KON_216 „LeseZertifikat“	Für jedes Paar von CardHandle und EF wird nun durch Aufruf von TUC_KON_216 „LeseZertifikat“ das Zertifikat ausgelesen. Falls TUC_KON_216 die Warnung 4256 zurückgibt, wird die Operation abgebrochen und Fehler 4258 zurückgegeben.
6.	Zertifikatsattribute extrahieren	Aus jedem Zertifikat werden die zu liefernden Attribute extrahiert. Die Ergebnisstruktur wird mit den erhaltenen Rückgabewerten gefüllt.

Tabelle 6: TAB_KON_604 Fehlercodes „ReadCardCertificate“

Fehlercod	ErrorTyp	Severit	Fehlertext
-----------	----------	---------	------------

e	e	y	
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4149	Technical	Error	Ungültige Zertifikatsreferenz
4090	Security	Error	Zugriff auf eGK nicht gestattet
4258	Technical	Error	<\$Crypt>Zertifikat nicht vorhanden auf Karte: <cardHandle>

【<=, Konnektor Highspeed, Konnektor PTV6, funkt. Eignung: Test Produkt/FA】

2.1 Änderung in api-telematik

Wegen der semantischen Änderung werden die Versionen von WSDL und XSD des CertificateService angepasst.

3 Änderung in gemILF_PS

In Kapitel 4.4.4 Zertifikatsdienst wird der Freitext wie folgt geändert:

Der CertificateService des Konnektors bietet Operationen zum Abfragen von Kartenzertifikaten und ihrer Gültigkeit an.

< PTV4 > Nach der Einführung von elliptischen Kurven auf TI-Signaturkarten ab der Generation G2.1 ist es möglich, bei ReadCardCertificate und CheckCertificateExpiration die Auswahl von ECC- und RSA-Zertifikaten zu steuern, und zwar durch eine Belegung des optionalen Parameters Crypt. Der Defaultwert ist "RSA". Wird beim Aufruf der Operation kein Crypt Parameter übergeben, so wird durch den Konnektor ein Defaultwert dafür verwendet, welcher sich aus der vorhandenen Kartengeneration gem. Tabelle 22 ergibt.

Tabelle 22: Tab_ILF_PS_Steuerung_Zertifikatsauswahl

Parameter Crypt	Smartcard Objektsystemversion < 4.4.0 oder HBA-V (Kartengeneration noch nicht G2.1)	SmartcardObjektsystemversion > (ab Kartengeneration G2.1)
nicht verwendet	RSA-Zertifikat	RSA ECC-Zertifikat
"ECC"	kein Zertifikat, Fehlermeldung	ECC-Zertifikat
"RSA"	RSA-Zertifikat	RSA-Zertifikat

< /PTV4 >

Unter der Tabelle 22 wird die neue Anforderung A_27609 aufgenommen:

A_27609 - Robustes Fehlerhandling des PS bei ReadCardCertificate und CheckCertificateExpiration

Wird bei Aufruf der Operationen ReadCardCertificate oder CheckCertificateExpiration der Crypt Parameter mit Crypt=ECC übergeben, so DARF das PS im Falle einer vorhandenen G2.0 Karte keinen Fehler an den Nutzer des PS weitergeben und MUSS vielmehr den Operationsaufruf mit Crypt=RSA wiederholen.

Freitext darunter:

Anstatt des reaktiven Ansatzes auf den Fehler des Konnektors zu reagieren kann PS auch den proaktiven Ansatz verfolgen, indem es vor dem Operationsaufruf selbst die Kartengeneration ermittelt und daraufhin selbstständig den Crypt Parameter lediglich passend zu Kryptografien von auf der Karte vorhandenen Zertifikaten wählt.

Freitext unter A_13533-01 - Überprüfung Ablaufdatum von Zertifikaten wird erweitert:

Der Operation CheckCertificateExpiration wird kein CardHandle übergeben. Für das Konnektorzertifikat wird der Eintrag selektiert, der keine CtID enthält. Für Einträge mit

CardHandle muss die Kartenart ermittelt werden. Es gibt Firmwareversionen, bei denen die gSMC-KT-Information fehlt.

Wird der Operation CheckCertificateExpiration kein Crypt Parameter übergeben, so kann das PS bei betreffenden Karten ab Generation G2.1 davon ausgehen, dass alle auf der Karte vorhandenen Zertifikate das gleiche Ablaufdatum haben, wie jenes, das von der Operation zurückgegeben wurde .