Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

1. Änderungen in gemSpec_Kon

1.1 Änderung in "TIP1-A_6727 Cross-Origin Resource Sharing"

Die Operation GetCards wird durch eine neue Operation GetLeCards ersetzt und ist damit über CORS nicht mehr erreichbar.

Der Konnektor darf bei positiven CORS Responses keine Informationen im http-Header zurückgeben, die dem Browser ein Caching der Antwort ermöglichen. (z.B. Cache-Control: no-cache)

⌦ TIP1-A_6727 Cross-Origin Resource Sharing

Der Konnektor MUSS Cross-Origin Resource Sharing gemäß [CORS] für sämtliche für die Clientsystemschnittstelle definierten Web-Services unterstützen.

Dabei MUSS der Konnektor über den Access-Controll-Allow-Origin HTTP-Header ausschließlich explizit zugelassenen ORIGINs den Zugriff auf explizit zugelassene Operationen erlauben. Der Konnektor DARF NICHT über den Eintrag `"*"` im Access-Controll-Allow-Origin HTTP-Header den Zugriff über jede ORIGIN ermöglichen.

Explizit zugelassene ORIGINs sind alle ORIGINS, die sämtliche der folgenden Bedingungen erfüllen:

- ORIGIN, wie vom Aufrufer angegeben
- ORIGIN ist gemäß [RFC3986] wie folgt definiert: "https://<host>[:<port>]"
- <host> ist ein FQDN aus dem Namensraum der TI, d.h. er hat die Top Level Domain DNS_TOP_LEVEL_DOMAIN_TI

Explizit zugelassene Operationen sind alle in TAB_KON_803 aufgeführten Operationen.

Tabelle 1 TAB_KON_803 Erlaubte Operationen beim CORS-Zugriff

Name des Service	Operation
`ConnectorServiceDirectory`	`GET /connector.sds`
~~`EventService`~~	~~`GetCards`~~
`EventService`	`GetLeCards`
~~`SignatureService`~~ `AuthSignatureService`	`ExternalAuthenticate`
`CertificateService`	`ReadCardCertificate`

© gematik – öffentlich_Entwurf

Name des Service	Operation
CardService	GetPinStatus
CardService	VerifyPin

Der Konnektor MUSS bei Responses auf Cross-Origin Requests den http-Header so zurückgeben, dass kein Caching der Antwort beim Browser erfolgt (z.B. Cache-Control: no-cache).⌫

1.2 Neuer Konfigurationsparameter zum Aktivieren/Deaktivieren von CORS (Einfügen in Kap.3.5.5)

⌦ TIP1-A_xxx2 Aktivieren/Deaktivieren von CORS

Die Managementschnittstelle MUSS es einem Administrator ermöglichen, die Funktionalität Cross-Origin Resource Sharing [CORS] zu aktivieren bzw. zu deaktivieren gemäß TAB_KON_xxx Konfigurationswerte CORS.

Tabelle xx TAB_KON_xxx Konfigurationswerte CORS

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
CORS_Mode	Enabled/Disabled	Der Administrator MUSS CORS aktivieren bzw. deaktivieren können. Enabled: Cross-Origin Resource Sharing gemäß [CORS] ist für die Web-Services der Clientsystemschnittstelle NICHT erlaubt. Disabled: Cross-Origin Resource Sharing gemäß [CORS] ist für die erlaubten Operationen der Clientsystemschnittstelle gemäß TAB_KON_803 erlaubt. Default-Wert: Enabled

⌫

1.3 Neue Operation GetLeCards im Systeminformationsdienst

⌦ TIP1-A_4603 Basisanwendung Systeminformationsdienst

Der Konnektor MUSS für Clients eine Basisanwendung Systeminformationsdienst anbieten.

Tabelle 2 TAB_KON_029 Basisanwendung Systeminformationsdienst

Name	EventService
Version	7.2.0 7.2.1 Siehe Anhang D (WSDL-Version)
Namensraum	Siehe Anhang D
Namensraum-Kürzel	EVT für Schema und EVTW für WSDL

© gematik – öffentlich_Entwurf

Operationen	Name	Kurzbeschreibung
	GetCardTerminals	Auflistung der verfügbaren Kartenterminals
	GetCards	Auflistung der gesteckten Karten
	GetLeCards	Auflistung der gesteckten Karten der Kartentypen HBAx und SM-B
	GetResourceInformation	Liefert Details zu einer Ressource (Kartenterminal, Karte, HSM)
	Subscribe	Anmeldung der Zustellung von Ereignissen
	Unsubsribe	Abmelden von der Zustellung von Ereignissen
	RenewSubscriptions	Gültigkeit bestehender Subscriptions verlängern
	GetSubscriptions	Abfrage der angemeldeten Zustellungen von Ereignissen
WSDL	EventService.wsdl	
Schema	EventService.xsd	

⌫

1.3 Neue Operation GetLeCards

Es wird Kapitel 4.1.6.5.8 neu aufgenommen:

4.1.6.5.8 GetLeCards

⌦ **TIP1-A_xxx1 Operation GetLeCards**

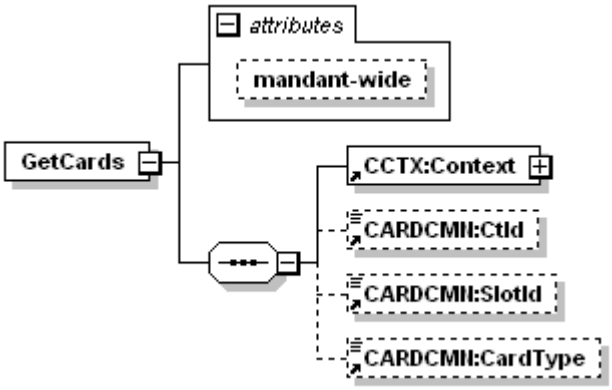
Der Konnektor MUSS an der Außenschnittstelle eine Operation GetLeCards, wie in Tabelle TAB_KON_xxx „Operation GetLeCards“ beschrieben, anbieten und MUSS dabei Kartentypen aus Tabelle 1: TAB_KON_500 Wertetabelle Kartentypen unterscheiden.

Tabelle 3: Tab_KON_xxx Operation GetLeCards

Name	GetLeCards
Beschreibung	Liefert Informationen zu den in den Kartenterminals verfügbaren Karten des Leistungerbringers zurück, die in Kartenterminals stecken, auf die Mandant und Clientsystem zugreifen dürfen. Insbesondere umfasst die Information die sog. Karten-Handles. Die Karten-Handles können bei anderen Operationen an der Außenschnittstelle des Konnektors zur Adressierung von Karten genutzt werden. Es werden ausschließlich Informationen der Kartentypen HBAx und SM-B zurückgegeben.

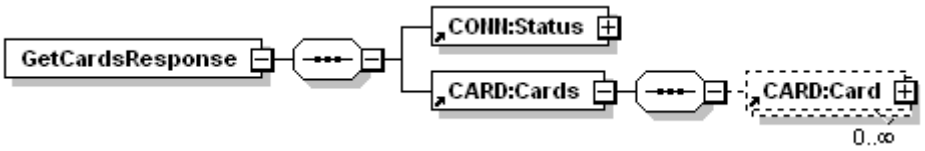
© gematik – öffentlich_Entwurf

Aufrufparameter



Name	Beschreibung
`@mandant-wide`	Wenn „true“, werden alle Karten zurückgegeben, auf die der Mandant und das aufrufende Clientsystem zugreifen darf. Wenn „false“ (Standardbelegung), werden nur Karten zurückgegeben, auf die von dem im Aufrufkontext spezifizierten Arbeitsplatz zugriffen werden darf.
`Context`	Aufrufkontext
`CtId`	Identifikation des Kartenterminals. Wenn angegeben, werden nur die Karten zurückgeliefert, die in diesem Kartenterminal verfügbar sind und von einem der Kartentypen KVK, HBAx oder SM-B entsprechen.
`SlotId`	Nummer des Slots, beginnend bei 1.
`CardType`	Ein Kartentyp gemäß Tabelle TAB_KON_500 „Wertetabelle Kartentypen“ als optionaler Filter. Wenn angegeben, werden nur Karten vom spezifizierten Typ zurückgegeben. Unterstützt werden die Kartentypen HBAx und SM-B.

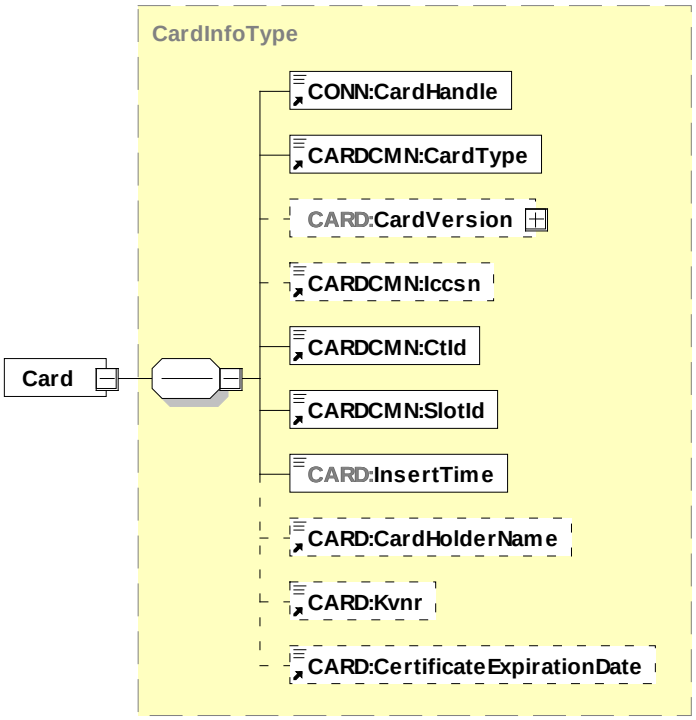
Antwort

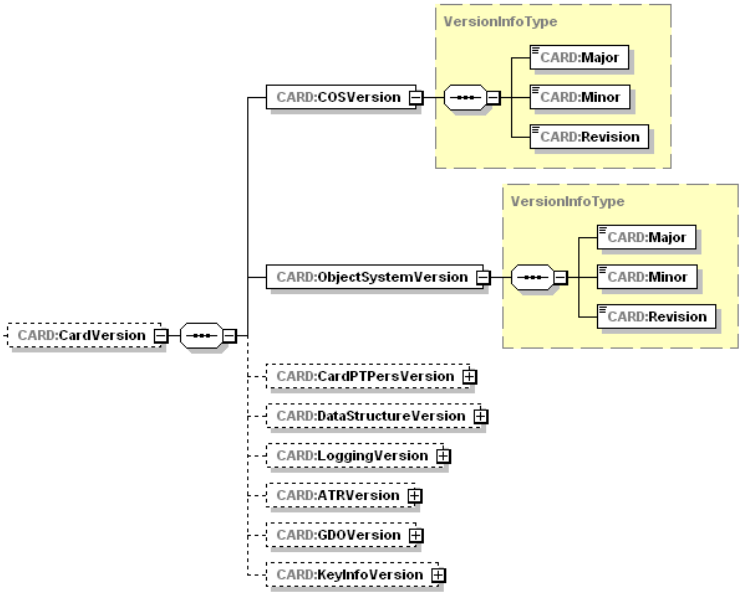


Name	Beschreibung
`Status`	Ergebnis der Operation

Im Element `Cards` wird die Liste der gesteckten Karten zurückgegeben. Für jede Karte wird dabei ein `Card`-Element angegeben. Leere Slots der Kartenterminals sind in dieser Liste nicht enthalten.

© gematik – öffentlich_Entwurf



Name	Beschreibung
`CardHandle`	Handle, mit dem die Karte in Folgeaufrufen adressiert werden kann. Der Konnektor garantiert, dass dieses Handle die gesteckte Karte eindeutig identifiziert und bei Entfernen der Karte aus dem Kartenterminal ungültig wird.
`CardType`	Erkannter Typ der Karte. Siehe Tabelle 1: TAB_KON_500 Wertetabelle Kartentypen
`CardVersion`	 Der Konnektor MUSS in CardVersion bei HBA und SM-B der Generation 2 die Versionsinformationen gemäß [gemSpec_Karten_Fach_TIP] übergeben, für G1+ aus

© gematik – öffentlich_Entwurf

		/MF/EF.Version. Bei HBA-VK MUSS das Element weggelassen werden.
	`Iccsn`	Falls auslesbar, die ICC-Serial-Number der Karte.
	`CtId`	Identifikation des Kartenterminals, in dem die Karte steckt.
	`SlotId`	Nummer des Slots (beginnend bei 1), in dem die Karte steckt.
	`InsertTime`	Gibt den Zeitpunkt an, zu dem der Konnektor die Karte erkannt hat. Die Zeit wird mit dem Datentyp `DateTime` in folgendem Format angegeben: `yyyy-mm-ddThh:mm:ss+hh:mm` Es ist also – gemäß ISO 8601 [ISO8601] – die lokale Zeit und die Differenz zur UTC anzugeben.
	`CardHolderName`	Name des Karteninhabers bzw. der Institution/Organisation (subject.commonName).
	`Kvnr`	Das Element MUSS weggelassen werden.
	`CertificateExpirationDate`	Ablaufdatum des Zertifikates (AUT bzw. OSIG).
Vorbe-dingungen	Keine.	
Nachbe-dingungen	Der Zustand der Karten und der Kartenterminals bleibt unverändert.	
Hinweise	Der Aufruf darf nur den im Konnektor verwalteten aktuellen Zustand der Karte liefern und keine Abfragen an die Kartenterminals absetzen.	

Der Ablauf der Operation GetLeCards ist in Tabelle 4: TAB_KON_xxx Ablauf LeOnly beschrieben:

Tabelle 4: TAB_KON_xxx Ablauf GetLeCards

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 {$context.mandantId; $context.clientsystemId; $context.workplaceId; doNotNeedCardSession; @mandant-wide} Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_253 „Liefere Karten_Liste“	Die Liste der Karten wird erstellt und zurückgegeben. Tritt hierbei ein Fehler auf, so bricht die Operation mit dem Fehler des TUCs ab. Wurde CardType nicht angegeben, dann ermittle die Liste der Karten für CardType=HBAx und für CardType=SM-B Wenn @mandant-wide=true dann ermittle die Liste der Karten für

© gematik – öffentlich_Entwurf

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
		alle Arbeitsplätze des Mandanten für das angegebene Clientsystem durch den Aufruf TUC_KON_253 „Liefere Karten_Liste“ { Clientsystem ID = $context.clientsystemId; Kartenterminal-ID = CtId; Slot-ID = SlotId; Mandanten ID = $context.mandantId; CardType = CardType } Wenn @mandant-wide=false dann ermittle die Liste der Karten für den Arbeitsplatz des Mandanten für das angegebene Clientsystem entsprechend $context durch den Aufruf TUC_KON_253 „Liefere Karten_Liste“ { Arbeitsplatz ID = $context.workplaceId; Clientsystem ID = $context.clientsystemId; Kartenterminal-ID = CtId; Slot-ID = SlotId; Mandanten ID = $context.mandantId; CardType = CardType }

Die Fehlerfälle der Operation GetLeCards sind in Tabelle 5 TAB_KON_xxx Fehlerfälle LeOnly dargestellt:

Tabelle 5 TAB_KON_xxx Fehlerfälle GetLeCards

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

⌫

1.4 Anpassung der Version in „Anhang D – Übersicht über die verwendeten Versionen“

TAB_KON_688 Version der Schemas aus dem Namensraum des Konnektors

	~~XSD Name~~	~~EventService.xsd~~
	~~XSD Schemaversion~~	~~7.2.1~~
	~~TargetNamespace~~	~~http://ws.gematik.de/conn/EventService/ v7.2~~
	XSD Name	EventService.xsd
	XSD Schemaversion	7.2.2
	TargetNamespace	http://ws.gematik.de/conn/EventService/ v7.2

Tabelle 6: TAB_KON_798 Schnittstellenversionen

Systeminformationsdienst (EventService)		
	WSDL Name	EventService.wsdl
	WSDL-Version	7.2.0

© gematik – öffentlich_Entwurf

	TargetNamespace	http://ws.gematik.de/conn/EventService/ WSDL/v7.2
	verwendete XSDs	CardService.xsd, CardServiceCommon.xsd, CardTerminalInfo.xsd, ConnectorCommon.xsd, ConnectorContext.xsd, EventService.xsd, ProductInformation.xsd, TelematikError.xsd
Systeminformationsdienst (EventService)		
	WSDL Name	EventService.wsdl
	WSDL-Version	7.2.1
	TargetNamespace	http://ws.gematik.de/conn/EventService/ WSDL/v7.2
	verwendete XSDs	CardService.xsd, CardServiceCommon.xsd, CardTerminalInfo.xsd, ConnectorCommon.xsd, ConnectorContext.xsd, EventService.xsd, ProductInformation.xsd, TelematikError.xsd

1.5 Anhang E „Übersicht Konfigurationsparameter und Zustandswerte“ wird erweitert um folgenden Tabelleneintrag:

Zustand swert?	ReferenzID	Belegung	Bedeutung und Administrator-Interaktion bzw. Zustandswerte
Interne Mechanismen			
	`CORS_Mode`	`Enabled/ Disabled`	Der Administrator MUSS CORS aktivieren bzw. deaktivieren können. `Enabled`: Cross-Origin Resource Sharing gemäß [CORS] ist für die Web-Services der Clientsystemschnittstelle NICHT erlaubt. `Disabled`: Cross-Origin Resource Sharing gemäß [CORS] ist für die erlaubten Operationen der Clientsystemschnittstelle gemäß TAB_KON_803 erlaubt. Default-Wert: `Enabled`

2. Änderungen in EventService.xsd

Das Schema EventService.xsd wird erweitert um die neue Operation `GetLeCards`.

Die Schnittstellenerweiterung ist abwärts kompatibel.

EventService.xsd (alt: version="7.2.1", neu: version="7.2.2") wird wie folgt erweitert:

© gematik – öffentlich_Entwurf

```
<schema xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:EVT="http://ws.gematik.de/conn/EventService/v7.2"
xmlns:CONN="http://ws.gematik.de/conn/ConnectorCommon/v5.0"
xmlns:CCTX="http://ws.gematik.de/conn/ConnectorContext/v2.0"
xmlns:CARD="http://ws.gematik.de/conn/CardService/v8.1"
xmlns:CT="http://ws.gematik.de/conn/CardTerminalInfo/v8.0"
xmlns:CARDCMN="http://ws.gematik.de/conn/CardServiceCommon/v2.0"
xmlns:HSM="http://ws.gematik.de/conn/HsmInfo/v8.0"
targetNamespace="http://ws.gematik.de/conn/EventService/v7.2" elementFormDefault="qualified"
attributeFormDefault="unqualified" version="7.2.2">

…
        <element name="GetLeCards">
                <annotation>
                        <documentation>Abfragen der in Kartenterminals verfügbaren Karten vom Kartentyp
        HBAx und SM-B</documentation>
                </annotation>
                <complexType>
                        <sequence>
                                <element ref="CCTX:Context"/>
                                <element ref="CARDCMN:CtId" minOccurs="0"/>
                                <element ref="CARDCMN:SlotId" minOccurs="0"/>
                                <element ref="CARDCMN:CardType" minOccurs="0"/>
                        </sequence>
                        <attribute name="mandant-wide" type="boolean" use="optional" default="false"/>
                </complexType>

        </element>
        <element name="GetLeCardsResponse">
                <annotation>
                        <documentation>Antwort des Aufrufs GetLeCards</documentation>
                </annotation>
                <complexType>
                        <sequence>
                                <element ref="CONN:Status"/>
                                <element ref="CARD:Cards"/>
                        </sequence>
                </complexType>

        </element>

…

</schema>
```

3. Änderungen in EventService.wsdl

EventService.wsdl (alt: version="7.2.0", neu: version="7.2.1") wird wie folgt erweitert:

Das Schema EventService.wsdl wird erweitert um die neue Operation `GetLeCards`:

```
<definitions ...>
...
        <message name="GetLeCardsRequestMessage">
                <part name="parameter" element="EVT:GetLeCards"/>

        </message>
        <message name="GetLeCardsResponseMessage">
                        <part name="parameter" element="EVT:GetLeCardsResponse"/>

        </message>

…
        <portType …>
```


© gematik – öffentlich_Entwurf

```
…
        <operation name="GetLeCards">
                <input message="EVTW:GetLeCardsRequestMessage"/>
                <output message="EVTW:GetLeCardsResponseMessage"/>
                <fault name="FaultMessage" message="EVTW:FaultMessage"/>

        </operation>

…

</portType>

<binding …>

…
        <operation name="GetLeCards">
                <soap:operation
        soapAction="http://ws.gematik.de/conn/EventService/v7.2#GetLeCards"/>
                <input>
                        <soap:body use="literal"/>
                </input>
                <output>
                        <soap:body use="literal"/>
                </output>
                <fault name="FaultMessage">
                        <soap:fault name="FaultMessage" use="literal"/>
                </fault>

        </operation>

…

</binding>
```


© gematik – öffentlich_Entwurf

4. Änderungen in gemProdT_Kon_PTV2

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_Kon_PTV2]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

3.1.1 Produkttest / Produktübergreifender Test

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Produkttyps verzeichnet, deren Umsetzung im Zuge von Zulassungstests durch die gematik geprüft wird.

Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest / Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_xxx1	Operation GetLeCards	gemSpec_Kon
TIP1-A_xxx2	Aktivieren/Deaktivieren von CORS	gemSpec_Kon

3.2.1 CC-Evaluierung

Der Produkttyp erfordert eine Zertifizierung nach ITSEC [ITSEC] oder Common Criteria (CC) [BSI_2006a] auf der Grundlage der Protection Profiles [PP_NK] und [PP_KON].

Für die Evaluierung sind die Inhalte der Schutzprofile normativ führend. Der Nachweis der im Folgenden aufgeführten Anforderungen erfolgt implizit durch die Vorlage des IT-Sicherheitszertifikats bei der gematik.

Wenn der Hersteller die Funktion CORS (TIP1-A_xxx2) umsetzt, muss diese auch evaluiert und zertifiziert werden. Dazu muss der Hersteller die CORS-spezifischen Inhalte aus dem [PP_KON]#7.2 in sein Security Target übernehmen.

Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "CC-Evaluierung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_xxx2	Aktivieren/Deaktivieren von CORS	gemSpec_Kon

© gematik – öffentlich_Entwurf