gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Konzept

Architektur der TI-Plattform

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.

ENTWURF

Version:	2.4.0 CC
Revision:	\main\rel_online\rel_ors1\rel_opb1\rel_ors2\100
Stand:	16.02.2018
Status:	Entwurf
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemKPT_Arch_TIP

Dokumentinformationen

Änderungen zur Vorversion

Erweiterung für Service Monitoring, weiteren Anwendungen, Administration Verzeichnisdienst, DNSSEC-Validierung und Wegfall von Attributzertifikaten.

Begriffliche Anpassung bzgl. der Gesamtverantwortung der gematik.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
2.2.0	05.10.17		Überarbeitung Online-Produktivbetrieb (Stufe 2.1)	gematik
2.3.0	18.12.17		Erweiterung für weitere Anwendungen des Gesundheitswesens und sichere Übermittlungsverfahren. Inhalte zur LE-AdV-Umgebung entfernt. Anpassung bei der tokenbasierten Authentisierung. Übernahme der Änderungen aus Release R1.6.4-1 und R1.6.4-2.	gematik
			Erweiterung für Service Monitoring, weiteren Anwendungen, Administration Verzeichnisdienst, DNSSEC-Validierung und Wegfall von Attributzertifikaten. Begriffliche Anpassung bzgl. der Gesamtverantwortung der gematik.	gematik
2.4.0 CC	16.02.18		Zur Abstimmung freigegeben	gematik

ENTWURF

Inhaltsverzeichnis

Dokumentinformationen **2**

Inhaltsverzeichnis **3**

1 Einordnung des Dokuments **10**

1.1 Zielsetzung **10**

1.2 Zielgruppe **10**

1.3 Geltungsbereich **10**

1.4 Abgrenzung des Dokuments **10**

1.5 Methodik **11**

2 Grundlagen der Architektur der TI-Plattform **12**

2.1 Architekturmerkmale **12**

2.1.1 TI-Plattform als Basis der Fachanwendungen 12

2.1.1.1 Schnittstelle zu den Fachanwendungen *14*

2.1.1.2 Anwendungsneutralität *14*

2.1.1.3 Dienstbaukasten und Erweiterbarkeit *14*

2.1.1.4 Weitere Anwendungen des Gesundheitswesens und sichere Übermittlungsverfahren *15*

2.1.2 Produkttypen, Produkte und Produktinstanzen 15

2.1.3 Logische Architekturschichten (Zonen) 16

2.1.4 Kontrolle der Kommunikationswege 18

2.2 Betrieb und Wartung (Operation and Maintenance) **20**

2.3 Bedarfsgerechte Leistungsfähigkeit (Performance) **20**

2.4 Sicherheitsleistung der TI-Plattform **20**

2.4.1 Abgrenzung zwischen TI-Plattform und Fachanwendung 20

2.4.2 Sicherheitsleistung der Produkttypen 21

2.5 Parallelbetrieb eGK-Generationen 1 und 2 ..... **22**

2.6 Rollen der TI-Plattform **22**

2.6.1 Personenkreise der Telematikinfrastruktur 22

2.6.2 Rollen 23

3 Leistungen der TI-Plattform in der Außensicht **27**

3.1 Qualifizierte elektronische Signatur **27**

3.2 Einfache digitale elektronische Signatur **27**

3.3 Ver- und Entschlüsselung **27**

3.4 Public Key Infrastructure (PKI) **27**

ENTWURF

3.5 Tokenbasierte Benutzerauthentisierung 28
3.6 Smartcards des Gesundheitswesens 28
3.7 Anbindung an das geschlossene Netzwerk der TI 28
3.8 Zugang zu ~~Bestandsnetzen~~ weiteren Anwendungen des Gesundheitswesens 29
3.9 Sicherer Internetzugang 29
3.10 Außensicht der TI-Plattform im Ganzen 29

4 Lösungen der Architektur der TI-Plattform 31
4.1 Einsatz von Smartcards in der TI 31
4.1.1 Domänen- / Informationsmodell der Karten der TI 32
4.1.1.1 Identitätsträger 33
4.1.1.2 Sicherer Datenspeicher 34
4.1.1.3 Autorisierung und Kartenadministration (Zugriffsregeln) 35
4.1.1.4 PINs 36
4.1.2 Objekttypen der Karten 37
4.1.3 Operationen auf Objekte der Karten 38
4.2 Zugriff auf Karten 40
4.3 Mandantenfähigkeit 41
4.4 Remote-PIN 43
4.5 Mobile Szenarien 45
4.6 Rechenzentrums-Consumer 46

5 Produkttypen der TI-Plattform 49
5.1 Übersicht des Gesamtsystems 49
5.2 Festlegungen zu Produkttypen der TI-Plattform 49
5.3 Produkttypen der Zone TI-Plattform dezentral 52
5.3.1 Produkttyp elektronische Gesundheitskarte (eGK) 53
5.3.2 Produkttyp Heilberufsausweis (HBA) 54
5.3.3 Produkttyp Security Module Card Organisationen des Gesundheitswesens (SMC-B) 54
5.3.4 Produkttyp Hardware Security Module Organisationen des Gesundheitswesens (HSM-B) 55
5.3.5 Produkttyp Security Module Card Kartenterminal (gSMC-KT) 56
5.3.6 Produkttyp Security Module Card Konnektor (gSMC-K) 56
5.3.7 Produkttyp eHealth-Kartenterminal (KT) 57
5.3.8 Produkttyp Mobiles Kartenterminal (MobKT) 58
5.3.9 Produkttyp Konnektor 60
5.3.9.1 Konfigurationsmodell des Konnektors 60
5.3.9.2 Anforderungen an den Konnektor 61
5.4 Produkttypen der Zone TI-Plattform zentral 64
5.4.1 Produkttyp Zentrales Netz TI (Zentrales Netz) 65
5.4.2 Produkttyp Zeitdienst 66
5.4.3 Produkttyp Namensdienst 66

ENTWURF

5.4.4 Produkttyp Verzeichnisdienst 68
5.4.5 Produkttyp TSL-Dienst 70
5.4.6 Produkttyp Konfigurationsdienst (Konfigdienst) 72
5.4.7 Produkttyp VPN-Zugangsdienst (Zugangsdienst) 73
5.4.8 Produkttyp Sicherheitsgateway Bestandsnetze (SG-BNet) 75
5.4.9 Produkttyp Trust Service Provider X.509 nonQES (TSP-X.509nonQES) 76
5.4.10 Produkttyp Trust Service Provider X.509 QES (TSP-X.509QES) 76
5.4.11 Produkttyp gematik Root-CA 77
5.4.12 Produkttyp Trust Service Provider CVC (TSP-CVC) 77
5.4.13 Produkttyp CVC-Root 78
5.4.14 Produkttyp OCSP-Responder Proxy (OCSP-Proxy) 78
5.4.15 Produkttyp Störungsampel 79
5.4.16 Produkttyp Service Monitoring 80

5.5 Interfaces der TI-Plattform Dezentral 82
5.5.1 Basisdienste 83
5.5.1.1 Benutzerinteraktion_KT 83
5.5.1.1.1 I_KT_Operations (Provided) 83
5.5.1.2 Erstellung_Prüfung_Signatur 83
5.5.1.2.1 I_Sign_Operations (Provided) 83
5.5.1.3 Erstellung_Prüfung_QES 85
5.5.1.3.1 I_SAK_Operations (Provided) 85
5.5.1.4 Token_Authentisierung 88
5.5.1.4.1 I_IDP_Auth_Active_Client (Provided) 88
5.5.1.4.2 I_IDP_Auth_Passive_Client (Provided) 89
5.5.1.4.3 I_Local_IDP_Service (Provided) 91
5.5.1.5 Information_Systemzustände 91
5.5.1.5.1 I_Poll_System_Information (Provided) 91
5.5.1.5.2 I_Notification (Required) 92
5.5.1.5.3 I_Notification_From_FM 93
5.5.1.5.4 I_Reg_Notification (Provided) 93
5.5.1.6 KSR 94
5.5.1.6.1 I_KSRC_Management (Provided) 94
5.5.1.6.2 I_KSRC_FM_Support (Provided) 95
5.5.1.6.3 I_KSRC_Local_Management (Provided) 96
5.5.1.6.4 I_KSR_Update (Provided) 96
5.5.1.7 Kartenverwaltung 97
5.5.1.7.1 I_KV_Card_Handling (Provided) 97
5.5.1.7.2 I_KV_Card_Reservation (Provided) 98
5.5.1.8 Kartenfreischaltung 98
5.5.1.8.1 I_KV_Card_Unlocking (Provided) 98
5.5.1.9 Komm_Transport 102
5.5.1.9.1 I_TLS_Client (Provided) 102

ENTWURF

5.5.1.10 Prüfung_Zertifikat ... 102
5.5.1.10.1 I_Cert_Verification (Provided) ... 102
5.5.1.11 Verschlüsselung_Entschlüsselung ... 103
5.5.1.11.1 I_Crypt_Operations (Provided) ... 103
5.5.1.11.2 I_Symm_Crypt_Operations (Provided) ... 105
5.5.1.12 Rollenmanagement_Identitätsmanagement ... 106
5.5.1.12.1 I_Role_Information (Provided) ... 106
5.5.1.13 Verzeichnis_Identitäten ... 106
5.5.1.13.1 I_Directory_Query (Provided) ... 106
5.5.1.14 Mobile_Offline_Dienste ... 106
5.5.1.14.1 I_MobKT_Temp_Storage (Provided) ... 106
5.5.1.14.2 I_MobKT_FMAccess (Provided) ... 107
5.5.1.14.3 I_MobKT_CommFM (Required) ... 108
5.5.1.14.4 I_MobKT_GUI (Provided) ... 109
5.5.1.14.5 I_MobKT_Printer (Provided) ... 110
5.5.1.14.6 I_MobKT_Management (Provided) ... 110
5.5.2 Infrastrukturdienste ... 111
5.5.2.1 Dienstlokalisierung ... 111
5.5.2.1.1 I_DNS_Service_Information (Provided) ... 111
5.5.2.2 Namensauflösung ... 111
5.5.2.2.1 I_DNS_Name_Information (Provided) ... 111
5.5.2.2.2 I_DNS_Name_Resolution (Provided) ... 112
5.5.2.3 Zeitinformation ... 112
5.5.2.3.1 I_NTP_Time_Information (Provided) ... 112
5.5.2.3.2 I_Synchronised_System_Time (Provided) ... 112
5.5.2.3.3 I_Change_System_Time (Provided) ... 113
5.5.2.4 Kartennutzung ... 113
5.5.2.4.1 I_KV_Card_Operations (Provided) ... 113
5.5.2.5 Kartenterminalverwaltung ... 118
5.5.2.5.1 I_KTV_Management (Provided) ... 118
5.5.2.5.2 I_KT_Communication (Provided) ... 118
5.5.2.6 Datenspeicher_FM ... 119
5.5.2.6.1 I_Local_Storage (Provided) ... 119
5.5.3 Netzwerkdienste ... 120
5.5.3.1 Datentransport/Sichere Online-Anbindung/Sicherer Internetzugang ... 120
5.5.3.1.1 I_IP_Transport (Provided) ... 120
5.5.3.2 Sichere_Anbindung_Client ... 121
5.5.3.2.1 I_Facade_Access_Configuration ... 121
5.6 Interfaces der TI-Plattform Zentral ... 122
5.6.1 Basisdienste ... 122

ENTWURF

5.6.1.1 KSR ... 122
5.6.1.1.1 I_KSRS_Download (Provided) ... 122
5.6.1.2 Komm_Transport ... 123
5.6.1.2.1 I_TLS (Required) ... 123
5.6.1.3 Konnektorregistrierung ... 123
5.6.1.3.1 I_Registration_Service (Provided) ... 123
5.6.1.4 Verzeichnis_Identitäten ... 125
5.6.1.4.1 I_Directory_Query (Provided) ... 125
5.6.1.4.2 I_~~Directory~~Data_Maintenance (Provided) ... 125
5.6.1.4.3 I_Directory_Application_Maintenance (Provided) ... 128
5.6.2 Infrastrukturdienste ... 129
5.6.2.1 Dienstlokalisierung ... 129
5.6.2.1.1 I_DNS_Service_Localization (Provided) ... 129
5.6.2.2 Namensauflösung ... 129
5.6.2.2.1 I_DNS_Name_Resolution (Provided) ... 129
5.6.2.3 PKI ... 130
5.6.2.3.1 I_OCSP_Status_Information (Provided) ... 130
5.6.2.3.2 I_TSL_Download (Provided) ... 131
5.6.2.3.3 I_BNetzA_VL_Download (Provided) ... 131
5.6.2.3.4 I_Cert_Provisioning ... 132
5.6.2.3.5 I_Cert_Revocation ... 132
5.6.2.3.6 I_CRL_Download (Provided) ... 133
5.6.2.4 Zeitinformation ... 133
5.6.2.4.1 I_NTP_Time_Information (Provided) ... 133
5.6.2.5 Monitoring des Betriebszustandes ... 134
5.6.2.5.1 I_Monitoring_Update (Provided) ... 134
5.6.2.5.2 I_Monitoring_Read (Provided) ... 134
5.6.2.6 Konfiguration von ~~Bestandsnetzen~~ angeschlossenen Netzen des Gesundheitswesens mit aAdG-NetG ... 135
5.6.2.6.1 I_KSRS_Net_Config (Provided) ... 135
5.6.3 Netzwerkdienste ... 135
5.6.3.1 Datentransport/Sichere Online-Anbindung/Sicherer Internetzugang ... 135
5.6.3.1.1 I_IP_Transport (Provided) ... 135
5.6.3.1.2 I_Secure_Channel_Tunnel (Provided) ... 136
5.6.3.1.3 I_Secure_Internet_Tunnel (Provided) ... 136
5.6.3.2 Zugang_Fremdnetze ... 137
5.6.3.2.1 I_Secure_Access_Bestandsnetz (Provided) ... 137
5.7 Prozess-Interfaces der TI-Plattform ... 137
5.7.1 P_Cert_Provisioning (Provided) ... 137
5.7.2 P_Cert_Revocation (Provided) ... 137
5.7.3 P_Trust_Approval (Provided) ... 138

ENTWURF

5.7.4 P_Sub_CA_Certification_CVC (Provided) 138
5.7.5 P_Sub_CA_Certification_X.509 (Provided)....138
5.7.6 P_CVC_Provisioning (Provided)....139
5.7.7 P_DNS_Name_Entry_Announcement (Provided)....139
5.7.8 P_DNS_Zone_Delegation (Provided) 139
5.7.9 P_DNSSEC_Key_Distribution (Provided) 139
5.7.10 P_DNS_Service_Entry_Announcement (Provided) 140
5.7.11 P_KSRS_Maintenance (Provided)....140
5.7.12 P_~~Directory~~Data_Maintenance (Provided)....140
5.7.13 P_Directory_Application_Registration (Provided) 141
~~5.7.14 P_Directory_Administration_Registration (Provided)~~ 141

6 Das Netzwerk der TI-Plattform 143

6.1.1 Zugangsnetz....144
6.1.2 Zentrales Netz 145
6.1.3 Sicherheitsgateway Bestandsnetze 146
6.1.4 Sicherer Internetzugang 147
6.1.5 Weiternutzung Internet 148
6.1.6 Volumenerfassung im Netzwerk der TI-Plattform....149

6.2 Festlegungen zu Adressierung, Routing und Priorisierung 149
6.2.1 Festlegungen zum einzusetzenden IP-Protokoll 150
6.2.2 Festlegungen zu Adressräumen 151
6.2.3 Festlegungen zum Routing 152
6.2.4 Festlegungen zu Namensräumen....152
6.2.5 Festlegungen zum TLS-Protokoll....153
6.2.6 Festlegungen zur Priorisierung auf Netzwerkebene....153

7 Abhängigkeiten zwischen Produkttypen der TI-Plattform 155

7.1 Prozessabläufe in fachanwendungsspezifischen Diensten 155
7.1.1 Erstellung und Prüfung von digitalen Signaturen (Erstellung_Prüfung_Signatur)....155
7.1.1.1 Erstellung von digitalen Signaturen....155
7.1.1.2 Prüfung von digitalen Signaturen....156
7.1.2 Prüfung von X.509-Zertifikaten (Prüfung_Zertifikat) 157
7.1.2.1 TSL-Validierung....157
7.1.2.2 Prüfung von X.509-Zertifikaten 158

7.2 Prozessabläufe zwischen Produkttypen der TI-Plattform....158
7.2.1 Benutzerinteraktion_KT 159
7.2.1.1 Ablauf Benutzerinteraktion am Kartenterminal....159
7.2.2 Erstellung_Prüfung_QES....159
7.2.2.1 Ablauf QES erzeugen 159
7.2.2.2 Ablauf QES prüfen....160
7.2.3 Information_Systemzustände 161
7.2.3.1 Ablauf Anmeldung zur Notifikation und Notifikation....161
7.2.3.2 Ablauf Sammeln der Umgebungsinformationen und Abfrage RessourcenInfo 162
7.2.4 Konfigurations- und Software Repository (KSR) 164
7.2.4.1 Ablauf Anzeigen verfügbarer Aktualisierungen 164
7.2.4.2 Ablauf Software oder Konfigurationen aus KSR aktualisieren....164

ENTWURF

7.2.4.3 Ablauf ~~Bestands~~Netzkonfigurationen aAdG-NetG aktualisieren 166
7.2.4.4 Ablauf Anzeigen verfügbarer Pakete für Fachmodul 167
7.2.4.5 Ablauf Paket für Fachmodul aus KSR laden 167
7.2.5 Aktualisierung von TSL und Vertrauensliste der BNetzA in Produkttypen 168
7.2.5.1 Ablauf Aktualisierung der TSL über die TI-Plattform 168
7.2.5.2 Ablauf Aktualisierung der Vertrauensliste der BNetzA über die TI-Plattform 169
7.2.6 Aktualisierung der CRL im Konnektor 170
7.2.6.1 Ablauf Aktualisierung der CRL im Konnektor 170
7.2.7 Prüfung von X.509-Zertifikaten (Prüfung_Zertifikat) 171
7.2.7.1 Ablauf Initialisierung Trust Store 171
7.2.7.2 Ablauf Zertifikat prüfen 172
7.2.8 Verzeichnis_Identitäten 172
7.2.8.1 Ablauf Abfrage des Verzeichnisses 172
7.2.9 Namensauflösung 173
7.2.9.1 Ablauf FQDN des TI-Namensraums auflösen 173
7.2.9.2 Ablauf FQDN für sichere Online-Anbindung auflösen 175
7.2.9.3 Ablauf FQDN aus ~~Bestandsnetzen~~ Netzen des Gesundheitswesens mit aAdG-NetG auflösen 175
7.2.10 Zeitinformation 176
7.2.10.1 Ablauf Zeitinformation der TI abfragen 176
7.2.11 Kartenzugriff 177
7.2.11.1 Ablauf generische Kartenoperation 177
7.2.11.2 Ablauf PIN-Eingabe direkt 179
7.2.11.3 Ablauf PIN-Eingabe mit Remote_PIN 181
7.2.12 Sichere Online-Anbindung 183
7.2.12.1 Ablauf Aufbau eines sicheren Kanals zur Anbindung an die zentrale TI-Plattform 183
7.2.13 Sicherer Internetzugang 184
7.2.13.1 Ablauf Aufbau eines sicheren Kanals zur Anbindung des sicheren Internetzugangs 184

Anhang A – Verzeichnisse 186
A1 – Abkürzungen 186
A2 – Glossar 188
A3 – Abbildungsverzeichnis 188
A4 – Tabellenverzeichnis 189
A5 – Referenzierte Dokumente 194
A5.1 – Dokumente der gematik 194
A5.2 – Weitere Dokumente 195

Anhang B – Kryptographische Endnutzer-Identitäten und deren Einsatz in der TI-Plattform 196

Anhang C – Datentypen der TI-Plattform 201

Anhang D – Informationsmodell der TI-Plattform 204

ENTWURF

1 Einordnung des Dokuments

1.1 Zielsetzung

Die Telematikinfrastruktur ist die gesetzlich geforderte und legitimierte Informations-, Kommunikations- und Sicherheitsinfrastruktur des deutschen Gesundheitswesens. Sie wird durch die Gesellschafter der gematik gestaltet.

Das vorliegende Architekturkonzept benennt vollständig und abschließend die Produkttypen der TI-Plattform und legt die Schnittstellen der Produkttypen auf konzeptueller Ebene fest. Hierzu werden neben den funktionalen Eigenschaften der Schnittstellen auch Schutzleistungen für Informationsobjekte und nichtfunktionale Leistungen wie die Antwortzeit festgelegt. Das vorliegende Konzept schließt damit die konzeptuelle Ebene der TI-Plattform ab und definiert die Basis für die technologische Ausprägung der Schnittstellen der Produkttypen der TI-Plattform.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter von Produkten der TI und an die Anbieter weiterer Anwendungen des Gesundheitswesens sowie der Gesundheitsforschung.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Schutzrechts-/Patentrechtshinweis:

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzung des Dokuments

Die Architektur der TI-Plattform hat als Zielsetzung die statische Darstellung des Gesamtsystems „TI-Plattform“ zum Start des Wirkbetriebes. Sie enthält keine Vorgaben zu Aufbau, Test, Zulassungsverfahren und Betrieb dieses Systems (siehe hier [gemKPT_Test] und [gemKPT_Betr]).

ENTWURF

Das vorliegende Dokument beschreibt als systemspezifisches Konzept ausschließlich das System TI-Plattform und grenzt sich damit gegen die Fachanwendungen ab.

1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen, deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

⌦ **TIP1-A_xxxx <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

ENTWURF

2 Grundlagen der Architektur der TI-Plattform

2.1 Architekturmerkmale

2.1.1 TI-Plattform als Basis der Fachanwendungen

Die Trennung von TI-Plattform und Fachanwendungen ist als dediziertes Ziel der TI-Plattform festgelegt worden und darin die Entkopplung der Systeme TI-Plattform und Fachanwendungen gefordert. Dabei ist es unerheblich, ob es sich um eine Fachanwendung der Telematikinfrastruktur oder um eine unbekannte Fachanwendung auf den Clientsystemen handelt. Ein grundlegendes Merkmal der Architektur ist die Entkopplung der TI-Plattform von den Fachanwendungen bzgl. der folgenden Aspekte:

- Technologische Entkopplung.
- Semantische und syntaktische Entkopplung.
- Entkopplung von Fehlerzuständen.
- Eindämmung von gegenseitigen Abhängigkeiten zwischen Fachanwendung und Plattform im Bereich der Releasezyklen.
- Entkopplung von Maßnahmen zur IT-Sicherheit und zum Datenschutz.

Die Dienste der TI-Plattform stellen den Komponenten der Fachanwendungen generische Funktionalitäten zur Verfügung.

Diese Dienste werden in folgende Kategorien eingeteilt:

- Basisdienst
- Infrastrukturdienste
- Netzwerkdienste

ENTWURF

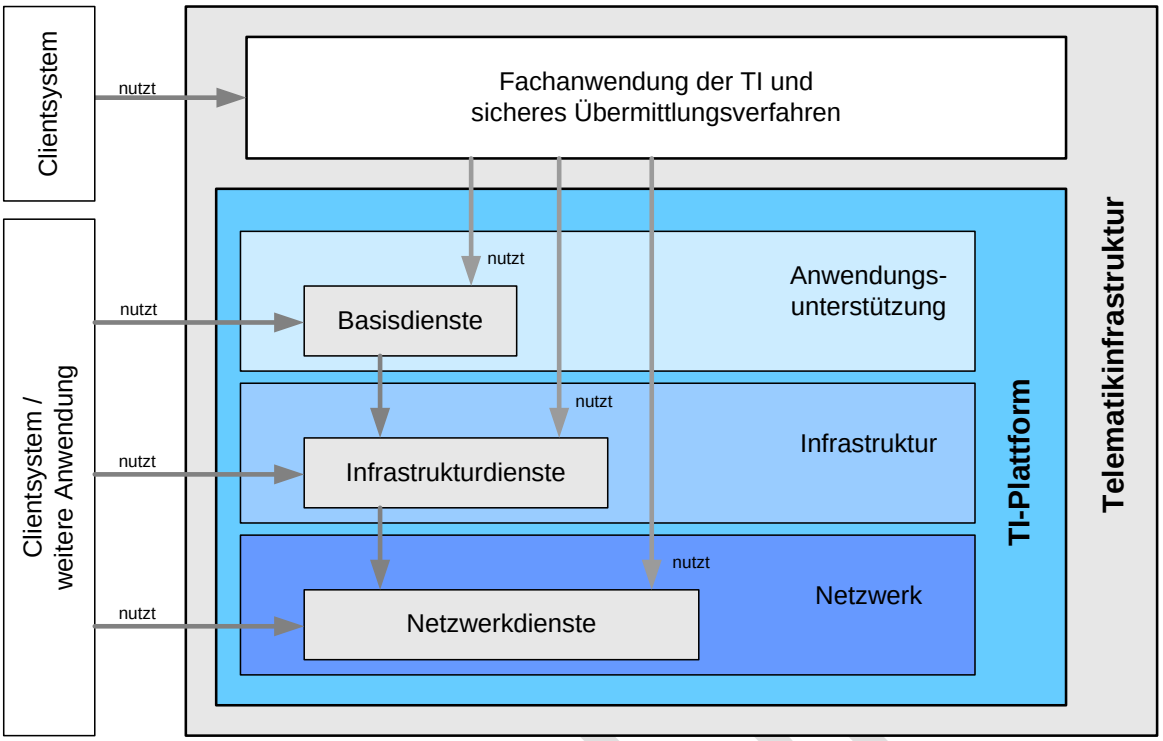


Abbildung 1: Dienst-Kategorien der TI-Plattform

Basis-, Infrastruktur- und Netzwerkdienste werden in den Schichten der TI-Plattform zur Unterstützung der Fachanwendungen mit allen nötigen technischen und organisatorischen Anteilen bereitgestellt. Dienste können und sollen andere Dienste nachnutzen, jedoch gemäß der Schichtenlogik niemals Dienste einer darüber liegenden Schicht.

Basisdienste bieten umfassende Leistungen auf der anwendungsunterstützenden Ebene an, wie z. B. die komplette Abwicklung einer Signaturvalidierung inklusive mathematischer Prüfungen und Zertifikatsprüfung.

Infrastrukturdienste bieten generische Funktionen auf Infrastrukturebene an und sind systemnäher als Basisdienste. Sie werden häufig direkt von Basisdiensten zur Erbringung ihrer Leistungen benötigt.

Netzwerkdienste bilden die Transportschnittstelle der dezentralen Komponenten zu dem geschlossenen zentralen Netz der TI-Plattform und ermöglichen den Transport von Daten zwischen den zentralen Diensten der TI-Plattform, den fachanwendungsspezifischen Diensten und den dezentralen Komponenten der TI-Plattform. Die Netzwerkdienste können von Infrastrukturdiensten, Basisdiensten und Fachdiensten direkt genutzt werden.

Für die Beschreibung der Netzwerkkommunikation werden folgende Begriffe verwendet:

- Netzwerkschicht – entspricht der OSI-Schicht 3
- Transportschicht – entspricht der OSI-Schicht 4
- Anwendungsschicht – entspricht den OSI-Schichten 5 bis 7
- Transportnetz – entspricht der Summe der OSI-Schichten 1 bis 4 die als Netzwerkdienste der TI-Plattform den Fachanwendungen und Clientsystemen bereitgestellt werden

2.1.1.1 Schnittstelle zu den Fachanwendungen

Die TI-Plattform stellt den Fachanwendungen klar definierte Leistungen zur Verfügung: An der Schnittstelle zu den Fachanwendungen bietet die TI-Plattform Dienste an. Kapitel 5.5 und 5.6 legen für alle Dienste auf Ebene von Operationen

- die spezifischen funktionalen und nichtfunktionalen Leistungsanforderungen an die TI-Plattform,
- sowie die durch den Schnittstellennutzer zu befolgende Regeln fest.

⌦ **TIP1-A_2197 Außenschnittstellen parallel nutzbar**

Die Außenschnittstellen der TI-Plattform SOLLEN so implementiert werden, dass sie parallel durch mehrere Aufrufer nutzbar sind.⌫

2.1.1.2 Anwendungsneutralität

Die Architektur der TI schichtet Funktionalitäten nach klar definierten Verantwortungsbereichen, die jeweils aufeinander aufbauen. Die oberste Ebene bilden die Fachanwendungen, die sich der Funktionalitäten der von der TI-Plattform bereitgestellten darunterliegenden Schichten (Basisdienste, Infrastrukturdienste, Netzwerkdienste) bedienen.

Dabei sind die Dienste, welche die TI-Plattform den Fachanwendungen anbietet, grundsätzlich anwendungsneutral. Dieser Ansatz wirkt sich positiv auf Wirtschaftlichkeit und Produkteinführungszeit bei der Einführung neuer Anwendungen aus.

Damit sind – soweit sich die Außenschnittstelle der TI-Plattform nicht ändert – Änderungen in der TI-Plattform von Änderungen der Fachanwendungen entkoppelt.

2.1.1.3 Dienstbaukasten und Erweiterbarkeit

Die TI-Plattform bietet den Fachanwendungen die freiwillige und flexible Nutzung von Diensten an. Die Fachanwendungen werden aus folgenden Gründen konzeptionell nicht eingeschränkt:

- Die Anwendungsneutralität der Dienste ermöglicht eine klare Trennung zwischen Dienst und Fachanwendung auf Konzeptionsebene.
- Wenn das Dienstangebot der TI-Plattform für eine Fachanwendung dessen Anforderungen gar nicht oder nicht bedarfsgerecht erfüllt, kann die Fachanwendung entweder eine Erweiterung des Dienstangebots der TI-Plattform motivieren oder eine eigene Alternativlösung einsetzen.

Um die Fachanwendungen in ihrem technischen Lösungsraum nicht unnötig einzuschränken, bieten Dienste der TI-Plattform ihre technische Schnittstelle vorzugsweise über bewährte (Reife, Verbreitung und Akzeptanz) Standards an.

So entsteht insgesamt ein Dienstbaukasten, aus dem sich die Fachanwendungen nach Bedarf bedienen können.

Bei der Schnittstelle zwischen Fachmodul und TI-Plattform im Konnektor, werden Schnittstellen auf logischer Ebene festgelegt.

ENTWURF

2.1.1.4 Weitere Anwendungen des Gesundheitswesens und sichere Übermittlungsverfahren

Neben den Fachanwendungen der Telematikinfrastruktur bietet die TI-Plafform auch Leistungen für weitere Anwendungen des Gesundheitswesens und sichere Übermittlungsverfahren an. Alle oben aufgeführten Qualitätsmerkmale der TI-Plattform im Bezug auf Fachanwendungen der Telematikinfrastruktur gelten auch im Bezug auf die weiteren Anwendungen des Gesundheitswesens und die sicheren Übermittlungsverfahren. Welche konkreten Leistungen der TI-Plattform für weitere Anwendungen des Gesundheitswesens angeboten werden, ist dem Kapitel 5.6 zu entnehmen. Sichere Übermittlungsverfahren erhalten Zugriff auf alle Leistungen, die auch den Fachwendungen der Telematikinfrastruktur angeboten werden.

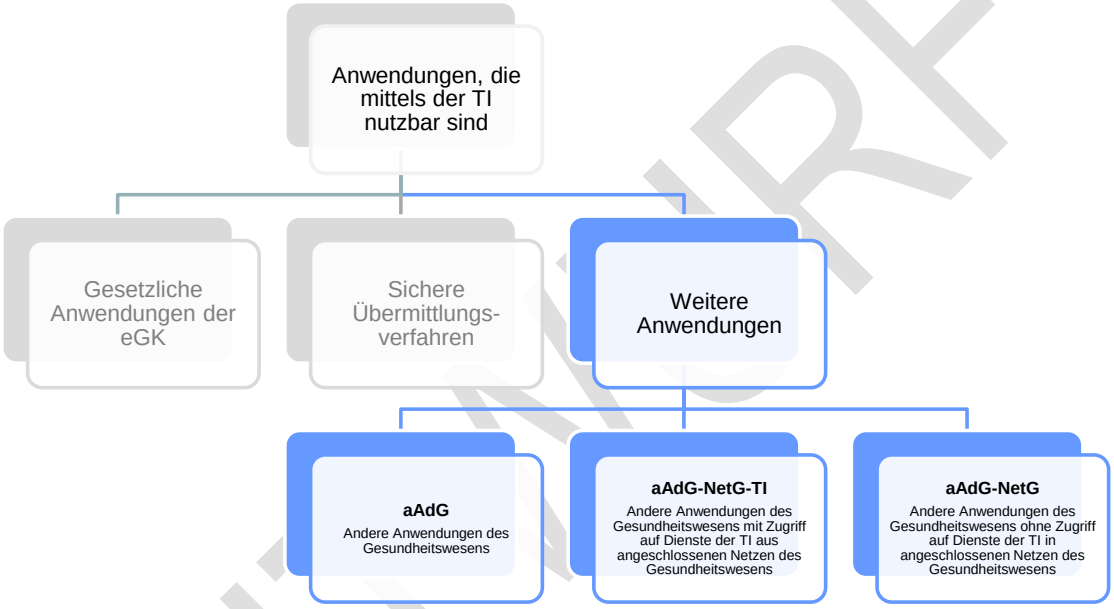


Abbildung 2: Anwendungskategorien von weiteren Anwendungen

Es werden drei Anwendungskategorien von weiteren Anwendungen unterschieden:

- Andere Anwendungen des Gesundheitswesens (aAdG)
- Andere Anwendungen des Gesundheitswesens mit Zugriff auf Dienste der TI aus angeschlossenen Netzen des Gesundheitswesens (aAdG-NetG-TI)
- Andere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens (aAdG-NetG)

2.1.2 Produkttypen, Produkte und Produktinstanzen

Produkttypen sind die kleinsten Bestandteile des Gesamtsystems TI, die als eine Einheit umgesetzt und betrieben werden können. Produkttypen mit allen ihren zugrundeliegenden Vorgaben sind auch die Grundlage für die Test- und Zulassungsverfahren. Produkttypen leiten sich durch eine Systemzerlegung der Systeme der TI – also der Fachanwendung und der TI-Plattform – ab.

ENTWURF

Durch die Konzepte und Spezifikationen der TI werden Produkttypen vollständig durch Anforderungen definiert. Basierend auf diesen Anforderungen können konkrete Umsetzungen in Produkten erfolgen. Im Wirkbetrieb werden schließlich Instanzen bzw. Installationen von Produkten mittels Produktinstanzen ausgeprägt. Es entsteht ein hierarchisches Informationsmodell für die Telematikinfrastruktur mit drei Ebenen.

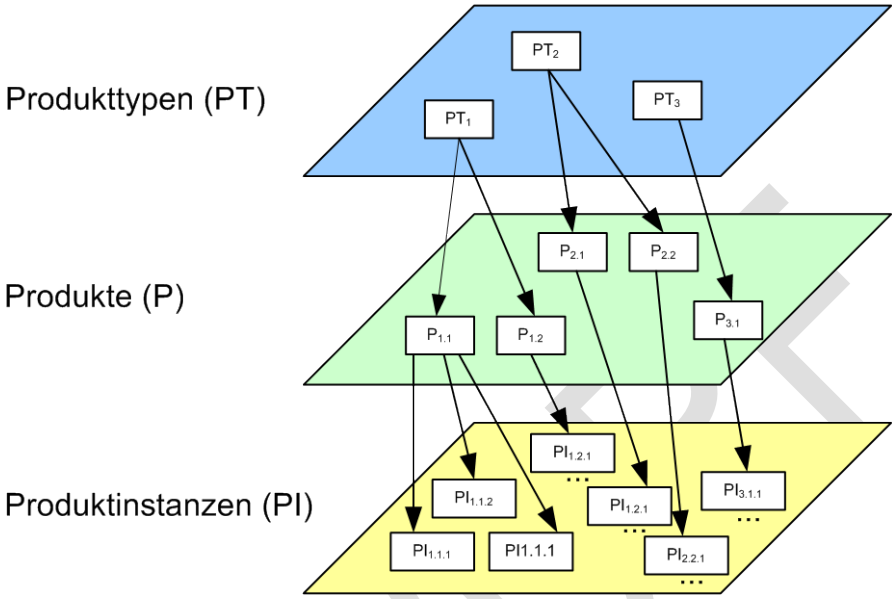


Abbildung 3: Modellierung der TI mittels Produkttypen, Produkten und Produktinstanzen

Kapitel 5 des vorliegenden Dokuments führt eine Systemzerlegung der TI-Plattform durch und leitet unter Berücksichtigung funktionaler und der genannten nichtfunktionalen Aspekte die Produkttypen her. Mit der Definition der Produkttypen und ihrer Schnittstellen sind kleinste Einheiten der Verantwortlichkeitsgrenzen für die Herstellung und Betrieb geschaffen.

Ein großer Freiheitsgrad in den Produktinstanzkardinalitäten unterstützt das Prinzip des diskriminierungsfreien Wettbewerbs:

- Die Anbindung verschiedener Instanzen von fachanwendungsspezifischen Diensten der gleichen Anwendung ist grundsätzlich möglich. Sie wird durch Ausgestaltung der Netzwerkdienste und der Dienstlokalisation unterstützt.
- Wo technisch, organisatorisch oder wirtschaftlich sinnvoll, wird die Möglichkeit von konkurrierenden Infrastrukturdiensten vorgesehen.

2.1.3 Logische Architekturschichten (Zonen)

Entlang vertikaler Architekturschichten vom Consumer zum Provider erfolgt in diesem Kapitel eine Zuordnung von Building Blocks. Die Architekturschichten sind ebenso wie die Building Blocks als logische Strukturen zu verstehen. Sie implizieren zunächst keine Trennung auf Hardwareebene. Die hier betrachteten logischen vertikalen Architekturschichten werden Zonen genannt. Abbildung 4 stellt die Verteilung der Building Blocks (graue Rechtecke) auf die Zonen dar. Die Trennung nach Fachanwendung und TI-Plattform wird durch eine Darstellung in zwei horizontale Schichten unterstrichen.

ENTWURF

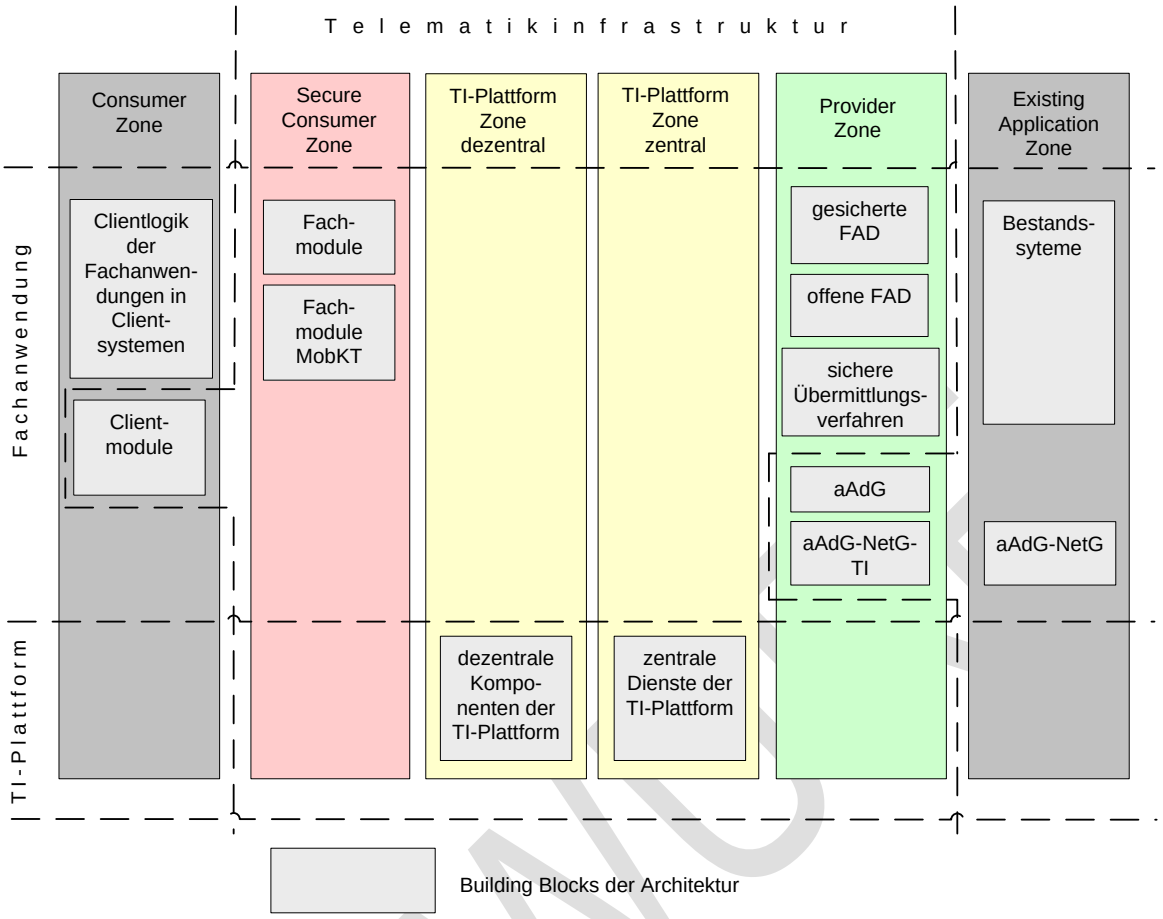


Abbildung 4: Logische Architekturschichten (Zonen) und Building Blocks

Die Consumer Zone enthält Komponenten des Benutzerinterfaces für fachliche Funktionalität (Clientsysteme) oder separat verteil- und installierbare Komponenten der Fachanwendung (Clientmodule). Komponenten dieser Zone haben eingeschränkten Zugriff auf die Basisdienste der TI-Plattform. Im Gegensatz dazu kann den Komponenten der Secure Consumer Zone Zugriff auf alle Basisdienste gewährt werden. Ein Clientsystem kann z. B. die Software sein, die auf dem Arbeitsplatzrechner des Arztes ausgeführt wird. Clientmodule[1] sind als Komponente der Fachanwendung identifizierbar und sind einem konkreten fachanwendungsspezifischen Dienst zugeordnet. In ihren Berechtigungen ggü. der TI-Plattform unterscheiden sich Clientmodule nicht von Clientsystemen. Daher wird im nachfolgenden Dokument nicht an allen Stellen zwischen Clientmodulen und Clientsystemen unterschieden. Aussagen für Clientsysteme gelten auch für Clientmodule.

Die TI-Plattform ist unterteilt in eine dezentrale Zone und eine zentrale Zone. Beide Zonen sind frei von Komponenten mit fachspezifischer Logik. Diese beiden Zonen erbringen die Basisdienste sowie die Infrastruktur- und Netzwerkdienste der TI-Plattform. Darüber hinaus dienen die Zonen der Vermittlung zwischen Consumer/Secure Consumer Zone und Provider Zone.

Die TI-Plattform Zone dezentral umfasst die Komponenten der TI-Plattform, die in den Räumen der Nutzer der TI betrieben werden - wie z. B. Konnektoren, Kartenterminals,

[1] Clientmodule sind Produkttypen von Anwendungen der TI. Festlegungen zu konkreten Produkttypen sind den Systemlösungen der entsprechenden Fachanwendungen zu entnehmen.

Smartcards. Sie dient als Schutz der Infrastruktur vor Bedrohungen aus dem Client-Netz und umgekehrt. Diese Zone wird nachfolgend auch als dezentrale TI-Plattform bezeichnet.

Zur TI-Plattform Zone zentral gehören die zentralen Dienste der TI-Plattform, wie OCSP-Responder, Konfigurationsdienst etc., hier wird die zentrale Kommunikationsleistung der Telematikinfrastruktur erbracht. Diese Zone wird nachfolgend auch als zentrale TI-Plattform bezeichnet.

In der Provider Zone werden die fachliche Logik, die fachlichen Schnittstellen der fachanwendungsspezifischen Dienste und die Dienste der sicheren Übermittlungsverfahren bereitgestellt. Die fachanwendungsspezifischen Dienste bilden einen Service Layer, der die Nutzung von Bestandssystemen ermöglicht. Auf die gesicherten fachanwendungsspezifischen Dienste kann nur von Fachmodulen und von fachanwendungsspezifischen Diensten nach Freischaltung[2] zugegriffen werden.
Auch Dienste von anderen Anwendungen des Gesundheitswesens mit Zugriff auf zentrale Dienste der TI-Plattform (aAdG und aAdG-NetG-TI, siehe auch [gemRL_NvTIwA]) stehen in der Provider Zone, sind aber nicht Teil der Telematikinfrastruktur.

Die Existing Application Zone umfasst die Bestandssysteme der Fachanwendungen (z. B. CMS). Auch ~~Bestandsnetze~~ Netze des Gesundheitswesens mit anderen Anwendungen des Gesundheitswesens ohne Zugriff auf zentrale Dienste sind hier eingeordnet.

Normalerweise ist ein Produkttyp genau einem Building Block der Architektur zugeordnet. Im dezentralen Bereich gibt es aber die Möglichkeit eines Rechenzentrum-Consumers, der Elemente der Zonen TI-Plattform dezentral, Consumer und ggf. auch Secure Consumer in einem Produkttyp vereint. Auch in so einem Fall werden alle Annahmen an die einzelnen Zonen, die Regelungshoheit für die Zone und die Anforderungen an die Übergänge zwischen den Zonen innerhalb des Produkttyps umgesetzt.

⌦ **TIP1-A_6094 Produkttypen über Zonengrenzen hinweg**

Alle Produkttypen, die sich über Zonengrenzen hinweg erstrecken, MÜSSEN innerhalb des Produkttyps alle Anforderungen, Zusicherungen und die Regelungshoheit in den enthaltenen Zonen sowie an deren Übergängen durchsetzen. ⌫

2.1.4 Kontrolle der Kommunikationswege

Die grundsätzlich erlaubten Kommunikationsmöglichkeiten zwischen den Zonen sind in Tabelle 1 definiert. Die Regelungshoheit der TI-Plattform beschränkt sich auf die TI-internen Kommunikationsmöglichkeiten (Zonen SC, TI_D, TI_Z und P).

Tabelle 1: Kommunikationsmatrix TI (Zonen)

[2] Die Dienst-zu-Dienst-Kommunikation zwischen fachanwendungsspezifischen Diensten, den Diensten der sicheren Übermittlungsverfahren bzw. zwischen weiteren Anwendungen des Gesundheitswesens in der Provider Zone über das zentrale Netz muss für jede Verbindung explizit freigeschaltet werden.

ENTWURF

	Consumer Zone (C)	Secure Consumer Zone (SC)	TI-Plattform-Zone dezentral (TI_D)	TI-Plattform-Zone zentral (TI_Z)	Provider Zone (P)	Existing Application Zone (EA)
Consumer Zone (C)	--[3]	X	X	--	X[4]	X[5]
Secure Consumer Zone (SC)	X[6]	X[7]	X	--	X	--
TI-Plattform-Zone dezentral (TI_D)	X[6]	X[6]	X	X	--	--
TI-Plattform-Zone zentral (TI_Z)	--	--	--	X	~~--~~X[8]	--
Provider Zone (P)	--	--	--	X	X	X
Existing Application Zone (EA)	--	--	--	--	X[9]	--

Die in diesem Rahmen zwischen Produkttypen erlaubten Kommunikationswege definiert Kapitel 7.2. Pro Operation wird festgelegt, welcher Produkttyp als Aufrufer erlaubt ist.

⌦ **TIP1-A_2198 Nur erlaubte Kommunikation zwischen Produkttypen möglich**

Die TI-Plattform MUSS sicherstellen, dass zonenübergreifend nur erlaubte Kommunikation zwischen Produkttypen möglich ist. Die Definition der Kommunikationswege erfolgt auf Grundlage der Parameter IP-Adresse, UDP/TCP-Port und Verbindungsrichtung, wobei auch definierte IP-Adressbereiche und/oder UDP/TCP-Portbereiche (z.B. pro Fachanwendung ~~und Bestandsnetz~~ oder weiterer Anwendung) möglich sind.⌫

In der TI-Plattform zentral ist die Kommunikation in Richtung aller zugelassenen Dienste und angeschlossenen ~~Bestandsnetze~~ weiteren Anwendungen im Rahmen des Test-, Bestätigungs- und Zulassungsverfahrens freizuschalten. Im dezentralen Bereich ist die Kommunikation zu Pflichtanwendungen gemäß §291a SGB V [SGB V] immer erlaubt. Die

[3] Die Kommunikation innerhalb der Consumer Zone unterliegt nicht der Regelungshoheit der Telematikinfrastruktur.

[4] Nur offene fachanwendungsspezifische Dienste sind aus der Consumer Zone erreichbar.

[5] Diese Kommunikation beschränkt sich auf die Anbindung ~~des SNK bzw. anderer angeschlossener Bestandsnetze~~ von Netzen des Gesundheitswesens mit anderen Anwendungen des Gesundheitswesens ohne Zugriff auf zentrale Dienste (aAdG-NetG) und den sicheren Internetzugang.

[6] Diese Kommunikation ist nur erlaubt, wenn nach dem Publish-Subscribe Pattern zuvor eine Registrierung vorgenommen wurde.

[7] Die Kommunikation zwischen Fachmodulen erfolgt nur, wenn die beteiligten Fachanwendungen diese vorgesehen haben.

[8] Diese Kommunikation ist nur für das Service Monitoring erlaubt.

[9] Diese Kommunikation darf nicht aus ~~dem SNK bzw. anderen angeschlossenen Bestandsnetzen~~ einem Netz des Gesundheitswesens mit anderen Anwendungen des Gesundheitswesens ohne Zugriff auf zentrale Dienste (aAdG-NetG) erfolgen.

ENTWURF

Kommunikation in Richtung aller ~~Bestandsnetze~~ Netze des Gesundheitswesens mit anderen Anwendungen des Gesundheitswesens ohne Zugriff auf zentrale Dienste (aAdG-NetG) ist grundsätzlich freigeschaltet, kann durch den Administrator aber für jedes einzelne ~~Bestands~~Netz explizit unterbunden werden. Dabei wird immer das ~~Bestands~~Netz als Ganzes und nicht einzelne Dienste im ~~Bestands~~Netz freigeschaltet.

2.2 Betrieb und Wartung (Operation and Maintenance)

Die übergreifenden betrieblichen Anforderungen an die Architektur der TI-Plattform und Fachdienste werden großteils in der übergreifenden Spezifikation Operation and Maintenance [gemSpec_OM] aufgegriffen und umgesetzt.

Damit Informationen zum aktuellen Betriebszustand der TI hinsichtlich ihrer Verfügbarkeit und der Einhaltung definierter Antwortzeiten auf Dienstebene an einer zentralen Stelle zusammengefasst und angezeigt werden können, führt die Architektur der TI-Plattform den Infrastrukturdienst „Monitoring Betriebszustand“ ein und setzt ihn durch den Produkttypen „Störungsampel“ um.

2.3 Bedarfsgerechte Leistungsfähigkeit (Performance)

Das vorliegende Dokument beinhaltet nicht das Performancemodell der TI-Plattform. Das Performancemodell wird unter Berücksichtigung der konzeptionellen Architektur auf Ebene der übergreifenden Spezifikationen festgelegt und weist die Leistungsparameter

- Antwortzeit je Einzelanfrage,
- Anfragerate je Einzelanfrage und
- Verfügbarkeit je Produkttyp

aus.

2.4 Sicherheitsleistung der TI-Plattform

2.4.1 Abgrenzung zwischen TI-Plattform und Fachanwendung

Für die Ende-zu-Ende-Sicherheit einer Fachanwendung ist ausschließlich die Fachanwendung selber verantwortlich. Die TI-Plattform stellt den Fachanwendungen ihre Funktionen mit definierten Sicherheitsniveaus zur Verfügung. Die korrekte Verwendung dieser Funktionen sowie die Kombination der Funktionen und die Ergänzung um Eigenleistungen zur Erreichung der seitens der Fachanwendungen benötigten Gesamtsicherheit obliegen der Fachanwendung.

Damit die Fachanwendungen dieses Prinzip erfolgreich anwenden können, benötigen Sie Angaben, welche maximalen Schutzbedarfe die Funktionen der TI-Plattform hinsichtlich Vertraulichkeit, Integrität und Authentizität verarbeiten können. Die jeweils durch die TI-Plattform garantierten maximalen Schutzbedarfe der transportierten und verarbeiteten Informationsobjekte werden für jeden Parameter einer jeden Operation ausgewiesen (siehe Kapitel 5.5 und 5.6). Die Fachanwendungen dürfen sich darauf verlassen, dass die

ENTWURF

TI-Plattform alle erforderlichen Maßnahmen einleiten wird, damit die garantierten Höhen der verarbeitbaren Schutzbedarfe erreicht werden.

Die TI-Plattform unterscheidet in der Bewertung und Verarbeitung zwei Klassen von Daten:

1. Daten der Fachanwendungen
2. Daten der TI-Plattform

Hinsichtlich der Daten der Fachanwendungen gilt, dass die TI-Plattform zu keinem Zeitpunkt Kenntnis über die Semantik der Fachdaten besitzt. Ob es sich im Einzelfall der seitens einer Fachanwendung an die TI-Plattform übergebenen Daten um Daten mit Personenbezug oder mit medizinischem Inhalt handelt, kann die TI-Plattform nicht erkennen. Die TI-Plattformoperationen weisen immer das von ihnen maximal bearbeitbare Sicherheitsniveau aus. Es obliegt der Fachanwendung in ihren Sicherheitskonzepten zu prüfen, welche konkreten Schutzbedarfe ihre Daten haben, die sie an die Schnittstellen der TI-Plattform übergibt bzw. von ihr erhält. Ferner wird die TI-Plattform Daten der Fachanwendungen nur für die von der Fachanwendung vorgegebene, notwendige Dauer des Transports oder die von der Fachanwendung angeforderte Bearbeitung in der TI-Plattform halten[10].

Hinsichtlich der Daten der TI-Plattform gilt, dass die Fachanwendungen bezüglich intern bewegter Plattformdaten keine Sicherheitsbetrachtungen durchführen müssen. Die TI-Plattform garantiert, dass alle in ihr intern bewegten Daten ihren Schutzbedarfen entsprechend ver- und bearbeitet werden.

Eine Verantwortung der Fachanwendung für Daten der TI-Plattform ergibt sich dann, wenn Daten der TI-Plattform an die Fachanwendungen weitergereicht werden. In diesem Fall übernimmt die Fachanwendung die Verantwortung für die sicherheitsgemäße Verarbeitung der entgegengenommenen Plattformdaten. Diese Daten sind im Rahmen der Sicherheitsanalyse der Fachanwendungen zu berücksichtigen. Beispiele hierfür sind Statusmeldungen der TI-Plattform an die Fachanwendung oder Ressourcenidentifikatoren mit erhöhtem Schutzbedarf.

2.4.2 Sicherheitsleistung der Produkttypen

Der in der TI-Plattform verfolgte grundsätzliche Ansatz zur Sicherung schutzbedürftiger Daten basiert auf dem Prinzip der Kapselung. Daten, die an eine Einheit übergeben werden, werden von dieser Einheit vertrauenswürdig verarbeitet. Diesem Prinzip folgend wird als Grundanforderung an jeden Produkttyp aufgenommen, dass Daten, die der Produkttyp über seine Außenschnittstellen erhalten hat oder die im Produkttyp erzeugt wurden, hinsichtlich Vertraulichkeit, Integrität und Authentizität zu schützen sind. Der Produkttyp wird in diesem Fall als Blackbox betrachtet, die grundsätzlich alle Daten in ihr vor einem unberechtigten Zugriff von Außen bis zu einer maximale Höhe schützt – unabhängig vom konkreten Schutzbedarf der einzelnen Daten. Die von einem Produkttyp zu erreichende Höhe der maximal verarbeitbaren Schutzbedarfe wird je Operation am Produkttyp ausgewiesen.

[10] Dies gilt auch für Fachdaten, die auf der eGK oder dem mobilen Kartenterminal gespeichert werden. Die Ordner der eGK bzw. die Speicherbereiche des mobilen Kartenterminals, in denen diese Daten abgelegt werden, gelten als Speicherort der Fachanwendungen.

ENTWURF

2.5 Parallelbetrieb eGK-Generationen 1 und 2

In der Konzeption der TI-Plattform werden eGK der Generationen 1 und 2 nicht unterschieden, da eGKs der Generation 2 vollständig kompatibel zu denen der Generation 1 sind. Die eGKs beider Generationen werden in Konzepten und Spezifikationen funktional immer wie Karten der Generation 1 genutzt. Dessen unbeachtet, besteht die Möglichkeit Identitäten und Zertifikate der Generation 2 zu nutzen, wo dies sinnvoll erscheint und aus Sicht der Kompatibilität möglich ist.

2.6 Rollen der TI-Plattform

2.6.1 Personenkreise der Telematikinfrastruktur

In §291a SGB V [SGB V] wird der zugriffsberechtigte Personenkreis für die Nutzung von §291a-Fachanwendungen abschließend festgelegt. Die TI-Plattform muss bei der Erbringung der Plattformleistungen diesen zugriffsberechtigte Personenkreis durch ein geeignetes Rollenmodell unterstützen. Tabelle 2 enthält den im Kontext der eGK beteiligten Personenkreis des §291a SGB V [SGB V].

Tabelle 2: Zugriffsberechtigter Personenkreis (PK) nach §291a SGB V

PK-Nr.	Zugriffsberechtiger Personenkreis	§291a SGB V
1	Versicherter	§291a Abs. 4 Satz 2 SGB V
2	Ärzte	§291a Abs. 4 Satz 1 Nr.1 a) SGB V und §291a Abs. 4 Satz 1 Nr.2 a) SGB V
3	Zahnärzte	§291a Abs. 4 Satz 1 Nr.1 b) SGB V und §291a Abs. 4 Satz 1 Nr.2 b) SGB V
4	Apotheker, Apothekerassistenten, Pharmazieingenieure, Apothekenassistenten	§291a Abs. 4 Satz 1 Nr.1 c) SGB V und §291a Abs. 4 Satz 1 Nr.2 c) SGB V
5	Personen, die bei den unter Nr. 2 bis Nr. 4 genannten oder im Krankenhaus als berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf tätig sind.	§291a Abs. 4 Satz 1 Nr.1 d) SGB V und §291a Abs. 4 Satz 1 Nr.2 d) SGB V
6	Sonstige Erbringer ärztlich verordneter Leistungen	§291a Abs. 4 Satz 1 Nr.1 e) SGB V
7	Angehörige eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert.	§291a Abs. 4 Satz 1 Nr.2 e) SGB V
8	Psychologischer Psychotherapeut und Kinder- und Jugendlichenpsychotherapeut	§291a Abs. 4 Satz 1 Nr.2 f) SGB V
9	Person, die bei einer Krankenkasse gemäß §291 SGB V tätig ist	Herausgeber der eGK nach §§291, 291a SGB V

Über die in §291a SGB V [SGB V] genannten Personenkreise hinaus, gibt es noch weitere Personenkreise, die nicht zur Nutzung von §291a-Fachanwendungen berechtigt sind, aber die Telematikinfrastruktur nutzen oder mit ihr interagieren. Tabelle 3 benennt diese Personenkreise.

ENTWURF

Tabelle 3: Personenkreis ohne Zugriffsberechtigung nach §291a SGB V

PK-Nr.	Personenkreis ohne Zugriffsberechtigung nach §291a SGB V	Abgrenzung zu §291a SGB V
10	Sonstige Personen	Umfasst alle Personen, die nicht unter die zugriffsberechtigten Personenkreise 1-9 und 11 fallen.
11	Mitarbeiter von Gesellschaftern der gematik und denen durch sie vertretenen Organisationen. Teilnehmender Personenkreis der TI gemäß. Gesellschafterbeschluss der gematik.	Im § 291a SGB V nicht erwähnt, jedoch im SGB V.

2.6.2 Rollen

In der Konzeption der Architektur der TI-Plattform werden die nachfolgend genannten fachlichen, betrieblichen und technischen Rollen verwendet.

Die fachlichen und betrieblichen Rollen werden auf den zugriffsberechtigten Personenkreis nach § 291a SGB V aus Tabelle 2 abgebildet. Eine Abbildung der technischen Rollen erfolgt nicht, da der zugriffsberechtigten Personenkreis nach § 291a SGB V sich auf Berechtigungen von Personen bzw. Personengruppen bezieht und unabhängig von einer technischen Umsetzung formuliert ist.

Die dargestellten Rollen können auf Ebene der Spezifikationen ergänzt und verfeinert werden.

Tabelle 4: Fachliche Rollen

Rolle	Beschreibung	PK nach §291a SGB V (siehe Tabelle 2 und Tabelle 3)
Versicherter	Ein Versicherter ist eine natürliche Person, die von einem Kostenträger eine eGK erhalten hat.	1
Leistungserbringer	Ein Leistungserbringer gehört zu einem zugriffsberechtigten Personenkreis nach § 291a Abs. 4 SGB V und erbringt Leistungen des Gesundheitswesens für Versicherte.	2, 3, 4, 5, 6, 7, 8
Mitarbeiter Kostenträger	Mitarbeiter, der bei einer Krankenkasse gemäß §291 SGB V tätig ist	9
Mitarbeiter Gesellschafterorganisation	Mitarbeiter von Gesellschaftern der gematik und denen durch sie vertretenen Organisationen. Nicht enthalten sind Mitarbeiter, die gemäß §291 SGB V tätig sind	11

Die fachliche Rolle „Leistungserbringer“ wird für die Schnittstellen zu den Fachanwendungen bereits auf Ebene der Konzeption in einer feineren Untergliederung benötigt.

Tabelle 5: Tab_ArchTIP_002 Rollenmodell in der Außensicht der TI-Plattform

Rolle	Beschreibung	PK nach §291a SGB V (siehe Tabelle 2)
Versicherter	Ein Versicherter ist eine natürliche Person, die von einem Kostenträger eine eGK erhalten hat.	1

ENTWURF

Rolle	Beschreibung	PK nach §291a SGB V (siehe Tabelle 2)
Arzt	Ärzte	2
Zahnarzt	Zahnärzte	3
Apotheker	Apotheker, Apothekerassistenten, Pharmazieingenieure, Apothekenassistenten	4
Mitarbeiter Arzt	Personen, die bei Ärzten als berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf tätig sind.	Teilmenge von 5
Mitarbeiter Zahnarzt	Personen, die bei Zahnärzten als berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf tätig sind.	Teilmenge von 5
Mitarbeiter Apotheker	Personen, die in Apotheken als berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf tätig sind.	Teilmenge von 5
Mitarbeiter Krankenhaus	Personen, die in Krankenhäusern als berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf tätig sind.	Teilmenge von 5
Sonstige Leitungserbringer	Sonstige Erbringer ärztlich verordneter Leistungen, §291a Abs. 4 Satz 1 Nr.1 e) SGB V	6
Anderer Heilberuf	Angehörige eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert (z. B. Rettungsassistent).	7
Psychotherapeut	Psychologischer Psychotherapeut und Kinder- und Jugendlichenpsychotherapeut	8
Mitarbeiter Kostenträger	Mitarbeiter, der bei einer Krankenkasse gemäß §291 SGB V tätig ist	9

Tabelle 6: Betriebliche Rollen

Rolle	Beschreibung	PK nach §291a SGB V (siehe Tabelle 2 und Tabelle 3)
Kartenherausgeber eGK	Herausgeber der eGK	9
Anbieter Kartenadministration eGK	Anbieter fachanwendungsspezifische Dienste der Kartenadministration der eGK	9
Kartenherausgeber HBA/SMC-B	Herausgeber des HBA oder der SMC-B	10
Anbieter Fachanwendungsspezifischer Dienst	Anbieter eines Fachanwendungsspezifischen Dienstes in der TI	10
Anbieter zentraler Dienst	Anbieter eines Dienstes in der zentralen TI-Plattform	10
Hersteller	Hersteller sind für die Entwicklung von Produkttypen der TI zuständig	10
Administrator	Fachpersonal zum Aufbau und Betrieb der Telematikinfrastruktur und der vorhandenen Primär- und Backend-Systeme. Es wird unterschieden zwischen: a) Administrator einer Organisation des Gesundheitswesens	10

ENTWURF

Rolle	Beschreibung	PK nach §291a SGB V (siehe Tabelle 2 und Tabelle 3)
	b) Administrator eines zentralen Dienstes	
gematik	Mitarbeiter gematik	10

Tabelle 7: Technische Rollen

Rolle	Beschreibung	PK nach §291a SGB V (siehe Tabelle 2 und Tabelle 3)
Clientsystem	Logischer Bezeichner für dezentrale Systeme, die als Clients mit der TI interagieren, aber selbst nicht als Bestandteil der TI betrachtet werden (z. B. PVS-, AVS-, KIS-Systeme, E-Mail-Clients). Mit diesem Bezeichner werden Hard- und Software-Bestandteile zusammengefasst.	nicht anwendbar
Clientmodul	Clientmodule unterliegen der Verantwortung der Fachanwendungen, gehören zur TI und nutzen Basis-, Infrastruktur- und Netzwerkdienste der TI-Plattform im gleichen Umfang wie Clientsysteme. Clientmodule sind als Komponente der Fachanwendung separat verteil- und installierbar und müssen nicht zwangsläufig an ein Primärsystem gebunden sein.	nicht anwendbar
Fachanwendungs-spezifischer Dienst	Fachanwendungsspezifische Dienste unterliegen der Verantwortung der Fachanwendungen, gehören zur TI und nutzen Basis-, Infrastruktur- und Netzwerkdienste der TI-Plattform. Fachanwendungsspezifische Dienste sind z.B. Fachdienste und anwendungsspezifische Intermediäre.	nicht anwendbar
Fachmodul	Ein dezentraler Anwendungsanteil der Fachanwendung innerhalb der TI mit sicherer Anbindung an die TI-Plattform unter Nutzung der Schnittstellen- und Ablaufdefinitionen der TI-Plattform. Fachmodule stellen geprüfte Client-Logik einer Fachanwendung dar, die durch ihre Umgebung (Secure Consumer Zone) vor Manipulation geschützt ist.	nicht anwendbar
Fachmodul MobKT	Ein Fachmodul, welches sich in einem mobilen Produkttyp der TI befindet.	nicht anwendbar
TI-Plattform	Produkttypen der TI-Plattform nutzen andere Produkttypen der TI-Plattform.	nicht anwendbar
Weitere Anwendungen des Gesundheitswesens mit Zugriff auf zentrale Dienste	Die weiteren Anwendungen des Gesundheitswesens mit Zugriff auf zentrale Dienste (aAdG und aAdG-NetG-TI, siehe [gemRL_NvTIwA]) unterliegen der Verantwortung der jeweiligen Anbieter und sind nicht Teil der TI. Die TI-Plattform stellt bestimmte zentrale Dienste zur Nutzung bereit und sichert durch Vorgaben an diese Anwendungen die Rückwirkungsfreiheit auf die TI.	nicht anwendbar
Weitere Anwendungen des Gesundheitswesens ohne Zugriff auf zentrale Dienste	Die weiteren Anwendungen des Gesundheitswesens ohne Zugriff auf zentrale Dienste (aAdG-NetG, siehe [gemRL_NvTIwA]) unterliegen der Verantwortung der jeweiligen Anbieter und sind nicht Teil der TI. Die TI-Plattform stellt nur die netztechnische Erreichbarkeit der Dienste bereit und sichert durch technische	nicht anwendbar

ENTWURF

Rolle	Beschreibung	PK nach §291a SGB V (siehe Tabelle 2 und Tabelle 3)
	Maßnahmen die Rückwirkungsfreiheit auf die TI.	
Sicheres Übermittlungsverfahren	Ein sicheres Übermittlungsverfahren nutzt die Leistungen der TI-Plattform, um innerhalb der TI die sichere Übermittlung von Daten zu gewährleisten.	nicht anwendbar

694

ENTWURF

3 Leistungen der TI-Plattform in der Außensicht

3.1 Qualifizierte elektronische Signatur

Eine qualifizierte elektronische Signatur gemäß [eIDAS] ist ein verlässliches Mittel um eine juristische Willenserklärung in elektronischer Form abzugeben oder andere rechtlich verbindliche Vorgänge abzusichern und so eine Rechtsicherheit (hier insbesondere Beweissicherheit) herzustellen. Die TI-Plattform bietet Leistungserbringern die Möglichkeit eine QES in ihre fachlichen Prozesse zu integrieren und so den Aufwand aufgrund papiergestützter Verfahren zu mindern. Die TI-Plattform unterstützt in diesem Zusammenhang auch die QES Stapelsignatur (gemäß TR-03114).

Eine detaillierte Beschreibung der angebotenen Leistung (insbesondere unterstützte Dokumentenformate und Policies) ist im Kapitel 5.5.1.3 zu finden.

3.2 Einfache digitale elektronische Signatur

In vielen fachlichen Abläufen ist der Nachweis der Integrität und Authentizität der zu verarbeitenden Daten unerlässlich. Die TI-Plattform unterstützt dies durch das Angebot einfache digitale elektronische Signaturen über Daten zu erstellen und zu prüfen.

Eine detaillierte Beschreibung der in diesem Zusammenhang durch die TI-Plattform angebotenen Leistung ist dem Kapitel 5.5.1.2 zu entnehmen.

3.3 Ver- und Entschlüsselung

Um die Vertraulichkeit fachlicher Daten zu gewährleisten, bietet die TI-Plattform an, diese zu verschlüsseln und an berechtigter Stelle wieder zu entschlüsseln. Dies ist besonders im Bereich von persönlichen medizinischen Daten in der Fachlichkeit unumgänglich.

Eine detaillierte Beschreibung der in diesem Zusammenhang durch die TI-Plattform angebotenen Leistung ist dem Kapitel 5.5.1.11 zu entnehmen.

3.4 Public Key Infrastructure (PKI)

Die vorhergehend beschriebenen Leistungen der TI-Plattform sind technisch nur umsetzbar, wenn eine Public Key Infrastructure besteht, auf welche die Dienste aufsetzen können. Die TI-Plattform bietet eine PKI an, welche die Bedürfnisse aller angebotenen Dienste abdeckt.

ENTWURF

3.5 Tokenbasierte Benutzerauthentisierung

Die tokenbasierte Benutzerauthentisierung basiert auf WS-Trust und WS-Federation um eine flexible Integration von Identity Providern (IDP[11]) bzw. Security Token Services (STS) zu ermöglichen. Die TI-Plattform stellt Funktionen zur Verfügung, um Benutzer als Mitarbeiter einer Leistungserbringerinstitution zu authentisieren. Dabei handelt es sich um eine Transformation von Zertifikatsdaten der SMC-B in eine entsprechende Identitätsbestätigung, ohne dass in diesem Zusammenhang eine Authentifizierung des Benutzers durch die TI-Plattform erfolgt.

Es ist eine Authentisierung als Mitarbeiter der Leistungserbringerinstitutionen direkt über eine SMC-B möglich oder ein lokaler Identity Provider (IDP) kann die Authentisierung durch eine SMC-B bestätigen lassen. Für die inhaltliche Korrektheit der Authentisierung des lokalen IDP ist allein der lokale IDP verantwortlich.

Die Tokenbasierte Benutzerauthentisierung der TI-Plattform stellt eine Unterstützungsleistung dar, durch die Identitätsbestätigungen gemäß WS-Trust und WS-Federation erzeugt werden können. Der Dienst umfasst keine Prüfung ob der Nutzer berechtigt ist und verifiziert nicht die Inhalte der Identitätsbestätigung. Die Aussagekraft der Identitätsbestätigung ist direkt abhängig davon, wie der Zugang zu den Komponenten der TI geregelt ist und dass die Komponenten der TI nicht unberechtigt verwendet werden können.

3.6 Smartcards des Gesundheitswesens

Der Nutzen einer PKI hängt maßgeblich davon ab, dass die Gewissheit besteht, dass private Schlüssel sicher gespeichert und sich unter alleiniger Kontrolle des Schlüsselinhabers befinden. Um dies mit der Anforderung nach einem orts-ungebundenen Einsatz des Schlüsselmaterials zu verbinden, speichert die TI-Plattform Schlüsselmaterial auf HBAs, eGKs und Security Module Cards (nachfolgend auch oft als „SMC“ oder „Karten“ referenziert). Diese stehen unter Aufsicht des jeweiligen Inhabers und stellen sicher, dass gespeichertes Schlüsselmaterial nicht exponiert wird.

Die eGK kann im gewissen Umfang zusätzlich als sicherer Speicherort für Fachdaten verwendet werden.

Der Zugriffsschutz für Fachdaten und Schlüsselmaterial wird durch die Security Module Card sichergestellt. Um den Zugriff freizuschalten ist je nach Informationsobjekt eine PIN-Eingabe oder eine Card-to-Card-Authentifizierung notwendig.

3.7 Anbindung an das geschlossene Netzwerk der TI

Die TI-Plattform stellt ein geschlossenes Netz für die bekannten Akteure des deutschen Gesundheitswesens zur Verfügung. An dieses können sich Leistungserbringer, Kostenträger oder fachanwendungsspezifische Dienste der Fachanwendungen der Telematikinfrastruktur unter Verwendung der entsprechenden Komponenten der TI-Plattform anbinden und über dieses Netz miteinander kommunizieren.

---

[11] Ein Identity Provider (IDP) ist ein Dienst gemäß WS-Trust bzw. WS-Federation, der Identitätsinformationen nach direkter Authentifizierung eines Nutzers erstellt, pflegt und verwaltet oder den Nutzer auf Basis der Identitätsinformation eines anderen IDPs authentifiziert.

ENTWURF

3.8 Zugang zu ~~Bestandsnetzen~~ weiteren Anwendungen des Gesundheitswesens

Neben der Telematikinfrastruktur existieren im deutschen Gesundheitswesen verschiedene weitere Anwendungen des Gesundheitswesens (teils in Netzen des Gesundheitswesens)~~ andere Bestandsnetze~~, die Leistungserbringern Fachanwendungen bereitstellen. Die TI-Plattform ermöglicht es Leistungserbringern, die ~~Fachanwendungen angeschlossener Bestandnetze~~ angeschlossenen weiteren Anwendungen des Gesundheitswesens über die TI-Plattform erreichen und nutzen zu können.

3.9 Sicherer Internetzugang

Neben dem sicheren Zugang in die Telematikinfrastruktur bietet die TI-Plattform Clientsystemen die Möglichkeit, über einen sicheren Internetzugang in das Internet zu gelangen. Der sichere Internetzugang wird zur optionalen Nutzung durch den VPN-Zugangsdienst bereitgestellt.

3.10 Außensicht der TI-Plattform im Ganzen

Nachfolgend wird die Außensicht der TI-Plattform in der Gesamtheit über alle Dienste dargestellt. Dabei ist der Darstellung zu entnehmen, für welche Nutzer die konkreten Dienste an den entsprechenden Schnittstellen bereitgestellt werden.

- Blau stellt Dienste dar, die ausschließlich Fachanwendungen der TI, sichere Übermittlungsverfahren und teils auch weiteren Anwendungen des Gesundheitswesens mit Zugriff auf zentrale Dienste zugänglich sind.
- Grün stellt Dienste dar, die sowohl Fachanwendungen der TI als auch Fachanwendungen auf Clientsystemen oder Clientmodulen zugänglich sind.
- Weiße Schnittstellen dienen administrativen Vorgängen. Das vorliegende Dokument weist nur administrative Schnittstellen aus, die für die konzeptionelle Erbringung einer funktionalen Leistung erforderlich sind. Weitere administrative Schnittstellen werden im Einklang mit der Konzeption des Betriebs auf Ebene der Spezifikationen der Produkttypen festgelegt.

Die detaillierte Beschreibung der verschiedenen Dienste ist den Kapiteln 5.5 und 5.6 zu entnehmen.

ENTWURF

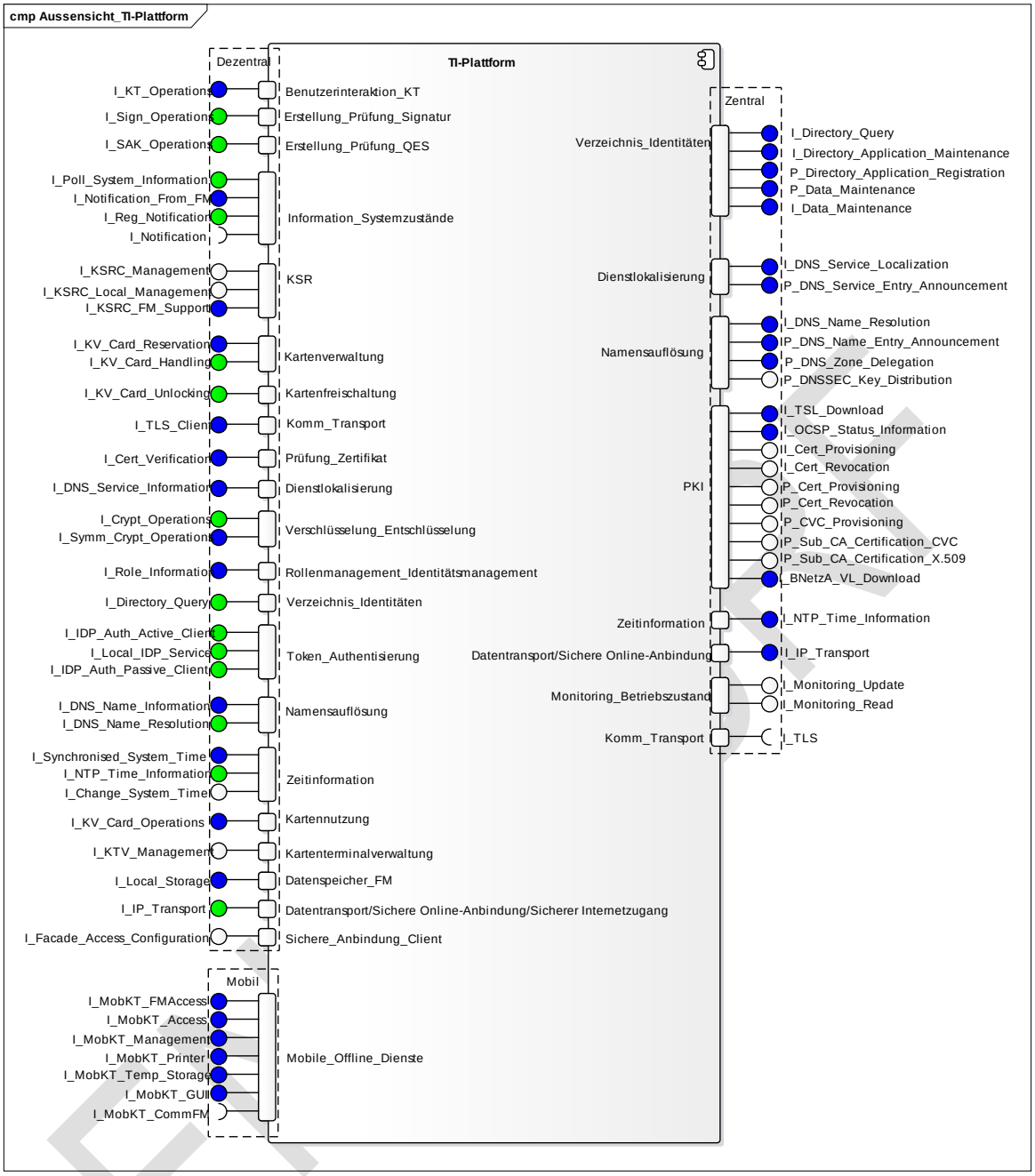


Abbildung 5: Außensicht der TI-Plattform

4 Lösungen der Architektur der TI-Plattform

4.1 Einsatz von Smartcards in der TI

In der TI werden Smartcards einerseits zur Realisierung eines mobilen Identitätsmanagements und andererseits als sicherer Speicher zum Transport von versicherten-bezogenen Daten verwendet. Sie speichern kryptographisches Schlüsselmaterial für Personen, Institutionen sowie Geräte des Gesundheitswesens und identifizieren diese zuverlässig. Weiterhin können auf Smartcards Daten von Anwendungen der TI gespeichert werden, was nur die elektronische Gesundheitskarte (eGK) betrifft. Technologiebedingt sind Smartcards nur bedingt als Datenspeicher geeignet. Daher beschränkt sich die Speicherung auf der eGK auf solche Daten, wo dies gesetzlich vorgesehen ist oder für die ein Konsens der Gesellschafter der gematik vorliegt.

So dient die eGK dem Versicherten als mobiles Identifikations- und, im Rahmen der gesetzlichen Vorgaben oder der Konsensentscheidungen der Gesellschafter der gematik, Speichermedium, um sich bei einem Arztbesuch in der Praxis des Leistungserbringers eindeutig zu authentisieren und, basierend darauf - i.V.m der eindeutigen Authentisierung des Arztes (HBA) - diesem Zugriff auf bestimmte Daten zu gewähren.

Der HBA bietet dem Leistungserbringer (LE) innerhalb seiner LE-Umgebung an verschiedenen Arbeitsplätzen oder ggf. umgebungsübergreifend, wenn der LE in verschiedenen LE-Umgebungen tätig ist, die Möglichkeit, sich in seiner Rolle als Arzt und als Person gegenüber Dritten auszuweisen. Anhand der SMC-B übergibt die Leistungserbringerorganisation der Leistungserbringerinstitution eine Identität, die deren sektorspezifische Kassenzulassung bestätigt.

Konnektoren und Kartenterminals werden als dezentrale Komponenten identitätslos produziert und erhalten erst über gSMC-K und gSMC-KT eine eindeutige und bestätigte Identität innerhalb der TI. gSMC-K und gSMC-KT werden nur in zugelassenen Komponenten installiert, wodurch sich alle Kommunikationspartner sicher sein können, mit zugelassenen Komponenten zu interagieren.

In der TI werden Smartcards in den folgenden Ausprägungen (Produkttypen) eingesetzt:

Tabelle 8: Smartcards in der TI

Produkttyp	Bezug	Beschreibung
eGK	Person	Die eGK dient zur eindeutigen Identifikation eines Versicherten in der TI und dem Nachweis eines bestehenden Leistungsanspruches. Der Versicherte kann mit seiner eGK Daten entschlüsseln sowie signieren. Gemäß den Vorgaben des § 291(a) SGB V und aufgrund von Konsensentscheidungen der Gesellschafter der gematik werden fachliche Datensätze geringen Umfangs auf der eGK gespeichert.
HBA	Person	Der HBA dient zur eindeutigen Identifikation des Leistungserbringers. Der HBA enthält kryptographisches Schlüsselmaterial, mit dem (qualifizierte) Signaturen erstellt sowie Daten entschlüsselt werden können.

ENTWURF

Produkttyp	Bezug	Beschreibung
SMC-B	Institution / Organisation	Die SMC-B dient zur eindeutigen Identifikation einer Organisation des Gesundheitswesens und deren Mitarbeitern[12]. Die SMC-B enthält kryptographisches Schlüsselmaterial, mit dem Signaturen erstellt sowie Daten entschlüsselt werden können.
gSMC-K gSMC-KT	Gerät	Gerätegebundene Smartcards dienen der eindeutigen Identifikation von dezentralen Komponenten der TI: • gSMC-K für einen Konnektor, • gSMC-KT für ein Kartenterminal.

Im Folgenden wird der Begriff „Karte“ synonym genutzt zu „Smartcard zur Nutzung innerhalb der TI, die einem der Produkttypen eGK, HBA, SMC-B, gSMC-K, gSMC-KT zugeordnet ist“.

Die nachfolgenden Kapitel definieren den übergreifenden Rahmen für die Karten der TI. Hier werden die übergreifenden Leistungen der Karten durch COS und Objektsystem definiert. Welche Leistung in welcher konkreten Karte oder durch eine Fachanwendung genutzt wird, ist der Produkttypbeschreibung in Kapitel 5.3 oder der entsprechenden Spezifikation der Fachanwendung zu entnehmen.

4.1.1 Domänen- / Informationsmodell der Karten der TI

Das Domänenmodell beschreibt konzeptionell den Lösungsbereich des Einsatzes von Karten in der TI-Plattform. Technische Details werden zu Informations- bzw. Domänenklassen zusammengefasst. Es werden folgenden Sub-Domänen definiert:

- Identität,
- Daten,
- Autorisierung und Kartenadministration (Zugriffsregeln).

[12] Wer konkret durch eine SMC-B in einer Organisation als deren Mitarbeiter identifiziert wird, legt die entsprechende Organisation eigenverantwortlich fest.

ENTWURF

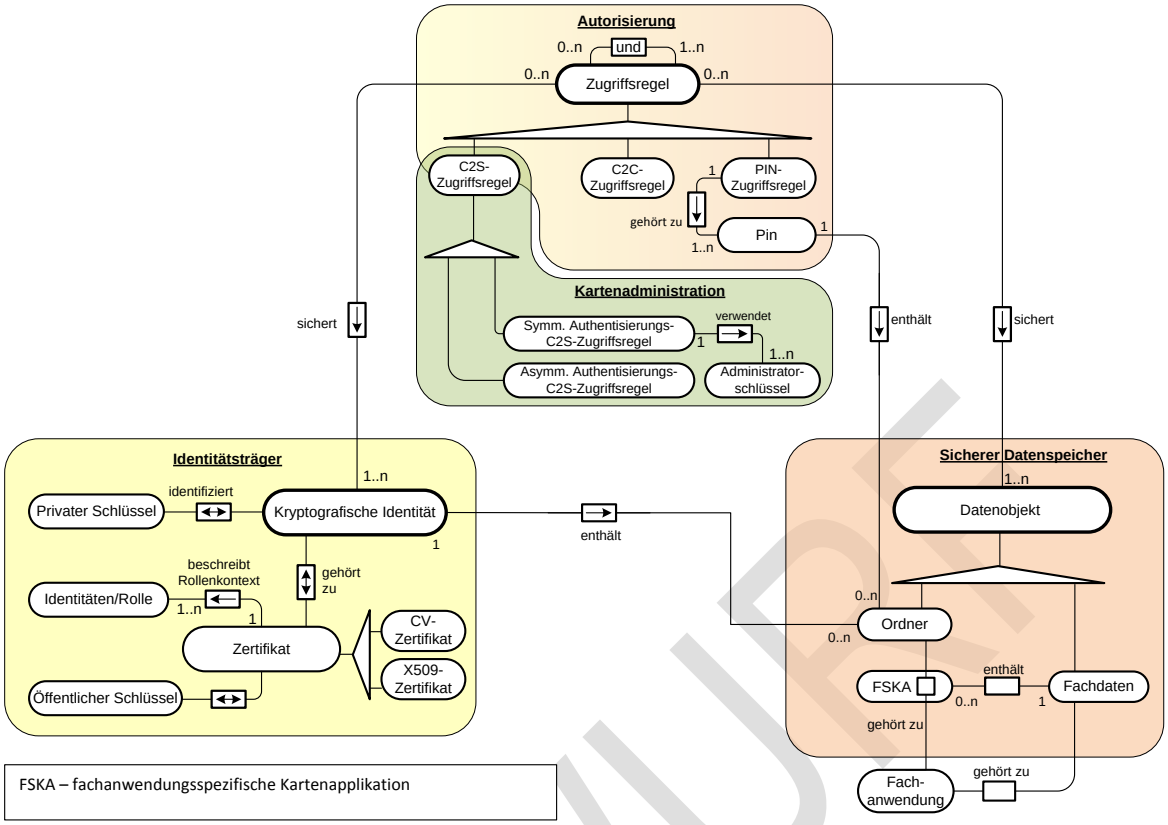


Abbildung 6: Domänenmodell Karten der TI[13]

4.1.1.1 Identitätsträger

Unter einer Identität im Kontext der Domäne „Karten der TI“ ist immer eine kryptographische Identität, bestehend aus einem privaten Schlüssel und dem dazugehörigen Zertifikat, zu verstehen. Hierzu werden eindeutige Identifikationsmerkmale der realen Identitäten an eindeutige technische Identifikationsmerkmale über Endnutzerzertifikate gekoppelt. Diese kryptographischen Identitäten werden zum Zweck der Erstellung und Prüfung von Signaturen, Authentisierung und zur Ver- und Entschlüsselung von Daten verwendet, wobei geheimes Schlüsselmaterial die Smartcard nie verlässt, weil die kryptographischen Operationen innerhalb der Smartcard ausgeführt werden. Der Mechanismus der Authentisierung ist Grundlage der Autorisierung des Zugriffs auf Fachdaten.

Eine Smartcard speichert eine oder mehrere Identitäten pro Verwendungszweck für Personen, Institutionen oder Geräte der TI (vgl. Anhang B).

⌦ **TIP1-A_5898 Speicherung von Kryptographischen Identitäten auf Smartcards**

Alle Produkttypen, die Smartcards darstellen, MÜSSEN die Möglichkeit bereitstellen, pro Smartcard mehrere kryptographische Identitäten für unterschiedliche Verwendungszwecke sicher zu speichern. ⌫

Zur Erfüllung des Einsatzzwecks der jeweiligen Identität muss die Smartcard die nötigen kryptographischen Operationen anbieten.

[13] Die Notation der Abbildung entspricht den Fundamental Modeling Concepts (FMC, www.fmc-modeling.org).

ENTWURF

⌦ **TIP1-A_5901 Bereitstellung von kryptographischen Operationen**

Alle Produkttypen, die Smartcards darstellen, MÜSSEN die jeweils möglichen kryptographischen Operationen für gespeicherte Identitäten bereitstellen. Diese Operationen sind:

- Entschlüsslung,
- Authentisierung von Identitäten,
- Signaturerstellung und
- Schlüsselerzeugung. ⌫

4.1.1.2 Sicherer Datenspeicher

Smartcards sind eingeschränkt auch als sicherer Datenspeicher einsetzbar. Die Speicherung von Daten auf der eGK beschränkt sich auf solche Daten, wo dies gesetzlich vorgesehen ist oder für die ein Konsens der Gesellschafter der gematik vorliegt. Diese Daten sind somit ohne weitergehende Schutzmaßnahmen transportabel und können am jeweiligen Bestimmungsort, bspw. eines authentisierten Leistungserbringers, durch Erfüllung zugeordneter Zugriffsregeln, zur Verwendung freigegeben werden.

⌦ **TIP1-A_5942 Speicherung von Daten auf Smartcards**

Alle Produkttypen, die Smartcards darstellen, MÜSSEN Fachdaten sicher und zugriffsgeschützt speichern können. Technologiebedingt wird diese Leistung nur auf der eGK im gesetzlich vorgegebenen Rahmen oder wenn ein Konsens der Gesellschafter der gematik vorliegt genutzt.⌫

Dieses Leistungsmerkmal wird nur im Produkttyp eGK verwendet.

Datenobjekte können strukturiert und hierarchisch organisiert, analog zu einem PC-Dateisystem, auf Smartcards gespeichert werden. Dazu bieten Smartcards Ordner an, die bzgl. des Inhalts und der Struktur der gespeicherten Datenobjekte unter Hoheit der TI-Plattform oder einer zugeordneten Fachanwendung stehen. Der Ordner einer Fachanwendung wird nachfolgend „fachanwendungsspezifische Karten-Applikationen“ genannt. In der TI werden fachanwendungsspezifische Karten-Applikationen nur auf dem Produkttyp eGK umgesetzt.

⌦ **TIP1-A_5729 Speicherstruktur von Daten auf einer Smartcard**

Alle Produkttypen, die Smartcards darstellen, MÜSSEN zur Speicherung von Datenobjekten Ordner anbieten, in dem entweder die TI-Plattform oder die jeweils zugeordneten Fachanwendungen fachlich zusammenhängende Fachdaten, kryptographischen Identitäten oder PINs strukturiert (ggf. hierarchisch) ablegen können. Der Ordner einer Fachanwendung wird fachanwendungsspezifische Karten-Applikation genannt.⌫

Bestimmte Umstände können es erforderlich machen, eine fachanwendungsspezifische Karten-Applikation aus datenschutzrechlichen Gründen zu verbergen. Die betroffene fachanwendungsspezifische Karten-Applikation wird dazu auf der eGK deaktiviert. Eine deaktivierte fachanwendungsspezifische Karten-Applikation kann zu einem späteren Zeitpunkt wieder aktiviert und dadurch sichtbar gemacht werden.

⌦ **TIP1-A_5728 De-/Aktivierung von Applikationen einer Karte**

ENTWURF

Alle Produkttypen, die Smartcards darstellen, MÜSSEN eine gespeicherte fachanwendungsspezifische Karten-Applikation, über Zugriffsregeln geschützt, aktivieren bzw. deaktivieren können. Nach erfolgter Deaktivierung ist nur noch die Operation ‚Aktivierung' auf die fachanwendungsspezifische Karten-Applikation anwendbar. ⌫

4.1.1.3 Autorisierung und Kartenadministration (Zugriffsregeln)

Vorrangiges Ziel einer Karte ist es, die auf ihr gespeicherten Kartenobjekte vor unberechtigtem Zugriff zu schützen. Daher ist für jedes Kartenobjekt festzulegen, unter welchen Bedingungen welche Identität mit welcher Operation auf dieses Kartenobjekt zugreifen darf. Der Zugriffsschutz erfordert zwei Schritte:

1. Authentifizierung des Zugreifenden und
2. Autorisierung des Zugriffs auf Basis von Zugriffsregeln.

Für die Authentifizierung werden durch die Karten folgende Mechanismen unterstützt.

⌦ **TIP1-A_5722 Arten der Authentifizierung auf Karten**

Alle Produkttypen, die Smartcards darstellen, MÜSSEN die folgenden Authentifizierungsarten unterstützen:

- PIN-Eingabe zur Benutzerverifikation des Karteninhabers oder eines Berechtigten im Besitz der Karte,
- Card-to-Card (C2C) auf Basis von authentifizierten CV-Zertifikaten für Inhaber/Rollen anderer Karten,
- Card-to-Server (C2S) auf Basis von authentifizierten CV-Zertifikaten oder geheimer symmetrischer Schlüssel für administrationsberechtigte Dienste.⌫

Die Authentifizierung auf Basis von CV-Zertifikaten (C2C, C2S) erfordert die Prüfung der Zertifikatskette. Dafür sind auf der prüfenden Karte öffentliche Schlüssel akzeptierter Wurzel-Zertifizierungsstellen (Vertrauensanker der CVC-Hierarchie) vorhanden. Es können ausschließlich CV-Zertifikate erfolgreich authentifiziert werden, die auf einen dieser Vertrauensanker zurückführbar sind. Unterschieden wird zwischen dem CV-Vertrauensanker der TI-Plattform (CVC-Root) und eventuell existierende CV-Vertrauensanker als Basis der asymmetrischen Authentifizierung bei der Kartenadministration (Administrations-Root).

⌦ **TIP1-A_5907 Kartenspeicherung des öffentlichen Schlüssels der CVC-Root-CA**

Alle Produkttypen, die Smartcards darstellen, MÜSSEN den, zum Zeitpunkt der Herausgabe der Smartcard aktuellen, öffentlichen Schlüssel der CVC-Root (Vertrauensanker der CVC-Hierarchie) sowie ggf. notwendige Schlüssel von Administrations-Roots speichern.⌫

⌦ **TIP1-A_5720 Prüfung auf gemeinsamen Vertrauensanker**

Alle Produkttypen, die Smartcards darstellen, MÜSSEN für eine erfolgreiche Authentifizierung auf Basis von CV-Zertifikaten das zu prüfende CV-Zertifikat auf einen gespeicherten Vertrauensanker zurückführen können.⌫

ENTWURF

⌦ **TIP1-A_6771 C2C-Authentifizierung nur für mathematisch gültige CV-Zertifikate**

Alle Produkttypen, die Smartcards darstellen, MÜSSEN die mathematische Korrektheit der Signatur des CV-Zertifikats zur Authentisierung prüfen. ⌫

⌦ **TIP1-A_5724 C2C-Authentifizierung nur für zeitlich gültige CV-Zertifikate**

Alle Produkttypen, die Smartcards darstellen, MÜSSEN die Gültigkeitsdauer des CV-Zertifikats zur Authentisierung prüfen. Gültig ist jedes CV-Zertifikat, das nicht nachweislich abgelaufen ist. ⌫

Die notwendigen Zugriffsberechtigungen für Operationen (vgl. Kap. 4.1.3) mit Datenobjekten der Karten werden über Zugriffsregeln formuliert. Diese sind auf den Karten an den entsprechenden Datenobjekten zugeordnet und durch die Karte nach erfolgreicher Authentifizierung durchgesetzt werden. Sie definieren unter welchen Bedingungen und nach welchen erfolgreichen Authentifizierungen auf Datenobjekte zugegriffen werden kann.

⌦ **TIP1-A_5904 Kartenspeicherung und Durchsetzung von Zugriffsregeln**

Alle Produkttypen, die Smartcards darstellen, MUSSEN zu jedem Datenobjekt eine oder mehrere Zugriffsregeln speichern und durchsetzen, die festlegen, unter welchen Bedingungen und nach welchen erfolgreichen Authentifizierungen welche Operation mit dem Datenobjekt möglich ist.⌫

CV-Zertifikate tragen neben dem öffentlichen Schlüssel einer Identität auch Informationen zur Rolle der Identität oder feingranulare Berechtigungsinformationen für Zugriffe auf Datenobjekte. Die prüfende Karte autorisiert Zugriffe auf ihre Karten-Objekte nur unter Beachtung der Berechtigugnsinformationen der CV-Zertifikate.

⌦ **TIP1-A_5721 Zugriffsregeln auf Basis von CV-Zertifikaten**

Alle Produkttypen, die Smartcards darstellen, MÜSSEN Zugriffsregeln auf Basis aller Berechtigungen aus authentifizierten CV-Zertifikaten unterstützen.⌫

4.1.1.4 PINs

Da die PIN das persönliche Geheimnis des Karteninhabers oder eines Berechtigten im Besitz der Karte darstellt, muss diese durch ihn, bzw. den Berechtigten bestimmbar/änderbar sein.

⌦ **TIP1-A_5726 PIN Aktualisierung**

Alle Produkttypen, die Smartcards darstellen, MÜSSEN PIN-Änderungen durch Zugriffsberechtigte unterstützen ⌫

Zur Verbesserung der Benutzbarkeit soll die Karte die Möglichkeit bieten, eine zentrale PIN für viele Applikationen zu nutzen. Die Entscheidung ob eine konkrete PIN als Referenz auf die zentrale PIN (Multireferenz-PIN) oder als normale PIN mit eigenem Geheimnis ausgeprägt wird, obliegt der Fachanwendung und der anwendungstechnischen Notwendigkeit der Abgrenzung zu weiteren, auf der Karte gespeicherten Anwendungen. Im Allgemeinen wird die Ausprägung als Multireferenz-PIN gewählt, um dem Kartenbesitzer das Wissen um viele verschiedene PINs zu ersparen. Jede PIN hat einen eigenen Verifikationsstatus unabhängig davon, ob sie als normale PIN oder als Multireferenz-PIN ausgeprägt ist.

ENTWURF

⌦ **TIP1-A_5727 Multireferenz-PIN**

Alle Produkttypen, die Smartcards darstellen, MÜSSEN ermöglichen, dass PINs als Referenz auf eine zentrale PIN oder als normale PIN mit eigenem Geheimnis ausgeprägt werden kann. Jede PIN MUSS einen eigenen Verifikationsstatus besitzen, unabhängig davon welche Ausprägung sie hat. ⌫

⌦ **TIP1-A_2545 PIN/PUK der Smartcards, Länge**

Alle Produkttypen, die Smartcards darstellen und über eine PIN/PUK verfügen, MÜSSEN eine PIN der Länge zwischen 6 und 8 Ziffern und eine PUK mit einer Länge von 8 Ziffern besitzen.⌫

⌦ **TIP1-A_2546 PIN/PUK der Smartcards, Auswahl**

Alle Produkttypen, die Smartcards darstellen und über eine PIN/PUK verfügen, MÜSSEN sicherstellen, dass die PIN/PUK-Auswahl gemäß einer der folgenden Techniken erfolgen kann:

- zugewiesene zufällige oder pseudozufällige PIN/PUK
- zugewiesene abgeleitete PIN/PUK
- durch Kunden gewählte PIN.⌫

⌦ **TIP1-A_2547 PIN/PUK der Smartcards, Sperrung durch Nutzung der PUK**

Alle Produkttypen, die Smartcards darstellen und über eine PIN/PUK verfügen, MÜSSEN sicherstellen, dass ein PUK nicht häufiger als maximal zehnmal verwendbar ist.⌫

⌦ **TIP1-A_5755 An-/Abschaltung der Prüfung einer PIN**

Alle Produkttypen, die Smartcards darstellen, MÜSSEN, über Zugriffsregeln geschützt, die PIN-Prüfung an- und abschalten können. Nach erfolgter Abschaltung gilt die PIN als dauerhaft erfolgreich geprüft. Die Möglichkeit gilt sowohl für normale PINs als auch für jede einzelne Multireferenz-PIN.⌫

4.1.2 Objekttypen der Karten

Die Karte setzt die oben genannten Elemente der Sub-Domänen in Form von Karten-Objekten, wie in Tabelle 9: Karten-Objekttypen und Domänen-Mapping aufgeführt, um.

Tabelle 9: Karten-Objekttypen und Domänen-Mapping

Domäne	Karten-Objekttyp	Inhalt / Kommentar
Identitätsträger	Kryptographisch Identität	Ein Tupel aus privatem Schlüssel und zugehörigem Zertifikat inkl. korrespondierendem öffentlichen Schlüssel. Unter Verwendung spezieller kryptografischer Operationen mit diesen Schlüsseln kann eine Vertrauensbeziehung zum Besitzer einer Identität hergestellt werden.
	Privater Schlüssel	Der geheime Teil eines asymmetrischen Schlüsselpaars. Dieser Schlüssel wird durch die

ENTWURF

Domäne	Karten-Objekttyp	Inhalt / Kommentar
		Karte vor unberechtigtem Zugriff geschützt. Ein Auslesen ist nicht möglich und alle Operationen mit diesem Schlüssel laufen geschützt innerhalb der Karte.
	Zertifikat	Durch ein Zertifikat werden bestimmte Identitäts- und Rolleninformationen von Personen, Geräten oder Diensten mit dem ebenfalls enthaltenen öffentlichen Schlüssel verbunden. Das Zertifikat wird durch eine vertrauenswürdige CA bestätigt und ist kryptografisch gesichert. Über die kryptografische Bindung des öffentlichen Schlüssels an den privaten Schlüssel können die im Zertifikat enthaltenen Informationen dem Besitzer des privaten Schlüssels zugeordnet werden.
	CV-Zertifikat	Card Verifiable Certificate (CVC) sind Zertifikate, deren Gültigkeit durch die Smartcard selbst geprüft werden kann. Diese erlauben den rollenbasierten Zugriff auf Smartcards der TI.
	X.509-Zertifikat	X.509-Zertifikate enthalten komplexe Informationen und werden in kryptografischen Operationen in Anwendungen eingesetzt.
Autorisierung und Karten-administration (Zugriffsregeln)	Symmetrischer Schlüssel (AdminSchlüssel)	Wird als „Shared Secret“ zur Authentisierung zu Administrationszwecken für Karten der TI eingesetzt. Dieser Schlüssel ist kartenindividuell.
	PIN	Die Persönliche Identifikationsnummer ist ein Geheimnis des Karteninhabers oder eines anderen Berechtigten, mit dem er sich gegenüber der Karte authentisiert.
Sicherer Datenspeicher	Datenobjekt	Speicherobjekt auf einer Karte.
	Ordner	Ordner können Fachdaten, weitere Ordner sowie kryptographische Identitäten und PINs enthalten.
	Fachanwendungsspezi-fische Karten-Applikation	Ein Ordner unter der Hoheit einer konkreten Fachanwendung
	Fachdaten	Fachliche Anwendungsdaten einer Fachanwendung.

4.1.3 Operationen auf Objekte der Karten

Die oben beschriebenen Funktionalitäten auf gespeicherte Objekte bieten die Karten über die in Tabelle 10 genannten, fachlichen Schnittstellen und Operationen an.

⌦ TIP1-A_5908 Umsetzung von logischen Schnittstellen zu konkreten Kartenkommandos

Alle Produkttypen, die Smartcards darstellen, MÜSSEN zur Umsetzung der nachfolgend genannten logischen Schnittstellen und Operationen entsprechende Kartenkommandos bereitstellen.

Tabelle 10: Operationen auf Karten der TI

ENTWURF

Logische Schnittstelle	Operation auf Objekt (Beschreibung)	Objekttyp
I_Card_Data_Operations	Operationen zum elementaren Zugriff auf Datenobjekte (Lesen, Schreiben, Löschen) sowie Operationen zum aktivieren und deaktivieren von Datenobjekten.	Datenobjekte
I_Card_Auth_Operations	Operationen zur Authentifizierung einer zweiten Komponente (Karte oder Dienst).	Schlüssel, Zertifikate
	Operationen zur Authentifizierung einer Person und zur Verwaltung der PIN.	PIN
I_Card_Crypt_Operations	Kryptographische Operationen die benötigt werden für: - Signaturerstellung, - Entschlüsselung, - Authentisierung, - Schlüsselerzeugung.	Schlüssel

⌫

Die in Tabelle 10 genannten, logischen Schnittstellen decken den Funktionsumfang der benötigten Kartenoperationen zur Speicherung von (Fach-)Daten, Authentisierung, Ver-/Entschlüsselung und Signatur ab und werden nachfolgend im Dokument unter der logischen Schnittstelle I_Smartcard_Operations subsummiert.

Kartenzugriffe in der TI werden vom Konnektor gekapselt. Die vom Konnektor innerhalb der TI gekapselten Operationen sind über die folgenden logischen Schnittstellen erreichbar:

Tabelle 11: Mapping logische Smartcard- zu Konnektor-Schnittstellen

Vom **Konnektor** bereitgestellte Interfaces	Vom **Konnektor** bereitgestellte Operationen	Von **Karten** angebotene, logische Interfaces
I_KV_Card_Operations (vgl. Kap. 5.5.2.4.1)	extract_card_data	**I_Card_Data_Operations**
	read_Card_Data	
	erase_Card_Data	
	write_Card_Data	
	write_eGK_Protocol	
	sign_Data	**I_Card_Crypt_Operations**
	decrypt_Data	
I_KV_Card_Unlocking (vgl. Kap. 5.5.1.8.1)		**I_Card_Auth_Operations**
	do_Reset	
	do_C2C	
	verify_PIN	
	unblock_PIN	
	initialize_PIN	
	change_PIN	

Vom **Konnektor** bereitgestellte Interfaces	Vom **Konnektor** bereitgestellte Operationen	Von **Karten** angebotene, logische Interfaces
	enable_PIN	
	disable_PIN	
	get_PIN_Status	

Die in Tabelle 11 dargestellten Operationen des Konnektors entsprechen funktional den Operationen der angegebenen logischen Kartenschnittstelle. Daher werden diese an den Karten-Interfaces nachfolgend nicht mehr einzeln beschrieben.

4.2 Zugriff auf Karten

Bei personen- und organisations-/institutionsbezogenen Karten wird ein Mechanismus umgesetzt, der es dem Karteninhaber ermöglicht, seine Karte (sprich, die über die Karte erreichbaren Funktionen) unter seiner Kontrolle zu behalten.

Da sich im Zuge von Karteninteraktionen der Sicherheitszustand der Karte über eine PIN-Eingabe oder eine Card-to-Card-Freischaltung ändern kann, muss sichergestellt sein, dass nachfolgend nur berechtigte Anwender diesen erhöhten Sicherheitszustand der Karte nutzen können. Welche Anwender berechtigt sind, hängt vom Kartentyp ab. Bei organisations-/institutionsbezogenen Karten dürfen alle berechtigten Mitarbeiter der Organisation/Institution, mit der die Karte assoziiert ist, die erreichten Sicherheitszustände dieser Karte nutzen. Der Sicherheitszustand des HBA ist an die Person gebunden, die sich authentisiert hat. Für die eGK gilt das Zwei-Karten-Prinzip. Ein erreichter Sicherheitszustand darf nur im Zusammenhang mit der organisations-/institutions- oder personenbezogenen Karte genutzt werden, die die eGK freigeschaltet hat. Die Freischaltung einer eGK durch PIN.home ist ebenfalls möglich, aber da Umgebungen, die nicht Bestandteil der dezentralen TI–Plattform sind, in diesem Dokument nicht betrachtet werden, werden hierzu keine konzeptionellen Aussagen getroffen.

Der Konnektor benötigt daher zuverlässige Informationen über den Aufrufkontext, in dem eine Kartenoperation ausgeführt werden soll. Der Aufrufkontext besteht aus personenbezogenen und systembezogenen Informationsanteilen. Um die Mandantenfähigkeit des Konnektors zu gewährleisten, muss der Aufrufkontext auch den Mandantenbezug enthalten.

Dezentralen Ressourcen der TI-Plattform (z. B. Karten) werden auf konzeptioneller Ebene über RessourceIdentifier adressiert. Vor der Nutzung von direkten Kartenoperationen und solchen Operationen, die Kartenzugriffe implizieren, wie Signieren oder Entschlüsseln, muss der Aufrufer den RessourceIdentifier der Karte zusammen mit dem Aufrufkontext einmalig an die TI-Plattform übermitteln. Aus der Kombination von RessourceIdentifier der Karte und Aufrufkontext erzeugt der Konnektor eine Referenz (**CardUsageReference**), die für alle folgenden Kartenoperationen innerhalb desselben Aufrufkontexts zu verwenden ist.

Anhand der CardUsageReference ermittelt der Konnektor bei jedem Aufruf den gespeicherten Aufrufkontext und steuert damit den Zugriff auf Karten mit möglicherweise erhöhtem Sicherheitszustand.

Die abstrakte Definition der CardUsageReference reicht aus, um auf Konzeptebene die Interaktionen der Clientsysteme und Fachmodule über den Konnektor mit den Karten

ENTWURF

modellieren zu können. Wie der spätere tatsächliche technische Mechanismus ausgestaltet werden wird, der die obigen Anforderungen (Abgrenzung der Sicherheitszustände von verschiedenen Aufrufern) umsetzt, wird auf Spezifikationsebene unter Berücksichtigung von Sicherheitsaspekten entschieden.

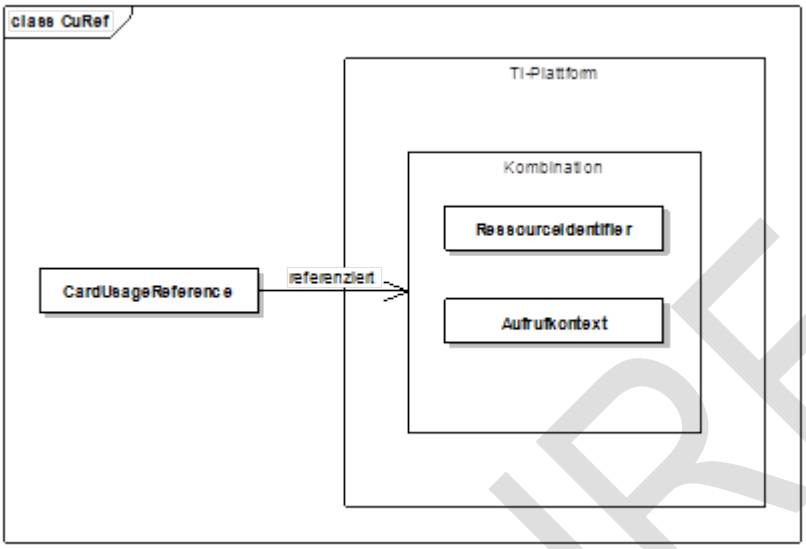


Abbildung 7: CardUsageReference

4.3 Mandantenfähigkeit

Mandantenfähigkeit bedeutet für die TI-Plattform, dass mehrere Organisationseinheiten dezentrale Produkttypen der TI-Plattform gemeinsam nutzen, wobei eine strikte Trennung der Daten einzelner Mandanten vorgenommen werden muss.

Produkttypen der TI-Plattform müssen dann mandantenfähig implementiert werden, wenn sie entweder

a) Daten verarbeiten, die nur im Kontext eines definierten Mandantenbezugs gelesen, erzeugt oder verändert werden dürfen und / oder

b) andere dezentrale Produkttypen verwalten und verwenden, die im Kontext eines definierten Mandantenbezugs stehen.

Anwendung der Kriterien auf die Komponenten der TI-Plattform

Das Kriterium a) trifft nur auf die Produkttypen SMC-B und HSM-B zu. Beide Produkttypen beinhalten private Schlüssel (Daten) für einen oder mehrere Mandanten. Alle anderen Produkttypen der TI-Plattform bearbeiten nur Daten, die im direkten Nutzerbezug stehen.

Das Kriterium b) trifft nur auf den Konnektor zu. Dieser verwaltet die lokalen Kartenterminals, die lokal verfügbaren Karten bzw. HSM (eGK, SMC-B/HSM-B, HBA) und steuert die Zugriffe auf diese Komponenten. Alle anderen Komponenten der TI-Plattform sind nur für sich selbst verantwortlich.

Hinweis: Für Fachmodule und Fachdienste kann Kriterium a) durchaus erfüllt sein. Diese werden jedoch hier nicht betrachtet.

Umsetzung der Mandantenfähigkeit in der TI-Plattform

ENTWURF

SMC-B

SMCs besitzen keine Benutzerverwaltung und können daher nicht eigenständig erkennen, ob ein aufrufender Nutzer zu einem bestimmten Mandanten gehört. SMCs (wie alle Smartcards) koppeln die Nutzung privater Schlüssel an die Erreichung des dafür nötigen Sicherheitszustands. Dieser wird erreicht, wenn (je nach Konfiguration) eine erfolgreiche PIN-Verifikation oder ein erfolgreiches Card to Card durchgeführt wurde. Anschließend können die privaten Schlüssel genutzt werden. Die Smartcard verlässt sich dabei darauf, dass ihre Umgebung sicherstellt, dass nur der Benutzer die privaten Schlüssel nutzen darf, der ursächlich die Erreichung des erhöhten Sicherheitszustands auch erfolgreich ausgelöst hat.

Die SMC delegiert die Durchsetzung der mandantenbezogenen Datentrennung an die Außenwelt, die mit ihr interagiert, in diesem Fall an die Fachmodule und den Konnektor. Da Fachmodule in der Hoheit der Fachanwendungen liegen, ist die mandantenbezogene Nutzung der SMC-B durch die Fachanwendungen umzusetzen. Die Betrachtung der Bedeutung für den Konnektor erfolgt im nächsten Abschnitt.

HSM-B

Grundsätzlich gelten die Aussagen der SMC-B auch für das HSM-B. Das HSM-B kann allerdings zusätzlich Daten für mehrere Mandanten beinhalten und muss eine Selektion bei Zugriff auf die Daten mit Mandantenbezug unterstützen.

Konnektor

Mandantenfähigkeit bedeutet für den Konnektor eine sichere Umgebung für jeden Mandanten innerhalb der dem Konnektor zugeordneten Leistungserbringer- oder Kostenträgerumgebung zu schaffen. Ein Beispiel ist eine Praxisgemeinschaft mit einem Konnektor und jeweils einem Mandanten pro Arzt. Die konkreten Konstellationen können hier, speziell im Krankenhausumfeld, sehr unterschiedlich sein und müssen durch den Ansatz abdeckbar sein.

⌦ **TIP1-A_2200 Mandantenfähigkeit des Konnektors**

Der Konnektor MUSS mandantenfähig sein und dabei folgende Vorgaben erfüllen:

1. Mandantenübergreifend MUSS ein Abbild der Umgebung jedes Mandanten am Konnektor persistent konfiguriert werden können,
   a. in dem die Bestandteile der Leistungserbringer-, Gesellschafterorganisations- oder Kostenträgerumgebung (Arbeitsplätze, Primärsysteme, Kartenterminals und HSM-B/SMC-Bs)
   b. als auch die Beziehungen innerhalb dieser Bestandteile sowie zwischen ihnen und den Mandanten definiert werden.
2. Bei der Konfiguration des Abbildes der Umgebung MÜSSEN Arbeitsplätze, Primärsysteme und Kartenterminals mehreren Mandaten gleichzeitig zugeordnet und damit in wechselndem Mandantenkontext verwendet werden können.
3. Beim Aufruf einer Konnektorschnittstelle, für die der Mandantenbezug relevant ist, MUSS im Aufruf die Mandanteninformation mitgegeben werden, so dass eine Mandantenzuordnung durch den Konnektor erfolgen kann.

ENTWURF

4. Entsprechend des Mandanten im Kontext der modellierten Vertrauensumgebung MUSS pro Aufruf einer Konnektorschnittstelle eine Zugriffsautorisierung (ja/nein) erfolgen.

5. Anfragen über den dynamischen Zustand der Leistungserbringer- oder Kostenträgerumgebung (etwa über die Liste der gesteckten Karten) MUSS der Konnektor im Rahmen des Mandantenkontextes beantworten.

6. Die Registrierung (Subscription) für Ereignis-Mitteilungen (Event-Notification), wie die von Kartensteck-Ereignissen MUSS mandantenbezogen erfolgen. Die Verteilung der Ereignisse-Mitteilungen MUSS dann im Einklang mit der Registrierung mandantenbezogen erfolgen. ⌫

Durch die Delegation der mandantenbezogenen Datentrennung der SMC-Bs an den Konnektor, ist er in der Pflicht sicherzustellen, dass nur Aufrufer im erlaubten Mandantenkontext die SMC-B nutzen. Der Konnektor seinerseits verwendet die SMC-B nie eigenmächtig, d. h. es findet keine implizite Nutzung der SMC-B durch den Konnektor statt. Alle SMC-B-Interaktionen geschehen durch einen Aufruf eines Clientsystems (Primärsystems). Daher wird diese Pflicht vollständig durch die oben aufgeführte Zugriffsautorisierung erfüllt. Analoge Aussagen gelten für das HSM-B, wobei hier durch den Konnektor eine Selektion der Daten und Funktionen mit Mandantenbezug (gedanklich der zugrundeliegenden SMC-B) auf dem HSM-B durchzuführen ist.

Primärsysteme sind vertrauenswürdig, und der Konnektor ist gehalten „der Userverwaltung und -authentisierung der Primärsysteme für einen Zugriff auf Karten des Leistungserbringers und institutionsbezogene Sicherheitsmodule [zu] vertrauen [,] um in den dezentralen Komponenten der TI-Plattform auf eine weitere User-Verwaltung verzichten zu können“. Eine eigene Benutzerverwaltung innerhalb des Konnektors ist daher nicht erforderlich und damit auch keine mandantenfähige Benutzerverwaltung. Ebenso kann der Konnektor die Information der Mandantenzuordnung vom Primärsystem als Aufrufparameter erhalten und dieser Information vertrauen.

Eine Detaillierung der Umsetzung der Mandantenfähigkeit erfolgt in der Spezifikation des Produkttyps Konnektor. Fachmodule müssen die TI-Plattform an den definierten Schnittstellen mit der benötigten Mandanteninformation versorgen.

4.4 Remote-PIN

Die Telematikinfrastruktur ermöglicht dem Anwender für alle angebotenen Funktionen, die PIN-Eingaben an HBAs oder an SMC-B/HSM-B benötigen, die für diese Funktion nötige PIN wahlweise lokal einzugeben oder per Remote-PIN-Eingabe durchzuführen.

Das Verfahren zur Remote-PIN-Eingabe ermöglicht es Fachmodulen und Clientsystemen, die PIN-Eingabe für eine Smartcard Y in einem Kartenterminal Y über ein zweites Kartenterminal X vorzunehmen.

Um den Schutzbedarf der PIN hinsichtlich des Schutzziels Vertraulichkeit beim Transport zu erfüllen, wird über eine Smartcard X im Kartenterminal X ein sicherer Kanal zur Smartcard Y im Kartenterminal Y oder zu einem HSM-B aufgebaut. Beim Aufbau des Kanals findet eine gegenseitige Authentisierung der Karten mittels CV-Zertifikaten statt.

Smartcard X agiert als Remote-PIN-Sender und Smartcard Y als Remote-PIN-Empfänger. Die PIN wird zum Transport vom Remote-PIN-Sender verschlüsselt und erst vom Remote-PIN-Empfänger im Rahmen der Verifikation entschlüsselt.

ENTWURF

Die beteiligten Komponenten des Remote-PIN-Verfahrens skizziert Abbildung 8:

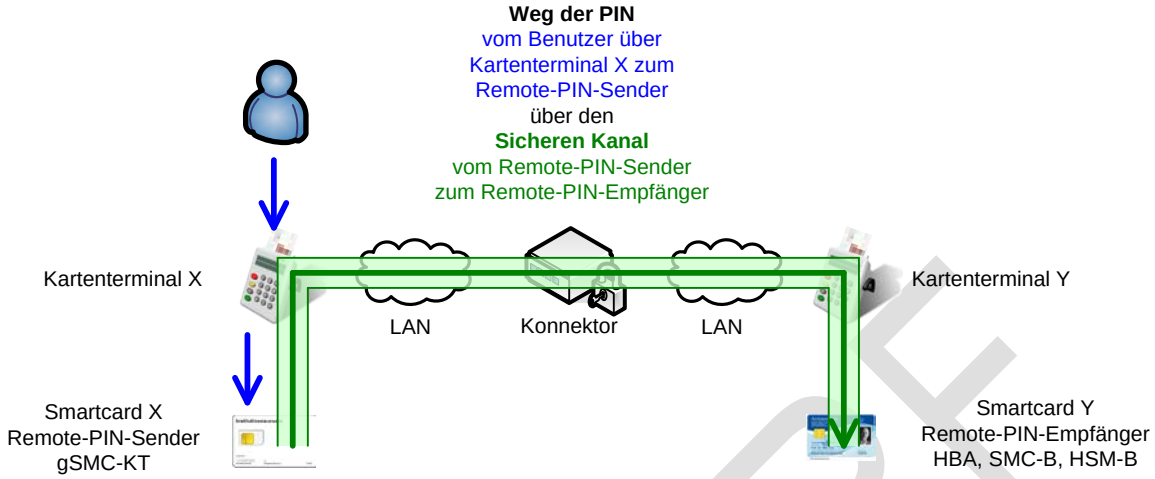


Abbildung 8: Beteiligte Komponenten beim Remote-PIN-Verfahren

Den Ablauf des Remote-PIN-Verfahrens legt Kapitel 7.2.11.3 normativ fest.

Folgende Anforderungen werden an die beteiligten Komponenten des Remote-PIN-Verfahrens gestellt:

⌦ **TIP1-A_2447 Kartenfreischaltung im Remote-PIN-Verfahren**

Der Konnektor MUSS am Interface I_KV_Card_Unlocking für die Operationen verify_PIN, initialize_PIN, unblock_PIN und change_PIN als eine Ausführungsvariante das Remote-PIN-Verfahren implementieren.⌫

⌦ **TIP1-A_2448 Remote-PIN-Sender**

Der Produkttyp gSMC-KT MUSS als Remote-PIN-Sender nutzbar sein und über die notwendigen Zertifikate verfügen. Dabei authentisiert sich die gSMC-KT mit der Identität ID.SMC.AUTD_RPS_CVC.⌫

⌦ **TIP1-A_2449 Remote-PIN-Empfänger**

Die Produkttypen HBA, SMC-B und HSM-B MÜSSEN als Remote-PIN-Empfänger nutzbar sein und über die notwendigen Zertifikate verfügen. Dabei authentisiert sich der HBA mit der Identität ID.HPC.AUTD_SUK_CVC und die SMC-B bzw. das HSM-B mit der Identität ID.SMC.AUTD_RPE_CVC.⌫

⌦ **TIP1-A_2450 Löschung PIN beim Remote-PIN-Sender und Kartenterminal**

Das Kartenterminal, an dem die Remote-PIN eingegeben wird und die als Remote-PIN-Sender agierende Smartcard MÜSSEN die eingegebene PIN nach der Übertragung sicher löschen. ⌫

⌦ **TIP1-A_2451 Sicherer Kanal zwischen Remote-PIN-Sender und -Empfänger**

Remote-PIN-Sender- und -Empfänger MÜSSEN folgende Sicherheitseigenschaften gewährleisten:

ENTWURF

- Sie MÜSSEN sicherstellen, dass jede PIN/PUK jeweils für die Zielkarte Ende-zu-Ende verschlüsselt wird.
- Sie MÜSSEN sicherstellen, dass für die Verschlüsselung ein geeignetes Verfahren aus der TR-03116 verwendet wird (inkl. der Entropieanforderungen an die Schlüssel, die diese Verfahren steuern).
- Sie MÜSSEN sicherstellen, dass jede Übertragung einer PIN/PUK nur zwischen in der TI zugelassenen Smart Cards erfolgen kann.
- Sie MÜSSEN sicherstellen, dass für den Schutz jeder PIN/PUK einer Karte für jeden einzelnen verschlüsselten Transport einer PIN/PUK verschiedene Schlüssel oder unterschiedliche initiale Vektoren verwendet werden.⌫

⌦ **TIP1-A_2453 Remote-PIN-Empfänger dem Anwender aufgezeigt**

Der Konnektor MUSS über das Kartenterminal, in dem die PIN-Eingabe beim Remote-PIN-Verfahren erfolgt, dem Anwender unmissverständlich anzeigen, für welche Karte oder welches Sicherheitsmodul er eine PIN eingeben soll.⌫

⌦ **TIP1-A_2454 Remote-PIN-Verfahren konform TR-03114**

Das Remote-PIN-Verfahren MUSS analog zur technischen Richtlinie des [BSI-TR-03114] gestaltet sein. Alle in der technischen Richtlinie für den Akteur SMC-A festgelegten Anforderungen werden durch die gSMC-KT als Remote-PIN-Sender umgesetzt.⌫

4.5 Mobile Szenarien

Bei der Beschreibung der in der Architektur der TI-Plattform definierten Dienste wird zunächst davon ausgegangen, dass die nutzenden Systeme an das Netz des Gesundheitswesens angebunden sind und bei Bedarf Leistungen online abrufen können. Hierfür wird die TI-Plattform mit einem geschlossenen Netz aufgebaut, in der die besonderen Sicherheits- und Nutzungsforderungen des Gesundheitssektors umgesetzt werden.

Es gibt allerdings auch bei vollständiger Vernetzung aller Partner im Gesundheitswesen Szenarien, in denen keine Online-Verbindung möglich ist. Diese Szenarien werden unter dem Begriff Mobile Offline-Szenarien zusammengefasst. Mobile Offline-Szenarien werden durch mobile Fachmodule im Produkttyp Mobiles Kartenterminal (MobKT) realisiert. Dieses mobile Kartenterminal bietet den mobilen Fachmodulen die notwendigen Leistungsmerkmale in einer Ausprägung ohne Online-Verbindung an.

Bezüglich der Dienste des mobilen Kartenterminals lassen sich drei Fälle unterscheiden:

- Dienste, die für die mobilen Offline-Szenarien und den stationären Fall identisch sind.
- Dienste, die sich in ihrer Funktionalität unterscheiden, weil z. B. im stationären Fall eine Online-Anbindung gefordert ist, die in den mobilen Offline-Szenarien nicht zur Verfügung steht.
- Dienste, die nur für den mobilen Fall zur Verfügung stehen.

ENTWURF

In den Dienstbeschreibungen wird ersichtlich, welcher der Fälle auf den jeweiligen Dienst zutrifft. Die Zuordnung eines Dienstes zum mobilen Szenario wird durch die ausgewiesene Berechtigung für mobile Fachmodule für diesen Dienst ersichtlich.

Dieser Logik folgend, gibt es nur am Produkttyp Mobiles Kartenterminal (siehe Kapitel 5.3.8) eine zusammenhängende Darstellung der Dienste für die mobilen Offline-Szenarien.

Ungeachtet der Tatsache, dass Dienste für die mobilen Offline-Szenarien und den stationären Fall funktional identisch sein können, sind Anforderungen an die zu verarbeitende Größe von Fachdaten der einzelnen Dienste nur verbindlich für den stationären Fall. Die Größe der verarbeitbaren Fachdaten in mobilen Szenarien orientiert sich an den Bedürfnissen der Fachanwendungen, aber auch an der Leistungsfähigkeit der eingesetzten Systeme und wird daher erst in der Spezifikation des Mobilen Kartenterminals abschließend festgelegt.

4.6 Rechenzentrums-Consumer

Ein Rechenzentrums-Consumer (RZ-Consumer) beschreibt einen möglichen Produkttyp einer Fachanwendung der TI, der in der Rolle eines Consumers mit der TI interagiert und dabei sowohl Anteile der TI-Plattform als auch Anteile der Fachanwendung enthält. Er vereint die Zonen TI-Plattform dezentral, Consumer und ggf. Secure Consumer in einem Produkttyp. Der Betrieb des RZ-Consumers in einem Rechenzentrum gemäß von der TI definierten Anforderungen ermöglicht die Durchsetzung von Anforderungen an den RZ-Consumer und erleichtert die Umsetzung von Sicherheitsanforderungen, da Annahmen bzgl. der Umgebung getroffen werden können.

Der RZ-Consumer ist an das Zentrale Netz der TI angebunden. Die in ihm enthaltenen Leistungen der TI-Plattform beschränken sich auf die Absicherung ggü. dem Zentralen Netz und dem Zugriff auf zentrale Dienste. Die Leistungen der TI-Plattform im RZ-Consumer werden durch den Consumer-Adapter der TI-Plattform im RZ-Consumer durchgesetzt.

Hinweis: Der RZ-Consumer ist KEIN Produkttyp der TI-Plattform und kann daher nicht analog der Produkttypen der TI-Plattform in diesem Konzept beschrieben werden. Er ist ein konzeptioneller Begriff für einen möglichen Produkttyp einer Fachanwendung und wird in der Systemlösungen der Fachanwendung, die einen RZ-Consumer realisiert, beschrieben.

Die Einführung der virtuellen Komponente „Consumer-Adapter“ schafft die Möglichkeit, dass Leistungen der TI-Plattform in einen Produkttyp der Fachanwendung eingebracht werden (ähnlich einer Library), so dass die Verantwortung der TI-Plattform bzgl. der Absicherung von zentralen Diensten und die Störungsfreiheit anderer Teilnehmer der TI gewährleistet wird. Es kann so darauf verzichtet werden, dass zwei in Reihe geschaltete separate Produkttypen der Fachanwendung und der TI-Plattform geschaffen werden müssen, die beide spezifiziert, entwickelt und zugelassen werden müssten.

⌦ **TIP1-A_6095 RZ-Consumer nur in Rechenzentren**

Ein Rechenzentrums-Consumer MUSS in einem Rechenzentrum betrieben werden.⌫

⌦ **TIP1-A_6096 Schutz von Fachmodulen in RZ-Consumern**

ENTWURF

Die Architektur eines Rechenzentrums-Consumers MUSS sicherstellen, dass Fachmodule authentisch und integer gehalten werden. Dies bedeutet, dass ein Fachmodul den Vorgaben der Fachanwendung genügt und nicht unerwünscht verändert wird.⌫

⌦ **TIP1-A_6097 Zugriff auf die eGK in RZ-Consumern**

Die Architektur eines Rechenzentrums-Consumers MUSS sicherstellen, dass nur Fachmodule direkten Zugriff auf die eGK haben.⌫

⌦ **TIP1-A_6098 Schutz gesicherter Fachdienste in RZ-Consumern**

Die Architektur eines Rechenzentrums-Consumers MUSS sicherstellen, dass nur Fachmodule Zugriff auf gesicherte Fachanwendungsspezifische Dienste haben.⌫

⌦ **TIP1-A_6099 Zertifikatsprüfung in RZ-Consumern**

Der Consumer-Adapter der TI-Plattform im RZ-Consumer MUSS innerhalb des RZ-Consumers eine Zertifikatsprüfung gemäß der logischen Operation I_Cert_Verification::verify_Certificate anbieten.⌫

⌦ **TIP1-A_6770 TSL-Download in RZ-Consumern**

Der Consumer-Adapter der TI-Plattform im RZ-Consumer MUSS innerhalb des RZ-Consumers den Download der TSL gemäß der logischen Operation I_TSL_Download::download_TSL anbieten.⌫

⌦ **TIP1-A_6100 Adressauflösung in RZ-Consumern**

Der Consumer-Adapter der TI-Plattform im RZ-Consumer MUSS innerhalb des RZ-Consumers eine Netzwerkadressenauflösung gemäß der logischen Operation I_DNS_Name_Information::get_IP_Address anbieten.⌫

⌦ **TIP1-A_6048 Service-Lokalisierung in RZ-Consumern**

Der Consumer-Adapter der TI-Plattform im RZ-Consumer MUSS innerhalb des RZ-Consumers eine Service-Lokalisierung gemäß der logischen Operation I_DNS_Service_Localization::get_Service_Location anbieten.⌫

⌦ **TIP1-A_6101 Zeitinformation in RZ-Consumern**

Der Consumer-Adapter der TI-Plattform im RZ-Consumer MUSS innerhalb des RZ-Consumers eine Zeitinformation gemäß der logischen Operation I_NTP_Time_Information::sync_Time anbieten.⌫

⌦ **TIP1-A_6546 Datentransport in RZ-Consumern**

Der Consumer-Adapter der TI-Plattform im RZ-Consumer MUSS innerhalb des RZ-Consumers einen Datentransport gemäß der logischen Operation I_IP_Transport::send_Data anbieten.⌫

⌦ **TIP1-A_6548 Verzeichnisdienstabfragen in RZ-Consumern**

Der Consumer-Adapter der TI-Plattform im RZ-Consumer MUSS innerhalb des RZ-Consumers die Abfrage des Verzeichnisdienstes gemäß der logischen Operation I_Directory_Query::search_Directory anbieten.⌫

⌦ **TIP1-A_6549 Kein direkter Zugriff auf zentrale Dienste in RZ-Consumern**

ENTWURF

Der Consumer-Adapter der TI-Plattform im RZ-Consumer MUSS den direkten Zugriff auf das Zentrale Netz und die zentralen Dienste verhindern.⌫

ENTWURF

5 Produkttypen der TI-Plattform

In diesem Kapitel werden die Produkttypen der TI-Plattform festgelegt. Dabei wird auf konzeptioneller Ebene die Verantwortlichkeit eines jeden Produkttyps benannt und die Bereitstellungspunkte der Leistungen der TI-Plattform auf die Produkttypen verteilt.

5.1 Übersicht des Gesamtsystems

Abbildung 9 zeigt eine Übersicht des Gesamtsystems Telematikinfrastruktur, um so ein Verständnis der Verteilung der verschiedenen Produkttypen zu unterstützen. Die Darstellung erfolgt in diesem Fall in einer Netzwerksicht, da dies dem zu vermittelnden Bild am nächsten kommt. Nachfolgend wird die produkttypbezogene Modellierung aber vornehmlich in UML erfolgen.

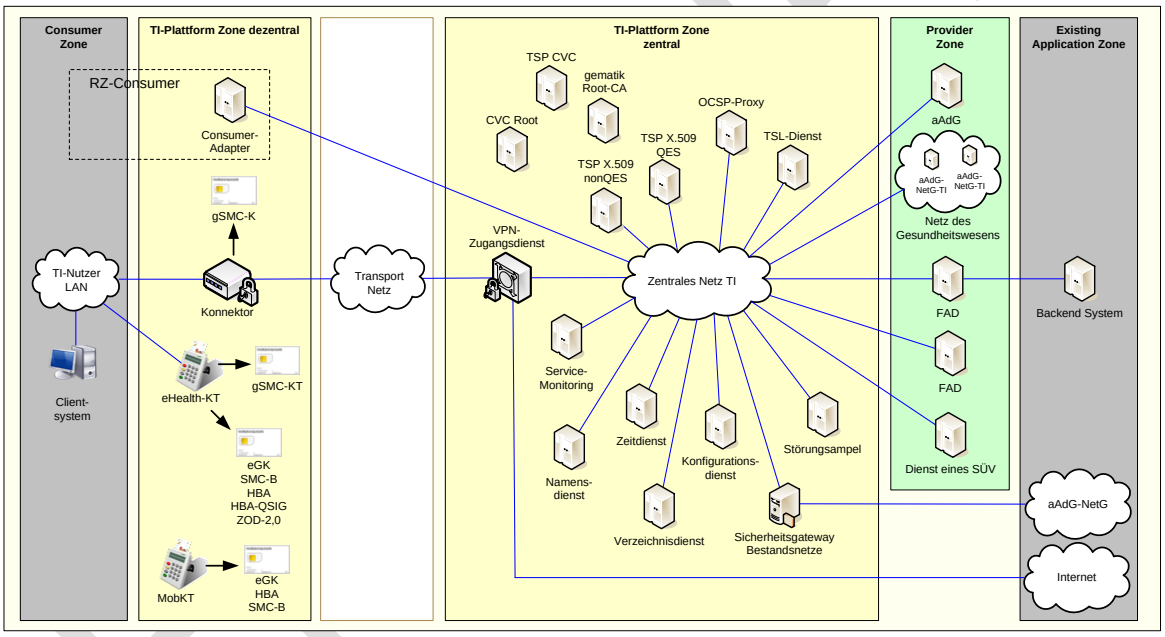


Abbildung 9: Übersicht des Gesamtsystems der TI

5.2 Festlegungen zu Produkttypen der TI-Plattform

In diesem Kapitel werden Aspekte der Produkttypen aufgegriffen, die mehrere oder alle Produkttypen der TI-Plattform betreffen.

⌦ **TIP1-A_2214 TI-Plattform, Festlegung der Produkttypen**

Die TI-Plattform MUSS die nachfolgend definierten Produkttypen bereitstellen. Weitere Produkttypen sind nicht zulässig.

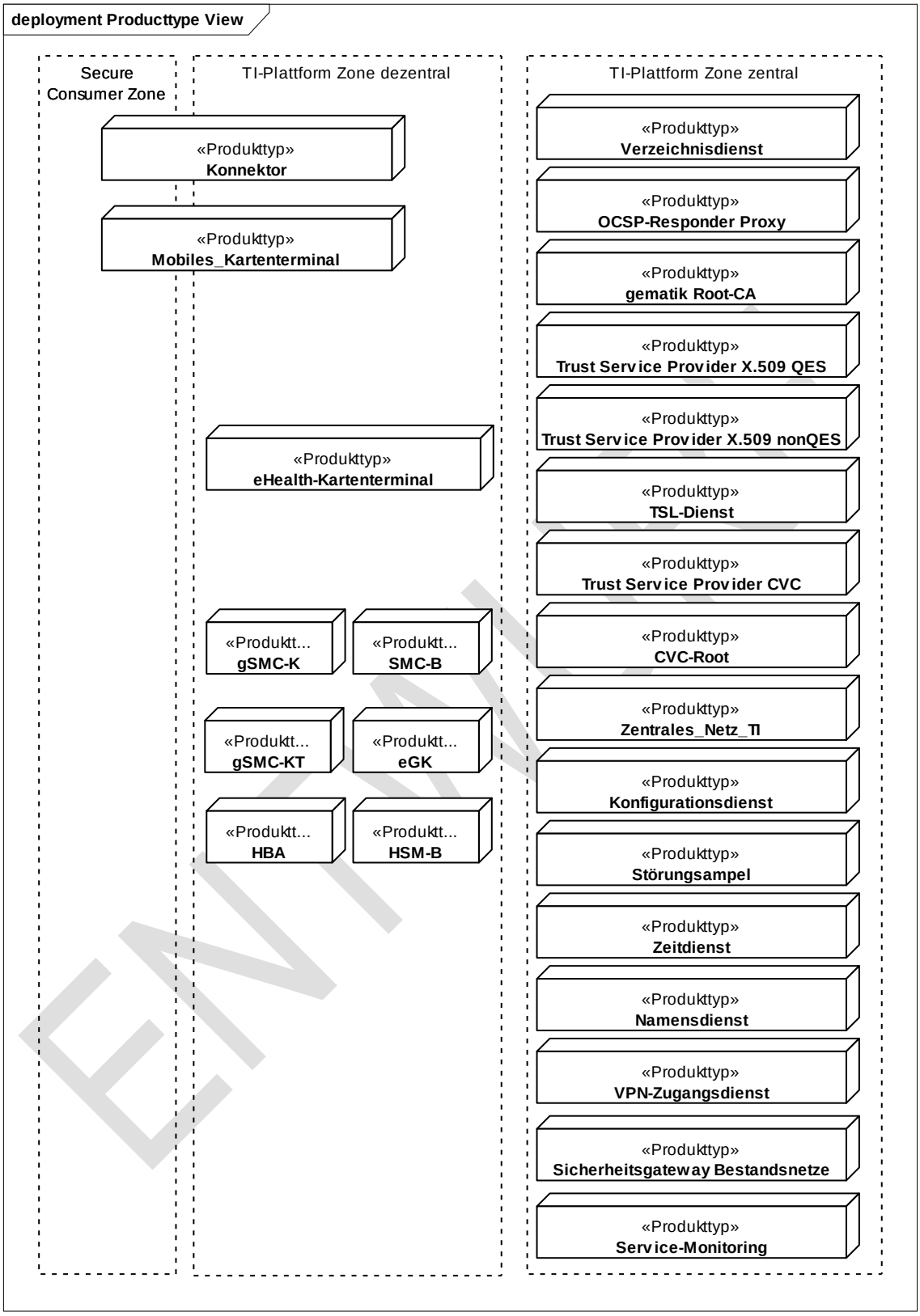


Abbildung 10: Produkttypsicht

⌫

Nachfolgend werden Festlegungen getroffen, die mehrere oder sogar alle Produkttypen betreffen und nicht direkt an eine funktionale Leistung der TI-Plattform gebunden sind.

⌦ **TIP1-A_2199 Dezentrale Komponenten der TI-Plattform, zwei Versionen Firmware und Konfigurationsstand**

Jeder Produkttyp der dezentralen Komponenten der TI-Plattform (ausgenommen Karten und HSM-B) SOLL, sofern sie/er aktualisierbar ist, in der Lage sein, mindestens zwei Versionen von Firmware inklusive Konfigurationsstände vorhalten zu können, um so ein lokales Rollback zu ermöglichen. Das Vorhalten der Versionen kann auch im KSR erfolgen, so dass die Versionen der Firmware nicht im Produkttyp gespeichert werden müssen.⌫

⌦ **TIP1-A_2216 Dezentrale Komponenten der TI-Plattform, Selbstschutz gegen Angriffe**

Produkttypen, die dezentrale Komponenten der TI-Plattform implementieren, MÜSSEN sich abhängig von ihrer Einsatzumgebung durch technische oder organisatorische Maßnahmen gegen Angriffe schützen.⌫

⌦ **TIP1-A_2474 Schlüssel sicher speichern**

Alle Produkttypen der zentralen TI-Plattform, das eHealth-Kartenterminal und der Konnektor MÜSSEN Schlüssel sicher speichern und ihr Auslesen verhindern.⌫

⌦ **TIP1-A_2217 Sichere Speicherung des Vertrauensankers der PKI**

Alle Produkttypen, die X.509-Zertifikate prüfen, MÜSSEN den Vertrauensanker der PKI in Form TSL-Signer-CA-Zertifikat in aktueller Version enthalten und sicher speichern.⌫

⌦ **TIP1-A_2463 Sichere Speicherung des Key Signing Keys des TI Trust Anchors**

Alle Produkttypen, die DNSSEC validieren, MÜSSEN den Key Signing Key des TI Trust Anchors in aktueller Version enthalten und sicher speichern. Der Konnektor MUSS zusätzlich den Key Signing Key des Transportnetzes in aktueller Version enthalten. Der Key Signing Key darf dabei nur durch autorisierte Akteure eingebracht werden.⌫

⌦ **TIP1-A_2465 Robustheit gegenüber fehlerhafter Eingabe und Datenübertragung**

Produkttypen der dezentralen TI-Plattform DÜRFEN NICHT durch fehlerhafte Eingaben des Nutzers oder fehlerhafte Datenübertragungen in ihrer gesamtheitlichen funktionalen und nichtfunktionalen Leistungsfähigkeit beeinträchtigt werden.⌫

⌦ **TIP1-A_2218 Synchron mit Zeitdienst, Zentrale Dienste**

Produkttypen der Zone „TI-Plattform Zone zentral“ SOLLEN mit der vom Produkttyp Zeitdienst bereitgestellten Zeitinformation synchron sein. ⌫

ENTWURF

⌦ **TIP1-A_2684 Synchron mit Zeitdienst, Ersatzverfahren für Zentrale Dienste**

Produkttypen der Zone „TI-Plattform Zone zentral“, die keinen Zugang zum Zeitdienst haben, MÜSSEN ein Ersatzverfahren einsetzen, das eine maximale Abweichung von einer Sekunde gegenüber der gesetzlichen Zeit gewährleistet.⌫

⌦ **TIP1-A_2219 Synchron mit Zeitdienst, Konnektor**

Der Produkttyp Konnektor MUSS mit der vom Produkttyp VPN-Zugangsdienst bereitgestellten Zeitinformation synchron sein.⌫

~~**TIP1-A_2220 Prüfung von DNS-Abfragen mittels DNSSEC in der TI-Plattform**~~

~~Alle Produkttypen der TI-Plattform, die den Namensdienst nutzen oder FQDN im Transportnetz auflösen, MÜSSEN die Ergebnisse von Abfragen mit Hilfe des DNSSEC-Verfahrens auf Authentizität und Integrität prüfen.~~

⌦ **TIP1-A_2221 Einbringung des Vertrauensankers der PKI bei Erstinbetriebnahme**

Alle Produkttypen, die X.509-Zertifikate prüfen, MÜSSEN bei einer Erstinbetriebnahme sicherstellen, dass der Vertrauensanker der PKI in Form des TSL-Signer-CA-Zertifikats sicher in die Komponente eingebracht wird.⌫

⌦ **TIP1-A_2222 Speicherung der TSL-Inhalte in lokalem Trust Store**

Alle Produkttypen, die X.509-Zertifikate prüfen, MÜSSEN die Inhalte der TSL nach erfolgreicher Vertrauensraum- und syntaktischer Prüfung in einem lokalen Trust Store sicher speichern und zum weiteren Abruf lokal zugreifbar halten.⌫

⌦ **TIP1-A_2223 Regelmäßiges Update der TSL**

Alle Produkttypen, die X.509-Zertifikate prüfen, MÜSSEN in einem definierten Prüfintervall das Vorhandensein einer aktualisierten TSL prüfen und anhand der Versionsnummer in der TSL entscheiden, ob die im TSL-Trust-Store vorhandene TSL beibehalten wird oder durch eine neuere Version ersetzt werden muss.⌫

⌦ **TIP1-A_2224 Kompatibilität von zugelassenen Implementierungen der Produkttypen**

Zugelassene Produkte der TI-Plattform MÜSSEN gegen andere zugelassene Produkte desselben Produkttyps ausgetauscht werden können, ohne die Funktionsfähigkeit der TI-Plattform negativ zu beeinflussen.⌫

Für die Details der Schnittstellen siehe Kapitel 5.5, 5.6 und 5.7.

5.3 Produkttypen der Zone TI-Plattform dezentral

Produkttypen der dezentralen Zone der TI-Plattform bilden alle Anteile des Building Blocks „dezentrale Komponenten der TI-Plattform“ der Zone „TI-Plattform – dezentral“ vollständig ab.

Dabei unterliegen Produkttypen der TI-Plattform die eine Smartcard darstellen dem Bestandsschutz. Die Spezifikation der Smartcards der Generation 2 ist nicht Bestandteil dieses Projektes. Daher werden die Smartcards in den folgenden Abschnitten nur kurz beschrieben.

ENTWURF

5.3.1 Produkttyp elektronische Gesundheitskarte (eGK)

Die eGK ist eine Smartcard und wird zur Authentisierung des Versicherten in der TI sowie zur Signatur und Entschlüsselung von Daten des Versicherten eingesetzt. Zusätzlich können auf der eGK in begrenztem Umfang Daten der Fachanwendungen in sog. Fachanwendungsspezifischen Karten-Applikationen (vgl. Kap. 4.1.1) gespeichert werden. Die Zugriffsmöglichkeiten auf die jeweiligen Daten können auf bestimmte Rollen eingeschränkt werden.

⌦ **TIP1-A_2226 Produkttyp eGK, Schnittstellen und Prozesse**

Der Produkttyp eGK MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 12: Schnittstellen und Prozesse des Produkttyps eGK

eGK		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_ICC_Contacts	eHealth-Kartenterminal, MobKT	Aufgrund des bestehenden Bestandsschutzes erfolgt in diesem Dokument keine weitere Beschreibung dieser Schnittstelle.
I_Card_Data_Operations	Konnektor	Nachfolgend werden die logischen Karten-Schnittstellen im Dokument stellvertretend unter I_Smartcard_Operations zusammengefasst.
I_Card_Auth_Operations	Konnektor	
I_Card_Crypt_Operations	Konnektor	
Benötigte Schnittstellen		
Fachliche Prozesse	**Bedingungen**	

⌫

⌦ **TIP1-A_2494 Produkttyp eGK, Zugriffsschutz auf Objekte**

Die eGK MUSS in der Lage sein, gegenüber den berechtigten Akteursgruppen, den Zugriffsschutz auf Objekte in ihrem Datenspeicher für jedes Objekt getrennt festzulegen.⌫

⌦ **TIP1-A_5754 eGK Identitäten**

Der Produkttyp eGK MUSS alle in der Tabelle Tab_ArchTIP_001 für die eGK vorgesehenen kryptografischen Identitäten bereitstellen.⌫

⌦ **TIP1-A_5716 eGK Datenspeicher**

Der Produkttyp eGK MUSS ausreichend Speicherplatz für die Basisdaten sowie die Daten der gesetzlich oder durch die Konsensentscheidung der Gesellschafter der gematik für eine Speicherung auf der eGK vorgesehenen Fachanwendungen enthalten.⌫

⌦ **TIP1-A_5756 eGK Zugriffsprotokoll**

Der Produkttyp eGK MUSS einen Zugriffsprotokollspeicher mit 50 Einträgen zur Verfügung stellen. Die Einträge des Zugriffsprotokollspeichers MÜSSEN zyklisch überschreibbar sein.⌫

ENTWURF

5.3.2 Produkttyp Heilberufsausweis (HBA)

Der HBA ist eine Smartcard und wird zur Authentisierung des Leistungserbringers in der TI sowie zur Signatur und Entschlüsselung von Daten der Fachanwendungen eingesetzt.

⌦ **TIP1-A_2227 Produkttyp HBA, Schnittstellen und Prozesse**

Der Produkttyp HBA MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 13: Schnittstellen und Prozesse des Produkttyps HBA

HBA		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_ICC_Contacts	eHealth-Kartenterminal, MobKT	Aufgrund des bestehenden Bestandsschutzes erfolgt in diesem Dokument keine weitere Beschreibung dieser Schnittstelle.
I_Card_Auth_Operations	Konnektor	Nachfolgend werden die logischen Karten-Schnittstellen im Dokument stellvertretend unter I_Smartcard_Operations zusammengefasst.
I_Card_Crypt_Operations	Konnektor	
Benötigte Schnittstellen		
Fachliche Prozesse	**Bedingungen**	

⌫

⌦ **TIP1-A_5757 HBA Identitäten**

Der Produkttyp HBA MUSS alle in der Tabelle Tab_ArchTIP_001 für den HBA vorgesehenen kryptografischen Identitäten bereitstellen.⌫

~~**TIP1-A_5760 HBA qualifizierte Attributzertifikate**~~

~~Der Produkttyp HBA MUSS die Möglichkeit bieten, qualifizierte Attributzertifikate zu speichern.~~

5.3.3 Produkttyp Security Module Card Organisationen des Gesundheitswesens (SMC-B)

Die SMC-B ist eine Smartcard und wird zur Authentisierung der Organisationen des Gesundheitswesens in der TI sowie zur Signatur und Entschlüsselung von Daten der Fachanwendungen eingesetzt.

⌦ **TIP1-A_2228 Produkttyp SMC-B, Schnittstellen und Prozesse**

Der Produkttyp SMC-B MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 14: Schnittstellen und Prozesse des Produkttyps SMC-B

SMC-B		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_ICC_Contacts	eHealth-Kartenterminal, MobKT	Aufgrund des bestehenden Bestandsschutzes erfolgt in diesem Dokument keine weitere Beschreibung dieser Schnittstelle.
I_Card_Auth_Operations	Konnektor	Nachfolgend werden die logischen Karten-

ENTWURF

I_Card_Crypt_Operations	Konnektor	Schnittstellen im Dokument stellvertretend unter I_Smartcard_Operations zusammengefasst.
Benötigte Schnittstellen		
Fachliche Prozesse	**Bedingungen**	

⌫

⌦ **TIP1-A_5761 SMC-B Identitäten**

Der Produkttyp SMC-B MUSS alle in der Tabelle Tab_ArchTIP_001 für die SMC-B vorgesehenen kryptografischen Identitäten bereitstellen.⌫

⌦ **TIP1-A_5817 Produkttyp SMC-B, kein Zugriff auf die eGK durch Gesellschafterorganisationen**

Der Produkttyp SMC-B einer Gesellschafterorganisation DARF NICHT Zugriff auf die eGK ermöglichen.⌫

5.3.4 Produkttyp Hardware Security Module Organisationen des Gesundheitswesens (HSM-B)

Der Produkttyp HSM-B ist für die Telematikinfrastruktur vorgesehen. Fragen der Umsetzung eines HSM-Bs sind derzeit in Klärung.

Das HSM-B ist ein spezielles HSM und wird zur Authentisierung von Organisationen des Gesundheitswesens in der TI sowie zur Signatur und Entschlüsselung von Daten der Fachanwendungen eingesetzt. Es kann in größeren Organisationen des Gesundheitswesens anstatt der SMC-B zum Einsatz kommen, falls die Performance der SMC-B nicht ausreichend ist.

⌦ **TIP1-A_2229 Produkttyp HSM-B, Schnittstellen und Prozesse**

Der Produkttyp HSM-B MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 15: Schnittstellen und Prozesse des Produkttyps HSM-B

HSM-B		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_HSM_Operations	Konnektor	Die Schnittstelle entspricht funktional der Schnittstelle I_Smartcard_Operations, erlaubt aber die Selektion eines Mandaten (SMC-B) im Kontext der Operationen, da das HSM-B mehrere SMC-B ersetzten kann. Aufgrund des bestehenden Bestandsschutzes erfolgt in diesem Dokument keine weitere Beschreibung dieser Schnittstelle
I_Poll_System_Information	Konnektor	
Benötigte Schnittstellen		
Fachliche Prozesse	**Bedingungen**	

⌫

⌦ **TIP1-A_2499 Produkttyp HSM-B, Funktionalität analog der SMC-B**

ENTWURF

Der Produkttyp HSM-B MUSS vollständig alle Funktionen einer oder mehrer SMC-Bs (sowohl X.509-Operationen als auch die CVC-Operationen) ersetzen.⌫

⌦ **TIP1-A_2500 Produkttyp HSM-B, Schnittstellentechnik**

Der Produkttyp HSM-B KANN sich in seiner Schnittstellentechnik von SMC-Bs unterscheiden. Seine Schnittstelle muss nicht über APDUs angeboten werden.⌫

⌦ **TIP1-A_5824 Produkttyp HSM-B, kein Zugriff auf die eGK durch Gesellschafterorganisationen**

Der Produkttyp HSM-B einer Gesellschafterorganisation DARF NICHT Zugriff auf die eGK ermöglichen.⌫

5.3.5 Produkttyp Security Module Card Kartenterminal (gSMC-KT)

Die gSMC-KT dient zur Authentisierung des Kartenterminals bei der Kommunikation mit dem Konnektor.

⌦ **TIP1-A_2230 Produkttyp gSMC-KT, Schnittstellen und Prozesse**

Der Produkttyp gSMC-KT MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 16: Schnittstellen und Prozesse des Produkttyps gSMC-KT

gSMC-KT		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_Card_Auth_Operations	Konnektor, eHealth-KT	Nachfolgend werden die logischen Karten-Schnittstellen im Dokument stellvertretend unter I_Smartcard_Operations zusammengefasst.
I_Card_Crypt_Operations	Konnektor, eHealth-KT	
Benötigte Schnittstellen		
Fachliche Prozesse	**Bedingungen**	

⌫

⌦ **TIP1-A_5723 gSMC-KT Identitäten**

Der Produkttyp gSMC-KT MUSS alle in der Tabelle Tab_ArchTIP_001 für die gSMC-KT vorgesehenen kryptografischen Identitäten bereitstellen.⌫

5.3.6 Produkttyp Security Module Card Konnektor (gSMC-K)

Die gSMC-K dient zur Authentisierung des Konnektors bei der Kommunikation mit dem VPN-Zugangsdienst, dem Kartenterminal und dem HBA.

⌦ **TIP1-A_2231 Produkttyp gSMC-K, Schnittstellen und Prozesse**

Der Produkttyp gSMC-K MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 17: Schnittstellen und Prozesse des Produkttyps gSMC-K

ENTWURF

gSMC-K		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_Card_Auth_Operations	Konnektor	Nachfolgend werden die logischen Karten-Schnittstellen im Dokument stellvertretend unter I_Smartcard_Operations zusammengefasst.
I_Card_Crypt_Operations	Konnektor	
Benötigte Schnittstellen		
Fachliche Prozesse	**Bedingungen**	

⌫

⌦ **TIP1-A_5764 gSMC-K Identitäten**

Der Produkttyp gSMC-K MUSS alle in der Tabelle Tab_ArchTIP_001 für die gSMC-K vorgesehenen kryptografischen Identitäten bereitstellen.⌫

5.3.7 Produkttyp eHealth-Kartenterminal (KT)

Das eHealth-Kartenterminal dient der Interaktion mit Smartcards. Gemäß Bestandsschutz ist die hardwareseitige Ausprägung der Kartenterminals durch die eHealth-Spezifikation zum Online-Rollout R4.0.0 gesetzt. Dies bedeutet im Wesentlichen: Einhaltung des SICCT-Standards, Netzanschluss, Display, PIN-Pad, mindestens einen ID-1- sowie einen ID-000-Steckplatz.

⌦ **TIP1-A_2232 Produkttyp eHealth-Kartenterminal, Schnittstellen und Prozesse**

Der Produkttyp eHealth-Kartenterminal MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 18: Schnittstellen und Prozesse des Produkttyps eHealth-Kartenterminal

eHealth-Kartenterminal		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_KT_Communication	Konnektor	
I_KSR_Update	Konnektor	
I_KSRC_Local_Management	Admin einer Organisation des Gesundheitswesens	
I_Poll_System_Information	Konnektor	
Benötigte Schnittstellen		
I_ICC_Contacts, I_Notification, I_NTP_Time_Information (optional)		
Fachliche Prozesse	**Nutzer**	**Bedingungen**

⌫

⌦ **TIP1-A_2548 eHealth-Kartenterminal, Unterstützung der unbeobachteten PIN-Eingaben**

Der Produkttyp eHealth-Kartenterminal MUSS durch technische oder organisatorische Maßnahmen den Karteninhaber dabei unterstützen, die PIN/PUK unbeobachtet von anderen eingeben zu können. Bei der Umsetzung der Anforderung sind die Vorgaben der Arbeitsgruppe „Einsatzumgebung Kartenterminal“ zu berücksichtigen.⌫

Die nachfolgenden Festlegungen stehen nicht im Konflikt mit dem geltenden physikalischen und elektrophysikalischen Bestandschutz des eHealth-Kartenterminals, da sie

ENTWURF

entweder die Firmware des KTs betreffen oder durch Vorgaben der Arbeitsgruppe „Einsatzumgebung Kartenterminal“[14] adressiert werden.

⌦ **TIP1-A_2504 Produkttyp eHealth-Kartenterminal, Integrität der PIN/PUK**

Der Produkttyp eHealth-Kartenterminal MUSS sicherstellen, dass die PIN/PUK einer personenbezogenen oder institutsbezogenen Smartcard nach der Eingabe innerhalb des eHealth-Kartenterminals nicht verändert werden kann.⌫

⌦ **TIP1-A_2505 Produkttyp eHealth-Kartenterminal, Verwahrung der PIN/PUK**

Der Produkttyp eHealth-Kartenterminal DARF die PIN/PUK einer personenbezogenen oder institutsbezogenen Smartcard NICHT über eine andere Schnittstelle nach außen geben, als über die zur gesteckten Smartcard.⌫

⌦ **TIP1-A_2506 Produkttyp eHealth-Kartenterminal, Schutz vor Abhören**

Der Produkttyp eHealth-Kartenterminal MUSS sicherstellen, dass nicht unbemerkt eine Abhörvorrichtung innerhalb des Gerätes eingerichtet werden kann.⌫

⌦ **TIP1-A_2507 Produkttyp eHealth-Kartenterminal, Schutz vor Veränderung**

Der Produkttyp eHealth-Kartenterminal MUSS sicherstellen, dass nicht unbemerkt die Hard- oder Software des Terminals verändert werden kann.⌫

⌦ **TIP1-A_2508 Produkttyp eHealth-Kartenterminal, Erkennbarkeit von Angriffen**

Der Produkttyp eHealth-Kartenterminal MUSS sicherstellen, dass Angriffe am Gerät physische Schäden in der Art anrichten, dass sie vor der Wiederinbetriebnahme des Gerätes mit hoher Wahrscheinlichkeit entdeckt werden.⌫

⌦ **TIP1-A_2549 eHealth-Kartenterminal, Sicherheitsziele aus Schutzprofilen**

Der Produkttyp eHealth-Kartenterminal MUSS konform zu den bisherigen Sicherheitszielen aus den Schutzprofilen des BSI und den für das eHealth-Kartenterminal verbindlichen technischen Richtlinien des BSI aufgebaut sein.⌫

5.3.8 Produkttyp Mobiles Kartenterminal (MobKT)

Das mobile Kartenterminal ist ein Gerät, mit welchem mobil mit Karten des Gesundheitswesens interagiert werden kann. Es vereint die Funktionen eines eHealth-Kartenterminals (Karten-Slots, Display, PIN-Pad) mit den Funktionen eines mobilen Kleincomputers/PDAs (grafische Benutzerführung, Daten speichern/laden/bearbeiten). Auf einem mobilen Kartenterminal werden mobile Fachmodule betrieben, die die Funktionen zur fachlichen Interaktion bereitstellen. Mobile Fachmodule steuern die Benutzerinteraktion sowie die fachlogische Kommunikation mit Daten und Schlüsseln der lokal gesteckten Karten.

Ein mobiles Kartenterminal hat keinen Zugang zur zentralen TI-Plattform oder einem Konnektor. Es wird zur Übertragung von Daten lokal an einen Arbeitsplatzrechner angeschlossen und kommuniziert ausschließlich mit diesem. Optional kann ein mobiles Kartenterminal auch so gestaltet werden, dass es als eHealth-Kartenterminal betrieben werden kann.

---

[14] Bei den Vorgaben der Arbeitsgruppe „Einsatzumgebung Kartenterminal“ handelt es sich um gematik-interne Vorgaben, die bei der Umsetzung von Anforderungen an das eHealth-Kartenterminal innerhalb der Spezifikationen der gematik berücksichtigt worden sind.

ENTWURF

Die HBA-Vorläuferkarten HBA-qSig und ZOD-2.0 werden im mobilen Kartenterminal nicht unterstützt.

⌦ **TIP1-A_2233 Produkttyp Mobiles Kartenterminal, Schnittstellen und Prozesse**

Der Produkttyp Mobiles Kartenterminal MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 19: Schnittstellen und Prozesse des Produkttyps Mobiles Kartenterminal

Mobiles Kartenterminal		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_MobKT_Temp_Storage	Fachmodul_MobKT	
I_MobKT_GUI	Fachmodul_MobKT	
I_MobKT_Printer	Fachmodul_MobKT	
I_KSRC_Local_Management	Admin einer Organisation des Gesundheitswesens	
I_KV_Card_Unlocking	Fachmodul_MobKT	
I_Poll_System_Information	Fachmodul_MobKT	
I_Notification_From_FM	Fachmodul_MobKT	
I_Reg_Notification	Fachmodul_MobKT	
I_Synchronised_System_Time	Fachmodul_MobKT	
I_KV_Card_Handling	Fachmodul_MobKT	
I_KV_Card_Operations	Fachmodul_MobKT	Bei langlaufenden Operationen muss kontinuierlich über den Fortgang der Operation informiert werden.
I_Change_System_Time	Admin einer Organisation des Gesundheitswesens	
I_Cert_Verification	Fachmodul_MobKT	
I_MobKT_Management	Admin einer Organisation des Gesundheitswesens	
I_MobKT_FMAccess	Clientsystem	
I_MobKT_Access	Clientsystem	
I_KV_Card_Reservation	Fachmodul_MobKT	
Benötigte Schnittstellen		
I_ICC_Contacts, I_Notification, PrinterConnector (repräsentiert den Anschluss eines externen Druckers, optional), I_MobKT_CommFM		
Fachliche Prozesse	**Nutzer**	**Bedingungen**

⌫

⌦ **TIP1-A_2509 Produkttyp Mobiles Kartenterminal, Größe von Fachdaten**

Der Produkttyp Mobiles Kartenterminal MUSS sich bei der Festlegung der verarbeitbaren Größe von Fachdaten an der Leistungsfähigkeit des migrationsfähigen, mobilen Kartenterminals der Stufe 1 orientieren. Die Anforderungen an die zu verarbeitende Größe von Fachdaten der einzelnen Dienste sind nur verbindlich für den stationären Fall.⌫

Die Leistungsfähigkeit des migrationsfähigen, mobilen Kartenterminals der Stufe 1 ist beschrieben in [Spezifikation Mobiles Kartenterminal Ausbaustufe 1].

⌦ **TIP1-A_2511 Produkttyp Mobiles Kartenterminal, Fachmodule in die Firmware einbinden**

Der Produkttyp Mobiles Kartenterminal KANN zur Komplexitäts- und damit Kostenreduktion Fachmodule auf Geräten für mobile Offline-Basisdienste an die Firmware des Geräts binden.⌫

⌦ **TIP1-A_2550 Mobiles Kartenterminal, Sicherheitsziele aus Schutzprofilen**

Der Produkttyp Mobiles Kartenterminal MUSS konform zu den bisherigen Sicherheitszielen aus den Schutzprofilen des BSI und den für das Mobile Kartenterminal verbindlichen technischen Richtlinien des BSI aufgebaut sein. ⌫

5.3.9 Produkttyp Konnektor

Der Konnektor, als Bestandteil der TI verbindet die Clientsysteme der Leistungserbringer und Kostenträger auf dezentraler Seite mit der TI. Dazu implementiert der Konnektor Teile der Basis- und Infrastrukturdienste der TI-Plattform und stellt die relevanten Basisdienste und Infrastrukturdienste den Clientsystemen zur Verfügung. Ferner beinhaltet der Konnektor die Fachmodule der Fachanwendungen.

Der Zugriff auf eHealth-Kartenterminals sowie der Zugriff auf eGK, HBA und SMC-B im lokalen Netz erfolgt ausschließlich über den Konnektor. Weiterhin stellt der Konnektor einen Signaturproxy bereit. Der Signaturproxy gehört zwar zum Produkttyp Konnektor, wird aber als Softwarekomponente auf Arbeitsplatzrechnern der Leistungserbringer installiert.

Der Konnektor stellt eine sichere Verbindung über ein unsicheres Transportnetz (z. B. Internet) in das zentrale Netz der TI bereit. Er schützt das lokale Netzwerk des Leistungserbringers oder Kostenträgers und die dort installierten Clientsysteme vor Angriffen aus der TI und umgekehrt, die TI vor Angriffen aus dem lokalen Netzwerk des Leistungserbringers oder Kostenträgers.

Für die Nutzung ~~der Bestandsnetzanbindung~~ von angeschlossenen Netzen des Gesundheitswesens mit aAdG-NetG und die Weiternutzung vorhandener Internetzugänge ermöglicht der Konnektor die Auflösung von FQDN aus den entsprechenden Namensräumen und die Weiterleitung von IP-Paketen an die jeweiligen Adressräume. Der Konnektor ermöglicht zusätzlich die Nutzung eines sicheren Internetzugangs über einen getrennten VPN-Kanal.

5.3.9.1 Konfigurationsmodell des Konnektors

Entsprechend (LH-BasisTI-A_1982) und (LH-BasisTI-A_1983) muss der Konnektor ein Konfigurationsmodell unterstützen, um unterschiedliche durch die gematik definierte Funktionsumfänge auf der gleichen Hard- und Firmwarebasis zu unterstützen. Durch Konfigurationsänderungen am Konnektor muss ein Wechsel zwischen den definierten Funktionsumfängen möglich sein.

Durch die definierten Funktionsumfänge soll einerseits das Standalone-Szenario mit einer physischen Trennung durch 2 Konnektoren unterstützt werden, andererseits die QES getrennt aktivierbar gemacht werden.

Hierzu müssen Konnektoren ohne spezielle Konfiguration den Basisfunktionsumfang unterstützen um als primärsystemseitige Sicherheitskomponente im Standalone-Szenario mit physischer Trennung eingesetzt werden zu können. Im Basisfunktionsumfang muss eine Online-Verbindung in die TI unterbunden werden, weiterhin darf keine QES unterstützt werden. Alle anderen Dienste der TI-Plattform werden unterstützt, sind ggf. aber durch die fehlende Online-Anbindung eingeschränkt.

⌦ **TIP1-A_2459 Basisfunktionsumfang Konnektor (LU_Offline)**

ENTWURF

Der Konnektor MUSS ohne spezielle Konfiguration den Basisfunktionsumfang besitzen (LU_Offline). Hierbei sind keine Online-Verbindungen in die TI möglich und der Basisdienst Erstellung_Prüfung_QES darf nicht unterstützt werden.⌫

Durch zwei unabhängig von einander zu betrachtende Konnektorkonfigurationen LU_Online und LU_SAK kann die Online-Anbindung an die TI und die QES konfiguriert und der Basisfunktionsumfang des Konnektors erweitert werden. Insgesamt werden durch den Basisfunktionsumfang des Konnektors und die zwei unabhängigen Konfigurationen vier Funktionsumfänge des Konnektors unterstützt.

1. LU_Offline
2. LU_Offline + LU_Online
3. LU_Offline + LU_SAK
4. LU_Offline + LU_Online + LU_SAK

⌦ **TIP1-A_2460 Konnektorkonfiguration LU_Online und LU_SAK**

Der Konnektor MUSS zwei unabhängig voneinander zu betrachtende Konnektorkonfigurationen LU_Online und LU_SAK unterstützen. Bei Durchführung der Konfiguration LU_Online werden Online-Verbindungen des Konnektors in die zentrale TI-Plattform unterstützt. Bei Durchführung der Konfiguration LU_SAK wird der Basisdienst Erstellung_Prüfung_QES unterstützt.⌫

Hinweis: Falls die Konfiguration LU_SAK ohne die Konfiguration LU_Online vorhanden ist, wird der Basisdienst Erstellung_Prüfung_QES lediglich im Offline-Modus unterstützt, d. h. analog zu dem Fall einer fehlenden bzw. gestörten Online-Verbindung.

5.3.9.2 Anforderungen an den Konnektor

⌦ **TIP1-A_2234 Produkttyp Konnektor, Schnittstellen und Prozesse**

Der Produkttyp Konnektor MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 20: Schnittstellen und Prozesse des Produkttyps Konnektor

Konnektor		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_Cert_Verification	Clientsystem, Fachmodul	
I_IP_Transport	Clientsystem, Fachmodul	
I_Crypt_Operations	Clientsystem, Fachmodul	
I_Symm_Crypt_Operations	Fachmodul	
I_DNS_Name_Information	Fachmodul	
I_DNS_Name_Resolution	Clientsystem	
I_DNS_Service_Information	Fachmodul	
I_Facade_Access_Configuration	Admin einer Organisation des Gesundheitswesens	
I_Facade_PrivAccess_Configuration	Admin einer Organisation des Gesundheitswesens	
I_KSRC_Local_Management	Admin einer Organisation des Gesundheitswesens	

ENTWURF

I_KSRC_Management	Admin einer Organisation des Gesundheitswesens	
I_KSRC_FM_Support	Fachmodul	
I_KV_Card_Handling	Clientsystem, Fachmodul	
I_KV_Card_Operations	Fachmodul	Bei langlaufenden Operationen muss kontinuierlich über den Fortgang der Operation informiert werden.
I_Notification_From_FM	Fachmodul	
I_NTP_Time_Information	Clientsystem, eHealth-Kartenterminal	
I_Poll_System_Information	Clientsystem, Fachmodul	
I_Reg_Notification	Clientsystem, Fachmodul	
I_SAK_Operations	Clientsystem, Fachmodul	
I_Sign_Operations	Clientsystem, Fachmodul	
I_Synchronised_System_Time	Fachmodul	
I_KV_Card_Unlocking	Clientsystem, Fachmodul	
I_KT_Operations	Fachmodul	
I_KTV_Management	Admin einer Organisation des Gesundheitswesens	
I_Change_System_Time	Admin einer Organisation des Gesundheitswesens	Ist nur im Offline-Fall zu verwenden.
I_KV_Card_Reservation	Fachmodul,	
I_Notification	eHealth-Kartenterminal	
I_Directory_Query	Clientsystem, Fachmodul	
I_Role_Information	Fachmodul	
I_Local_Storage	Fachmodul	
I_IDP_Auth_Active_Client	Clientsystem	
I_IDP_Auth_Passive_Client	Clientsystem	
I_Local_IDP_Service	Lokaler IDP	
Benötigte Schnittstellen		
I_Smartcard_Operations [1)], I_KVK_Read [1)], I_HSM_Operations (optional) [2)], I_Notification, I_Poll_System_Information, I_OCSP_Status_Information, I_DNS_Name_Resolution, I_NTP_Time_Information, I_KSR_Update, I_KSRS_Download. I_KT_Communication, I_DNS_Service_Localization, I_Secure_Channel_Tunnel, I_TLS, I_TSL_Download, I_BNetzA_VL_Download, I_Secure_Internet_Tunnel, I_CRL_Download, I_Registration_Service, I_KSRS_Net_Config, I_Directory_Query [1)] Aufgrund des bestehenden Bestandsschutzes erfolgt in diesem Dokument keine weitere Beschreibung dieser Schnittstelle [2)] Optional benötigte Schnittstelle, da die Unterstützung eines HSM-B durch den Konnektor optional ist		
Fachliche Prozesse	**Nutzer**	**Bedingungen**

⌫

⌦ **TIP1-A_2512 Produkttyp Konnektor, Erreichbarkeit von Fachmodulen**

Der Produkttyp Konnektor MUSS die dafür vorgesehenen Interfaces der Fachmodule für Clientsysteme erreichbar machen.⌫

⌦ **TIP1-A_2513 Produkttyp Konnektor, nur zugelassene Fachmodule**

Der Produkttyp Konnektor MUSS sicherstellen, dass nur zugelassene Fachmodule in ihn eingebracht werden können. Ein sicheres Nachladen der SAK und von Fachmodulen MUSS möglich sein.⌫

⌦ **TIP1-A_2514 Produkttyp Konnektor, Schreibschutz KVK**

Der Produkttyp Konnektor DARF NICHT schreibend auf eine KVK zugreifen.⌫

⌦ **TIP1-A_2515 Produkttyp Konnektor, Bedarfsgerechtigkeit**

Der Produkttyp Konnektor MUSS Bedarfe von 1-Personen-Praxen bis hin zu einem großen Krankenhaus, der höchsten Versorgungsstufe, Universitätskliniken und zentralisierten IT-Strukturen der Krankenhäuser berücksichtigen.⌫

⌦ **TIP1-A_6716 Produkttyp Konnektor, Verwaltung einer eigenen Zone**

Der Produkttyp Konnektor MUSS einen Nameserver implementieren, der die Zone "konlan." autoritativ verwaltet. Der Produkttyp Konnektor MUSS es Clientsystemen ermöglichen, die LAN-seitige IP-Adresse des Konnektors durch Abfrage des fest vorgegebenen FQDN "konnektor.konlan" aufzulösen.⌫

⌦ **TIP1-A_2516 Produkttyp Konnektor, VPN-Verbindung nur bei LU_Online**

Der Produkttyp Konnektor DARF NICHT eine VPN-Verbindung über die Schnittstelle I_Secure_Channel_Tunnel oder I_Secure_Internet_Tunnel aufbauen, wenn LU_Online nicht konfiguriert wurde.⌫

⌦ **TIP1-A_2517 Produkttyp Konnektor, Benachrichtigungsschnittstelle**

Der Produkttyp Konnektor SOLL bei der Benachrichtigung von Clientsystemen Notification WebServices verwenden und dabei das WS-I-Basic-Profile und einen der Standards WS-Notification oder WS-Eventing einsetzen.⌫

Hinweis: Die Entscheidung zur Umsetzung von TIP1-A_2517 wird auf der Ebene der Spezifikation des Produkttyps Konnektor getroffen.

⌦ **TIP1-A_2518 Produkttyp Konnektor, OCSP über http-Forwarder**

Der Produkttyp Konnektor MUSS alle OCSP-Requests über den http-Forwarder des VPN-Zugangsdienstes an die entsprechenden OCSP-Responder senden.⌫

⌦ **TIP1-A_2551 Konnektor, Sicherheitsziele aus Schutzprofilen**

Der Produkttyp Konnektor MUSS konform zu den bisherigen Sicherheitszielen aus den Schutzprofilen des BSI und den für den Konnektor verbindlichen technischen Richtlinien des BSI aufgebaut sein. ⌫

⌦ **TIP1-A_2398 Produkttyp Konnektor, Signaturproxy für die Anzeige auf Arbeitsplatzrechner**

Der Produkttyp Konnektor MUSS einen Signaturproxy bereitstellen, der die Inhalte einer qualifizierten Signatur auf dem Arbeitsplatzrechner des Leistungserbringers anzeigen kann. ⌫

⌦ **TIP1-A_6789 Produkttyp Konnektor, Schnittstellen des Signaturproxys**

ENTWURF

Der Produkttyp Konnektor MUSS einen Signaturproxy bereitstellen, der Clientsystemen die Schnittstelle I_SAK_Operations anbietet. Für die funktionale Leistung jenseits der Anzeige von Inhalten nutzt der Signaturproxy die Schnittstelle I_SAK_Operations des Konnektors nach. ⌫

⌦ **TIP1-A_6790 Produkttyp Konnektor, Aufgaben des Signaturproxys**

Der Produkttyp Konnektor MUSS einen Signaturproxy bereitstellen, der dem Leistungserbringer bei Erstellung und Prüfung einer qualifizierten Signatur den Inhalt der Dokumente, Ereignisse während der Verarbeitung und Prüfergebnisse anzeigen kann und dem Leistungserbringer die Möglichkeit der Bestätigung für die Erstellung der qualifizierten Signatur bietet. ⌫

⌦ **TIP1-A_6077 Produkttyp Konnektor, Veröffentlichung get_Metadata**

Der Produkttyp Konnektor MUSS in der Zone "konlan." den Endpunkt der Operation I_IDP_Auth_Active_Client::get_Metadata veröffentlichen.⌫

⌦ **TIP1-A_6670 Produkttyp Konnektor, informieren über vorhandene Updates**

Der Produkttyp Konnektor MUSS Clientsysteme über das Vorhandensein von Software-Updates des Konnektors informieren und dabei die Kritikalität, den Zeitpunkt bis zu dem das Update durchgeführt sein muss und den alternativen Download-Punkt des Updates im Internet mitteilen.⌫

⌦ **TIP1-A_6671 Produkttyp Konnektor, Verhalten, wenn kritische Updates nicht durchgeführt wurden**

Der Produkttyp Konnektor MUSS den Zugang zur TI sperren, wenn ein kritisches Software-Update nicht bis zum geforderten Zeitpunkt durchgeführt wurde. Die Sperrung erfolgt dadurch, dass ab diesem Zeitpunkt keine VPN-Verbindung mehr zum VPN-Zugangsdienst aufgebaut wird. ⌫

⌦ **TIP1-A_6672 Produkttyp Konnektor, Benachrichtigung über zeitweilige Sperrung des Zugangs zur TI**

Der Produkttyp Konnektor MUSS Clientsysteme über die Sperrung des Zugangs zur TI aufgrund eines nicht durchgeführten Software-Updates aussagekräftig informieren.⌫

⌦ **TIP1-A_6722 Produkttyp Konnektor, nur neue Vertrauensliste der BNetzA beziehen**

Der Produkttyp Konnektor MUSS per Hash prüfen, ob die in der TI-Plattform bereitgestellte Vertrauensliste der BNetzA aktueller ist als die bereits gespeicherte und nur in diesem Fall die Vertrauensliste aktualisieren.⌫

5.4 Produkttypen der Zone TI-Plattform zentral

Produkttypen der zentralen Zone der TI-Plattform bilden alle Anteile des Building Blocks „zentrale Dienste der TI-Plattform“ der Zone „TI-Plattform – zentral“ vollständig ab.

ENTWURF

5.4.1 Produkttyp Zentrales Netz TI (Zentrales Netz)

Das Zentrale Netz TI ermöglicht den Transport von IP-Daten zwischen den angeschlossenen Nutzern der TI. Dies beinhaltet die Infrastruktur zur Kontrolle des Zugangs zum Zentralen Netz der TI und die eigentliche zentrale Transportplattform.

Um das Zentrale Netz der TI vor Angriffen aus den angeschlossenen Fachdiensten sowie aus angeschlossenen ~~Fremdnetzen~~ weiteren Anwendungen oder sicheren Übermittlungsverfahren und umgekehrt, die Fachdienste vor Angriffen aus dem Zentralen Netzwerk der TI, zu schützen, wird an jedem Übergangspunkt eine Stateful Inspection Firewall eingesetzt. Diese ermöglicht ausschließlich die fachlich erforderliche Kommunikation in den zulässigen Kommunikationsrichtungen. D. h. Dienste der TI-Plattform-Zone zentral dürfen nur mit Diensten innerhalb dieser Zone Verbindungen aufbauen und fachanwendungsspezifische Dienste dürfen nur Verbindungen zu anderen fachanwendungsspezifischen Diensten sowie zu zentralen Diensten der TI-Plattform aufbauen. Weitere Anwendungen des Gesundheitswesens in der Provider Zone (aAdG bzw. aAdG-NetG-TI) dürfen nur mit anderen aAdG bzw. aAdG-NetG-TI kommunizieren. Ein Verbindungsaufbau in die TI aus ~~Fremdnetzen~~ Netzen des Gesundheitswesens mit Anwendungen des Gesundheitswesens ohne Zugriff auf zentrale Dienste (aAdG-NetG) wird verhindert. Nur Clientsysteme aus der Consumer Zone dürfen auf ~~Fremdnetze~~ aAdG-NetG zugreifen.

⌦ **TIP1-A_2235 Produkttyp Zentrales Netz-TI, Schnittstellen und Prozesse**

Der Produkttyp Zentrales Netz-TI MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 21: Schnittstellen und Prozesse des Produkttyps Zentrales Netz TI

Zentrales Netz TI		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_IP Transport	FA_spez_Dienst, Zeitdienst, Namensdienst, TSL-Dienst, Konfigurationsdienst, VPN-Zugangsdienst, Trust Service Provider X.509 nonQES, Trust Service Provider X.509 QES, Störungsampel, Verzeichnisdienst, Sicherheitsgateway Bestandsnetze, OCSP-Responder Proxy, gematik Root-CA, aAdG, aAdG-NetG-TI, SÜV	
Benötigte Schnittstellen		
Fachliche Prozesse	**Nutzer**	**Bedingungen**

⌫

⌦ **TIP1-A_2519 Produkttyp Zentrales Netz-TI, nur zugelassene Fachdienste anbinden**

ENTWURF

Der Produkttyp Zentrales Netz-TI MUSS sicherstellen, dass nur zugelassene Fachdienste an die zentrale TI-Plattform angebunden werden können.⌫

5.4.2 Produkttyp Zeitdienst

Auf Basis von NTP-Servern wird die gesetzliche Zeit den NTP-Clients der Dienste und Komponenten der TI zur Verfügung gestellt. Der Zeitdienst dient dabei als Zeitquelle für die TI, mit der sich andere NTP-Server und NTP-Clients synchronisieren.

⌦ **TIP1-A_2236 Produkttyp Zeitdienst, Schnittstellen und Prozesse**

Der Produkttyp Zeitdienst MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 22: Schnittstellen und Prozesse des Produkttyps Zeitdienst

Zeitdienst		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_NTP_Time_Information	FA_spez_Dienst, Namensdienst, TSL-Dienst, Konfigurationsdienst, VPN-Zugangsdienst, Trust Service Provider, aAdG, aAdG-NetG-TI, SÜV	
Benötigte Schnittstellen		
I_DNS_Name_Resolution, I_IP Transport		
Fachliche Prozesse	**Bedingungen**	

⌫

⌦ **TIP1-A_2520 Produkttyp Zeitdienst, maximale Abweichung zur gesetzlichen Zeit**

Der Produkttyp Zeitdienst MUSS gewährleisten, dass die Abweichung der bereitgestellten Zeitinformation von der gesetzlichen Zeit nicht mehr als 1 Sekunde beträgt.⌫

⌦ **TIP1-A_2521 Produkttyp Zeitdienst, Ausfallsicherheit**

Der Produkttyp Zeitdienst MUSS gewährleisten, dass der Ausfall oder die Fehlfunktion (z. B. False Ticker und False Speaker) von einzelnen seiner Komponenten erkannt und kompensiert werden.⌫

5.4.3 Produkttyp Namensdienst

Zur Auflösung von Fully Qualified Domain Names (FQDN) in IP-Adressen wird in der TI das Domain Name System (DNS) verwendet. Das Wurzelverzeichnis (DNS-Root) der TI wird über den Namensdienst bereitgestellt.

Der Betrieb und die Verwaltung des Namensraumes der TI erfolgt durch den Betreiber dieses Produkttyps. Der Betrieb und die Verwaltung von definierten Teilen des Namensraumes (Subdomains) kann an andere Dienstbetreiber delegiert werden (DNS-Zone-Delegation).

ENTWURF

Weiterhin wird der Namensdienst zur Lokalisierung von Diensten (DNS-Service Discovery) genutzt.

⌧ **TIP1-A_2237 Produkttyp Namensdienst, Schnittstellen und Prozesse**

Der Produkttyp Namensdienst MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 23: Schnittstellen und Prozesse des Produkttyps Namensdienst

Namensdienst		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_DNS_Name_Resolution	FA_spez_Dienst, Zentrales Netz TI, Zeitdienst, TSL-Dienst, Konfigurationsdienst, VPN-Zugangsdienst, Trust Service Provider, Konnektor, Trust Service Provider X.509 nonQES, Trust Service Provider X.509 QES, Verzeichnisdienst, Sicherheitsgateway Bestandsnetze, OCSP-Responder Proxy, gematik Root-CA, aAdG, aAdG-NetG-TI, SÜV	
I_DNS_Service_Localization	Konnektor	
Benötigte Schnittstellen		
I_NTP_Time_Information, I_IP Transport		
Fachliche Prozesse	**Nutzer**	**Bedingungen**
P_DNS_Name_Entry_Announcement	FA_spez_Dienst, Zentrales Netz TI, Zeitdienst, TSL-Dienst, Konfigurationsdienst, VPN-Zugangsdienst, Trust Service Provider, aAdG, aAdG-NetG-TI, SÜV	inklusive Änderung und Deregistrierung
P_DNSSEC_Key_Distribution	FA_spez_Dienst, VPN-Zugangsdienst, Zeitdienst, TSL-Dienst, Konfigurationsdienst, Trust Service Provider	
P_DNS_Service_Entry_Announcement	FA_spez_Dienst, VPN-Zugangsdienst, Zeitdienst, TSL-Dienst, Konfigurationsdienst, Trust Service Provider, aAdG, aAdG-NetG-TI, SÜV	inklusive Änderung und Deregistrierung
P_DNS_Zone_Delegation	FA_spez_Dienst, VPN-Zugangsdienst, Zeitdienst, TSL-Dienst, Konfigurationsdienst,	

ENTWURF

	Trust Service Provider	

Eine Instanz dieses Produkttyps existiert daher genau ein Mal in der TI. ⌫

5.4.4 Produkttyp Verzeichnisdienst

⌦ **TIP1-A_5774 Produkttyp Verzeichnisdienst, Schnittstellen und Prozesse**

Der Produkttyp Verzeichnisdienst MUSS ~~alle Festlegungen gemäß Tabelle "Produkttyp Verzeichnisdienst" erfüllen~~ die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 24: Schnittstellen und Prozesse des Produkttyps Verzeichnisdienst

Verzeichnisdienst		
Beschreibung	Der Verzeichnisdienst beinhaltet alle serverseitigen Anteile des Basisdienstes Verzeichnis_Identitäten. Dazu zählen im Besonderen die Speicherung aller Einträge von Leistungserbringern und Organisationen/Institutionen mit allen definierten Attributen, die in das Verzeichnis aufgenommen werden sollen. Anhand einer Suchanfrage können Konnektor und fachanwendungsspezifische Dienste Daten abfragen (z. B. X.509 Zertifikate). Ferner können Einträge des Verzeichnisses durch berechtigte fachanwendungs spezifische Dienste geändert, hinzugefügt und gelöscht werden.	
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_Directory_Query	TIP, FA_spez_Dienst, aAdG, aAdG-NetG-TI, SÜV	
I_~~Directory~~Data_Maintenance	~~FA_spez_Dienst~~ Inhaber des Eintrages	~~Die Schnittstelle wird über TLS mit beidseitiger Authentifizierung bereitgestellt~~ Die Schnittstelle MUSS als Anwendung zur Nutzung in der Consumer Zone angeboten werden. Zusätzlich MUSS sie in einer direkt durch das Clientsystem nutzbaren Variante realisiert sein.
I_Directory_Application_Maintenance	FA_spez_Dienst	Die Schnittstelle wird über TLS mit beidseitiger Authentifizierung bereitgestellt
Benötigte Schnittstellen		
I_NTP_Time_Information, I_DNS_Name_Resolution, I_IP Transport, I_OCSP_Status_Information, alle für die Schnittstelle I_Data_Maintenance benötigten Schnittstellen des Produkttyps Konnektor.		
Fachliche Prozesse	**Nutzer**	**Bedingungen**
P_~~Directory~~Data_Maintenance	Inhaber des Eintrages	
P_Directory_Application_Registration	FA_spez_Dienst	

⌫

⌦ **TIP1-A_5775 Produkttyp Verzeichnisdienst, Datenmodell Verzeichnisdienst**

Der Produkttyp Verzeichnisdienst MUSS ein Datenmodell mit folgenden logischen Elementen definieren:

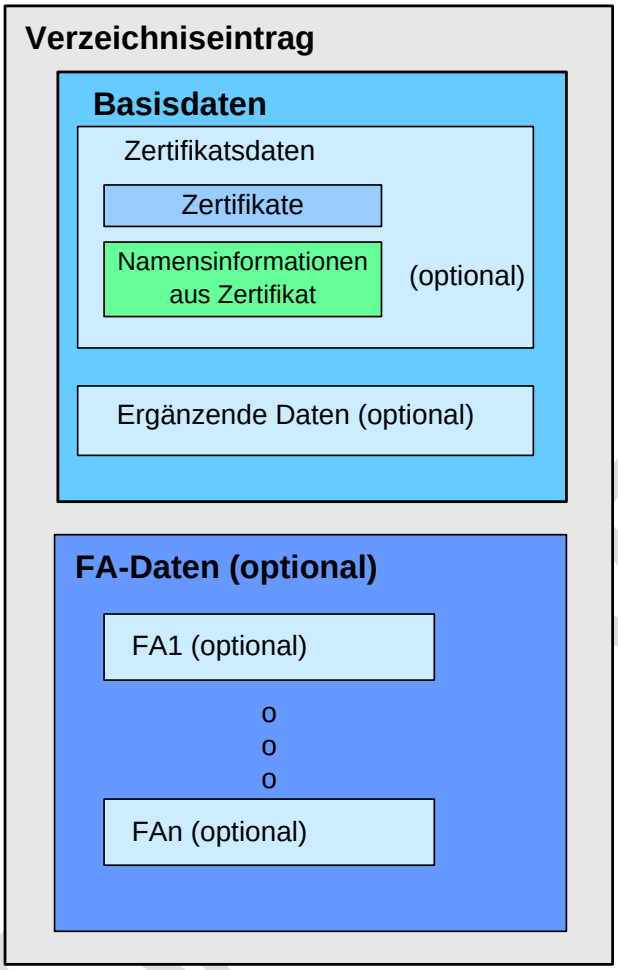


Abbildung 11: Datenmodell Verzeichnisdienst

Basisdaten: Die Basisdaten enthalten vom Inhaber des Eintrages bereitgestellte Verzeichnisdaten.

Zertifikatsdaten: Die Zertifikatsdaten enthalten die Zertifikate und aus Zertifikaten entnommenen Daten.

- **Zertifikate**: Im Verzeichnisdienst hinterlegte Zertifikate.
- **Namensinformationen**: Diese optionalen Daten werden – auf Wunsch des Inhabers des Eintrages – aus dem Zertifikat entnommen und in diesen Attributen des Verzeichniseintrags gespeichert.

Ergänzende Daten: Die optionalen Daten enthalten Angaben des Inhabers des Eintrages. Dies können z.B. eine Postadresse und ein Anzeigename sein.

FA-Daten: Enthält Daten von Fachanwendungen. Der Inhalt wird durch die jeweilige Fachanwendung definiert.⌧

⌦ **TIP1-A_5776 Produkttyp Verzeichnisdienst, Logische Datenunabhängigkeit von Fachanwendungsdaten**

Der Verzeichnisdienst MUSS sicherstellen, dass die Daten einer Fachanwendung unabhängig von den Daten aller anderen Fachanwendungen sind.⌫

⌦ **TIP1-A_5777 Produkttyp Verzeichnisdienst, Ordnungskriterium Datenmodell Verzeichnisdienst**

Der Produkttyp Verzeichnisdienst MUSS die Telematik-ID als Ordnungskriterium für das Datenmodell verwenden.⌫

⌦ **TIP1-A_5778 Produkttyp Verzeichnisdienst, Löschen Basiseintrag Verzeichnisdienst**

Der Produkttyp Verzeichnisdienst MUSS einen Eintrag komplett löschen sobald die Basisdaten dieses Eintrags gelöscht wurden.⌫

⌦ **TIP1-A_5779 Produkttyp Verzeichnisdienst, Datenpflege Verzeichnisdienst**

Der Produkttyp Verzeichnisdienst MUSS periodisch die Zertifikate in den Verzeichniseinträgen auf Ablauf des Gültigkeitszeitraums und Sperrstatus prüfen. Abgelaufene oder gesperrte Zertifikate MÜSSEN durch den Verzeichnisdienst gelöscht werden. Enthält ein Verzeichniseintrag kein gültiges Zertifikat mehr, MUSS der gesamte Verzeichniseintrag gelöscht werden. Die Löschung des gesamten Verzeichniseintrags KANN zeitlich versetzt erfolgen, um dem Nutzer die Chance der Aktualisierung des Eintrages vor dessen Löschung zu bieten.⌫

⌦ **TIP1-A_5780 Produkttyp Verzeichnisdienst, Verzeichnisdienstoperationen – Sichtbare und suchbare Daten**

Im Produkttyp Verzeichnisdienst MÜSSEN alle Basisdaten und fachanwendungsspezifischen Daten sicht- und suchbar sein. Die Telematik-ID DARF am Interface I_Directory_Query NICHT sicht- oder suchbar sein.⌫

⌦ **TIP1-A_7287 Produkttyp Verzeichnisdienst, Komponente Administration Basisdaten**

Der Produkttyp Verzeichnisdienst MUSS eine Komponente Administration Basisdaten in der Provider Zone realisieren, die die Schnittstelle I_Data_Maintenance bereitstellt.⌫

⌦ **TIP1-A_7288 Produkttyp Verzeichnisdienst, Zonenübergreifende Kommunikation**

Der Produkttyp Verzeichnisdienst MUSS die zonenübergreifende Kommunikation entsprechend des Schutzbedarfs der Daten absichern.⌫

⌦ **TIP1-A_7289 Produkttyp Verzeichnisdienst, Zonenübergreifende Kommunikation**

Der Produkttyp Verzeichnisdienst MUSS für die Schnittstelle I_Data_Maintenance die Leistungen des Produkttyps Konnektor nachnutzen.⌫

5.4.5 Produkttyp TSL-Dienst

Durch den TSL-Dienst wird der zentrale Vertrauensraum der X.509-PKI der TI bereitgestellt. Er stellt zusätzlich die Vertrauensliste der BNetzA in der TI bereit.

ENTWURF

⌦ **TIP1-A_2238 Produkttyp TSL-Dienst, Schnittstellen und Prozesse**

Der Produkttyp TSL-Dienst MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 25: Schnittstellen und Prozesse des Produkttyps TSL-Dienst

TSL-Dienst		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_OCSP_Status_Information	FA_spez_Dienst, Konnektor, VPN-Zugangsdienst, Zeitdienst, Namensdienst, Konfigurationsdienst, Trust Service Provider X.509 nonQES, Trust Service Provider X.509 QES, Verzeichnisdienst, Sicherheitsgateway Bestandsnetze, OCSP-Responder Proxy, gematik Root-CA, aAdG, aAdG-NetG-TI, SÜV	
I_TSL_Download	FA_spez_Dienst, Konnektor, VPN-Zugangsdienst, Zeitdienst, Namensdienst, Konfigurationsdienst, Trust Service Provider X.509 nonQES, Trust Service Provider X.509 QES, Verzeichnisdienst, Sicherheitsgateway Bestandsnetze, OCSP-Responder Proxy, gematik Root-CA, aAdG, aAdG-NetG-TI, SÜV	
I_BNetzA_VL_Download	Konnektor	
Benötigte Schnittstellen		
I_NTP_Time_Information, I_DNS_Name_Resolution, I_IP Transport, P_Sub_CA_Certification_X.509		
Fachliche Prozesse	**Nutzer**	**Bedingungen**
P_Trust_Approval	Trust Service Provider X.509 nonQES, Trust Service Provider X.509 QES	

⌫

⌦ **TIP1-A_2524 Produkttyp TSL-Dienst, Bereitstellung im Internet**

Der Produkttyp TSL-Dienst MUSS die TSL als zentralen Vertrauensraum auch im Internet zum Download bereitstellen.⌫

⌦ **TIP1-A_2525 Produkttyp TSL-Dienst, Bereitstellung TSL-Signer-CA-Zertifikat**

Der Produkttyp TSL-Dienst MUSS in Verbindung mit der TSL auch das TSL-Signer-CA-Zertifikat inklusive Prüfinformationen (z. B. Fingerprint) bereitstellen.⌫

⌦ **TIP1-A_5450 Produkttyp TSL-Dienst, Bereitstellung Komponenten-CA-Zertifikat**

Der Produkttyp TSL-Dienst MUSS in Verbindung mit der TSL auch das Komponenten-CA-Zertifikat inklusive Prüfinformationen (z. B. Fingerprint) bereitstellen.⌫

⌦ **TIP1-A_6723 Produkttyp TSL-Dienst, Vertrauensliste der BNetzA beziehen**

Der Produkttyp TSL-Dienst MUSS die aktuelle Vertrauensliste der BNetzA und den dafür bereitgestellten Hash-Wert aus dem Internet laden und in der TI bereitstellen.⌫

⌦ **TIP1-A_6773 Produkttyp TSL-Dienst, BNetzA-VL und deren Hash gesichert beziehen**

Der Produkttyp TSL-Dienst DARF die aktuelle Vertrauensliste der BNetzA und den dafür bereitgestellten Hash-Wert NICHT ohne TLS-Sicherung aus dem Internet laden.⌫

⌦ **TIP1-A_6734 Produkttyp TSL-Dienst, nur neue Vertrauensliste der BNetzA beziehen**

Der Produkttyp TSL-Dienst MUSS per Hash prüfen, ob die im Internet bereitgestellte Vertrauensliste der BNetzA aktueller ist als die bereits gespeicherte und nur in diesem Fall die Vertrauensliste aktualisieren.⌫

⌦ **TIP1-A_5277 OCSP-Responder für HBA-Vorläuferkarten in der TSL**

Die gematik MUSS in die TSL URIs für OCSP-Responder der Zertifikate von unterstützten HBA-Vorläuferkarten aufnehmen.⌫

5.4.6 Produkttyp Konfigurationsdienst (Konfigdienst)

Der Konfigurationsdienst stellt für die Produkttypen Konnektor und eHealth-Kartenterminal Konfigurationsdaten und Softwareupdates bereit. Der Produkttyp MobKT wird nicht durch den Konfigurationsdienst unterstützt.

⌦ **TIP1-A_2239 Produkttyp Konfigurationsdienst, Schnittstellen und Prozesse**

Der Produkttyp Konfigurationsdienst MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 26: Schnittstellen und Prozesse des Produkttyps Konfigurationsdienst

Konfigurationsdienst		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_KSRS_Download	Konnektor	
I_KSRS_Net_Config	Konnektor	
Benötigte Schnittstellen		
I_NTP_Time_Information, I_DNS_Name_Resolution, I_IP Transport		
Fachliche Prozesse	**Nutzer**	**Bedingungen**
P_KSRS_Maintenance	Admin Zentraler Dienst	

ENTWURF

⌫

⌦ **TIP1-A_2527 Produkttyp Konfigurationsdienst, Erhebung statistischer Daten**

Der Produkttyp Konfigurationsdienst MUSS zu jedem erfolgten Download die neue Versionsnummer des Produkts und bei Anfragen für vorhandene Softwarepakete die aktuelle Versionsnummer des angefragten Produkts zur statistischen Auswertung speichern. Diese statistischen Daten MÜSSEN dem Gesamt~~betriebs~~verantwortlichen der TI zyklisch bereitgestellt werden.⌫

⌦ **TIP1-A_6673 Produkttyp Konfigurationsdienst, erweiterte Informationen zu Softwarepaketen des Konnektors**

Der Produkttyp Konfigurationsdienst MUSS mit jedem Softwarepaket für einen Konnektor die folgenden Informationen bereitstellen:

- Kritikalität des Updates,
- Zeitpunkt bis zu dem das Update durchgeführt werden muss und
- alternativen Download-Punkt für das Update im Internet. ⌫

5.4.7 Produkttyp VPN-Zugangsdienst (Zugangsdienst)

Der VPN-Zugangsdienst ermöglicht den Konnektoren einen IPsec-Tunnel über ein Transportnetz zum VPN-Zugangsdienst aufzubauen und verbindet darüber die Organisationen des Gesundheitswesens mit dem zentralen Netz der TI.

Zusätzlich ermöglicht der VPN-Zugangsdienst den Konnektoren den Aufbau eines separaten IPSec-Tunnels über das Transportnetz, durch den der sichere Internetzugang erreichbar ist.

⌦ **TIP1-A_2240 Produkttyp VPN-Zugangsdienst, Schnittstellen und Prozesse**

Der Produkttyp VPN-Zugangsdienst MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 27: Schnittstellen und Prozesse des Produkttyps VPN-Zugangsdienst

VPN-Zugangsdienst		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_Secure_Channel_Tunnel	Konnektor	
I_DNS_Name_Resolution	Konnektor	Zur Auflösung von FQDN des VPN-Zugangsdienstes und des CRL-Downloads des TSP-X.509nonQES (Namensraum Transportnetz)
I_NTP_Time_Information	Konnektor	
I_DNS_Name_Resolution	Konnektor	Zur Auflösung von FQDN des Namensraums TI
I_Secure_Internet_Tunnel	Konnektor	
I_DNS_Name_Resolution	Konnektor	Zur Auflösung von FQDN des Namensraumes Internet.
I_Registration_Service	Konnektor	Diese Schnittstelle muss im Internet angeboten werden.
Benötigte Schnittstellen		
I_Secure_Access_Bestandsnetz (nur wenn Produkttyp Sicherheitsgateway Bestandsnetze genutzt wird), I_NTP_Time_Information, I_DNS_Name_Resolution, I_IP Transport		
Fachliche Prozesse	**Nutzer**	**Bedingungen**

⌫

ENTWURF

⌦ **TIP1-A_2528 Produkttyp VPN-Zugangsdienst, Sicherung ggü. dem Transportnetz**

Der Produkttyp VPN-Zugangsdienst MUSS Richtung Transportnetz durch einen Paketfilter gesichert werden.⌫

⌦ **TIP1-A_2531 Produkttyp VPN-Zugangsdienst, http-Forwarder für OCSP-Requests**

Der Produkttyp VPN-Zugangsdienst MUSS einen http-Forwarder bereitstellen, über den die OCSP-Requests der verbundenen Konnektoren an die entsprechenden OCSP-Responder weitergeleitet werden.⌫

⌦ **TIP1-A_3666 Produkttyp VPN-Zugangsdienst, Sicherung ggü. dem Internet**

Der Produkttyp VPN-Zugangsdienst MUSS Richtung Internet durch eine Stateful Inspection Firewall gesichert werden.⌫

⌦ **TIP1-A_3667 Produkttyp VPN-Zugangsdienst, Trennung von TI- und Internet-Datenverkehr**

Der Produkttyp VPN-Zugangsdienst MUSS eine informationstechnische Trennung des Datenverkehrs des sicheren Internetzugangs gegenüber dem Datenverkehr in das zentrale Netz durchsetzen.⌫

⌦ **TIP1-A_3668 Produkttyp VPN-Zugangsdienst, kein Datenverkehr zwischen zentralem Netz und Internet**

Der Produkttyp VPN-Zugangsdienst MUSS verhindern, dass Datenverkehr des sicheren Internetzugangs in das zentrale Netz oder Datenverkehr der TI in das Internet gelangt. ⌫

⌦ **TIP1-A_3669 Produkttyp VPN-Zugangsdienst, Absicherung über SIS**

Der Produkttyp VPN-Zugangsdienst MUSS den Datenverkehr des sicheren Internetzugangs über einen Secure Internet Service (SIS) absichern.⌫

⌦ **TIP1-A_3670 Produkttyp VPN-Zugangsdienst, 3-stufige Lösung für SIS**

Der SIS des Produkttyps VPN-Zugangsdienst MUSS eine Paketfilter-Application-Level-Gateway-Paketfilter-Struktur (P-A-P) entsprechend den Vorgaben des BSI zur Konzeption von Sicherheitsgateways [BSI-SiGw] umsetzen.⌫

⌦ **TIP1-A_3671 Produkttyp VPN-Zugangsdienst, Schutz vor Schadsoftware durch SIS**

Der SIS des Produkttyps VPN-Zugangsdienst MUSS Maßnahmen zum Schutz vor Schadsoftware umsetzen.⌫

⌦ **TIP1-A_3672 Produkttyp VPN-Zugangsdienst, Application Level Proxy durch SIS**

Der SIS des Produkttyps VPN-Zugangsdienst MUSS Application Level Proxies für gängige Standardprotokolle bereitstellen.⌫

⌦ **TIP1-A_3673 Produkttyp VPN-Zugangsdienst, Paketfilter durch SIS**

Der SIS des Produkttyps VPN-Zugangsdienst MUSS Paketfilter mit Stateful-Inspection-Funktion bereitstellen.⌫

ENTWURF

⌦ **TIP1-A_3674 Produkttyp VPN-Zugangsdienst, Contentfilter durch SIS**

Der SIS des Produkttyps VPN-Zugangsdienst MUSS Contentfilter für aktive Inhalte bereitstellen.⌫

⌦ **TIP1-A_3675 Produkttyp VPN-Zugangsdienst, URL-Filter durch SIS**

Der SIS des Produkttyps VPN-Zugangsdienst MUSS einen URL-Filter bereitstellen.⌫

5.4.8 Produkttyp Sicherheitsgateway Bestandsnetze (SG-BNet)

Der Produkttyp Sicherheitsgateway Bestandsnetze ermöglicht den Clientsystemen die Nutzung ~~Diensten in Bestandsnetzen~~ von anderen Anwendungen des Gesundheitswesens ohne Zugriff auf zentrale Dienste (aAdG-NetG) in angeschlossenen Netzen des Gesundheitswesens, wie dem sicheren Netz der KVen (SNK).

Jedes ~~Bestandsnetz~~ Netz des Gesundheitswesens mit aAdG-NetG wird über eine eigene Instanz des Produkttyps Sicherheitsgateway Bestandsnetze an die TI angebunden. D.h. für jedes ~~Bestandsnetz~~ Netz des Gesundheitswesens mit aAdG-NetG werden separate Verbindungsregeln verwaltet und es ist eine Rückwirkungsfreiheit zwischen den angebundenen ~~Bestandsnetz~~ Netzen des Gesundheitswesens mit aAdG-NetG gesichert. Ob dies durch physikalische oder virtuelle Instanzen erreicht wird, ist nicht festgelegt.

Um die TI vom SNK bzw. anderen ~~Bestandsnetz~~ Netzen des Gesundheitswesens mit aAdG-NetG abzuschotten, werden an diesen Netzübergängen Sicherheitsgateways eingesetzt werden.

⌦ **TIP1-A_2241 Produkttyp Sicherheitsgateway Bestandsnetze, Schnittstellen und Prozesse**

Der Produkttyp Sicherheitsgateway Bestandsnetze MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 28: Schnittstellen und Prozesse des Produkttyps Sicherheitsgateway Bestandsnetze

Sicherheitsgateway Bestandsnetze		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_Secure_Access_Bestandsnetz	Clientsystem	Zugriff erfolgt über den Konnektor und den VPN-Zugangsdienst
Benötigte Schnittstellen		
I_NTP_Time_Information, I_DNS_Name_Resolution, I_IP Transport		
Fachliche Prozesse	**Nutzer**	**Bedingungen**

⌫

⌦ **TIP1-A_2532 Produkttyp Sicherheitsgateway Bestandsnetze, Sicherung ggü. ~~dem Bestandsnetz~~ Netzen des Gesundheitswesens mit aAdG-NetG**

Der Produkttyp Sicherheitsgateway Bestandsnetze MUSS Richtung ~~Bestandsnetz~~ der angeschlossenern Netze des Gesundheitswesens mit aAdG-NetG durch Stateful Inspection Firewalls gesichert werden.⌫

⌦ **TIP1-A_2533 Produkttyp Sicherheitsgateway Bestandsnetze, kein Verbindungsaufbau aus ~~Bestandsnetzen~~ Netzen des Gesundheitswesens mit aAdG-NetG**

ENTWURF

Der Produkttyp Sicherheitsgateway Bestandsnetze MUSS den Verbindungsaufbau aus ~~Bestandsnetzen~~ angeschlossenen Netzen des Gesundheitswesens mit aAdG-NetG in Richtung TI verhindern.⌫

5.4.9 Produkttyp Trust Service Provider X.509 nonQES (TSP-X.509nonQES)

Der Trust Service Provider X.509 nonQES stellt X.509-nonQES-Zertifikate für berechtigte Personen (z. B. Zertifikate des HBA und der eGK), Organisationen und technische Komponenten aus und ermöglicht die Abfrage des Sperrstatus von durch ihn ausgestellten X.509-nonQES-Zertifikaten.

⌦ **TIP1-A_2242 Produkttyp Trust Service Provider X.509 nonQES, Schnittstellen und Prozesse**

Der Produkttyp Trust Service Provider X.509 nonQES MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 29: Schnittstellen und Prozesse des Produkttyps Trust Service Provider X.509 nonQES

Trust Service Provider X.509 nonQES		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_Cert_Provisioning	Hersteller, Betreiber_ZD, Betreiber_FD, aAdG, aAdG-NetG-TI, SÜV	
I_Cert_Revocation	Hersteller, Betreiber_ZD, Betreiber_FD, aAdG, aAdG-NetG-TI, SÜV	
I_OCSP_Status_Information	FA_spez_Dienst, Konnektor, VPN-Zugangsdienst, aAdG, aAdG-NetG-TI, SÜV	Für Zertifikate der Identitäten ID.HCI.OSIG, ID.HP.ENC, ID.HCI.ENC, ID.HP.AUT und ID.HCI.AUT muss diese Schnittstelle auch im Internet angeboten werden.
I_CRL_Download	Konnektor	Diese Schnittstelle muss nur durch Herausgeber der Identitäten ID.VPNK.VPN und ID.VPNK.VPN-SIS im Transportnetz bereitgestellt werden.
Benötigte Schnittstellen		
P_Sub_CA_Certification_X.509, I_NTP_Time_Information, I_DNS_Name_Resolution, I_IP Transport		
Fachliche Prozesse	**Nutzer**	**Bedingungen**
P_Cert_Provisioning	LE, Kartenherausgeber	
P_Cert_Revocation	LE, Kartenherausgeber	

⌫

5.4.10 Produkttyp Trust Service Provider X.509 QES (TSP-X.509QES)

Der Trust Service Provider X.509 QES stellt X.509-QES-Zertifikate für berechtigte Personen (z. B. Zertifikate des HBA und der eGK) aus und ermöglicht die Abfrage des Sperrstatus von durch ihn ausgestellten X.509-QES-Zertifikaten.

⌦ **TIP1-A_2552 Produkttyp Trust Service Provider X.509 QES, Schnittstellen und Prozesse**

Der Produkttyp Trust Service Provider X.509 QES MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 30: Schnittstellen und Prozesse des Produkttyps Trust Service Provider X.509 QES

Trust Service Provider X.509 QES		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_OCSP_Status_Information	FA_spez_Dienst, Konnektor, VPN-Zugangsdienst	Gemäß gesetzlichen Vorgaben muss die Statusauskunft auch im Internet bereitgestellt werden.
Benötigte Schnittstellen		
I_NTP_Time_Information, I_DNS_Name_Resolution, I_IP Transport		
Fachliche Prozesse	**Nutzer**	**Bedingungen**
P_Cert_Provisioning	LE	
P_Cert_Revocation	LE	

⌫

5.4.11 Produkttyp gematik Root-CA

Die gematik Root-CA stellt X.509-Sub-CA-Zertifikate (nur nonQES) für berechtigte TSPs aus. Die CA-Zertifikate für eGKs können auf eigenen PKI-Strukturen basieren oder sich auch von der gematik Root-CA ableiten.

⌦ **TIP1-A_2553 Produkttyp gematik Root-CA, Schnittstellen und Prozesse**

Der Produkttyp gematik Root-CA MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 18: Schnittstellen und Prozesse des Produkttyps gematik Root-CA

gematik Root-CA		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_OCSP_Status_Information		Die gematik Root-CA muss für ihr eigenes Zertifikat und für alle von ihr abgeleiteten CA-Zertifikate, welche HBA- und SMC-B-Zertifikate ausstellen, eine Statusauskunft über diese Schnittstelle im Internet bereitstellen.
Benötigte Schnittstellen		
Fachliche Prozesse	**Nutzer**	**Bedingungen**
P_Sub_CA_Certification_X.509	TSP-X.509nonQES	

⌫

5.4.12 Produkttyp Trust Service Provider CVC (TSP-CVC)

Der Trust Service Provider CVC betreibt eine von der gematik CVC-Root-CA abgeleitete CVC-Sub-CA (CA der zweiten Ebene) nach den Regularien der gematik und erstellt CV-Zertifikate mit den spezifizierten Rollenattributen für berechtigte Personen (HBA, eGK) und Organisationen/Institutionen (SM-B).

⌦ **TIP1-A_2243 Produkttyp Trust Service Provider CVC, Schnittstellen und Prozesse**

ENTWURF

Der Produkttyp Trust Service Provider CVC MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 31: Schnittstellen und Prozesse des Produkttyps Trust Service Provider CVC

Trust Service Provider CVC		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
Benötigte Schnittstellen		
P_Sub_CA_Certification_CVC		
Fachliche Prozesse	**Nutzer**	**Bedingungen**
P_CVC_Provisioning	Kartenherausgeber	

⌫

5.4.13 Produkttyp CVC-Root

Die CVC-Root ist die zentrale Root-CA der PKI für CV-Zertifikate in der TI.

⌦ **TIP1-A_2245 Produkttyp CVC-Root, Schnittstellen und Prozesse**

Der Produkttyp CVC-Root MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 32: Schnittstellen und Prozesse des Produkttyps CVC-Root

CVC-Root		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
Benötigte Schnittstellen		
Fachliche Prozesse	**Nutzer**	**Bedingungen**
P_Sub_CA_Certification_CVC	TSP CVC	

⌫

5.4.14 Produkttyp OCSP-Responder Proxy (OCSP-Proxy)

Der OCSP-Responder Proxy ermöglicht es Statusauskünfte für Zertifikate aus dem Vertrauensraum der TI, deren OCSP-Responder im Internet stehen, innerhalb der TI verfügbar zu machen. Dafür leitet er die entsprechenden Anfragen ins Internet weiter und liefert die zugehörige Statusauskunft zurück. Dies wird für die zeitlich begrenzt unterstützten HBA-Vorläuferkarten benötigt.

⌦ **TIP1-A_2246 Produkttyp OCSP-Responder Proxy, Schnittstellen und Prozesse**

Der Produkttyp OCSP-Responder Proxy MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 33: Schnittstellen und Prozesse des Produkttyps OCSP-Responder Proxy

OCSP-Responder Proxy		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_OCSP_Status_Information	Konnektor	Über diese Schnittstelle wird die Statusinformation für Zertifikate der unterstützten HBA-Vorläuferkarten in der TI-Plattform verfügbar gemacht.
Benötigte Schnittstellen		

ENTWURF

I_NTP_Time_Information, I_DNS_Name_Resolution, I_IP Transport		
Fachliche Prozesse	**Nutzer**	**Bedingungen**

⌫

⌦ **TIP1-A_2538 Produkttyp OCSP-Responder Proxy, sicherer Internetzugang**

Der Produkttyp OCSP-Responder Proxy MUSS über einen sicheren Internetzugang verfügen, beschränkt auf die Adressen der OCSP-Responder der unterstützten HBA-Vorläuferkarten.⌫

⌦ **TIP1-A_5278 Produkttyp OCSP-Responder Proxy, Bereitstellung Statusinformationen HBA-Vorläuferkarten**

Der Produkttyp OCSP-Responder Proxy MUSS die Statusinformation der Zertifikate der unterstützten HBA-Vorläuferkarten in der TI-Plattform bereitstellen.⌫

⌦ **TIP1-A_5279 Produkttyp OCSP-Responder Proxy, Statusinformationen HBA-Vorläuferkarten aus dem Internet beziehen**

Der Produkttyp OCSP-Responder Proxy MUSS den aktuellen Status für Zertifikate der unterstützten HBA-Vorläuferkarten über die entsprechenden OCSP-Responder im Internet ermitteln.⌫

5.4.15 Produkttyp Störungsampel

Die Störungsampel spiegelt zentral den Betriebsstatus der zentralen Dienste der TI-Plattform und der fachspezifischen Dienste wieder.

⌦ **TIP1-A_2247 Produkttyp Störungsampel, Schnittstellen und Prozesse**

Der Produkttyp Störungsampel MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 34: Schnittstellen und Prozesse des Produkttyps Störungsampel

Störungsampel		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_Monitoring_Update	Betreiber_ZD, Betreiber_FD, SÜV	
I_Monitoring_Read		Diese Schnittstelle MUSS im Internet für die nachfolgenden Nutzer angeboten werden. • Anbieter in ihrer Rolle als betriebsverantwortliche Instanz, • die Supportdienstleistenden, • die Servicebetriebsverantwortlichen der TI, • die gematik als gesamt~~betriebs~~verantwortliche Instanz der TI.
Benötigte Schnittstellen		
I_NTP_Time_Information, I_DNS_Name_Resolution, I_IP Transport		
Fachliche Prozesse	**Nutzer**	**Bedingungen**

⌫

⌦ **TIP1-A_2540 Produkttyp Störungsampel, Generierung Gesamtfunktionsstatus**

ENTWURF

Der Produkttyp Störungsampel MUSS konsolidiert Daten über den Funktionsstatus und die Performance der zentralen Produktinstanzen der TI erfassen und daraus eine Sicht auf den Gesamtfunktionsstatus der TI generieren.⌫

⌦ **TIP1-A_2541 Produkttyp Störungsampel, Detailsicht zentraler Produktinstanzen**

Der Produkttyp Störungsampel MUSS eine Detailsicht der TI-Services bereitstellen, die den Funktionsstatus der einzelnen zum Anwendungsservices / TI-Plattform-Service gehörenden zentralen Produktinstanzen visualisiert.⌫

⌦ **TIP1-A_2542 Produkttyp Störungsampel, Detailsicht Dienstinstanzen**

Der Produkttyp Störungsampel MUSS eine Sicht der einzelnen Dienstinstanzen realisieren.⌫

⌦ **TIP1-A_2543 Produkttyp Störungsampel, Rollen- und Berechtigungskonzept**

Der Produkttyp Störungsampel MUSS ein - dem Schutzbedarf angemessenes - Rollen- und Berechtigungskonzept für deren Nutzung implementieren, das es erlaubt, Detailinformationen für definierte Nutzergruppen zu verbergen bzw. freizuschalten.⌫

⌦ **TIP1-A_2544 Produkttyp Störungsampel, Authentifizierung von Nutzern**

Die Nutzer des Produkttyps Störungsampel MÜSSEN sich zur Nutzung registrieren und ihren Anspruch auf deren Nutzung nachweisen, indem sie den Nachweis der Zugehörigkeit zu einer der o.g. Rollen erbringen. Authentisierte Nutzer der Störungsampel sollen diese mit geringem technischen Aufwand nutzen können.⌫

5.4.16 Produkttyp Service Monitoring

Perspektivisch wird das Service Monitoring die Aufgaben der Störungsampel übernehmen. In der Übergangsphase sind beide Produkttypen aktiv und ihre Nutzung wird betrieblich koordiniert.

Das Service Monitoring testet durch Probes die Verfügbarkeit zentraler Dienster, sicherer Übermittlungsverfahren und fachanwendungsspezifischer Dienste. Darüber hinaus sammelt es die Performance-Reports der verschiedenen Dienste ein. Die Erkenntnisse zum Betriebsstatus der einzelnen Dienste werden berechtigten Nutzern des Dienstes bereitgestellt.

⌦ **TIP1-A_7060 Produkttyp Service Monitoring, Schnittstellen und Prozesse**

Der Produkttyp Service Monitoring MUSS die im Folgenden definierten Schnittstellen und Prozesse implementieren.

Tabelle 35: Schnittstellen und Prozesse des Produkttyps Service Monitoring

Service Monitoring		
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_Monitoring_Update	Betreiber_ZD, Betreiber_FD, SÜV	
I_Monitoring_Read		Diese Schnittstelle MUSS im Internet für die nachfolgenden Nutzer angeboten werden. • Anbieter in ihrer Rolle als betriebsverantwortliche Instanz,

ENTWURF

		• die Supportdienstleistenden, • die Servicebetriebsverantwortlichen der TI, • die gematik als gesamtverantwortliche Instanz der TI. Die Schnittstelle MUSS mit einer GUI und als machinenverwertbare Variante angeboten werden.
Benötigte Schnittstellen		
Alle durch die TI fachlich definierten Schnittstellen der zentralen Dienste, fachanwendungsspezifischen Dienste und sicheren Übermittlungsverfahren.		
Fachliche Prozesse	**Nutzer**	**Bedingungen**

⌫

⌦ **TIP1-A_7040 Produkttyp Service Monitoring, Monitoring der Verfügbarkeit mittels Probes**

Der Produkttyp Service Monitoring MUSS die Verfügbarkeit aller definierten Schnittstellen der fachanwendungsspezifischen Dienste, der zentralen Dienste der TI-Plattform und der Dienste sicherer Übermittlungsverfahren durch Abfrage der Schnittstellen über Aufrufe, die das Verhalten der echten Nutzer der Schnittstellen simulieren (sogenannten Probes), ermitteln. ⌫

⌦ **TIP1-A_7061 Produkttyp Service Monitoring, Prüfung im Internet und zentralen Netz**

Der Produkttyp Service-Monitoring MUSS die Verfügbarkeit von Schnittstellen sowohl im zentralen Netz der TI als auch im Internet prüfen, wenn die Schnittstelle in diesen Netzen vorgeschrieben ist. ⌫

⌦ **TIP1-A_7062 Produkttyp Service Monitoring, implizite Probes**

Der Produkttyp Service Monitoring KANN Probes für verschiedene Schnittstellen zusammenfassen, wenn ein Probe implizit verschiedene andere Schnittstellen nutzt (z. B. bei der Kommunikation über das zentrale Netz). ⌫

⌦ **TIP1-A_7041 Produkttyp Service Monitoring, Client-Anforderungen der Schnittstellen**

Der Produkttyp Service Monitoring MUSS die Probes so implementieren, dass alle Anforderungen an den Client, auf deren Einhaltung sich die Dienste verlassen, erfüllt sind. ⌫

⌦ **TIP1-A_7042 Produkttyp Service Monitoring, keine Beeinträchtigung der Dienste**

Der Produkttyp Service Monitoring DARF die mittels Probes überwachten Dienste im Bezug auf Sicherheit, Funktionalität und geforderter Performanz NICHT beeinflussen. ⌫

⌦ **TIP1-A_7043 Produkttyp Service Monitoring, Ursachen-Analyse**

Der Produkttyp Service Monitoring MUSS die Probes so implementieren, dass im Falle einer negativen Verfügbarkeitsmessung weitere Abfrageschritte ausgeführt werden, um die Ursache der Nicht-Verfügbarkeit genauer zu bestimmen.⌫

⌦ **TIP1-A_7059 Produkttyp Service Monitoring, Monitoring für Dienste über den SZZP**

ENTWURF

Der Produkttyp Service Monitoring MUSS Anbietern von Diensten der TI, die über einen SZZP an das zentrale Netz der TI angeschlossen sind, ermöglichen, mit eigenen Probes aus ihrem Rechenzentrum heraus über den SZZP die Schnittstellen ihrer Dienste zu überwachen. ⌫

⌦ **TIP1-A_7058 Produkttyp Service Monitoring, keine realen Anwendungsfälle auslösen**

Der Produkttyp Service Monitoring DARF mittels Probes NICHT Anwendungsfälle für reale Nutzer einer Anwendung auslösen oder Zugriff auf personenbezogene Daten erhalten. ⌫

5.5 Interfaces der TI-Plattform Dezentral

In den nachfolgenden Kapiteln werden alle Außenschnittstellen der Produkttypen der TI-Plattform mit ihren Operationen und Parametern beschrieben und detailliert **für** welchen Nutzer sie angeboten werden. Dabei sind folgende Nutzer vorgesehen: Leistungserbringer (**LE**), Clientsystem oder Clientmodule (**CS**), Fachmodul (**FM**), Fachmodul für mobile Kartenterminals (**MFM**), TI-Plattform (**TIP**), fachanwendungsspezifische Dienste (**FAD**), sichere Übermittlungsverfahren (**SÜV**), weitere Anwendungen des Gesundheitswesens in der Provider Zone (**WA**) und Administratoren (**A**). Neben der Benennung des Interfaces und der Operation mit ihren Parametern und Ergebnissen ist auch vermerkt, ob das Interface von der TI-Plattform bereitgestellt (provided) oder benötigt (required) wird.

An den Operationen ist ferner ausgewiesen, welche Schutzleistung die TI-Plattform für die übergebenen Parameter im Bezug auf Vertraulichkeit, Integrität und Authentizität (**V, I, A**) übernimmt, bzw. welcher Schutzbedarf für die Ergebnisse der Operationen gesehen wird. Ferner wird ausgewiesen, welche Schutzleistung die Operationen im Bezug auf Verfügbarkeit und Nichtabstreitbarkeit haben. Bei der Festlegung der Schutzleistung bzw. des Schutzbedarfs wurde immer das Maximumprinzip angewendet. Sie werden zur Erreichung der Schutzziele der TI benötigt. In Tabelle 36 werden die für die Dokumentation verwendeten Abkürzungen erklärt.

Tabelle 36: Legende zu den Abkürzungen in den Operationstabellen

Abkürzung	Bedeutung
SH	sehr hoch
H	hoch
M	mittel
N	niedrig
NA	nicht anwendbar
KS	kein Schaden

Für alle Parameter der Operationen wird jeweils ausgewiesen, wie sie im Informationsmodell der TI-Plattform einzuordnen sind. Dabei wird ein Kürzel (z. B. IM101) als Referenz zum Informationsmodell in Abbildung 51 verwendet.

Die aus Kapitel 4.3 geforderten Parameter, die für eine Umsetzung der Mandantenfähigkeit benötigt werden, sind nur für die Operationen an der Schnittstelle I_KV_Card_Handling explizit ausgewiesen, da diese Operationen einen sehr starken Bezug zur Mandantenfähigkeit haben. Für alle anderen Operationen mit Bezug zur Mandantenfähigkeit werden keine zusätzlichen Parameter zum Call-Context beschrieben. Die Information darüber, welche Operationen betroffen sind, können dem Kapitel 3.1 entnommen werden.

ENTWURF

5.5.1 Basisdienste

5.5.1.1 Benutzerinteraktion_KT

5.5.1.1.1 I_KT_Operations (Provided)

⌦ **TIP1-A_2248 Schnittstelle I_KT_Operations**

Die Schnittstelle I_KT_Operations MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2249 Logische Operation I_KT_Operations::interact_with_User**

Die Schnittstelle I_KT_Operations MUSS die logische Operation interact_with_User implementieren.

Tabelle 37: Operation interact_with_User

I_KT_Operations					Berechtigung: FM
interact_with_User	Parameter				V, I, A
	In	KT_Ident	RessourceIdentifier	IM412	M/M/M
	In	Data	Text	IM101	SH/SH/SH
	In	Timeout	Timeinformation	IM307	M/H/H
	Out	UserData	Text	IM101	SH/SH/SH
Die Operation interact_with_User sendet eine Textanzeige an ein Kartenterminal und fragt bei Bedarf Informationen vom Anwender an (Eingabe über PIN-Pad). PIN-Eingaben sind hierbei ausgeschlossen. Die Operation bietet dem Aufrufer optional an, unter Nutzung des Parameters (Timeout) zu definieren, wie lange auf eine Eingabe des Anwenders gewartet werden soll. Die Länge des Anzeigetextes (Data) orientiert sich an den techn. Möglichkeiten des Kartenterminals, wobei ein Scrollen des Textes erlaubt ist.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.5.1.2 Erstellung_Prüfung_Signatur

5.5.1.2.1 I_Sign_Operations (Provided)

⌦ **TIP1-A_2250 Schnittstelle I_Sign_Operations**

Die Schnittstelle I_Sign_Operations MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2251 Logische Operation I_Sign_Operations::sign_Document**

Die Schnittstelle I_Sign_Operations MUSS die logische Operation sign_Document implementieren.

Tabelle 38: Operation sign_Document

I_Sign_Operations					Berechtigung: CS, FM
sign_Document	Parameter				V, I, A
	In	DataToBeSigned	DocumentType	IM101	SH/SH/SH
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	KeyRef	KeyReference	IM412	M/H/H
	In	Schema	XmlSchema	IM301	KS/H/H
	Out	SignedData	SignedDocumentType	IM102	SH/M/M

ENTWURF

Der Aufrufer erzeugt über diese Operation eine digitale Signatur am übergebenen Dokument (*DataToBeSigned*). Die dabei zu verwendende kryptographische Identität wird durch die Referenz KeyRef auf den privaten Schlüssel festgelegt. Anhand der CardUsageReference (*CuRef*) wird die zu verwendende Karte adressiert und werden die Zugriffsrechte geprüft. Für XML-Dokumente kann optional ein XML-Schema (*Schema*) übergeben werden, gegen welches das Dokument geprüft wird. Sollte die Schemaprüfung fehlschlagen, wird die Signaturerstellung abgebrochen. Die Signatur wird entsprechend des angewendeten Signaturformats in das Ergebnisdokument (*SignedData*) eingebettet. Karten, die im Ablauf dieser Operation genutzt werden, befinden sich nach Beendigung der Operation im gleichen Sicherheitszustand wie vor der Operation. Für die Erstellung der Signatur wird die Operation sign_Data nachgenutzt. Es werden die nachfolgenden Dokumententypen mit dem genannten Signaturformat unterstützt: • Binär, Text und MIME mit CMS • XML (einschließlich der WS-Trust Elemente X.509-Token und SAML-Token) mit XAdES • PDF/A mit PDF-Signatur Die Signatur kann mit folgenden kryptographischen Identitäten erfolgen: • eGK: ID.CH.AUT, ID.CH.AUTN für Fachmodule • SMC-B: ID.HCI.OSIG für Fachmodule und Clientsysteme Die Operation unterstützt mindestens Dokumente bis zu einer Größe von 25 MB. **Anmerkung:** Abweichend vom Lastenheft wird bei der Erstellung einer Signatur die Gültigkeit und der Gültigkeitszeitraum des genutzten Zertifikats nicht online geprüft. Dieser Schritt ist unnötig, da auch bei der Prüfung der Signatur das Zertifikat mit überprüft wird und sonst dasselbe Zertifikat zwei Mal geprüft würde. Der Ersteller der Signatur und somit auch der Besitzer des privaten Schlüssels entscheidet ob er eine Signatur mit diesem Schlüssel erstellen möchte.
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA

⌫

⌦ **TIP1-A_2252 Logische Operation I_Sign_Operations::verify_Document**

Die Schnittstelle I_Sign_Operations MUSS die logische Operation verify_Document implementieren.

Tabelle 39: Operation verify_Document

I_Sign_Operations					Berechtigung: CS, FM
verify_Document	Parameter				V, I, A
	In	SignedData	SignedDocumentType	IM102	SH/M/M
	In	Certificate	CertificateX.509	IM404	M/M/M
	Out	VerificationResult	VerificationResultType	IM420	M/H/H
Diese Operation überprüft die digitale Signatur des übergebenen Dokuments (*SignedData*) unter Verwendung des übergebenen Signer-Zertifikats (*Certificate*). Dabei wird erst die Gültigkeit des Signer-Zertifikats bei Erstellung der Signatur durch Nachnutzung der Operation „verify_Certificate“ geprüft. Dies umfasst die Prüfung im Online- wie auch im Offline-Fall. War das genutzte Zertifikat bei Erstellung der Signatur nicht gültig, dann ist auch die Signatur nicht gültig. Das Signer-Zertifikat muss entweder bereits im signierten Dokument enthalten sein oder über den optionalen Parameter *Certificate* separat übergeben werden. Im Ergebnis der Operation (*VerificationResult*) wird dokumentiert, ob die Prüfung erfolgreich war, sie fehlgeschlagen ist oder nur teilweise erfolgen konnte, da z.B. die Online-Statusprüfung des Zertifikats nicht durchgeführt werden konnte. Im Fall einer teilweise erfolgten Prüfung werden die nicht erfolgten Prüfschritte mitgeteilt. Es werden die nachfolgenden Dokumententypen mit dem genannten Signaturformat unterstützt: • Binär, Text und S/MIME mit CMS • XML (einschließlich der WS-Trust Elemente X.509-Token und SAML-Token) mit XAdES • PDF/A mit PDF-Signatur Die Signatur von folgenden kryptographischen Identitäten kann geprüft werden: • eGK: ID.CH.AUT, ID.CH.AUTN für Fachmodule • SMC-B: ID.HCI.OSIG für Fachmodule und Clientsysteme Die Operation unterstützt mindestens Dokumente bis zu einer Größe von 25 MB.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

ENTWURF

⌦ **TIP1-A_5075 Logische Operation I_Sign_Operations::external_Authenticate**

Die Schnittstelle I_Sign_Operations MUSS die logische Operation external_Authenticate implementieren.

Tabelle 40: Operation external_Authenticate

I_Sign_Operations					Berechtigung: CS, FM
external_Authenticate	Parameter				V, I, A
	In	Hash	Binary	IM101	SH/SH/SH
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	Out	SignedHash	SignedBinary	IM102	SH/M/M
Die Operation erzeugt eine PKCS#1-Signatur an dem übergebenen Hash-Wert (*Hash*), um somit beliebigen externen Authentisierungsmechanismen die Möglichkeit zu bieten, eine Authentisierung unter Verwendung eines HBAs oder einer SMC-B durchzuführen. Die zu verwendende Karte wird in (*CuRef*) referenziert. Die dann zu verwendende Identität wird durch die Operation ermittelt. Der signierte Hash-Wert (*SignedHash*) wird als Ergebnis der Operation zurück geliefert. Die Signatur kann mit folgenden kryptographischen Identitäten erfolgen: • HBA (zeitlich begrenzt auch die HBA-Vorläuferkarten HBA-qSig und ZOD-2.0): ID.HP.AUT für Fachmodule und Clientsysteme • SMC-B: ID.HCI.AUT für Fachmodule und Clientsysteme					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_5084 Logische Operation I_Sign_Operations::get_Certificate**

Die Schnittstelle I_Sign_Operations MUSS die logische Operation get_Certificate implementieren.

Tabelle 41: Operation get_Certificate

I_Sign_Operations					Berechtigung: CS, FM
get_Certificate	Parameter				V, I, A
	In	ResID	RessourceIdentifier	IM412	M/H/H
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	Out	Certificate	CertificateX.509	IM404	M/M/M
Die Operation liefert ein X.509-Zertifikat von einer gesteckten Karte. Anhand der CardUsageReference (*CuRef*) wird die zu verwendende Karte adressiert und werden die Zugriffsrechte geprüft. Das konkrete Zertifikat wird durch die Resource-ID (*ResID*) referenziert und im Ergebnis (*Certificate*) zurück geliefert. Abrufbar sind alle X.509-Zertifikate von • HBA (zeitlich begrenzt auch die HBA-Vorläuferkarten HBA-qSig und ZOD-2.0) und SMC-B für Clientsysteme • eGK, HBA und SMC-B für Fachmodule					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA1.3.0					

⌫

5.5.1.3 Erstellung_Prüfung_QES

5.5.1.3.1 I_SAK_Operations (Provided)

⌦ **TIP1-A_2253 Schnittstelle I_SAK_Operations**

Die Schnittstelle I_SAK_Operations MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2254 Logische Operation I_SAK_Operations::sign_Document_QES**

ENTWURF

Die Schnittstelle I_SAK_Operations MUSS die logische Operation sign_Document_QES implementieren.

Tabelle 42: Operation sign_Document_QES

I_SAK_Operations					Berechtigung: CS, FM
	Parameter				V, I, A
sign_Document_QES	In	DataToBeSigned	List of DocumentType	IM101	SH/SH/SH (Dokument) SH/SH/SH (Liste)
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	Policies	List of Text	IM302	KS/H/H
	Out	SignedData	List of SignedDocumentType	IM103	SH/M/M (Dokument) SH/SH/SH (Liste)

Mit dieser Operation wird eine qualifizierte elektronische Signatur (QES) gemäß [eIDAS] für jedes der übergebenen Dokumente (*DataToBeSigned*) erzeugt. Die QES wird mit dem HBA unter Verwendung der kryptographischen Identität ID.HP.QES des HBA-Inhabers erstellt. Zu nutzende Karten sind zeitlich begrenzt auch die HBA-Vorläuferkarten HBA-qSig und ZOD-2.0. Zugriffsrechte auf die zu verwendende Karte werden anhand der übergebenen CardUsageReference (*CuRef*) geprüft.

Es wird die Übereinstimmung der Eigenschaften der Dokumente mit den Vorgaben der übergebenen Policies (*Policies)* überprüft. Die Policies beinhalten spezifische Signaturformatfestlegungen und Darstellungsvorgaben für die jeweils verwendeten Datenformate. Für XML-Dokumente beinhalten die Policies ein XML-Schema, gegen welches das XML-Dokument geprüft wird. Sollte die Schemaprüfung fehlschlagen, wird die Signaturerstellung abgebrochen.
Des Weiteren muss vor Erstellung der Signatur geprüft werden, ob die Gültigkeitsdauer des Signaturzertifikats überschritten ist.
~~Die Verwendung von Attributzertifikaten wird unterstützt.~~
Die erzeugte Signatur wird jeweils entsprechend des angewendeten Signaturformats in das Ergebnisdokument (*SignedData*) eingebettet. Als Signaturzeitpunkt wird die Systemzeit zum Zeitpunkt der Erstellung verwendet.
Sofern verfügbar wird die aktuelle Sperrinformation (OCSP-Response) des Signaturzertifikats in das Ergebnisdokument (*SignedData*) eingebettet.
Am Ende der Operation wird das/werden die signierten Dokumente an den Aufrufer übergeben (*SignedData*).
Es werden die nachfolgenden Dokumententypen mit dem genannten Signaturformat unterstützt:

- Text und TIFF mit CMS
- XML mit XAdES
- PDF/A mit PDF-Signatur

Es werden die folgenden Formen der Signatur unterstützt:

- Einzelsignatur für alle angegebenen Formate
- Stapelsignatur für alle angegebenen Formate
- Parallelsignatur für die Formate Text, TIFF und XML
- Gegensignatur für alle angegebenen Formate

Bei Nichtvorhandensein der Konfiguration LU_SAK muss die Operation unmittelbar mit einer Fehlermeldung abgebrochen werden bzw. darf nicht angeboten werden.
<u>Eigenschaften der Stapelsignatur</u>
Im Falle der Stapelsignatur enthält der Parameter *DataToBeSigned* eine Liste von zu signierenden Dokumenten.

- Jedes Dokument des Stapels wird einzeln qualifiziert signiert.
- Stapelsignatur ist für alle für die Einzelsignatur unterstützten Formate möglich.
- Gemischte Formate innerhalb eines Stapels sind möglich.
- Innerhalb eines Stapels werden Erst-, Gegen- und Parallelsignatur auch in gemischter Form unterstützt.
- Die Stapelgröße muss unabhängig von Limitierungen auf dem HBA festgelegt werden.
- Die Stapelsignatur fordert für jeden Stapel vor dem Signieren der Dokumente einmal eine PIN-Eingabe des Benutzers und signiert die Dokumente eines Stapels in unmittelbarer Folge ohne wiederholte PIN-Eingabe des Benutzers. Wenn die festgelegte Stapelgröße die Limitierung auf dem HBA übersteigt, werden Teilstapel gebildet, für die jeweils eine separate PIN-Eingabe erforderlich ist.
- Dokumente verschiedener Versicherter können innerhalb eines Stapels signiert werden.

ENTWURF

• Die Stapelsignatur kann bis zum Auslösen der qualifizierten elektronischen Signaturen (PIN-Eingabe) und während der Stapelabarbeitung kontrolliert abgebrochen werden. Die Operation unterstützt mindestens Dokumente bis zu einer Größe von 25 MB. Die Performancevorgaben gelten für Einzelsignaturen.
Verfügbarkeit: NA, Nichtabstreitbarkeit: SH

⌫

⌦ **TIP1-A_2255 Logische Operation I_SAK_Operations::verify_Document_QES**

Die Schnittstelle I_SAK_Operations MUSS die logische Operation verify_Document_QES implementieren.

Tabelle 43: Operation verify_Document_QES

I_SAK_Operations					Berechtigung: CS, FM
verify_Document_QES	Parameter				V, I, A
	In	SignedData	SignedDocumentType	IM103	SH/M/M
	In	Certificate	CertificateX.509	IM404	M/M/M
	In	Policies	Text	IM302	KS/H/H
	Out	VerificationResult	VerificationResultType	IM420	M/H/H
Diese Operation überprüft die qualifizierte elektronische Signatur (QES) des übergebenen Dokuments (*SignedData*) gemäß [eIDAS] unter Verwendung des mit dem Dokument übergebenen Signaturzertifikats. Das Signaturzertifikat muss entweder bereits im signierten Dokument enthalten sein oder über den optionalen Parameter *Certificate* separat übergeben werden. Es wird zuerst die Gültigkeit des Signaturzertifikats durch Nachnutzung des Dienstes „Prüfung_Zertifikat“ geprüft. Dies umfasst die Prüfung im Online- wie auch im Offline-Fall. Sollte das übergebene Dokument (*SignedData*) eine Sperrinformation (OCSP-Response) für das Signaturzertifikat enthalten, so wird diese bei der Prüfung des Zertifikates verwendet. War das genutzte Zertifikat bei Erstellung der Signatur nicht gültig, dann ist auch die Signatur im rechtlichen Sinn nicht gültig. Im Ergebnis der Operation (*VerificationResult*) wird dokumentiert, ob die Prüfung erfolgreich war oder ob sie fehlgeschlagen ist. Falls die Prüfung nicht vollständig erfolgen konnte, da z.B. die Online-Statusprüfung des Zertifikats nicht möglich war (Offline-Fall), muss dies dem Nutzer mitgeteilt werden. Dazu werden die durchgeführten Prüfschritte im Ergebnis der Operation (*VerificationResult*) aufgeführt. Falls ein Algorithmus oder Parameter, der zur Signatur genutzt wurde, nicht mehr als geeignet betrachtet wird, muss die Signaturprüfung trotzdem durchgeführt werden. Das Ergebnis der Signaturprüfung muss im Parameter *VerificationResult* enthalten sein. In den *SignedData* enthaltene qualifizierte Zeitstempel werden ausgewertet. Vor der Prüfung der Signatur muss der Status der verwendeten Algorithmen gegen den aktuell gültigen Algorithmenkatalog der zuständigen Behörde (BNetzA) geprüft werden. Es werden die nachfolgenden Dokumententypen mit dem genannten Signaturformat unterstützt: • Text und TIFF mit CMS • XML mit XAdES • PDF/A mit PDF-Signatur Bei der Prüfung werden die folgenden Formen der Signatur unterstützt: • Einzelsignatur für alle angegebenen Formate • Parallelsignatur für die Formate Text, TIFF und XML • Gegensignatur für alle angegebenen Formate Bei Nichtvorhandensein der Konfiguration LU_SAK muss die Operation unmittelbar mit einer Fehlermeldung abgebrochen werden bzw. darf nicht angeboten werden. Es werden nur Signaturen der kryptographischen Identitäten von Leistungserbringern (zulässige Karten: HBA wie auch zeitlich begrenzt die HBA-Vorläuferkarten HBA-qSig und ZOD-2.0) geprüft. ~~Die Verwendung von Attributzertifikaten wird unterstützt.~~ Die Operation unterstützt mindestens Dokumente bis zu einer Größe von 25 MB.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

ENTWURF

5.5.1.4 Token_Authentisierung

5.5.1.4.1 I_IDP_Auth_Active_Client (Provided)

⌦ **TIP1-A_6035 Schnittstelle I_IDP_Auth_Active_Client**

Die Schnittstelle I_IDP_Auth_Active_Client MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_6036 Logische Operation I_IDP_Auth_Active_Client::get_Metadata**

Die Schnittstelle I_IDP_Auth_Active_Client MUSS die logische Operation get_Metadata implementieren.

Tabelle 44: Operation get_Metadata

I_IDP_Auth_Active_Client					Berechtigung: CS
get_Metadata	Parameter				V, I, A
	Out	Metadata	InterfaceInformation	IM427	kS/M/M
Diese Operation basiert auf WS-Transfer [WS-Transfer2011] und gibt Metadaten zurück, die die Schnittstelle beschreiben (*Metadata*). Die Metadaten sind in [WS-MetadataExchange2011] spezifiziert und beinhalten WSDL, WS-Policy und referenzieren verwendete XML Schema. Der Endpunkt dieser Operation wird im Netzwerk des Anwenders mittels SRV Resource Record veröffentlicht.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: N					

⌫

⌦ **TIP1-A_6037 Logische Operation I_IDP_Auth_Active_Client::issue_Identity_Assertion**

Die Schnittstelle I_IDP_Auth_Active_Client MUSS die logische Operation issue_Identity_Assertion implementieren.

Tabelle 45: Operation issue_Identity_Assertion

I_IDP_Auth_Active_Client					Berechtigung: CS
issue_Identity_Assertion	Parameter				V, I, A
	In	BinarySecurityToken	CertificateX.509	IM404	M/H/H
	In	Lifetime	TimeInformation	IM101	M/H/H
	In	Timestamp	TimeInformation	IM101	M/H/H
	In	UseKey	SessionKey	IM101	M/H/H
	In	AppliesTo	Identifier	IM101	M/H/H
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	Out	SecurityToken	IdentityAssertion	IM426	M/M/M
Diese Operation ermöglicht das Ausstellen von Identitätsbestätigungen (*SecurityToken*) basierend auf WS-Trust, SAML2.0 Assertions, und WS Federation 1.2 für Active Requestor Profile mit Holder-of-Key. Zur Sicherstellung einer zeitlichen Konsistenz übergibt der Aufrufer seine aktuelle Zeit (*Timestamp*). Sollte diese von der lokalen Zeit über mehr als eine Minute abweichen, wird die Ausstellung einer Identitätsbestätigung verweigert. Die Festlegung der Gültigkeitsdauer (*Lifetime*), der Referenz auf den aufrufenden Dienst (*AppliesTo*) und ein öffentlicher Schlüssel (*UseKey)* werden durch den Anwender festgelegt und in die Identitätsbestätigung integriert. Sollte der UseKey selbst-signiert sein, so erfolgt keine Prüfung dieser Signatur. Sollte keine *Lifetime* übergeben werden, so wird eine Gültigkeit von 3 Stunden gesetzt. Um die durch diese Operation erstellten Identitätsbestätigungen von denen eines lokalen IDPs unterscheiden zu können, tragen die Identitätsbestätigungen im Feld Aussteller (Issuer) die Bezeichnung „IDP der TI-Plattform“. Die in einer Identitätsbestätigung enthaltenen Identitätsinformationen werden ausschließlich aus dem Zertifikat der kryptografischen Identität ID.HCI.OSIG der über die Parameter *CuRef* und *BinarySecurityToken* ausgewählten SMC-B übernommen und mit derselben Identität signiert.					

ENTWURF

Die Gültigkeit von Identitätsbestätigungen ist auf den anfragenden Dienst beschränkt (*AppliesTo*). Somit wird verhindert, dass sich Dienste Identitätsbestätigungen ausstellen lassen können die zum Zugriff auf andere Dienste berechtigen.
Verfügbarkeit: NA, Nichtabstreitbarkeit: M

⌫

⌦ **TIP1-A_6038 Logische Operation I_IDP_Auth_Active_Client::renew_Identity_Assertion**

Die Schnittstelle I_IDP_Auth_Active_Client MUSS die logische Operation renew_Identity_Assertion implementieren.

Tabelle 46: Operation renew_Identity_Assertion

I_IDP_Auth_Active_Client					Berechtigung: CS
renew_Identity_Assertion	Parameter				V, I, A
	In	RenewTarget	IdentityAssertion	IM426	M/M/M
	Out	SecurityToken	IdentityAssertion	IM426	M/M/M
Diese Schnittstelle ermöglicht das Erneuern einer alten Identitätsbestätigung (*RenewTarget*) basierend auf WS-Trust, SAML2.0 Assertions, und WS Federation 1.2 für Active Requestor Profile. In *RenewTarget* wird eine Referenz auf die alte Identitätsbestätigung übergeben. Die erneuerte Identitätsbestätigung (SecurityToken) wird grundsätzlich nicht verändert, sondern unterscheidet sich zur ursprünglichen Identitätsbestätigung lediglich durch eine, um die ursprünglich bestätigte Gültigkeitsdauer, aktualisierte Gültigkeitsdauer und eine aktualisierte Signatur. Abgelaufene Identitätsbestätigung können nicht erneuert werden.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: M					

⌫

⌦ **TIP1-A_6039 Logische Operation I_IDP_Auth_Active_Client::cancel_Identity_Assertion**

Die Schnittstelle I_IDP_Auth_Active_Client MUSS die logische Operation cancel_Identity_Assertion implementieren.

Tabelle 47: Operation cancel_Identity_Assertion

I_IDP_Auth_Active_Client					Berechtigung: CS
cancel_Identity_Assertion	Parameter				V, I, A
	In	CancelTarget	IdentityAssertion	IM426	M/M/M
Diese Schnittstelle ermöglicht das Annullieren von Identitätsbestätigungen (*CancelTarget*) basierend auf WS-Trust, SAML2.0 Assertions, und WS Federation 1.2 für Active Requestor Profile. In *CancelTarget* wird eine Referenz auf die alte Identitätsbestätigung übergeben. Der Anwender wird abgemeldet, so dass dessen Identitätsbestätigung nicht mehr erneuert werden kann.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.5.1.4.2 I_IDP_Auth_Passive_Client (Provided)

⌦ **TIP1-A_6776 Schnittstelle I_IDP_Auth_Passive_Client**

Die Schnittstelle I_IDP_Auth_Passive_Client MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_6040 Logische Operation I_IDP_Auth_Passive_Client::signin**

ENTWURF

Die Schnittstelle I_IDP_Auth_Passive_Client MUSS die logische Operation signin implementieren.

Tabelle 48: Operation signin

I_IDP_Auth_Passive_Client					Berechtigung: CS
signin	Parameter				V, I, A
	In	wfresh	TimeInformation	IM101	M/H/H
	In	wct	TimeInformation	IM101	M/H/H
	In	wtrealm	Identifier	IM101	M/H/H
	In	wreply	URI	IM304	M/H/H
	In	wctx	SessionContext	IM101	M/H/H
	Out	wresult	IdentityAssertion	IM426	M/M/M
	Out	wctx	SessionContext	IM101	M/H/H
Diese Schnittstelle ermöglicht das Ausstellen von Identitätsbestätigungen (*wresult*) basierend auf WS-Trust, SAML2.0 Assertions, und WS Federation 1.2 für Passive Requestor Profile . Zur Sicherstellung einer zeitlichen Konsistenz übergibt der Aufrufer seine aktuelle Zeit (*wct*). Sollte diese von der lokalen Zeit über mehr als eine Minute abweichen, wird die Ausstellung einer Identitätsbestätigung verweigert. Die Festlegung der Gültigkeitsdauer (*wfresh*) und die Bindung an den aufrufenden Dienst (*wtrealm*) werden durch den Anwender festgelegt und in die Identitätsbestätigung integriert. Sollte keine Gültigkeitsdauer übergeben werden, so wird eine Gültigkeit von 3 Stunden gesetzt. Um die durch diese Operation erstellten Identitätsbestätigungen von denen eines lokalen IDPs unterscheiden zu können, tragen die Identitätsbestätigungen im Feld Aussteller (Issuer) die Bezeichnung „IDP der TI-Plattform“. Die in einer Identitätsbestätigung enthaltenen Identitätsinformationen werden ausschließlich aus dem Zertifikat der kryptografischen Identität ID.HCI.OSIG der im Browser konfigurierten SMC-B übernommen und mit derselben Identität signiert. Sollte keine SMC-B im Browser konfiguriert sein, fragt die Operation ab, welche SMC-B verwendet werden soll und speichert die Auswahl im Browser für nachfolgende Aufrufe. Die Gültigkeit von Identitätsbestätigungen ist auf den anfragenden Dienst beschränkt (*wtrealm*). Somit wird verhindert, dass sich Dienste Identitätsbestätigungen ausstellen lassen können die zum Zugriff auf andere Dienste berechtigen. Damit liegt es in der Verantwortung des anfragenden Dienstes, den Parameter (*wtrealm*) so zu wählen, dass er eindeutig erkennen kann, dass eine Identitätsbestätigung durch ihn erstellt wurde. Die Operation legt einen Session-Cookie für die erzeugte Identitäts-Session im Browser an. Nach Abschluss der Operation wird ein HTTP-Redirect auf *wreply* ausgeführt und dabei die erzeugte Identitätsbestätigung (*wresult*) und der gelieferte SessionContext (*wctx*) übergeben.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: M					

⌫

⌦ **TIP1-A_6041 Logische Operation I_IDP_Auth_Passive_Client::signout**

Die Schnittstelle I_IDP_Auth_Passive_Client MUSS die logische Operation signout implementieren.

Tabelle 49: Operation signout

I_IDP_Auth_Passive_Client					Berechtigung: CS
signout	Parameter				V, I, A
	In	wreply	URI	IM304	M/H/H
	In	SessionId	Session	IM410	M/H/H
Diese Schnittstelle ermöglicht das Abmelden basierend auf WS-Trust, SAML2.0 Assertions, und WS Federation 1.2 für Passive Requestor Profile. Mit Aufruf dieser Operation loggen sich Anwender aus und die Identitäts-Session (*SessionId*) und der zugehörige Session-Cookie im Browser werden gelöscht. Nach Abschluss der Operation wird ein HTTP-Redirect auf *wreply* ausgeführt.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

ENTWURF

5.5.1.4.3 I_Local_IDP_Service (Provided)

⌦ **TIP1-A_6042 Schnittstelle I_Local_IDP_Service**

Die Schnittstelle I_Local_IDP_Service MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_6043 Logische Operation I_Local_IDP_Service::sign_Token**

Die Schnittstelle I_Local_IDP_Service MUSS die logische Operation sign_Token implementieren.

Tabelle 50: Operation sign_Token

I_Local_IDP_Service					Berechtigung: CS
sign_Token	Parameter				V, I, A
	In	Token	IdentityAssertion	IM426	H/SH/SH
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	Out	SignedToken	IdentityAssertion	IM426	H/M/M
Die Operation erzeugt eine Signatur über die dentitätsbestätigung (*Token*) des lokalen IDP. Signiert wird mit der kryptografischen Identität ID.HCI.OSIG der über den Parameter *CuRef* festgelegten SMC-B. Die zu signierende Identitätsbestätigung (*Token*) muss SAML2.0 Assertion entsprechen. Die Signatur wird nur erzeugt, wenn als Aussteller der Identitätsbestätigung (Issuer) nicht der „IDP der TI-Plattform“ ausgewiesen wird, um die Identitätsbestätigung unterscheiden zu können. Die signierte Identitätsbestätigung (*SignedToken*) mit eingebettetem Signaturzertifikat wird als Ergebnis der Operation zurück geliefert.					
Verfügbarkeit: NA, Nichtabstreitbarkeit:M					

⌫

5.5.1.5 Information_Systemzustände

5.5.1.5.1 I_Poll_System_Information (Provided)

⌦ **TIP1-A_2264 Schnittstelle I_Poll_System_Information**

Die Schnittstelle I_Poll_System_Information MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2265 Logische Operation I_Poll_System_Information::get_Ressource_List**

Die Schnittstelle I_Poll_System_Information MUSS die logische Operation get_Ressource_List implementieren.

Tabelle 51: Operation get_Ressource_List

I_Poll_System_Information					Berechtigung: CS, FM, MFM
get_Ressource_List	Parameter				V, I, A
	In	Filter	Text	IM306	M/M/M
	Out	ResList	RessourceList	IM410	M/H/H
Die Operation liefert eine Liste der dezentralen Komponenten, die für die Komponente, die diese Operation umsetzt, aktuell erreichbar sind. Die Liste kann über den kontextbezogenen Filterparameter eingeschränkt werden (bsp. „liefere nur KTs“). Die zurückgegebene Liste enthält pro Listenelement die Informationen RessourceIdentifier, RessourceType und RessourceName. Unterschiedliche dezentrale Komponenten liefern unterschiedliche Inhalte: ➢ Ein MobKT listet: Slots, gesteckte Karten, Drucker ➢ Eine Kartenterminalverwaltung listet die verwalteten KTs					

ENTWURF

➢ Eine Kartenverwaltung liefert eine Liste der verwalteten Karten ➢ Eine Kartenterminal listet seine Funktionalen Einheiten (Display, PIN-Pad, Slots)
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA

⌫

⌦ **TIP1-A_2266 Logische Operation I_Poll_System_Information::get_Ressource_Information**

Die Schnittstelle I_Poll_System_Information MUSS die logische Operation get_Ressource_Information implementieren.

Tabelle 52: Operation get_Ressource_Information

I_Poll_System_Information					Berechtigung: CS, FM, MFM
get_Ressource_Information	Parameter				V, I, A
	In	ResIdentifier	RessourceIdentifier	IM412	M/H/H
	Out	ResDetail	RessourceDetails	IM411	M/H/H
Die Operation liefert statische und dynamische Informationen der dezentralen Komponente, die über ResIdentifier selektiert wird. Die Liste aller aktuell verfügbaren ResIdentifier ist über get_Ressource_List abrufbar. Der Rückgabewert ResDetail ist ein komplexer Datentyp zur Aufnahme aller statischen und dynamischen Informationen einer dezentralen Komponente. Der Datentyp fasst Informationen über die Produkttypen KT, Karte, MobKT zusammen. Er enthält unter anderem (sofern zutreffend): - RessourceIdentifier - CardInfo - Status Online/Offline - Betriebszustand der Komponente (OK=Normal, Warnung=Admin-Interaktion sinnvoll, Kritisch=Fachlich eingeschränkt, Admin-Interaktion erforderlich) - verfügbare technische Zertifikate (zur Ermittlung der verbleibenden Gültigkeitsdauer) - Versionsinformationen Unterschiedliche dezentrale Komponenten liefern unterschiedliche Inhalte: ➢ Eine Systeminformation liefert die Informationen, die sie von den erreichbaren Komponenten erhalten kann (MobKT, Kartenterminalverwaltung, Kartenverwaltung, VPN-Client, Kartenterminal). ➢ Ein MobKT liefert alle Statusinformationen des gesamten Geräts (User eingeloggt, welche Karten gesteckt, Status der Karten, Freier Speicher des Zwischenspeichers etc.). ➢ Eine Kartenterminalverwaltung liefert Informationen zu einem KT (welche funktionalen Einheiten hat es: Display, PIN-Pad, Slots, etc., den Status der KTs, welche Slots sind belegt etc.). Sie erhält diese Information selbst durch Abfrage der von ihr verwalteten Kartenterminals. ➢ Eine Kartenverwaltung liefert Informationen zu einer Karte (Eigenschaften der Karte: Kartentyp, Version, PIN-Status etc.). ➢ Ein Kartenterminal liefert Informationen über seine funktionalen Einheiten (Display, PIN-Pad, Slots, etc.) und seiner aktuellen Zuständen (Gerätestatus, welche Slots sind belegt etc.).					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.5.1.5.2 I_Notification (Required)

⌦ **TIP1-A_2267 Schnittstelle I_Notification**

Die Schnittstelle I_Notification MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2268 Logische Operation I_Notification::notify**

Die Schnittstelle I_Notification MUSS die logische Operation notify implementieren.

Tabelle 53: Operation notify

ENTWURF

I_Notification					Berechtigung: TIP
notify	Parameter				V, I, A
	In	EventInfo	EventInformation	IM415	M/H/H
Diese Operation der Schnittstelle I_Notification muss seitens einer Komponente angeboten werden, wenn dieses automatisch über Ereignisse dezentraler Komponenten informiert werden möchte (anzumelden über register_for_Notifications). Tritt ein Ereignis ein, auf das sich die Komponente abonniert hat, wird diese Operation aufgerufen. Der Übergabewert EventInfo beinhaltet dann nähere Informationen zum eingetretenen Ereignis. Diese sind unter anderem: - Betriebszustandswechsel - Wechsel in den verfügbaren Karten - Bedarf einer PIN-Verifikation - Fortschrittsfeedback (bei lang andauernden Operationen) - Informationen über Interaktionsbedarf Unterschiedliche dezentrale Komponenten liefern unterschiedliche Inhalte: ➢ Eine Systeminformation reicht die Ereignisse weiter, die an sie von den erreichbaren Komponenten gesendet wurden (MobKT, Kartenterminalverwaltung, Kartenverwaltung, VPN-Client, Kartenterminal, sowie Meldungen von Fachmodulen und mobilen Fachmodulen eingetragen über I_Notify_From_FM). ➢ Ein MobKT meldet Statusänderungen des gesamten Geräts (User angemeldet, Karte gesteckt, Kartenstatus verändert etc.). ➢ Eine Kartenterminalverwaltung meldet Ereignisse, die an sie von den von ihr verwalteten KTs gesendet wurden ➢ Eine Kartenverwaltung meldet Zustandsänderungen an den von ihr verwalteten Karten (gesteckt, gezogen, PIN-Status verändert, PIN-Eingabe erwartet etc.). ➢ Ein Kartenterminal meldet eingetretene Ereignisse der Art: Ankündigung eines terminalseitig initiierten Verbindungsabbruchs, Slotstatusänderungen (Karte gesteckt, Karte entfernt), Tastaturereignis etc.					
Verfügbarkeit: N, Nichtabstreitbarkeit: NA					

⌫

5.5.1.5.3 I_Notification_From_FM

⌦ **TIP1-A_2269 Schnittstelle I_Notification_From_FM**

Die Schnittstelle I_Notification_From_FM MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2270 Logische Operation I_Notification_From_FM::notify**

Die Schnittstelle I_Notification_From_FM MUSS die logische Operation notify implementieren.

Tabelle 54: Operation notify

I_Notification_From_FM					Berechtigung: FM, MFM
notify	Parameter				V, I, A
	In	EventInfo	EventInformation	IM415	M/H/H
Auch Fachmodule und mobile Fachmodule können Ereignisse generieren, die über Information_Systemzustände anderen Fachmodulen und Clientsystemen aktiv und passiv zur Verfügung gestellt werden. EventInfo wird nach einem Aufruf dieser Operation über notify (I_Notification) an alle Empfänger versendet, die auf diesen Ereignistyp abonniert haben.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.5.1.5.4 I_Reg_Notification (Provided)

⌦ **TIP1-A_2271 Schnittstelle I_Reg_Notification**

ENTWURF

Die Schnittstelle I_Reg_Notification MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2272 Logische Operation I_Reg_Notification::register_for_Notifications**

Die Schnittstelle I_Reg_Notification MUSS die logische Operation register_for_Notifications implementieren.

Tabelle 55: Operation register_for_Notifications

I_Reg_Notification					Berechtigung: CS, FM, MFM
register_for_Notifications	Parameter				V, I, A
	In	NotifyAddress	NotificationAddress	IM304	M/H/H
	In	Filter	Text	IM306	M/M/M
Wollen sich Komponenten über ihre I_Notification-Schnittstelle über Ereignisse informieren lassen, so müssen sie hierzu zuerst die Ereignisse abonnieren. Dem Ereignissender muss mitgeteilt werden, an welche Adresse die eingetretenen Ereignisse gesendet werden sollen. Ferner kann der Aufrufer über den Filterparameter die Ereignisse einschränken, über die er informiert werden möchte. Über einen entsprechenden Filter-Wert kann das Abonnement auch wieder gekündigt werden („notify OFF“). Abonnements werden nicht persistiert. Startet die Komponente, die die Ereignisse aussendet neu, ist deren Liste der Empfänger für Ereignisse leer.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.5.1.6 KSR

5.5.1.6.1 I_KSRC_Management (Provided)

⌦ **TIP1-A_2273 Schnittstelle I_KSRC_Management**

Die Schnittstelle I_KSRC_Management MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2274 Logische Operation I_KSRC_Management::list_available_Updates**

Die Schnittstelle I_KSRC_Management MUSS die logische Operation list_available_Updates implementieren.

Tabelle 56: Operation list_available_Updates

I_KSRC_Management					Berechtigung: A
list_available_Updates	Parameter				V, I, A
	In	ClientType	KSRClientType	IM413	M/M/M
	In	ClientStatus	KSRClientStatus	IM414	M/H/H
	Out	AvailableUpdates	List of UpdateIdentifier	IM417	M/H/H (UpdateIdentifier) M/H/H (Liste)
Die Operation ermöglicht dem Administrator, die Liste der aktuell verfügbaren Software- und Konfigurations-Updates für eine dezentrale Komponente abzufragen. Die Angabe des Typs der dezentralen Komponente, für die die Abfrage erfolgen soll, erfolgt über den Parameter *ClientType*. Der Update-Status der abfragenden dezentralen Komponente beschreibt die aktuell verwendeten Versionen und wird durch den Parameter *ClientStatus* angegeben. Die Operation analysiert den Update-Status der anfragenden Komponente (*ClientStatus*) und liefert Informationen über aktuell verfügbare Updates zurück (*AvailableUpdates*).					
Verfügbarkeit: N, Nichtabstreitbarkeit: NA					

ENTWURF

⌫

⌦ **TIP1-A_2275 Logische Operation I_KSRC_Management::do_Update**

Die Schnittstelle I_KSRC_Management MUSS die logische Operation do_Update implementieren.

Tabelle 57: Operation do_Update

I_KSRC_Management					Berechtigung: A
do_Update	Parameter				V, I, A
	In	ClientType	KSRClientType	IM413	M/M/M
	In	UpdateIdentifier	UpdateIdentifier	IM417	M/H/H
Der Administrator stößt über diese Operation die Durchführung einer Aktualisierung der Software oder Konfiguration einer dezentralen Komponente (*ClientType*) aus dem KSR-Server an. Der Parameter *UpdateIdentifier* enthält die Identifikation des gewünschten Updates. Es wird die Operation I_KSRS_Download::get_Updates genutzt, um das gewünschte Update zu erhalten.					
Verfügbarkeit: N, Nichtabstreitbarkeit: H					

⌫

5.5.1.6.2 I_KSRC_FM_Support (Provided)

⌦ **TIP1-A_6049 Schnittstelle I_KSRC_FM_Support**

Die Schnittstelle I_KSRC_FM_Support MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_6050 Logische Operation I_KSRC_FM_Support::list_available_Packages**

Die Schnittstelle I_KSRC_FM_Support MUSS die logische Operation list_available_Packages implementieren.

Tabelle 58: Operation list_available_Packages

I_KSRC_FM_Support					Berechtigung: FM
list_available_Packages	Parameter				V, I, A
	In	ClientType	KSRClientType	IM413	M/M/M
	In	ClientStatus	KSRClientStatus	IM414	M/H/H
	Out	AvailablePackages	List of UpdateIdentifier	IM417	M/H/H (UpdateIdentifier) M/H/H (Liste)
Die Operation ermöglicht dem Fachmodul, die Liste der aktuell im KSR verfügbaren Pakete abzufragen. Die Angabe des Typs des Fachmoduls, für das die Abfrage erfolgen soll, erfolgt über den Parameter *ClientType*. Die aktuell im Fachmodul verwendete Version des Pakets wird durch den Parameter *ClientStatus* angegeben. Die Operation analysiert die aktuelle verwendete Version des Pakets (*ClientStatus*) und liefert Informationen über verfügbare Pakete zurück (*AvailableUpdates*). Bei den im KSR hinterlegten Paketen handelt es sich nicht um die Fachmodule selbst, sondern um Pakete mit Daten, die zur Unterstützung der fachlichen Anwendungsfälle benötigt werden.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_6058 Logische Operation I_KSRC_FM_Support::load_Package**

Die Schnittstelle I_KSRC_FM_Support MUSS die logische Operation load_Package implementieren.

ENTWURF

Tabelle 59: Operation load_Package

I_KSRC_FM_Support					Berechtigung: FM
load_Package	Parameter				V, I, A
	In	ClientType	KSRClientType	IM413	M/M/M
	In	PackageIdentifier	UpdateIdentifier	IM417	M/H/H
	Out	Package	UpdatePackage	IM416	M/M/M
Das Fachmodul lädt über diese Operation ein bestimmtes Paket (*Package*) aus dem KSR. Das gewünschte Paket wird über seinen Identifier (*PackageIdentifier*) benannt. Es wird die Operation I_KSRS_Download::get_Updates genutzt, um das gewünschte Paket zu erhalten. Es werden maximal Pakete mit einer Größe von 25MB unterstützt. Bei den im KSR hinterlegten Paketen handelt es sich nicht um die Fachmodule selbst, sondern um Pakete mit Daten, die zur Unterstützung der fachlichen Anwendungsfälle benötigt werden.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: H					

⌫

5.5.1.6.3 I_KSRC_Local_Management (Provided)

⌦ **TIP1-A_2276 Schnittstelle I_KSRC_Local_Management**

Die Schnittstelle I_KSRC_Local_Management MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2277 Logische Operation I_KSRC_Local_Management::do_local_Update**

Die Schnittstelle I_KSRC_Local_Management MUSS die logische Operation do_local_Update implementieren.

Tabelle 60: Operation do_local_Update

I_KSRC_Local_Management					Berechtigung: A
do_local_Update	Parameter				V, I, A
	In	UpdatePackage	UpdatePackage	IM416	M/M/M
Der Administrator stößt über diese Operation die Durchführung einer Aktualisierung der Software oder Konfiguration einer dezentralen Komponente an. Der Administrator muss das Update-Paket (*updatePackage*) auf einem lokalen Datenträger bereitstellen.					
Verfügbarkeit: N, Nichtabstreitbarkeit: H					

⌫

5.5.1.6.4 I_KSR_Update (Provided)

⌦ **TIP1-A_2278 Schnittstelle I_KSR_Update**

Die Schnittstelle I_KSR_Update MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2279 Logische Operation I_KSR_Update::perform_Update**

Die Schnittstelle I_KSR_Update MUSS die logische Operation perform_Update implementieren.

Tabelle 61: Operation perform_Update

I_KSR_Update					Berechtigung: TIP
perform_Update	Parameter				V, I, A
	In	UpdatePackage	UpdatePackage	IM416	M/M/M
Die Operation führt das Update einer dezentralen Komponente mit einem Aktualisierungspaket (*UpdatePackage*) aus. Das eHealth-Kartenterminal nutzt hierfür die Standard-SICCT-Schnittstelle für das Update des					

ENTWURF

SICCT-Kartenterminals.
Verfügbarkeit: N, Nichtabstreitbarkeit: H

⌫

5.5.1.7 Kartenverwaltung

5.5.1.7.1 I_KV_Card_Handling (Provided)

⌦ **TIP1-A_2280 Schnittstelle I_KV_Card_Handling**

Die Schnittstelle I_KV_Card_Handling MUSS alle zugehörigen logischen Operationen implementieren.⌫

Diese Schnittstelle enthält die Verwaltungsoperationen der Karten, darunter Operationen zum Erzeugen und Verwerfen von CardUsageReferences. Eine CardUsageReference ist ein Verweis auf ein geordnetes Paar aus einem RessourceIdentifier einer Karte und einem Aufrufkontext. Sie ist für den Zeitraum der Kartennutzung mit diesem Kontext mit der Karte assoziiert.

Auch das MobKT bietet diese Schnittstelle an.

⌦ **TIP1-A_2281 Logische Operation I_KV_Card_Handling::get_Card_Usage_Reference**

Die Schnittstelle I_KV_Card_Handling MUSS die logische Operation get_Card_Usage_Reference implementieren.

Tabelle 62: Operation get_Card_Usage_Reference

I_KV_Card_Handling					Berechtigung: CS, FM, MFM
get_Card_Usage_Reference	Parameter				V, I, A
	In	ResID	RessourceIdentifier	IM412	M/H/H
	In	CallCon	CallContext	IM309	SH/SH/SH
	Out	CuRef	CardUsageReference	IM308	SH/SH/SH
Die Operation get_Card_Usage_Reference liefert zu einer gewählten Karte (*ResID*) und einem Aufrufkontext (*CallCon*) eine CardUsageReferenz zurück (*CuRef*). Die CardUsageReference wird innerhalb dieser Operation neu angelegt, wenn für diese Karte und zu diesem Aufrufkontext noch keine vorhanden ist. Die erzeugte CardUsageReference hat eine ausreichend hohe Entropie, so dass sie nicht erraten werden kann und nicht zufällig auf eine andere Kombination von RessourceIdentifier und Aufrufkontext in der Kartenverwaltung zeigen kann. Die gewählte Karte wird anhand der *ResID* identifiziert, die ein User aus der Ergebnisliste der Operation get_Ressource_List selektiert hat. In die CardUsageReference fließen genau die Informationen aus dem Aufrufkontext ein, die für eine spätere kartentypspezifische Berechtigungsprüfung benötigt werden. Dadurch können alle Anwender, bei denen diese Parameter übereinstimmen, dieselbe CardUsageReference bekommen und einen eventuell erhöhten Sicherheitszustand gemeinsam nutzen. Die CardUsageReference wird in allen folgenden Operationsaufrufen von CS, FM und MFM als Verweis auf die Karte verwendet, mit der die Operation durchgeführt werden soll.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2282 Logische Operation I_KV_Card_Handling::discard_Card_Usage_Reference**

Die Schnittstelle I_KV_Card_Handling MUSS die logische Operation discard_Card_Usage_Reference implementieren.

Tabelle 63: Operation discard_Card_Usage_Reference

ENTWURF

I_KV_Card_Handling					Berechtigung: CS, FM, MFM
discard_Card_Usage_Reference	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
Die Operation discard_Card_Usage_Reference bewirkt, dass das n-Tupel, auf das die CardUsageReference verweist, aus der Kartenverwaltung gelöscht wird. Die Karte selbst kann weiterhin einen erhöhten Sicherheitszustand besitzen; er ist lediglich mit dieser CardUsageReference nicht mehr zugänglich. Um den Sicherheitszustand der Karte überhaupt abzubauen, muss die Operation do_Reset aufgerufen werden.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.5.1.7.2 I_KV_Card_Reservation (Provided)

⌦ **TIP1-A_2283 Schnittstelle I_KV_Card_Reservation**

Die Schnittstelle I_KV_Card_Reservation MUSS alle zugehörigen logischen Operationen implementieren.⌫

Diese Schnittstelle ist sowohl im stationären Konnektor vorhanden als auch im MobKT.

⌦ **TIP1-A_2284 Logische Operation I_KV_Card_Reservation::handle_Session**

Die Schnittstelle I_KV_Card_Reservation MUSS die logische Operation handle_Session implementieren.

Tabelle 64: Operation handle_Session

I_KV_Card_Reservation					Berechtigung: FM, MFM
handle_Session	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	LockedMode	OnOffType	IM307	M/H/H
Die Operation handle_Session bewirkt die exklusive Nutzung (LockedMode=ON) einer Smartcard bzw. die Beendigung der exklusiven Nutzung (LockedMode=OFF). Der exklusive Nutzer wird durch den mit *CuRef* assoziierten Aufrufkontext identifiziert. Zugriffe von anderen Akteuren auf diese Karte sind für den Zeitraum der exklusiven Nutzung gesperrt, d.h. sie werden mit einer Fehlermeldung abgewiesen. Bei Beendigung der exklusiven Nutzung bleibt der erreichte Sicherheitszustand erhalten; die exklusive Nutzung dient nur dazu, eine Sequenz von Kartenzugriffen ungestört durchführen zu können. Im Rahmen einer QES muss diese Operation nicht explizit vom Fachmodul aufgerufen werden, da die SAK sich um die Exklusivität der Kartennutzung kümmert.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.5.1.8 Kartenfreischaltung

5.5.1.8.1 I_KV_Card_Unlocking (Provided)

⌦ **TIP1-A_2285 Schnittstelle I_KV_Card_Unlocking**

Die Schnittstelle I_KV_Card_Unlocking MUSS alle zugehörigen logischen Operationen implementieren.⌫

Diese Schnittstelle enthält die Operationen zum Freischalten von Karten mittels PIN oder einseitiger Authentisierung einer Karte durch eine andere sowie die Operationen zum Ändern einer PIN, inkl. Transport-PIN, zum Freischalten einer gesperrten PIN durch die Eingabe des passenden PUK und die Abfrage des PIN-Status. Im stationären Fall kön-

ENTWURF

nen die PIN-Eingabeoperationen wahlweise direkt oder als Remote-PIN durchgeführt werden; am MobKT ist nur die Direkteingabe möglich.

⌦ **TIP1-A_2286 Logische Operation I_KV_Card_Unlocking::verify_PIN**

Die Schnittstelle I_KV_Card_Unlocking MUSS die logische Operation verify_PIN implementieren.

Tabelle 65: Operation verify_PIN

I_KV_Card_Unlocking					Berechtigung: CS, FM, MFM
verify_PIN	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	PinReference	PINReference	IM409	M/H/H
	In	RemotePINQuelle	RessourceIdentifier	IM412	M/M/M
	In	UsageInformation	Text	IM101	SH/SH/SH
Die Operation verify_PIN veranlasst eine Aufforderung am Kartenterminal zur Eingabe der durch *PinReference* bezeichneten PIN - unabhängig davon, ob die PIN zuvor bereits erfolgreich eingegeben und geprüft wurde. Das Kartenterminal übermittelt die PIN zum Verifizieren an die gewählte Karte. Das Prüfergebnis gibt Aufschluss über Erfolg oder Misserfolg der PIN-Verifikation und ggf. die Anzahl der verbleibenden Versuche zur PIN-Eingabe. Hierbei wird vorausgesetzt, dass die Modalitäten der PIN-Eingabe, wie Anzeigetexte, Timeouts o.ä., im Konnektor persistent konfiguriert sind. Andernfalls ist als zusätzlicher Parameter ein Controlblock zu übergeben. Der Nutzer muss über die *UsageInformation* einen Anzeigetext für das Kartenterminal angeben der für die PIN-Eingabe ausweist, welche Anwendung die PIN-Eingabe für welchen Verwendungszweck angestoßen hat. Im Fall des Remote-PIN-Verfahrens wird der Remote-PIN-Sender über den Parameter RemotePINQuelle identifiziert. Fehlt der Parameter RemotePINQuelle wird von lokaler PIN-Eingabe ausgegangen. Als Remote-PIN-Sender wird der Produkttyp gSMC-KT akzeptiert, als Remote-PIN-Empfänger die Produkttypen HBA, SMC-B und HSM-B. Die erwartete Länge der einzugebenden PIN muss dem Nutzer angezeigt werden. Die Eingabezeit für Nutzer zur Eingabe der PIN beträgt mindestens 30 Sekunden. Die Anzahl der maximalen Fehlversuche ist auf drei begrenzt.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: H					

⌫

⌦ **TIP1-A_2287 Logische Operation I_KV_Card_Unlocking::unblock_PIN**

Die Schnittstelle I_KV_Card_Unlocking MUSS die logische Operation unblock_PIN implementieren.

Tabelle 66: Operation unblock_PIN

I_KV_Card_Unlocking					Berechtigung: CS, FM, MFM
unblock_PIN	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	PinReference	PINReference	IM409	M/H/H
	In	OperationMode	OperationMode	IM307	M/H/H
	In	KT_Ident	RessourceIdentifier	IM412	M/M/M
Die Operation unblock_PIN veranlasst das Entsperren einer blockierten PIN. Dabei fordert das Kartenterminal den Nutzer für das Entsperren der PIN des Karteninhabers zur Eingabe eines PUK, für alle anderen PINs zur Eingabe der PIN des Karteninhabers auf . Je nach *OperationMode* kann zur Eingabe einer neuen PIN aufgefordert werden. Für PIN.QES ist jedoch keine neue PIN erlaubt. Bezüglich Eingabemodalitäten (Controlblock) und Remote-PIN gilt das bei verify_PIN Beschriebene. Die Eingabezeit für Nutzer zur Eingabe der PUK oder PIN beträgt mindestens 30 Sekunden.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: N					

⌫

⌦ **TIP1-A_2288 Logische Operation I_KV_Card_Unlocking::initialize_PIN**

ENTWURF

Die Schnittstelle I_KV_Card_Unlocking MUSS die logische Operation initialize_PIN implementieren.

Tabelle 67: Operation initialize_PIN

I_KV_Card_Unlocking					Berechtigung: CS, FM, MFM
initialize_PIN	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	PinReference	PINReference	IM409	M/H/H
	In	KT_Ident	RessourceIdentifier	IM412	M/M/M
	Out	VerificationResult	VerificationResultType	IM420	M/H/H
Die Operation initialize_PIN steuert die Änderung einer Transport-PIN in eine Echt-PIN durch Eingaben des Nutzers am Kartenterminal. Ist die PIN keine Transport-PIN, so bricht die Funktion mit einer Fehlermeldung ab. Bezüglich Eingabe-Modalitäten und Remote-PIN gilt das bei verify_PIN Gesagte. Die Eingabezeit für Nutzer zur Eingabe der PIN beträgt mindestens 30 Sekunden.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: H					

⌫

⌦ **TIP1-A_2289 Logische Operation I_KV_Card_Unlocking::change_PIN**

Die Schnittstelle I_KV_Card_Unlocking MUSS die logische Operation change_PIN implementieren.

Tabelle 68: Operation change_PIN

I_KV_Card_Unlocking					Berechtigung: CS, FM, MFM
change_PIN	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	PinReference	PINReference	IM409	M/H/H
	In	KT_Ident	RessourceIdentifier	IM412	M/M/M
Die Operation change_PIN steuert die Änderung einer PIN durch Eingaben des Nutzers am Kartenterminal. Für eine Änderungserlaubnis wird der Anwender zur Eingabe der PIN des Karteninhabers aufgefordert. Bezüglich Eingabe-Modalitäten und Remote-PIN gilt das bei verify_PIN Beschriebene. Die Eingabezeit für Nutzer zur Eingabe der PIN beträgt mindestens 30 Sekunden.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: H					

⌫

⌦ **TIP1-A_5929 Logische Operation I_KV_Card_Unlocking::enable_PIN**

Die Schnittstelle I_KV_Card_Unlocking MUSS die logische Operation enable_PIN implementieren.

Tabelle 69: Operation enable_PIN

I_KV_Card_Unlocking					Berechtigung: CS, FM, MFM
enable_PIN	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	PinReference	PINReference	IM409	M/H/H
	In	KT_Ident	RessourceIdentifier	IM412	M/M/M
Die Operation enable_PIN steuert die Aktivierung der deaktivierten PIN einer spezifischen Anwendung auf der eGK durch Eingaben des Nutzers am Kartenterminal. Für eine Aktivierungserlaubnis wird der Karteninhaber zur Eingabe seiner PIN aufgefordert. Nach erfolgter Aktivierung der PIN ist ein Zugriff auf die spezifische Anwendung der eGK nur noch nach erfolgreicher PIN-Verifizierung möglich. Bezüglich Eingabe-Modalitäten gilt das bei verify_PIN Beschriebene. Die Eingabezeit für Karteninhaber zur Eingabe der PIN beträgt mindestens 30 Sekunden.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: H					

ENTWURF

⌫

⌦ **TIP1-A_5930 Logische Operation I_KV_Card_Unlocking::disable_PIN**

Die Schnittstelle I_KV_Card_Unlocking MUSS die logische Operation disable_PIN implementieren.

Tabelle 70: Operation disable_PIN

I_KV_Card_Unlocking					Berechtigung: CS, FM, MFM
disable_PIN	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	PinReference	PINReference	IM409	M/H/H
	In	KT_Ident	RessourceIdentifier	IM412	M/M/M
Die Operation disable_PIN steuert die Deaktivierung einer PIN einer spezifischen Anwendung auf der eGK durch Eingaben des Nutzers am Kartenterminal. Für eine Deaktivierungserlaubnis wird der Karteninhaber zur Eingabe seiner PIN aufgefordert. Nach erfolgter Deaktivierung der PIN ist ein Zugriff auf die spezifische Anwendung der eGK ohne PIN-Verifizierung möglich. Bezüglich Eingabe-Modalitäten gilt das bei verify_PIN Beschriebene. Die Eingabezeit für Karteninhaber zur Eingabe der PIN beträgt mindestens 30 Sekunden.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: H					

⌫

⌦ **TIP1-A_2290 Logische Operation I_KV_Card_Unlocking::get_PIN_Status**

Die Schnittstelle I_KV_Card_Unlocking MUSS die logische Operation get_PIN_Status implementieren.

Tabelle 71: Operation get_PIN_Status

I_KV_Card_Unlocking					Berechtigung: CS, FM, MFM
get_PIN_Status	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	PinReference	PINReference	IM409	M/H/H
	Out	StatusInformation	PINStatus	IM408	M/M/M
Die Operation get_PIN_Status liefert den Status der durch *PinReference* bezeichneten PIN einer gewählten Karte. Der PIN-Status enthält Angaben zum Sicherheitszustand, ob sie deaktiviert ist, den verbleibenden PIN-Eingabeversuchen und zum Transportstatus.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: N					

⌫

⌦ **TIP1-A_2292 Logische Operation I_KV_Card_Unlocking::do_C2C**

Die Schnittstelle I_KV_Card_Unlocking MUSS die logische Operation do_C2C implementieren.

Tabelle 72: Operation do_C2C

I_KV_Card_Unlocking					Berechtigung: FM, MFM
do_C2C	Parameter				V, I, A
	In	TargetCardRef	CardUsageReference	IM308	SH/SH/SH
	In	SourceCardRef	CardUsageReference	IM308	SH/SH/SH
	In	C2CMode	C2CType	IM307	M/H/H
Die Operation do_C2C führt eine Card-to-Card-Authentisierung zwischen zwei Smartcards durch. *TargetCardRef* identifiziert die Karte, die freigeschaltet werden soll (z.B. eGK), *SourceCardRef* die freischaltende (z.B. SMC-B). *C2CMode* legt die Art der Authentisierung fest**:**					

ENTWURF

• einseitig, gegenseitig • mit oder ohne Aushandlung von Schlüsseln für einen sicheren Kanal • Authentisierungsart wie z.B. Rollenauthentisierung oder Geräteauthentisierung (entsprechend den auf den Smartcards enthaltenen CV-Zertifikaten). • Optimierte Freischaltung/Authentisierung der eGK bei der die eGK durch die Source freigeschaltet aber durch den Konnektor authentifiziert wird. Folgende Karten setzen dabei die benannten Identitäten ein: Source: HBA: ID.HPC.AUTR_CVC, SMC-B: ID.SMC.AUTR_CVC Target: eGK: ID.eGK.AUT_CVC Eine SMC-B einer Gesellschafterorganisation darf eine eGK nicht freischalten.
Verfügbarkeit: M, Nichtabstreitbarkeit: NA

⌫

5.5.1.9 Komm_Transport

5.5.1.9.1 I_TLS_Client (Provided)

⌦ **TIP1-A_2293 Schnittstelle I_TLS_Client**

Die Schnittstelle I_TLS_Client MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2294 Logische Operation send_Secure (TI-Plattform dezentral)**

Die Schnittstelle I_TLS_Client MUSS die logische Operation send_Secure implementieren.

Tabelle 73: Operation send_Secure

I_TLS_Client					Berechtigung: FM
send_Secure	Parameter				V, I, A
	In	Address	URI	IM304	M/M/M
	In	Identity	RessourceIdentifier	IM412	M/M/M
	In	InData	Binary	IM101	H/H/H
	Out	OutData	Binary	IM101	H/H/H
I_TLS_Client ist die Schnittstelle, über die mit der logischen Operation send_Secure eine durch SM-B authentifizierte TLS-Verbindung zu einem fachanwendungsspezifischen Dienst aufgebaut und genutzt werden kann, um beliebige fachliche Nachrichten zu übertragen. Zur gegenseitigen Authentisierung der Kommunikationspartner und Verschlüsselung der Kommunikationsinhalte können auf Seite des Konnektors die vorhandenen organisationsbezogenen Sicherheitsmodule (SM-B) eingesetzt werden (optionale Client-Authentifizierung). Der fachanwendungsspezifische Dienst verwendet die Identität ID.FD.TLS-S. Diese Identität wird durch die Operation beim Verbindungsaufbau geprüft.					
Verfügbarkeit: H, Nichtabstreitbarkeit: H					

⌫

5.5.1.10 Prüfung_Zertifikat

5.5.1.10.1 I_Cert_Verification (Provided)

⌦ **TIP1-A_2295 Schnittstelle I_Cert_Verification**

Die Schnittstelle I_Cert_Verification MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2296 Logische Operation I_Cert_Verification::verify_Certificate**

ENTWURF

Die Schnittstelle I_Cert_Verification MUSS die logische Operation verify_Certificate implementieren.

Tabelle 74: Operation verify_Certificate

I_Cert_Verification					Berechtigung: CS, FM, MFM
verify_Certificate	Parameter				V, I, A
	In	Certificate	CertificateX.509	IM404	M/M/M
	Out	VerificationResult	VerificationResultType	IM420	M/H/H
	Out	Role	RoleType	IM406	M/H/H
Die Operation kapselt alle relevanten Prüfschritte bzgl. des Zertifikatsstatus, dabei werden mindestens die vier folgenden Prüfschritte durchgeführt: Prüfung auf Zugehörigkeit zum Vertrauensraum durch Abfrage des TSL-Trust-Stores, mathematische Prüfung der Integrität und Signatur des Zertifikats, Prüfung der zeitlichen Gültigkeit durch Abgleich mit der Systemzeit, Prüfung des Revocation-Status durch Abfrage des relevanten OCSP-Responders. Neben dem Ergebnis der Zertifikatsprüfung wird als weiterer Rückgabeparameter die im Zertifikat hinterlegte Rolle an das aufrufende System zurück geliefert. HINWEIS: im Offline-Szenario des mobilen Kartenterminals kann eine Prüfung des Revocation-Status durch Online-Abfrage des relevanten OCSP-Responders nicht erfolgen. Die verbindliche Beschreibung der Schritte erfolgt in [gemKPT_PKI_TIP#6.5]. Die Beschreibung der Prüfschritte der QES-Zertifikatsprüfung erfolgt in [gemKPT_PKI_TIP#6.6]. Der Prüfvorgang selbst kann abhängig von den einzelnen Prüfschritten folgende Status haben: - Prüfvorgang komplett durchgeführt - Prüfvorgang durchgeführt mit Einschränkungen (einzelne Prüfschritte konnten nicht durchgeführt werden) - Prüfvorgang fehlgeschlagen (kritische Prüfschritte konnten nicht durchgeführt werden) Als Prüfergebnis („VerificationResult“) eines durchgeführten Prüfvorgangs sind möglich: - Zertifikat ist gültig - Zertifikat ist gültig mit Einschränkung (Online-Prüfung des Gültigkeitsstatus konnte nicht durchgeführt werden) - Zertifikat ist nicht gültig Fehlgeschlagene Prüfvorgänge können kein Prüfergebnis liefern. Weitere Informationen zu Prüfvorgang, Abbruchbedingungen und deren Auswirkungen auf das Prüfergebnis siehe [gemKPT_PKI_TIP#6.7]. Die Operation muss selbst entscheiden, welche Art der Prüfung (QES, nonQES) vorgenommen wird.					
Verfügbarkeit: M, Nichtabstreitbarkeit: NA					

⌫

5.5.1.11 Verschlüsselung_Entschlüsselung

5.5.1.11.1 I_Crypt_Operations (Provided)

⌦ **TIP1-A_2297 Schnittstelle I_Crypt_Operations**

Die Schnittstelle I_Crypt_Operations MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2298 Logische Operation I_Crypt_Operations::encrypt_Document**

Die Schnittstelle I_Crypt_Operations MUSS die logische Operation encrypt_Document implementieren.

Tabelle 75: Operation encrypt_Document

I_Crypt_Operations					Berechtigung: CS, FM
encrypt_Document	Parameter				V, I, A
	In	Data	DocumentType	IM101	SH/SH/SH
	In	Certificates	List of CertificateX.509	IM404	M/M/M (für ein Zertifikat) M/SH/SH (für die

ENTWURF

					Liste)
	Out	EncryptedData	EncDocumentType	IM105	M/SH/SH
Diese Operation verschlüsselt das übergebene Dokument (*Data*) für alle in der übergebenen Zertifikatliste (*Certificates*) enthaltenen öffentlichen Schlüssel unter Verwendung eines hybriden Verschlüsselungsverfahrens. Dabei wird erst die Gültigkeit der einzelnen Zertifikate durch Nachnutzung der Operation „verify_Certificate“ geprüft. Dies umfasst die Prüfung im Online- wie auch im Offline-Fall. Sollte die Prüfung eines der Zertifikate als nicht gültig ausweisen, bricht die Operation ab. Bei unklarer Statuslage im Offline-Fall arbeitet die Operation weiter, weist aber die nicht erfolgte Online-Prüfung des Status der Zertifikate aber im Ergebnis aus. Nachfolgend wird ein symmetrischer Schlüssel in ausreichender Qualität erzeugt, das Dokument symmetrisch verschlüsselt und ein hybrider Schlüssel für jedes Zertifikat der Liste erzeugt. Die Operation liefert ein verschlüsseltes Dokument (*EncryptedData*) im unten aufgeführten Format zurück. Das Dokument enthält das symmetrisch verschlüsselte Dokument und alle erzeugten hybriden Schlüssel. Es werden die nachfolgenden Dokumententypen mit dem jeweiligen Verschlüsselungsverfahren unterstützt: • Binär, PDF/A und MIME mit CMS • XML (einschließlich der WS-Trust Elemente X.509-Token und SAML-Token) mit XMLEnc Es werden die folgenden kryptographischen Identitäten unterstützt: • eGK: ID.CH.ENC, ID.CH.ENCV für Fachmodule • SMC-B: ID.HCI.ENC für Fachmodule und Clientsysteme • HBA: ID.HP.ENC für Fachmodule und Clientsysteme Die Operation ermöglicht auch die Verschlüsselung für Zertifikate, die nicht aus dem Vertrauensraum der TI stammen, wenn die CA dieser Zertifikate in einem lokalen Trust Store hinterlegt und somit als vertrauenswürdig deklariert wurden. In diesem Fall wird auf eine Statusprüfung für das Verschlüsselungszertifikat verzichtet. Zu nutzen sind zeitlich begrenzt auch die HBA-Vorläuferkarten HBA-qSig und ZOD-2.0 mit ihren für die Verschlüsselung vorgesehenen kryptographischen Identitäten. Die Operation unterstützt mindestens Dokumente bis zu einer Größe von 25 MB.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2299 Logische Operation I_Crypt_Operations::decrypt_Document**

Die Schnittstelle I_Crypt_Operations MUSS die logische Operation decrypt_Document implementieren.

Tabelle 76: Operation decrypt_Document

I_Crypt_Operations					Berechtigung: CS, FM
decrypt_Document	Parameter				V, I, A
	In	EncryptedData	EncDocumentType	IM105	M/SH/SH
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	KeyRef	KeyReference	IM403	M/H/H
	Out	Data	DocumentType	IM101	SH/SH/SH
Diese Operation entschlüsselt das übergebene Dokument (*EncryptedData*) unter Verwendung des referenzierten privaten Schlüssels (*KeyRef*) der entschlüsselnden kryptographischen Identität. Wird kein privater Schlüssel referenziert und lassen Dokumententyp und die dazugehörige Policy dies zu, so ermittelt die Operation die benötigte Identität selber. Anhand der CardUsageReference (*CuRef*) wird die zu verwendende Karte adressiert und die Zugriffsrechte geprüft. Karten, die im Ablauf dieser Operation genutzt werden, befinden sich nach Beendigung der Operation im gleichen Sicherheitszustand, wie vor der Operation. Für die Entschlüsselung des hybriden Schlüssels wird die Operation „decrypt_Data“ nachgenutzt. Die Operation liefert das entschlüsselte Dokument (*Data*) zurück. Es werden die nachfolgenden Dokumententypen mit dem jeweiligen Verschlüsselungsverfahren unterstützt: • Binär, PDF/A und S/MIME mit CMS • XML (einschließlich der WS-Trust Elemente X.509-Token und SAML-Token) mit XMLEnc Es werden die folgenden kryptographischen Identitäten unterstützt: • eGK: ID.CH.ENC, ID.CH.ENCV für Fachmodule • SMC-B: ID.HCI.ENC für Fachmodule und Clientsysteme • HBA: ID.HP.ENC für Fachmodule und Clientsysteme					

ENTWURF

Zu nutzen sind zeitlich begrenzt auch die HBA-Vorläuferkarten HBA-qSig und ZOD-2.0 mit ihren für die Verschlüsselung vorgesehenen kryptographischen Identitäten. Die Operation unterstützt mindestens Dokumente bis zu einer Größe von 25 MB.
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA

⌫

5.5.1.11.2 I_Symm_Crypt_Operations (Provided)

⌦ **TIP1-A_3014 Schnittstelle I_Symm_Crypt_Operations**

Die Schnittstelle I_Symm_Crypt_Operations MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2300 Logische Operation I_Symm_Crypt_Operations::encrypt_Document_Symmetric**

Die Schnittstelle I_Symm_Crypt_Operations MUSS die logische Operation encrypt_Document_Symmetric implementieren.

Tabelle 77: Operation encrypt_Document_Symmetric

I_Symm_Crypt_Operations					Berechtigung: FM
encrypt_Document_Symmetric	Parameter				V, I, A
	In	Data	Binary	IM101	SH/SH/SH
	In	Key	SymmetricKey	IM402	SH/SH/SH
	Out	EncryptedData	EncBinary	IM105	M/SH/SH
	Out	NewKey	SymmetricKey	IM402	SH/SH/SH
Diese Operation verschlüsselt das übergebene Dokument (*Data*) in binärer Darstellung unter Verwendung eines symmetrischen Schlüsselalgorithmus. Dabei kann der zu verwendende Schlüssel (*Key*) optional übergeben werden. Wird kein Schlüssel übergeben, so wird ein Schlüssel in ausreichender Qualität erzeugt (*NewKey*) und mit dem verschlüsselten Dokument (*EncryptedData*) zusammen zurück geliefert. Die Operation unterstützt mindestens Dokumente bis zu einer Größe von 25 MB.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2301 Logische Operation I_Symm_Crypt_Operations::decrypt_Document_Symmetric**

Die Schnittstelle I_Symm_Crypt_Operations MUSS die logische Operation decrypt_Document_Symmetric implementieren.

Tabelle 78: Operation decrypt_Document_Symmetric

I_Symm_Crypt_Operations					Berechtigung: FM
decrypt_Document_Symmetric	Parameter				V, I, A
	In	EncryptedData	EncDocumentType	IM105	M/SH/SH
	In	Key	SymmetricKey	IM402	SH/SH/SH
	Out	Data	DocumentType	IM101	SH/SH/SH
Diese Operation entschlüsselt das übergebene Dokument (*EncryptedData*) in binärer Darstellung unter Verwendung eines symmetrischen Schlüsselalgorithmus. Der zu verwendende Schlüssel (*Key*) wird übergeben. Die Operation liefert das entschlüsselte Dokument (*Data*) zurück. Die Operation unterstützt mindestens Dokumente bis zu einer Größe von 25 MB.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

ENTWURF

5.5.1.12 Rollenmanagement_Identitätsmanagement

5.5.1.12.1 I_Role_Information (Provided)

⌦ **TIP1-A_5784 Schnittstelle I_Role_Information**

Die Schnittstelle I_Role_Information MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_5785 Logische Operation I_Role_Information::get_Role**

Die Schnittstelle I_Role_Information MUSS die logische Operation get_Role implementieren.

Tabelle 79: Operation get_Role

I_Role_Information					Berechtigung: FM
get_Role	Parameter				V, I, A
	In	ResID	RessourceIdentifier	IM412	M/H/H
	Out	Result	Role	IM406	M/H/H
Zur identifizierten Karte (*ResID*) wird die fachliche Rolle ermittelt und zurückgegeben. Die fachlichen Rollen definiert „Tab_ArchTIP_002 Rollenmodell in der Außensicht der TI-Plattform“.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.5.1.13 Verzeichnis_Identitäten

5.5.1.13.1 I_Directory_Query (Provided)

⌦ **TIP1-A_5786 Schnittstelle I_Directory_Query (TI-Plattform Dezentral)**

Die Schnittstelle I_Directory_Query (TI-Plattform Dezentral) MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_5787 Logische Operation I_Directory_Query::search_Directory (TI-Plattform Dezentral)**

Die Schnittstelle I_Directory_Query (TI-Plattform Dezentral) MUSS die logische Operation search_Directory implementieren.

Tabelle 80: Operation search_Directory

I_Directory_Query					Berechtigung: CS, FM
search_Directory	Parameter				V, I, A
	In	Query	DirectoryQuery	IM112	M/H/H
	Out	Result	DirectoryQueryResult	IM113	M/H/H
Das Protokoll zur Verzeichnisabfrage entspricht LDAP (RFC4511). *Query*: Enthält den Filter für die Suchanfrage. *Result*: Enthält das Ergebnis der Verzeichnisabfrage.					
Verfügbarkeit: H, Nichtabstreitbarkeit: N					

⌫

5.5.1.14 Mobile_Offline_Dienste

5.5.1.14.1 I_MobKT_Temp_Storage (Provided)

⌦ **TIP1-A_2302 Schnittstelle I_MobKT_Temp_Storage**

ENTWURF

Die Schnittstelle I_MobKT_Temp_Storage MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2303 Logische Operation I_MobKT_Temp_Storage::read_Data**

Die Schnittstelle I_MobKT_Temp_Storage MUSS die logische Operation read_Data implementieren.

Tabelle 81: Operation read_Data

I_MobKT_Temp_Storage					Berechtigung: MFM
read_Data	Parameter				V, I, A
	In	MFM_ID	MFMType	IM421	M/H/H
	In	Filename	Text	IM110	M/H/H
	Out	Data	Binary	IM101	SH/SH/SH
Diese Operation ermöglicht das Lesen von Daten aus dem Zwischenspeicher des mobilen Kartenterminals. Die Daten werden automatisch entschlüsselt. Eine mögliche Komprimierung der Daten obliegt den Festlegungen der Fachanwendung.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2304 Logische Operation I_MobKT_Temp_Storage::erase_Data**

Die Schnittstelle I_MobKT_Temp_Storage MUSS die logische Operation erase_Data implementieren.

Tabelle 82: Operation erase_Data

I_MobKT_Temp_Storage					Berechtigung: MFM
erase_Data	Parameter				V, I, A
	In	MFM_ID	MFMType	IM421	M/H/H
Diese Operation ermöglicht das Löschen der Daten im Zwischenspeicher des mobilen Kartenterminals für eine Fachanwendung.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2305 Logische Operation I_MobKT_Temp_Storage::write_Data**

Die Schnittstelle I_MobKT_Temp_Storage MUSS die logische Operation write_Data implementieren.

Tabelle 83: Operation write_Data

I_MobKT_Temp_Storage					Berechtigung: MFM
write_Data	Parameter				V, I, A
	In	MFM_ID	MFMType	IM421	M/H/H
	In	Filename	Text	IM110	M/H/H
	In	Data	Binary	IM101	SH/SH/SH
Diese Operation ermöglicht das Schreiben von Daten in den Zwischenspeicher des mobilen Kartenterminals. Die zu speichernden Daten werden automatisch verschlüsselt abgelegt. Eine mögliche Komprimierung der Daten obliegt den Festlegungen der Fachanwendung.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.5.1.14.2 I_MobKT_FMAccess (Provided)

⌦ **TIP1-A_2309 Schnittstelle I_MobKT_FMAccess**

ENTWURF

Die Schnittstelle I_MobKT_FMAccess MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2310 Logische Operation I_MobKT_FMAccess::get_Data**

Die Schnittstelle I_MobKT_FMAccess MUSS die logische Operation get_Data implementieren.

Tabelle 84: Operation get_Data

I_MobKT_FMAccess					Berechtigung: CS
get_Data	Parameter				V, I, A
	In	MFM_ID	MFMType	IM421	M/H/H
	In	Data_Description	DataType	IM101	M/H/H
	Out	Data	Binary	IM101	SH/SH/SH
Diese Operation ermöglicht dem Clientsystems das Lesen von Daten eines mobilen Fachmoduls. Die MobKT-Plattform leitet die Anfrage an das mittels MFM_ID identifizierte mobile Fachmodul via I_MobKT_CommFM::get_Data zur Bearbeitung weiter. Die von dort erhaltene Antwort wird über Data an das aufrufende Clientsystem zurückgeliefert. Die möglichen zulässigen Werte für Data_Description sind daher die Summe der erlaubten Werte, die seitens aller mobilen Fachanwendungen vorgegeben werden. Eine mögliche Komprimierung der Daten obliegt den Festlegungen der Fachanwendung.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2311 Logische Operation I_MobKT_FMAccess::put_Data**

Die Schnittstelle I_MobKT_FMAccess MUSS die logische Operation put_Data implementieren.

Tabelle 85: Operation put_Data

I_MobKT_FMAccess					Berechtigung: CS
put_Data	Parameter				V, I, A
	In	MFM_ID	MFMType	IM421	M/H/H
	In	Data_Description	DataType	IM101	M/H/H
	In	Data	Binary	IM101	SH/SH/SH
Diese Operation ermöglicht dem Clientsystems Daten an ein mobiles Fachmodul zu übertragen. Die MobKT-Plattform leitet die Anfrage an das mittels MFM_ID identifizierte mobile Fachmodul via I_MobKT_CommFM::put_Data zur Bearbeitung weiter. Die möglichen zulässigen Werte für Data_Description sind daher die Summe der erlaubten Werte, die seitens aller mobilen Fachanwendungen vorgegeben werden. Eine mögliche Komprimierung der Daten obliegt den Festlegungen der Fachanwendung.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.5.1.14.3 I_MobKT_CommFM (Required)

⌦ **TIP1-A_2312 Schnittstelle I_MobKT_CommFM**

Die Schnittstelle I_MobKT_CommFM MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2313 Logische Operation I_MobKT_CommFM::get_Data**

Die Schnittstelle I_MobKT_CommFM MUSS die logische Operation get_Data implementieren.

Tabelle 86: Operation get_Data

ENTWURF

I_MobKT_CommFM					Berechtigung: TIP
get_Data	Parameter				V, I, A
	In	Data_Description	DataType	IM101	M/H/H
	Out	Data	Binary	IM101	SH/SH/SH
Diese seitens des mobilen Fachmoduls bereitgestellte Operation liefert die fachspezifischen Daten des mobilen Fachmoduls, die über Data_Description referenziert werden über Data zurück. Eine mögliche Komprimierung der Daten obliegt den Festlegungen der Fachanwendung.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2314 Logische Operation I_MobKT_CommFM::put_Data**

Die Schnittstelle I_MobKT_CommFM MUSS die logische Operation put_Data implementieren.

Tabelle 87: Operation put_Data

I_MobKT_CommFM					Berechtigung: TIP
put_Data	Parameter				V, I, A
	In	Data_Description	DataType	IM101	M/H/H
	In	Data	Binary	IM101	SH/SH/SH
Diese seitens des mobilen Fachmoduls bereitgestellte Operation nimmt die in Data übergebenen fachspezifischen Daten entgegen und verarbeitet sie gemäß Data_Description. Eine mögliche Komprimierung der Daten obliegt den Festlegungen der Fachanwendung.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.5.1.14.4 I_MobKT_GUI (Provided)

⌦ **TIP1-A_2315 Schnittstelle I_MobKT_GUI**

Die Schnittstelle I_MobKT_GUI MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2316 Logische Operation I_MobKT_GUI::show_Data**

Die Schnittstelle I_MobKT_GUI MUSS die logische Operation show_Data implementieren.

Tabelle 88: Operation show_Data

I_MobKT_GUI					Berechtigung: MFM
show_Data	Parameter				V, I, A
	In	MFM_ID	MFMType	IM421	M/H/H
	In	Data	Text	IM101	SH/SH/SH
Diese Operation ermöglicht die Anzeige von Daten am Display des mobilen Kartenterminals. Am Display der MobKT-Plattform werden die vom Fachmodul übergebenen Daten angezeigt. Die Operation steht stellvertretend für alle herstellerspezifischen Funktionen, mittels derer ein mobiles Fachmodul die Ausgaben der graphischen Benutzerschnittstelle befüllen kann. Die Ausprägung der Funktionen ist davon abhängig, welche Möglichkeiten das jeweilige Gerät bietet und welche Interaktionstechnik der MobKT-Hersteller für sein Benutzerinterface vorsieht. Zusammen mit den Funktionen hinter type_Data bilden sie das Framework zur GUI des MobKT					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2317 Logische Operation I_MobKT_GUI::type_Data**

Die Schnittstelle I_MobKT_GUI MUSS die logische Operation type_Data implementieren.

Tabelle 89: Operation type_Data

ENTWURF

I_MobKT_GUI					Berechtigung: MFM
type_Data	Parameter				V, I, A
	In	MFM_ID	MFMType	IM421	M/H/H
	Out	Data	Text	IM101	SH/SH/SH
Diese Operation ermöglicht die Eingabe von Daten mit der Tastatur des mobilen Kartenterminals. Die an der Tastatur eingegebenen Daten werden an das Fachmodul übergeben. Die Operation steht stellvertretend für alle herstellerspezifischen Funktionen, mittels derer ein mobiles Fachmodul Eingaben des Benutzers entgegennehmen kann. Die Ausprägung der Funktionen ist davon abhängig, welche Möglichkeiten das jeweilige Gerät bietet und welche Interaktionstechnik der MobKT-Hersteller für sein Benutzerinterface vorsieht. Zusammen mit den Funktionen von show_Data bilden sie das Framework zur GUI des MobKT.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.5.1.14.5 I_MobKT_Printer (Provided)

⌦ **TIP1-A_2318 Schnittstelle I_MobKT_Printer**

Die Schnittstelle I_MobKT_Printer MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2319 Logische Operation I_MobKT_Printer::print_Document**

Die Schnittstelle I_MobKT_Printer MUSS die logische Operation print_Document implementieren.

Tabelle 90: Operation print_Document

I_MobKT_Printer					Berechtigung: MFM
print_Document	Parameter				V, I, A
	In	PrintData	Text	IM101	SH/SH/SH
Diese Operation ermöglicht das Drucken eines Dokuments über einen am mobilen Kartenterminal angeschlossenen Drucker. Das MobKT stellt dafür die physische Druckerschnittstelle und den Druckertreiber zur Verfügung. Das mobile Fachmodul ist für die Aufbereitung der zu druckenden Daten verantwortlich und übergibt die Druckdaten per PrintData an diese Operation. Ob das MobKT die Druckdaten sequenziell bearbeitet oder einen Druckerspooler bereitstellt ist herstellerspezifisch. Sollte kein Drucker angeschlossen sein, meldet die Operation einen Fehler.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.5.1.14.6 I_MobKT_Management (Provided)

⌦ **TIP1-A_2320 Schnittstelle I_MobKT_Management**

Die Schnittstelle I_MobKT_Management MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2321 Logische Operation I_MobKT_Management::configure_MobKT**

Die Schnittstelle I_MobKT_Management MUSS die logische Operation configure_MobKT implementieren.

Tabelle 91: Operation configure_MobKT

I_MobKT_Management					Berechtigung: A
configure_MobKT	Parameter				V, I, A
	In	InData	ConfigurationData	IM201	M/H/H
	Out	OutData	ConfigurationData	IM201	M/H/H
Diese Operation ermöglicht das Konfigurieren des mobilen Kartenterminals durch den Administrator.					

ENTWURF

Verfügbarkeit: N, Nichtabstreitbarkeit: H

⌫

5.5.2 Infrastrukturdienste

5.5.2.1 Dienstlokalisierung

5.5.2.1.1 I_DNS_Service_Information (Provided)

⌦ **TIP1-A_2322 Schnittstelle I_DNS_Service_Information**

Die Schnittstelle I_DNS_Service_Information MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2323 Logische Operation I_DNS_Service_ Information::get_Service_Information**

Die Schnittstelle I_DNS_Service_Information MUSS die logische Operation get_Service_ Information implementieren.

Tabelle 92: Operation get_Service_Information

I_DNS_Service_Information					Berechtigung: FM
get_Service_ Information	Parameter				V, I, A
	In	Query	Text	IM305	M/M/M
	Out	Address	URI	IM304	M/M/M
Durch eine mit fachlichen Merkmalen parametrisierte Abfrage kann der URI eines Fachdienstes ermittelt werden. ~~Die Operation liefert eine per DNSSEC validierte Antwort.~~					
Verfügbarkeit: H, Nichtabstreitbarkeit: NA					

⌫

5.5.2.2 Namensauflösung

5.5.2.2.1 I_DNS_Name_Information (Provided)

⌦ **TIP1-A_2324 Schnittstelle I_DNS_Name_Information (TI-Plattform Dezentral)**

Die Schnittstelle I_DNS_Name_Information (dezentral) MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2325 Logische Operation I_DNS_Name_Information::get_IP_Address (TI-Plattform Dezentral)**

Die Schnittstelle I_DNS_Name_Information (dezentral) MUSS die logische Operation get_IP_Address implementieren.

Tabelle 93: Operation get_IP_Address

I_DNS_Name_Information					Berechtigung: FM
get_IP_Address	Parameter				V, I, A
	In	Address	FQDN	IM304	M/M/M
	Out	IpAddr	IpAddress	IM304	M/M/M
Diese Operation ermöglicht die Auflösung von FQDN im Namensraum der TI in IP-Adressen. ~~Die Operation liefert eine per DNSSEC validierte Antwort.~~					
Verfügbarkeit: H, Nichtabstreitbarkeit: NA					

ENTWURF

⌫

5.5.2.2.2 I_DNS_Name_Resolution (Provided)

⌦ **TIP1-A_2327 Schnittstelle I_DNS_Name_Resolution**

Die Schnittstelle I_DNS_Name_Resolution MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2328 Logische Operation I_DNS_Name_Resolution::get_IP_Address**

Die Schnittstelle I_DNS_Name_Resolution MUSS die logische Operation get_IP_Address implementieren.

Tabelle 94: Operation get_IP_Address

I_DNS_Name_Resolution					Berechtigung: CS
get_IP_Address	Parameter				V, I, A
	In	Address	FQDN	IM304	M/M/M
	Out	IpAddr	IpAddress	IM304	M/M/M
Diese Operation ermöglicht die Auflösung von FQDN in IP-Adressen. Die Namensräume TI, angeschlossene ~~Bestandsnetze~~ Netze des Gesundheitswesens mit aAdG-NetG und Internet müssen auflösbar sein. Die Namensräume angeschlossene ~~Bestandsnetze~~ Netze des Gesundheitswesens mit aAdG-NetG und Internet werden nur aufgelöst, wenn die zuständigen DNS-Server bekannt sind. ~~Die Operation muss für den TI-Namensraum eine per DNSSEC signierte Antwort liefern.~~					
Verfügbarkeit: H, Nichtabstreitbarkeit: NA					

⌫

5.5.2.3 Zeitinformation

5.5.2.3.1 I_NTP_Time_Information (Provided)

⌦ **TIP1-A_2330 Schnittstelle I_NTP_Time_Information (TI-Plattform Dezentral)**

Die Schnittstelle I_NTP_Time_Information (dezentral) MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2331 Logische Operation I_NTP_Time_Information::sync_Time (TI-Plattform Dezentral)**

Die Schnittstelle I_NTP_Time_Information (dezentral) MUSS die logische Operation sync_Time implementieren.

Tabelle 95: Operation sync_Time

I_NTP_Time_Information					Berechtigung: CS
sync_Time	Parameter				V, I, A
	Out	TimeInformation	Time	IM418	M/H/H
Durch Aufruf dieser Operation erhält das Clientsystem die einheitliche Zeit der TI vom NTP-Server (dezentral).					
Verfügbarkeit: M, Nichtabstreitbarkeit: NA					

⌫

5.5.2.3.2 I_Synchronised_System_Time (Provided)

⌦ **TIP1-A_2332 Schnittstelle I_Synchronised_System_Time**

ENTWURF

Die Schnittstelle I_Synchronised_System_Time MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2333 Logische Operation I_Synchronised_System_Time::get_Time**

Die Schnittstelle I_Synchronised_System_Time MUSS die logische Operation get_Time implementieren.

Tabelle 96: Operation get_Time

I_Synchronised_System_Time					Berechtigung: FM, MFM
get_Time	Parameter				V, I, A
	Out	TimeInformation	Time	IM418	M/H/H
Durch Aufruf dieser Operation erhält das Fachmodul die aktuelle Zeitinformation vom Betriebssystem.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.5.2.3.3 I_Change_System_Time (Provided)

⌦ **TIP1-A_2334 Schnittstelle I_Change_System_Time**

Die Schnittstelle I_Change_System_Time MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2335 Logische Operation I_Change_System_Time::set_System_Time**

Die Schnittstelle I_Synchronised_System_Time MUSS die logische Operation set_System_Time implementieren.

Tabelle 97: Operation set_System_Time

I_Change_System_Time					Berechtigung: A
set_System_Time	Parameter				V, I, A
	In	TimeInformation	Time	IM418	M/H/H
Durch Aufruf dieser Operation wird die Systemzeit auf den übergebenen Wert geändert.					
Verfügbarkeit: N, Nichtabstreitbarkeit: H					

⌫

5.5.2.4 Kartennutzung

5.5.2.4.1 I_KV_Card_Operations (Provided)

⌦ **TIP1-A_2336 Schnittstelle I_KV_Card_Operations**

Die Schnittstelle I_KV_Card_Operations MUSS alle zugehörigen logischen Operationen implementieren.⌫

Diese Schnittstelle enthält kartennahe Zugriffskommandos und Sequenzen solcher Kommandos, die als komplexe Operationen gekapselt sind.

⌦ **TIP1-A_2337 Logische Operation I_KV_Card_Operations::extract_card_data**

Die Schnittstelle I_KV_Card_Operations MUSS die logische Operation extract_card_data implementieren.

Tabelle 98: Operation extract_card_data

I_KV_Card_Operations	Berechtigung: FM

ENTWURF

extract_card_data	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	Out	Data	Text	IM101	SH/SH/SH
Die Operation extract_card_data liefert Informationen (*Data*) zu einem ausgewählten Zertifikat der bestimmten Karte (*CuRef*). Welches Zertifikat für eine bestimmte Art von Karten genutzt wird, wird durch die TI-Plattform festgelegt. Beispiele: Institutionskennzeichen (Krankenkassen-ID) von der eGK, Rollenprofil der Institutskarte.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2338 Logische Operation I_KV_Card_Operations::read_Card_Data**

Die Schnittstelle I_KV_Card_Operations MUSS die logische Operation read_Card_Data implementieren.

Tabelle 99: Operation read_Card_Data

I_KV_Card_Operations					Berechtigung: FM, MFM
read_Card_Data	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	pathToData	CardDataPath	IM101	M/M/M
	In	cardDataDetails	CardDataDetails	IM101	M/M/M
	Out	Data	Binary	IM101	SH/SH/SH
Die Operation read_Card_Data liest Fachdaten von der eGK, die durch die CardUsageReference (*CuRef*) identifiziert wird. Der Parameter pathToData beschreibt die Datei, aus der die Daten gelesen werden sollen. Position und Länge der Daten bzw. Record-Nummer sind im Parameter CardDataDetails enthalten.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2339 Logische Operation I_KV_Card_Operations::read_KVK**

Die Schnittstelle I_KV_Card_Operations MUSS die logische Operation read_KVK implementieren.

Tabelle 100: Operation read_KVK

I_KV_Card_Operations					Berechtigung: FM, MFM
read_KVK	Parameter				V, I, A
	In	ResID	RessourceIdentifier	IM412	M/H/H
	Out	Data	ASN.1	IM101	SH/SH/SH
Die Operation liest die Daten einer ausgewählten KVK.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: N					

⌫

⌦ **TIP1-A_2340 Logische Operation I_KV_Card_Operations::write_Card_Data**

Die Schnittstelle I_KV_Card_Operations MUSS die logische Operation write_Card_Data implementieren.

Tabelle 101: Operation write_Card_Data

I_KV_Card_Operations					Berechtigung: FM
write_Card_Data	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	pathToData	CardDataPath	IM101	M/M/M
	In	cardDataDetails	CardDataDetails	IM101	M/M/M
	In	Data	Binary	IM101	SH/SH/SH
Die Operation write_Card_Data schreibt Fachdaten auf die eGK, die durch die CardUsageReference					

ENTWURF

(*CuRef*) identifiziert wird. Der Parameter pathToData beschreibt die Datei, in die die Daten geschrieben werden sollen. Position und Länge der Daten bzw. Record-Nummer sind im Parameter CardDataDetails enthalten.
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA

⌫

⌦ **TIP1-A_5799 Logische Operation I_KV_Card_Operations::erase_Card_Data**

Die Schnittstelle I_KV_Card_Operations MUSS die logische Operation erase_Card_Data implementieren.

Tabelle 102: Operation erase_Card_Data

I_KV_Card_Operations					Berechtigung: FM
erase_Card_Data	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	pathToData	CardDataPath	IM101	M/M/M
Die Operation erase_Card_Data löscht Fachdaten von der eGK, die durch die CardUsageReference (*CuRef*) identifiziert wird. Der Parameter pathToData identifiziert die transparente Datei der Smartcard bzw. den Record einer strukturierten Datei der eGK. Die Operation löscht jeweils vollständig den Inhalt der ausgewählten transparenten Datei bzw. des ausgewählten Records.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2341 Logische Operation I_KV_Card_Operations::verify_eGK**

Die Schnittstelle I_KV_Card_Operations MUSS die logische Operation verify_eGK implementieren.

Tabelle 103: Operation verify_eGK

I_KV_Card_Operations					Berechtigung: FM, MFM
verify_eGK	Parameter				V, I, A
	In	ResID	RessourceIdentifier	IM412	M/H/H
	Out	VerificationResult	VerificationResultType	IM420	M/H/H
Die Operation verify_eGK prüft, ob die über *ResId* identifizierte eGK in technischer Hinsicht gültig ist. Die eGK ist gültig, wenn: • der HCA-Ordner der eGK aktiv (nicht gesperrt) ist • das AUT-Zertifikat der eGK gültig ist. Dabei wird das AUT-Zertifikat durch die Operation verify_Certificate des Interfaces I_Cert_Verification geprüft. Die technische Nutzbarkeit der eGK sagt nichts über die vertragliche Gültigkeit der eGK aus.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2342 Logische Operation I_KV_Card_Operations::write_eGK_Protocol**

Die Schnittstelle I_KV_Card_Operations MUSS die logische Operation write_eGK_Protocol implementieren.

Tabelle 104: Operation write_eGK_Protocol

I_KV_Card_Operations					Berechtigung: FM, MFM
write_eGK_Protocol	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	accessProtocolEntry	AccessProtocolEntry	IM101	SH/SH/SH
Die Operation write_eGK_Protocol schreibt den Protokolleintrag accessProtocolEntry auf die eGK, die durch *CuRef* identifiziert wird. Voraussetzung ist, dass durch eine vorangegangene C2C-Authentisierung bereits der benötige Sicherheitszustand hergestellt wurde.					
Verfügbarkeit: M, Nichtabstreitbarkeit: H					

ENTWURF

⌫

⌦ **TIP1-A_7023 Logische Operation I_KV_Card_Operations::read_eGK_Protocol**

Die Schnittstelle I_KV_Card_Operations MUSS die logische Operation read_eGK_Protocol implementieren.

Tabelle 105: Operation read_eGK_Protocol

I_KV_Card_Operations					Berechtigung: FM
read_eGK_Protocol	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	Out	accessProtocol	List of AccessProtocolEntry	IM101	SH/SH/SH (AccessProtocolEntry) SH/SH/SH (Liste)
Die Operation read_eGK_Protocol liefert das Zugriffsprotokoll der eGK, die durch *CuRef* identifiziert wird. Voraussetzung ist, dass vorher bereits der benötigte Sicherheitszustand der eGK hergestellt wurde.					
Verfügbarkeit: M, Nichtabstreitbarkeit: M					

⌫

⌦ **TIP1-A_2343 Logische Operation I_KV_Card_Operations::decrypt_Data**

Die Schnittstelle I_KV_Card_Operations MUSS die logische Operation decrypt_Data implementieren.

Tabelle 106: Operation decrypt_Data

I_KV_Card_Operations					Berechtigung: FM, MFM
decrypt_Data	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	KeyRef	KeyReference	IM403	M/H/H
	In	AlgID	AlgorithmIdentifier	IM305	M/M/M
	In	ciphertext	Binary	IM105	M/SH/SH
	Out	plaintext	Binary	IM101	SH/SH/SH
Die Operation decrypt_Data entschlüsselt Binärdaten mit einem privaten Schlüssel (*KeyRef*) und nach einem der für diesen Schlüssel erlaubten Algorithmen (*AlgID*) einer ausgewählten Smartcard (*CuRef*). Nach Möglichkeit sollten Fachmodule jedoch die höherwertige Operation decrypt_Document des Interfaces I_Crypt_Operations verwenden, die decrypt_Data nutzt.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2344 Logische Operation I_KV_Card_Operations::sign_Data**

Die Schnittstelle I_KV_Card_Operations MUSS die logische Operation sign_Data implementieren.

Tabelle 107: Operation sign_Data

I_KV_Card_Operations					Berechtigung: FM, MFM
sign_Data	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	KeyRef	KeyReference	IM403	M/H/H
	In	AlgID	AlgorithmIdentifier	IM305	M/M/M
	In	DataToBeSigned	Binary	IM101	SH/SH/SH
	Out	Data	Binary	IM103	SH/M/M
Low-Level-Operation zum Signieren von Binärdaten mittels einer ausgewählten Smartcard. Nach					

ENTWURF

Möglichkeit sollten Fachmodule jedoch die höherwertigen Operationen sign_Document des Interfaces I_Sign_Operations oder sign_Document_QES des Interfaces I_SAK_Operations verwenden.
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA

⌫

⌦ **TIP1-A_7024 Logische Operation I_KV_Card_Operations::get_Random**

Die Schnittstelle I_KV_Card_Operations MUSS die logische Operation get_Random implementieren.

Tabelle 108: Operation get_Random

I_KV_Card_Operations					Berechtigung: FM
get_Random	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	Out	RandomValue	Binary	IM103	SH/SH/SH
Die Operation get_Random liefert eine Zufallszahl (*RandomValue*) hoher Qualität von der, durch *CuRef* identifizierten Smartcard. Die Qualität der Zufallszahl und damit der mögliche Verwendungszweck kann sich zwischen verschiedenen Karten der TI unterscheiden.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2345 Logische Operation I_KV_Card_Operations::send_APDU**

Die Schnittstelle I_KV_Card_Operations MUSS die logische Operation send_APDU implementieren.

Tabelle 109: Operation send_APDU

I_KV_Card_Operations					Berechtigung: FM
send_APDU	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
	In	CommandAPDU	APDU_K	IM422	SH/SH/SH
	Out	ResponseAPDU	APDU_R	IM423	SH/SH/SH
Low-Level-Operation zum Senden von Kartenkommandos (APDU) an die Karte. Nach Möglichkeit sollten Fachmodule jedoch die höherwertigen Operationen des Interfaces I_KV_Card_Operations verwenden. Die Komponenten HSM-B implementiert diese Operation nicht.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2346 Logische Operation I_KV_Card_Operations::do_Reset**

Die Schnittstelle I_KV_Card_Operations MUSS die logische Operation do_Reset implementieren.

Tabelle 110: Operation do_Reset

I_KV_Card_Operations					Berechtigung: FM
do_Reset	Parameter				V, I, A
	In	CuRef	CardUsageReference	IM308	SH/SH/SH
Low-Level-Operation zur Durchführung eines Resets einer selektierten Smartcard. Das Reset unterbricht ein eventuell mit dieser Karte laufendes C2C.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

ENTWURF

5.5.2.5 Kartenterminalverwaltung

5.5.2.5.1 I_KTV_Management (Provided)

⌦ **TIP1-A_2347 Schnittstelle I_KTV_Management**

Die Schnittstelle I_KTV_Management MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2348 Logische Operation I_KTV_Management::configure_KTs**

Die Schnittstelle I_KTV_Management MUSS die logische Operation configure_KTs implementieren.

Tabelle 111: Operation configure_KTs

I_KTV_Management					Berechtigung: A
configure_KTs	Parameter				V, I, A
	In	Data	ConfigurationData	IM201	M/M/M
	In	KT_Ident	RessourceIdentifier	IM412	M/M/M
Die Operation configure_KTs ermöglicht einem Administrator die Verwaltung der Kartenterminals im Netz. Dazu gehört: • Hinzufügen und Entfernen von Kartenterminals, • Durchführen des Pairings • Aktivieren / Deaktivieren von Kartenterminals ConfigurationData steht konzeptionell für alle Parameter, die dafür erforderlich sind. Die genaue Ausgestaltung der Administrationsschnittstelle wird erst im Rahmen der Spezifikation festgelegt.					
Verfügbarkeit: N, Nichtabstreitbarkeit: H					

⌫

5.5.2.5.2 I_KT_Communication (Provided)

⌦ **TIP1-A_2349 Schnittstelle I_KT_Communication**

Die Schnittstelle I_KT_Communication MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2350 Logische Operation I_KT_Communication::perform_Command**

Die Schnittstelle I_KT_Communication MUSS die logische Operation perform_Command implementieren.

Tabelle 112: Operation perform_Command

I_KT_Communication					Berechtigung: TIP
perform_Command	Parameter				V, I, A
	In	APDU_K	CommandAPDU	IM422	SH/SH/SH
	Out	APDU_R	ResponseAPDU	IM423	SH/SH/SH
Die Operation perform_Command bewirkt die Ausführung von Terminalkommandos. Sie steht als generische Operation für alle Kommandos, die an das Kartenterminal selbst gerichtet sind, z.B. request_icc, perform verification. Antwortzeiten werden zu den nachnutzenden Operationen angegeben. Aufgrund des Bestandsschutzes wird dieses Kommando durch die entsprechenden SICCT-Kommandos umgesetzt.					
Verfügbarkeit: M, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2351 Logische Operation I_KT_Communication::transfer_APDU**

ENTWURF

Die Schnittstelle I_KT_Communication MUSS die logische Operation transfer_APDU implementieren.

Tabelle 113: Operation transfer_APDU

I_KT_Communication					Berechtigung: TIP
transfer_APDU	Parameter				V, I, A
	In	APDU_K	CommandAPDU	IM422	SH/SH/SH
	Out	APDU_R	ResponseAPDU	IM423	SH/SH/SH
Die Operation transfer_APDU bewirkt die Weiterleitung der APDUs an die Karten. Aufgrund des Bestandsschutzes wird dieses Kommando entsprechend dem SICCT-Standard umgesetzt.					
Verfügbarkeit: M, Nichtabstreitbarkeit: NA					

⌫

5.5.2.6 Datenspeicher_FM

5.5.2.6.1 I_Local_Storage (Provided)

⌦ **TIP1-A_5800 Schnittstelle I_Local_Storage**

Die Schnittstelle I_Local_Storage MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_5801 Logische Operation I_Local_Storage::write_Data**

Die Schnittstelle I_Local_Storage MUSS die logische Operation write_Data implementieren.

Tabelle 114: Operation write_Data

I_Local_Storage					Berechtigung: FM
write_Data	Parameter				V, I, A
	In	DataKey	Text	IM110	M,H,H
	In	Data	Binary	IM101	SH,SH,SH
Die Daten (Data) werden unter einem zugehörigen Schlüssel (DataKey) lokal abgespeichert. Es wird sichergestellt, dass die Daten nur dem Fachmodul zugänglich sind, welches sie erzeugt hat.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_5802 Logische Operation I_Local_Storage::read_Data**

Die Schnittstelle I_Local_Storage MUSS die logische Operation read_Data implementieren.

Tabelle 115: Operation read_Data

I_Local_Storage					Berechtigung: FM
read_Data	Parameter				V, I, A
	In	DataKey	Text	IM110	M,H,H
	Out	Data	Binary	IM101	SH,SH,SH
Die Daten (Data), die unter einem zugehörigen Schlüssel (DataKey) lokal gespeichert sind, werden zurückgegeben. Es wird sichergestellt, dass die Daten nur dem Fachmodul zugänglich sind, welches sie erzeugt hat.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_5803 Logische Operation I_Local_Storage::erase_Data**

ENTWURF

Die Schnittstelle I_Local_Storage MUSS die logische Operation erase_Data implementieren.

Tabelle 116: Operation erase_Data

I_Local_Storage					Berechtigung: FM
erase_Data	Parameter				V, I, A
	In	DataKey	Text	IM110	M,H,H
Die Daten (Data), die unter einem zugehörigen Schlüssel (DataKey) lokal gespeichert sind, werden gelöscht. Es wird sichergestellt, dass die Daten nur von dem Fachmodul gelöscht werden können, welches sie erzeugt hat.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.5.3 Netzwerkdienste

5.5.3.1 Datentransport/Sichere Online-Anbindung/Sicherer Internetzugang

5.5.3.1.1 I_IP_Transport (Provided)

⌦ **TIP1-A_2352 Schnittstelle I_IP_Transport (TI-Plattform Dezentral)**

Die Schnittstelle I_IP_Transport (dezentral) MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2353 Logische Operation I_IP_Transport::send_Data_TI (TI-Plattform Dezentral)**

Die Schnittstelle I_IP_Transport (dezentral) MUSS die logische Operation send_Data_TI implementieren.

Tabelle 117: Operation send_Data_TI

I_IP_Transport					Berechtigung: CS, FM
send_Data_TI	Parameter				V, I, A
	In	IpAddr	IpAddress	IM304	M/M/M
	In	InData	Binary	IM101	M/M/M
	Out	OutData	Binary	IM101	M/M/M
Diese Operation ermöglicht das Senden und Empfangen von IP-Paketen zwischen Clients / Fachmodulen und fachanwendungsspezifischen Diensten. Clients können dabei nur mit offenen fachanwendungsspezifischen Diensten kommunizieren, wohingehend Fachmodule mit offenen und gesicherten fachanwendungsspezifischen Diensten kommunizieren können. Es erfolgt eine Kontrolle und Filterung des Datenverkehrs über einen konfigurierbaren Paketfilter mit Stateful Inspection. Aufgrund der Nutzung von IPv4 erfolgt eine IP-Adressumsetzung (NAT). Wenn höhere Sicherheitsanforderungen bestehen als durch diese Operation zugesichert sind, so müssen entsprechende Maßnahmen auf den darüberliegenden Protokollschichten erbracht werden (z. B. durch Einsatz von TLS).					
Verfügbarkeit: H, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_3676 Logische Operation I_IP_Transport::send_Data_External (TI-Plattform Dezentral)**

Die Schnittstelle I_IP_Transport (dezentral) MUSS die logische Operation send_Data_External implementieren.

ENTWURF

Tabelle 118: Operation send_Data_External

I_IP_Transport					Berechtigung: CS
send_Data_External	Parameter				V, I, A
	In	IpAddr	IpAddress	IM304	NA/NA/NA
	In	InData	Binary	IM101	NA/NA/NA
	Out	OutData	Binary	IM101	NA/NA/NA
Diese Operation ermöglicht das Senden und Empfangen von IP-Paketen zur Nutzung der ~~Bestandsnetzanbindung~~ angebundenen Netze mit aAdG-NetG, zur Nutzung des sicheren Internetzugangs und zur Weiternutzung vorhandener Internetzugänge. Die IP-Pakete werden an die jeweiligen Adressräume weitergeleitet. Eine Weiterleitung von IP-Paketen für den sicheren Internetzugang erfolgt nur, wenn der separate VPN-Kanal für den sicheren Internetzugang konfiguriert ist. Die Unterstützung der Weiternutzung vorhandener Internetzugänge beschränkt sich darauf, dass diese Operation • den Internetverkehr verwirft, wenn kein sicherer Internetzugang konfiguriert ist oder • dem Client mitteilt, über welches Gateway er diesen Verkehr versenden kann, wenn ein solches Gateway verfügbar ist. Es erfolgt eine Kontrolle und Filterung des Datenverkehrs über einen konfigurierbaren Paketfilter mit Stateful Inspection. Aufgrund der Nutzung von IPv4 erfolgt eine IP-Adressumsetzung (NAT).					
Verfügbarkeit: N, Nichtabstreitbarkeit: NA					

⌫

5.5.3.2 Sichere_Anbindung_Client

5.5.3.2.1 I_Facade_Access_Configuration

⌦ **TIP1-A_2354 Schnittstelle I_Facade_Access_Configuration**

Die Schnittstelle I_Facade_Access_Configuration MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2355 Logische Operation I_Facade_Access_Configuration::set_CS_Access_Mode**

Die Schnittstelle I_Facade_Access_Configuration MUSS die logische Operation set_CS_Access_Mode implementieren.

Tabelle 119: Operation set_CS_Access_Mode

I_Facade_Access_Configuration					Berechtigung: A
set_CS_Access_Mode	Parameter				V, I, A
	In	CSAM	CSAccessMode	IM307	M/H/H
Über diese Operation legt der Administrator über den Parameter CSAM fest, ob Clientsysteme • über eine vertrauliche Server-authentisierte Verbindung (server-authenticated) • über eine vertrauliche beidseitig authentisierte Verbindung (mutual-authenticated) • über eine nicht gesicherte Verbindung (unsecured) auf die Schnittstellen des Produkttyps zugreifen dürfen. Wenn der Zugriffsmodus auf „mutual-authenticated“ gesetzt wird, so kann über die Operationen add_Clientsystem und remove_Clientsystem festgelegt werden, welche Clients auf Basisdienste der TI-Plattform zugreifen dürfen. Für die beiden anderen Zugriffsmodi gilt, dass jedes Clientsystem Zugriff auf die Basisdienste hat. Bei eine Vertraulichen Verbindung authentisiert sich die TI-Plattform mit der Identität ID.AK.AUT.					
Verfügbarkeit: N, Nichtabstreitbarkeit: H					

⌫

⌦ **TIP1-A_2356 Logische Operation I_Facade_Access_Configuration::add_Clientsystem**

Die Schnittstelle I_Facade_Access_Configuration MUSS die logische Operation add_Clientsystem implementieren.

ENTWURF

Tabelle 120: Operation add_Clientsystem

I_Facade_Access_Configuration					Berechtigung: A
add_Clientsystem	Parameter				V, I, A
	In	CS	ClientsystemIdentifier	IM202	M/H/H
Die Operation nimmt das über Parameter CS identifizierbare Clientsystem in die Liste der zugriffsberechtigten Clientsysteme auf (Platzhalter sind in der Festlegung zum Identifier explizit gestattet, inkl. „all“). Nur den Clientsystemen, die sich in der so gefüllten Liste der zugriffsberechtigten Clientsysteme befinden, wird ein Zugriff auf die Basisdienste der TI-Plattform gewährleistet.					
Verfügbarkeit: N, Nichtabstreitbarkeit: H					

⌫

⌦ **TIP1-A_2357 Logische Operation I_Facade_Access_Configuration::remove_Clientsystem**

Die Schnittstelle I_Facade_Access_Configuration MUSS die logische Operation remove_Clientsystem implementieren.

Tabelle 121: Operation remove_Clientsystem

I_Facade_Access_Configuration					Berechtigung: A
remove_Clientsystem	Parameter				V, I, A
	In	CS	ClientsystemIdentifier	IM202	M/H/H
Die Operation nimmt das über CS identifizierbare Clientsystem aus der Liste der zugriffsberechtigten Clientsysteme (bei CS muss es sich um einen existierenden Eintrag der Liste handeln).					
Verfügbarkeit: N, Nichtabstreitbarkeit: H					

⌫

5.6 Interfaces der TI-Plattform Zentral

5.6.1 Basisdienste

5.6.1.1 KSR

5.6.1.1.1 I_KSRS_Download (Provided)

⌦ **TIP1-A_2358 Schnittstelle I_KSRS_Download**

Die Schnittstelle I_KSRS_Download MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2359 Logische Operation I_KSRS_Download::list_Updates**

Die Schnittstelle I_KSRS_Download MUSS die logische Operation list_Updates implementieren.

Tabelle 122: Operation list_Updates

I_KSRS_Download					Berechtigung: TIP
list_Updates	Parameter				V, I, A
	In	ClientType	KSRClientType	IM413	M/M/M
	In	ClientStatus	KSRClientStatus	IM414	M/H/H
	Out	AvailableUpdates	List of UpdateIdentifier	IM417	M/H/H (für ein UpdateIdentifier) M/H/H (für die Liste)

ENTWURF

Die Operation listet die auf einem KSR-Server verfügbaren Updates (AvailableUpdates) für eine dezentrale Komponente der TI-Plattform oder ein Fachmodul (ClientType) und für einen bestimmten Update-Status (ClientStatus) auf.
Verfügbarkeit: M, Nichtabstreitbarkeit: NA

⌫

⌦ **TIP1-A_2360 Logische Operation I_KSRS_Download::get_Updates**

Die Schnittstelle I_KSRS_Download MUSS die logische Operation get_Updates implementieren.

Tabelle 123: Operation get_Updates

I_KSRS_Download					Berechtigung: TIP
get_Updates	Parameter				V, I, A
	In	ClientType	KSRClientType	IM413	M/M/M
	In	UpdateIdentifier	UpdateIdentifier	IM417	M/H/H
	Out	UpdatePackage	UpdatePackage	IM416	M/M/M
Die Operation stellt die Übertragung eines Aktualisierungspakets (UpdatePackage) für eine dezentrale Komponente der TI-Plattform oder ein Fachmodul (ClientType) zur Verfügung. Die Auswahl des Aktualisierungspakets auf dem KSR-Server erfolgt auf Grundlage einer Update-Identifikation (UpdateIdentifier).					
Verfügbarkeit: M, Nichtabstreitbarkeit: NA					

⌫

5.6.1.2 Komm_Transport

5.6.1.2.1 I_TLS (Required)

⌦ **TIP1-A_2361 Schnittstelle I_TLS**

Die Schnittstelle I_TLS MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2362 Logische Operation I_TLS::send_Secure**

Die Schnittstelle I_TLS MUSS die logische Operation send_Secure implementieren.

Tabelle 124: Operation send_Secure

I_TLS					Berechtigung: TIP
send_Secure	Parameter				V, I, A
	In	InData	Binary	IM101	H/H/H
	Out	OutData	Binary	IM101	H/H/H
Benötigter Endpunkt am fachanwendungsspezifischen Dienst. Über die Operation send_Secure kann sicher mit dem fachanwendungsspezifischen Dienst kommuniziert werden. Dabei erfolgt beim Verbindungsaufbau eine Server- und Client-Authentifizierung.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.6.1.3 Konnektorregistrierung

5.6.1.3.1 I_Registration_Service (Provided)

⌦ **TIP1-A_5076 Schnittstelle I_Registration_Service**

Die Schnittstelle I_Registration_Service MUSS alle zugehörigen logischen Operationen implementieren.⌫

ENTWURF

⌦ **TIP1-A_5077 Logische Operation I_Registration_Service::register**

Die Schnittstelle I_Registration_Service MUSS die logische Operation register implementieren.

Tabelle 125: Operation register

I_Registration_Service					Berechtigung: A
register	Parameter				V, I, A
	In	KonCertificate	CertificateX.509	IM404	M/M/M
	In	ContractID	Text	IM101	M/M/M
	Out	RegStatus	Text	IM101	M/M/M
	Out	ContractStatus	Text	IM101	M/M/M
	Out	AdditionalInfo	Text	IM101	H/H/H
Die Operation ermöglicht die Registrierung eines Konnektors beim VPN-Zugangsdienst. Erst nach erfolgreicher Registrierung werden Datenpakete des Konnektors in das zentrale Netz weitergeleitet. Der Konnektor übermittelt das Zertifikat der Identität ID.NK.VPN (*KonCertificate*) und eine vom VPN-Zugangsdienst bereitgestellte eindeutige Vertrags-ID (*ContractID*) an den VPN-Zugangsdienst. Die übermittelten Daten sind mit der Identität ID.HCI.OSIG signiert, um nachzuweisen, dass der Konnektor in einem Leistungserbringer- oder Kostenträgerumfeld eingesetzt wird. Nach Prüfung der Gültigkeit des Konnektorzertifikats, der bestehenden Vertragsbeziehung und der Signatur der Daten mit der SMC-B wird der Konnektor für den Zugriff auf das zentrale Netz freigeschaltet. Als Ergebnis der Operation werden der Registrierungsstatus (*RegStatus*) und der Vertragstatus (*ContractStatus*) übermittelt. Es besteht auch die Möglichkeit weitere Informationen (*AdditionalInfo*) in Textform zu übermitteln.					
Verfügbarkeit: M, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_5078 Logische Operation I_Registration_Service::deregister**

Die Schnittstelle I_Registration_Service MUSS die logische Operation deregister implementieren.

Tabelle 126: Operation deregister

I_Registration_Service					Berechtigung: A
deregister	Parameter				V, I, A
	In	KonCertificate	CertificateX.509	IM404	M/M/M
	In	ContractID	Text	IM101	M/M/M
	Out	RegStatus	Text	IM101	M/M/M
	Out	ContractStatus	Text	IM101	M/M/M
	Out	AdditionalInfo	Text	IM101	H/H/H
Die Operation ermöglicht die Deregistrierung eines Konnektors beim VPN-Zugangsdienst. Nach erfolgreicher Registrierung werden Datenpakete des Konnektors nicht mehr in das zentrale Netz weiter geleitet. Der Konnektor übermittelt das Zertifikat der Identität ID.NK.VPN (*KonCertificate*) und eine vom VPN-Zugangsdienst bereitgestellte eindeutige Vertrags-ID (*ContractID*) an den VPN-Zugangsdienst. Die übermittelten Daten sind mit der Identität ID.HCI.OSIG signiert, um nachzuweisen, dass der Konnektor in einem Leistungserbringer- oder Kostenträgerumfeld eingesetzt wird. Nach Prüfung der Gültigkeit des Konnektorzertifikats, der bestehenden Vertragsbeziehung und der Signatur der Daten mit der SMC-B wird der zugriff des Konnektors auf das zentrale Netz gesperrt. Als Ergebnis der Operation werden der neue Registrierungsstatus (*RegStatus*) und der Vertragstatus (*ContractStatus*) übermittelt. Es besteht auch die Möglichkeit weitere Informationen (*AdditionalInfo*) in Textform zu übermitteln.					
Verfügbarkeit: H, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_5079 Logische Operation I_Registration_Service::get_Status**

Die Schnittstelle I_Registration_Service MUSS die logische Operation get_Status implementieren.

Tabelle 127: Operation get_Status

ENTWURF

I_Registration_Service					Berechtigung: A
get_Status	Parameter				V, I, A
	In	KonCertificate	CertificateX.509	IM404	M/M/M
	Out	Timestamp	Text	IM101	M/M/M
	Out	RegStatus	Text	IM101	M/M/M
	Out	ContractStatus	Text	IM101	M/M/M
	Out	AdditionalInfo	Text	IM101	H/H/H
Die Operation ermöglicht die aktuellen Registrierungsinformationen eines Konnektors beim VPN-Zugangsdienst abzufragen. Der Konnektor übermittelt das Zertifikat der Identität ID.NK.VPN (*KonCertificate*) an den VPN-Zugangsdienst. Nach Prüfung der Gültigkeit des Konnektorzertifikats und der bestehenden Vertragsbeziehung werden die entsprechenden Informationen gemeldet. Als Ergebnis der Operation werden der Registrierungsstatus (*RegStatus*) und der Vertragstatus (*ContractStatus*) übermittelt. Es besteht auch die Möglichkeit weitere Informationen (*AdditionalInfo*) in Textform zu übermitteln.					
Verfügbarkeit: KS, Nichtabstreitbarkeit: NA					

⌫

5.6.1.4 Verzeichnis_Identitäten

5.6.1.4.1 I_Directory_Query (Provided)

⌦ **TIP1-A_5804 Die Schnittstelle I_Directory_Query (TI-Plattform Zentral)**

Die Schnittstelle I_Directory_Query (TI-Plattform Zentral) MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_5805 Die Schnittstelle I_Directory_Query::search_Directory**

Die Schnittstelle I_Directory_Query (TI-Plattform Zentral) MUSS die logische Operation search_Directory implementieren.

Tabelle 128: Operation search_Directory

I_Directory_Query					Berechtigung: FAD, SÜV, TIP, WA
search_Directory	Parameter				Vertr./Integr./Auth.
	In	Query	DirectoryQuery	IM112	M/H/H
	Out	Result	DirectoryQueryResult	IM113	M/H/H
Die Operation liefert als Ergebnis eine Liste aller Verzeichniseinträge welche der Query entsprechen. Das Protokoll zur Verzeichnisabfrage entspricht LDAP (RFC4511). *Query*: Enthält den Filter für die Suchanfrage. *Result*: Enthält das Ergebnis der Verzeichnisabfrage.					
Verfügbarkeit: H, Nichtabstreitbarkeit: N					

⌫

5.6.1.4.2 I_~~Directory~~Data_Maintenance (Provided)

⌦ **TIP1-A_5806 Die Schnittstelle I_~~Directory~~Data_Maintenance**

Die Schnittstelle I_~~Directory~~Data_Maintenance MUSS alle zugehörigen logischen Operationen implementieren. Über diese Schnittstelle werden die Basisdaten von Verzeichniseinträgen erzeugt und manipuliert. Mit Operation delete_Directory_Entry wird der gesamte Verzeichniseintrag (inklusive eventuell vorhandener FA-Daten) gelöscht. ⌫

⌦ **TIP1-A_5807 Die Schnittstelle I_~~Directory~~Data_Maintenance::add_Directory_Entry**

ENTWURF

Die Schnittstelle I_~~Directory~~Data_Maintenance MUSS die logische Operation add_Directory_Entry implementieren.

Tabelle 129: Operation add_Directory_Entry

I_~~Directory~~Data_Maintenance					Berechtigung: ~~FAD, SÜV~~ Inhaber des Eintrages
add_Directory_Entry	Parameter				Vertr./Integr./Auth.
	In	Variant	DirectoryEntryVariant	IM114	M/H/H
	In	~~EncCertificate~~ Karte	~~CertificateX.509~~ ResourceIdentifier	~~IM404~~ IM412	~~M/M/M~~ M/H/H
	In	Attributes (optional)	DirectoryAttributes	IM115	M/H/H
Mit dieser Operation kann ein Verzeichniseintrag mit der im ENC-Zertifikat ~~(*EncCertifikat*)~~der ausgewählten *Karte* enthaltenen Telematik_ID erzeugt ~~oder erweitert~~ werden. Der Inhaber der Karte muss über eine PIN-Eingabe die rechtmäßige Nutzung nachweisen, sofern noch keine gültige Administrationssitzung besteht. *Variant* = "full" Eingangsparameter: *Variant*="full" Das ENC-Zertifikat wird im Verzeichniseintrag gespeichert. Außerdem werden • Telematik-ID und • Namensinformationen aus dem Zertifikat im Verzeichniseintrag gespeichert. *Variant*="minimal" Eingangsparameter: *Variant*="minimal" Das ENC-Zertifikat wird im Verzeichniseintrag gespeichert. Außerdem wird die • Telematik-ID aus dem Zertifikat im Verzeichniseintrag gespeichert. *Das* ~~*EncCertifikat*~~ ENC-Zertifikat der ausgewählten *Karte* wird im Verzeichniseintrag hinterlegt. Die ~~zusätzlichen~~optionalen Attribute (*Attributes*) werden ~~entsprechend ihren Werten mit einem neuen Wert überschrieben, gelöscht oder bleiben unverändert~~ in den Eintrag übernommen. ~~Ist für die Telematik-ID aus den übergebenen Zertifikaten bereits ein Verzeichniseintrag vorhanden wird dieser komplett durch die übergebenen Daten überschrieben.~~					
Verfügbarkeit: H, Nichtabstreitbarkeit: H					

⌫

⌦ **TIP1-A_5808 Die Schnittstelle I_~~Directory~~Data_Maintenance::read_Directory_Entry**

Die Schnittstelle I_~~Directory~~Data_Maintenance MUSS die logische Operation read_Directory_Entry implementieren.

Tabelle 130: Operation read_Directory_Entry

I_~~Directory~~Data_Maintenance					Berechtigung: ~~FAD, SÜV~~ Inhaber des Eintrages
read_Directory_Entry	Parameter				Vertr./Integr./Auth.
	In	~~TelematikID~~ Karte	~~Telematik_ID~~ ResourceIdentifier	~~IM424~~ IM412	M/H/H
	Out	Entry	DirectoryEntry	IM116	M/H/H
Mit dieser Operation kann der vollständige Verzeichniseintrag (*Entry*) bestehend aus ~~Telematik-ID,~~ Basisdaten und FA-Daten mit der Telematik-ID ~~(*TelematikID*)~~der ausgewählten *Karte* gelesen werden.					
Verfügbarkeit: M, Nichtabstreitbarkeit: N					

⌫

ENTWURF

⌦ **TIP1-A_5809 Die Schnittstelle I_~~Directory~~Data_Maintenance::modify_Directory_Entry**

Die Schnittstelle I_~~Directory~~Data_Maintenance MUSS die logische Operation modify_Directory_Entry implementieren.

Tabelle 131: Operation modify_Directory_Entry

I_~~Directory~~Data_Maintenance					Berechtigung: ~~FAD, SÜV~~ Inhaber des Eintrages
modify_Directory_Entry	Parameter				Vertr./Integr./Auth.
	In	Variant	DirectoryEntryVariant	IM114	M/H/H
	In	~~EncCertificate~~ Karte	~~CertificateX.509~~ ResourceIdentifier	~~IM404~~ IM412	~~M/M/M~~ M/H/H
	In	Attributes	DirectoryAttributes	IM115	M/H/H
Mit dieser Operation können die optionalen Attribute der Basisdaten des Verzeichniseintrags mit der im ENC-Zertifikat der ausgewählten *Karte* enthaltenen Telematik_ID modifiziert werden. Der Inhaber der Karte muss über eine PIN-Eingabe die rechtmäßige Nutzung nachweisen, sofern noch keine gültige Administrationssitzung besteht. Variant = "full" Eingangsparameter: Variant="full" Das ENC-Zertifikat der ausgewählten Karte wird zu den im Verzeichnisdienst gespeicherten Zertifikaten hinzugefügt, sofern sie dort noch nicht enthalten sind. Außerdem werden Namensinformationen aus dem Zertifikat im Verzeichniseintrag gespeichert. Variant="minimal" Eingangsparameter: Variant="minimal" Das ENC-Zertifikat der ausgewählten Karte wird zu den im Verzeichnisdienst gespeicherten Zertifikaten hinzugefügt, sofern es dort noch nicht enthalten ist. Eventuell im Verzeichniseintrag vorhandene Namensinformationen werden gelöscht. ~~Das *EncCertifikat* wird im Verzeichniseintrag hinterlegt.~~ Für die Attribute (*Attributes*) gibt es die Update-Optionen: Neuen Wert setzen, bestehenden Wert löschen, keine Änderung vornehmen.					
Verfügbarkeit: H, Nichtabstreitbarkeit: H					

⌫

⌦ **TIP1-A_5810 Die Schnittstelle I_~~Directory~~Data_Maintenance::delete_Directory_Entry**

Die Schnittstelle I_~~Directory~~Data_Maintenance MUSS die logische Operation delete_Directory_Entry implementieren.

Tabelle 132: Operation delete_Directory_Entry

I_~~Directory~~Data_Maintenance					Berechtigung: ~~FAD, SÜV~~ Inhaber des Eintrages
delete_Directory_Entry	Parameter				Vertr./Integr./Auth.
	In	~~TelematikID~~ Karte	~~Telematik_ID~~ ResourceIdentifier	~~IM424~~ IM412	M/H/H
Mit dieser Operation kann der Verzeichniseintrag mit der Telematik-ID ~~(*TelematikID*)~~ der ausgewählten *Karte* gelöscht werden. Der Inhaber der Karte muss über eine PIN-Eingabe die rechtmäßige Nutzung nachweisen.					
Verfügbarkeit: H, Nichtabstreitbarkeit: H					

⌫

ENTWURF

5.6.1.4.3 I_Directory_Application_Maintenance (Provided)

⌦ **TIP1-A_5811 Die Schnittstelle I_Directory_Application_Maintenance**

Die Schnittstelle I_Directory_Application_Maintenance MUSS alle zugehörigen logischen Operationen implementieren. Über diese Schnittstelle werden die FA-Daten von Verzeichniseinträgen erzeugt, manipuliert und gelöscht.⌫

⌦ **TIP1-A_5812 Die Schnittstelle I_Directory_Application_Maintenance::add_Directory_FA-Attributes**

Die Schnittstelle I_Directory_Application_Maintenance MUSS die logische Operation add_Directory_FA-Attributes implementieren.

Tabelle 133: Operation add_Directory_FA-Attributes

I_Directory_ Application_Maintenance					Berechtigung: FAD, SÜV
add_Directory_FA-Attributes	Parameter				Vertr./Integr./Auth.
	In	TelematikID	Telematik_ID	IM424	M/M/M
	In	FA-Attributes	DirectoryAttributes	IM115	M/H/H
Mit dieser Operation können dem existierenden Verzeichniseintrag mit der (*TelematikID)* fachanwendungsspezifische Attribute (*FA-Attributes)* hinzugefügt werden. Hinzugefügt werden können die Attribute welche zu der Fachanwendung des aufrufenden Dienstes gehören. Die Operation wird über eine TLS-Verbindung mit beidseitiger Authentifizierung angeboten. Der FAD authentisiert sich dabei mit ID.FD.TLS-C, der Verzeichnisdienst mit ID.ZD.TLS_S. Die Operation erlaubt nur die Verarbeitung der fachanwendungsspezifischen Daten des im TLS Verbindungsaufbaus identifizierten fachanwendungsspezifischen Fachdienstes.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: H					

⌫

⌦ **TIP1-A_5813 Die Schnittstelle I_Directory_Application_Maintenance::delete_Directory_FA-Attributes**

Die Schnittstelle I_Directory_Application_Maintenance MUSS die logische Operation delete_Directory_FA-Attributes implementieren.

Tabelle 134: Operation delete_Directory_FA-Attributes

I_Directory_ Application_Maintenance					Berechtigung: FAD, SÜV
delete_Directory_FA-Attributes	Parameter				Vertr./Integr./Auth.
	In	TelematikID	Telematik_ID	IM424	M/M/M
Mit dieser Operation werden alle fachanwendungsspezifischen Attribute - welche zu der Fachanwendung des aufrufenden Dienstes gehören - des Verzeichniseintrags mit der (*TelematikID)* gelöscht. Die Operation wird über eine TLS-Verbindung mit beidseitiger Authentifizierung angeboten. Der FAD authentisiert sich dabei mit ID.FD.TLS-C, der Verzeichnisdienst mit ID.ZD.TLS_S. Die Operation erlaubt nur die Verarbeitung der fachanwendungsspezifischen Daten des im TLS Verbindungsaufbaus identifizierten fachanwendungsspezifischen Fachdienstes.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: H					

⌫

⌦ **TIP1-A_5814 Die Schnittstelle I_Directory_Application_Maintenance::modify_Directory_FA-Attributes**

Die Schnittstelle I_Directory_ Application_Maintenance MUSS die logische Operation modify_Directory_FA-Attributes implementieren.

Tabelle 135: Operation modify_Directory_FA-Attributes

ENTWURF

I_Directory_ Application_Maintenance					Berechtigung: FAD, SÜV
modify_Directory_FA-Attributes	Parameter				Vertr./Integr./Auth.
	In	TelematikID	Telematik_ID	IM424	M/M/M
	In	FA-Attributes	DirectoryAttributes	IM115	M/H/H
Mit dieser Operation können fachanwendungsspezifische Attribute (*FA-Attributes*) von einem Verzeichniseintrag mit der (*TelematikID)* modifiziert werden. Modifiziert werden können die Attribute welche zu der Fachanwendung des aufrufenden Dienstes gehören. Für die Attribute gibt es die Update-Optionen: Neuen Wert setzen, bestehenden Wert löschen, keine Änderung vornehmen. Die Operation wird über eine TLS-Verbindung mit beidseitiger Authentifizierung angeboten. Der FAD authentisiert sich dabei mit ID.FD.TLS-C, der Verzeichnisdienst mit ID.ZD.TLS_S. Die Operation erlaubt nur die Verarbeitung der fachanwendungsspezifischen Daten des im TLS Verbindungsaufbaus identifizierten fachanwendungsspezifischen Fachdienstes.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: H					

⌫

5.6.2 Infrastrukturdienste

5.6.2.1 Dienstlokalisierung

5.6.2.1.1 I_DNS_Service_Localization (Provided)

⌦ **TIP1-A_2363 Schnittstelle I_DNS_Service_Localization (TI-Plattform Zentral)**

Die Schnittstelle I_DNS_Service_Localization (zentral) MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2364 Logische Operation I_DNS_Service_Localization::get_Service_Location (TI-Plattform Zentral)**

Die Schnittstelle I_DNS_Service_Localization (zentral) MUSS die logische Operation get_Service_Location implementieren.

Tabelle 136: Operation get_Service_Location

I_DNS_Service_Localization					Berechtigung: FAD, SÜV, WA
get_Service_Location	Parameter				V, I, A
	In	Query	Text	IM305	M/M/M
	~~In~~	~~DNSSECValidation~~	~~Boolean~~	~~IM307~~	~~M/M/M~~
	Out	Address	URI	IM304	M/M/M
	~~Out~~	~~DNSSECValidated~~	~~Boolean~~	~~IM420~~	~~M/H/H~~
Durch eine mit fachlichen Merkmalen parametrisierte Abfrage kann der URI eines Fachdienstes oder des Dienstes einer weiteren Anwendung des Gesundheitswesens in der Provider Zone ermittelt werden. Die Antworten sind per DNSSEC signiert.					
Verfügbarkeit: H, Nichtabstreitbarkeit: NA					

⌫

5.6.2.2 Namensauflösung

5.6.2.2.1 I_DNS_Name_Resolution (Provided)

⌦ **TIP1-A_2365 Schnittstelle I_DNS_Name_Resolution (TI-Plattform Zentral)**

ENTWURF

Die Schnittstelle I_DNS_Name_Resolution (zentral) MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2366 Logische Operation I_DNS_Name_Resolution::get_IP_Address (TI-Plattform Zentral)**

Die Schnittstelle I_DNS_Name_Resolution (zentral) MUSS die logische Operation get_IP_Address implementieren.

Tabelle 137: Operation get_IP_Address

I_DNS_Name_Resolution					Berechtigung: FAD, SÜV, TIP, WA
get_IP_Address	Parameter				V, I, A
	In	Address	FQDN	IM304	M/M/M
	~~In~~	~~DNSSECValidation~~	~~Boolean~~	~~IM307~~	~~M/M/M~~
	Out	IpAddr	IpAddress	IM304	M/M/M
	~~Out~~	~~DNSSECValidated~~	~~Boolean~~	~~IM420~~	~~M/H/H~~
Diese Operation ermöglicht die Auflösung von FQDN im Namensraum der TI in IP-Adressen für fachanwendungsspezifische Dienste und Produkttypen der Zone „TI-Plattform Zone zentral“. Die Antworten sind per DNSSEC signiert. ~~Fachanwendungsspezifische Dienste und Produkttypen der Zone „TI-Plattform Zone zentral“ müssen die Antworten auf Authentizität und Integrität prüfen (DNSSEC).~~					
Verfügbarkeit: H, Nichtabstreitbarkeit: NA					

⌫

⌦ **TIP1-A_2367 Logische Operation I_DNS_Name_Resolution::get_FQDN (TI-Plattform Zentral)**

Die Schnittstelle I_DNS_Name_Resolution (zentral) MUSS die logische Operation get_FQDN implementieren.

Tabelle 138: Operation get_FQDN

I_DNS_Name_Resolution					Berechtigung: FAD, SÜV, TIP, WA
get_FQDN	Parameter				V, I, A
	In	IpAddr	IpAddress	IM304	M/M/M
	~~In~~	~~DNSSECValidation~~	~~Boolean~~	~~IM307~~	~~M/M/M~~
	Out	Address	FQDN	IM304	M/M/M
	~~Out~~	~~DNSSECValidated~~	~~Boolean~~	~~IM420~~	~~M/H/H~~
Diese Operation ermöglicht die Auflösung von IP-Adressen in FQDN im Namensraum der TI für fachanwendungsspezifische Dienste und Produkttypen der Zone „TI-Plattform Zone zentral“. Die Antworten sind per DNSSEC signiert. ~~Fachanwendungsspezifische Dienste und Produkttypen der Zone „TI-Plattform Zone zentral“ müssen die Antworten auf Authentizität und Integrität prüfen (DNSSEC).~~					
Verfügbarkeit: H, Nichtabstreitbarkeit: NA					

⌫

5.6.2.3 PKI

5.6.2.3.1 I_OCSP_Status_Information (Provided)

⌦ **TIP1-A_2368 Schnittstelle I_OCSP_Status_Information**

Die Schnittstelle I_OCSP_Status_Information MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2369 Logische Operation I_OCSP_Status_Information::check_Revocation_Status**

ENTWURF

Die Schnittstelle I_OCSP_Status_Information MUSS die logische Operation check_Revocation_Status implementieren.

Tabelle 139: Operation check_Revocation_Status

I_OCSP_Status_Information					Berechtigung: FAD, SÜV, TIP, WA
check_Revocation_Status	Parameter				V, I, A
	In	Certificate	CertificateX.509	IM404	M/M/M
	Out	VerificationResult	VerificationResultType	IM420	M/SH/SH
Die Operation ermittelt den Sperrstatus eines Zertifikats (gesperrt, nicht gesperrt oder unbekannt). Die Beschreibung des Ablaufsschritts für nonQES-Endnutzerzertifikate erfolgt in [gemKPT_PKI_TIP#6.5]. Die Beschreibung des Ablaufsschritts für QES-Zertifikate erfolgt in [gemKPT_PKI_TIP#6.6]. Die Schnittstelle verhält sich • für alle X.509-Zertifikate (außer denen für eGK) gemäß [Common-PKI] unter obligatorischer Verwendung der CertHash-Erweiterung (Positive Statement), • für alle X.509-Zertifikate der eGK gemäß [RFC2560].					
Verfügbarkeit: H, Nichtabstreitbarkeit: M					

⌫

5.6.2.3.2 I_TSL_Download (Provided)

⌦ **TIP1-A_2370 Schnittstelle I_TSL_Download**

Die Schnittstelle I_TSL_Download MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2371 Logische Operation I_TSL_Download::download_TSL**

Die Schnittstelle I_TSL_Download MUSS die logische Operation download_TSL implementieren.

Tabelle 140: Operation download_TSL

I_TSL_Download					Berechtigung: FAD, SÜV, TIP, WA
download_TSL	Parameter				V, I, A
	Out	Data	XML	IM419	N/M/M
Die Operation lädt die TSL von einem TSL-Download-Punkt. Die Beschreibung des Ablaufsschrittes erfolgt in [gemKPT_PKI_TIP#6.3].					
Verfügbarkeit: H, Nichtabstreitbarkeit: N					

⌫

5.6.2.3.3 I_BNetzA_VL_Download (Provided)

⌦ **TIP1-A_6735 Schnittstelle I_BNetzA_VL_Download**

Die Schnittstelle I_BNetzA_VL_Download MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_6736 Logische Operation I_BNetzA_VL_Download::download_VL**

Die Schnittstelle I_BNetzA_VL_Download MUSS die logische Operation download_VL implementieren.

Tabelle 141: Operation download_VL

I_BNetzA_VL_Download	Berechtigung: TIP

ENTWURF

download_VL	Parameter				V, I, A
	Out	Vertrauenliste	XML	IM419	N/M/M
Die Operation stellt die aktuelle Vertrauensliste der BNetzA innerhalb der TI-Plattform bereit.					
Verfügbarkeit: H, Nichtabstreitbarkeit: N					

⌫

⌦ **TIP1-A_6737 Logische Operation I_BNetzA_VL_Download::get_Hash**

Die Schnittstelle I_BNetzA_VL_Download MUSS die logische Operation get_Hash implementieren.

Tabelle 142: Operation get_Hash

I_BNetzA_VL_Download					Berechtigung: TIP
Get_Hash	Parameter				V, I, A
	Out	Hash	Binary	IM421	N/H/H
Über diese Operation kann ein Hash über die aktuell in der TI-Plattform bereitgestellte Vertrauenliste der BNetzA bezogen werden. Durch den Vergleich von Hashes kann erkannt werden, ob eine neue Vertrauensliste bereitgestellt wurde.					
Verfügbarkeit: H, Nichtabstreitbarkeit: N					

⌫

5.6.2.3.4 I_Cert_Provisioning

⌦ **TIP1-A_2374 Schnittstelle I_Cert_Provisioning**

Die Schnittstelle I_Cert_Provisioning MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2375 Logische Operation I_Cert_Provisioning::provide_Certificate**

Die Schnittstelle I_Cert_Provisioning MUSS die logische Operation provide_Certificate implementieren.

Tabelle 143: Operation provide_Certificate

I_Cert_Provisioning					Berechtigung: Hersteller, Betreiber_ZD, Betreiber_FD, SÜV, WA
provide_Certificate	Parameter				V, I, A
	In	PublicKey	Binary	IM401	M/SH/SH
	In	CertificateContent	Text	IM406	M/H/H
	Out	Certificate	CertificateX.509	IM404	M/M/M
Diese Operation stellt dem berechtigten Anwender ein Zertifikat aus. Die Berechtigung und Authentizität des Antragstellers müssen geprüft werden. Aus dem öffentlichen Schlüssel (PublicKey) und den Zertifikatsinhaltsdaten (CertificateContent) wird durch den TSP das Zertifikat (Certificate) erstellt.					
Verfügbarkeit: M, Nichtabstreitbarkeit: H					

⌫

5.6.2.3.5 I_Cert_Revocation

⌦ **TIP1-A_2376 Schnittstelle I_Cert_Revocation**

Die Schnittstelle I_Cert_Revocation MUSS alle zugehörigen logischen Operationen implementieren.⌫

ENTWURF

⌦ **TIP1-A_2377 Logische Operation I_Cert_Revocation::revoke_Certificate**

Die Schnittstelle I_Cert_Revocation MUSS die logische Operation revoke_Certificate implementieren.

Tabelle 144: Operation revoke_Certificate

I_Cert_Revocation					Berechtigung: Hersteller, Betreiber_ZD, Betreiber_FD, SÜV, WA
revoke_Certificate	Parameter				V, I, A
	In	CertRef	CertificateReference	IM404	M/M/M
Diese Operation ermöglicht es dem Nutzer, ein Zertifikat für ungültig zu erklären. Hierzu wird eine Referenz auf das zu sperrende Zertifikat übergeben. Die Berechtigung und Authentizität des Nutzers müssen geprüft werden. Das Zertifikat ist danach ungültig und kann nicht mehr in der TI verwendet werden.					
Verfügbarkeit: H, Nichtabstreitbarkeit: H					

⌫

5.6.2.3.6 I_CRL_Download (Provided)

⌦ **TIP1-A_4461 Schnittstelle I_CRL_Download**

Die Schnittstelle I_CRL_Download MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_4462 Logische Operation I_CRL_Download::download_CRL**

Die Schnittstelle I_CRL_Download MUSS die logische Operation download_CRL implementieren.

Tabelle 145: Operation download_CRL

I_CRL_Download					Berechtigung: TIP
download_CRL	Parameter				V, I, A
	Out	Data	XML	IM419	N/M/M
Die Operation stellt eine CRL für die Identitäten ID.VPNK.VPN und ID.VPNK.VPN-SIS an einem CRL Distribution Point (CDP) über HTTP Version 1.1 bereit.					
Verfügbarkeit: M, Nichtabstreitbarkeit: M					

⌫

5.6.2.4 Zeitinformation

5.6.2.4.1 I_NTP_Time_Information (Provided)

⌦ **TIP1-A_2378 Schnittstelle I_NTP_Time_Information (TI-Plattform Zentral)**

Die Schnittstelle I_NTP_Time_Information (zentral) MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2379 Logische Operation I_NTP_Time_Information::sync_Time (TI-Plattform Zentral)**

Die Schnittstelle I_NTP_Time_Information (zentral) MUSS die logische Operation sync_Time implementieren.

ENTWURF

Tabelle 146: Operation sync_Time

I_NTP_Time_Information					Berechtigung: FAD, SÜV, TIP, WA
sync_Time	Parameter				V, I, A
	Out	TimeInformation	Time	IM418	M/H/H
Durch Aufruf dieser Operation erhält der fachanwendungsspezifische Dienst und Produkttypen der Zone „TI-Plattform Zone zentral“ sowie der Konnektor die aktuelle Zeitinformation vom NTP-Server (zentral).					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.6.2.5 Monitoring des Betriebszustandes

5.6.2.5.1 I_Monitoring_Update (Provided)

⌦ **TIP1-A_2686 Schnittstelle I_Monitoring_Update**

Die Schnittstelle I_Monitoring_Update MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2687 Logische Operation I_Monitoring_Update::update_Information**

Die Schnittstelle I_Monitoring_Update MUSS die logische Operation update_Information implementieren.

Tabelle 147: Operation update_Information

I_Monitoring_Update					Berechtigung: FAD, TIP, SÜV
update_Information	Parameter				V, I, A
	In	status	MonitoringInformation	IM424	M/M/M
Über diese Schnittstelle können Betreiber von fachanwendungsspezifischen Diensten, sicheren Übermittlungsverfahren und den zentralen Diensten der TI-Plattform die für die Diensterbringung relevanten Monitoringinformationen an die Störungsampel senden.					
Verfügbarkeit: M, Nichtabstreitbarkeit: M					

⌫

5.6.2.5.2 I_Monitoring_Read (Provided)

⌦ **TIP1-A_2688 Schnittstelle I_Monitoring_Read**

Die Schnittstelle I_Monitoring_Read MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2689 Logische Operation I_Monitoring_Read::read_Information**

Die Schnittstelle I_Monitoring_Read MUSS die logische Operation read_Information implementieren.

Tabelle 148: Operation update_Information

I_Monitoring_Read					Berechtigung: Betreiber_ZD, Betreiber_FD, SÜV, WA
read_Information	Parameter				V, I, A
	Out	status	MonitoringInformation	IM424	M/M/M
Über diese Schnittstelle können alle Zugriffsberechtigten die für sie relevanten Statusinformationen zu den fachanwendungsspezifischen Diensten, sicheren Übermittlungsverfahren und den zentralen					

ENTWURF

Diensten der TI-Plattform abfragen.
Verfügbarkeit: M, Nichtabstreitbarkeit: N

⌫

5.6.2.6 Konfiguration von ~~Bestandsnetzen~~ angeschlossenen Netzen des Gesundheitswesens mit aAdG-NetG

5.6.2.6.1 I_KSRS_Net_Config (Provided)

⌦ **TIP1-A_5114 Schnittstelle I_KSRS_Net_Config**

Die Schnittstelle I_KSRS_Net_Config MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_5115 Logische Operation I_KSRS_Net_Config::get_Ext_Net_Config**

Die Schnittstelle I_KSRS_Net_Config MUSS die logische Operation get_Ext_Net_Config implementieren.

Tabelle 149: Operation get_Ext_Net_Config

I_KSRS_Net_Config					Berechtigung: TIP
get_Ext_Net_Config	Parameter				V, I, A
	Out	netConfig	ConfigurationData	IM201	M/H/H
Diese Operation ermöglicht den Download einer Konfigurationsdatei (*netConfig*), in welcher alle durch den Konnektor benötigten Konfigurationsparameter der angeschlossenen ~~Bestandsnetze~~ Netze des Gesundheitswesens mit aAdG-NetG enthalten sind.					
Verfügbarkeit: NA, Nichtabstreitbarkeit: NA					

⌫

5.6.3 Netzwerkdienste

5.6.3.1 Datentransport/Sichere Online-Anbindung/Sicherer Internetzugang

5.6.3.1.1 I_IP_Transport (Provided)

⌦ **TIP1-A_2380 Schnittstelle I_IP_Transport (TI-Plattform Zentral)**

Die Schnittstelle I_IP_Transport (zentral) MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2381 Logische Operation I_IP_Transport::send_Data (TI-Plattform Zentral)**

Die Schnittstelle I_IP_Transport (zentral) MUSS die logische Operation send_Data implementieren.

Tabelle 150: Operation send_Data

I_IP_Transport					Berechtigung: FAD, SÜV, TIP, WA
send_Data	Parameter				V, I, A
	In	IpAddr	IpAddress	IM304	M/M/M
	In	InData	Binary	IM101	M/M/M
	Out	OutData	Binary	IM101	M/M/M
Diese Operation ermöglicht das Senden und Empfangen von IP-Paketen. Es wird nur der für die					

ENTWURF

Nutzung der TI erforderliche Datenverkehr weitergeleitet. Bei Nutzung von IPv4 erfolgt eine IP-Adressumsetzung (NAT). Wenn höhere Sicherheitsanforderungen bestehen, als durch diese Operation zugesichert sind, so müssen entsprechende Maßnahmen auf den darüberliegenden Protokollschichten erbracht werden (z. B. durch Einsatz von TLS).
Verfügbarkeit: H, Nichtabstreitbarkeit: NA

⌫

5.6.3.1.2 I_Secure_Channel_Tunnel (Provided)

⌦ **TIP1-A_2382 Schnittstelle I_Secure_Channel_Tunnel**

Die Schnittstelle I_Secure_Channel_Tunnel MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2469 Logische Operation I_Secure_Channel_Tunnel::send_secure_IP_Packet**

Die Schnittstelle I_Secure_Channel_Tunnel MUSS die logische Operation send_secure_IP_Packet implementieren.

Tabelle 151: Operation send_secure_IP_Packet

I_Secure_Channel_Tunnel					Berechtigung: TIP
send_secure_IP_Packet	Parameter				V, I, A
	In	Data	Binary	IM101	M/M/M
	Out	Data	Binary	IM101	M/M/M
Diese Operation ermöglicht das Senden und Empfangen von IP-Paketen der TI über einen sicheren Kanal.					
Verfügbarkeit: H, Nichtabstreitbarkeit: NA					

⌫

5.6.3.1.3 I_Secure_Internet_Tunnel (Provided)

⌦ **TIP1-A_3677 Schnittstelle I_Secure_Internet_Tunnel**

Die Schnittstelle I_Secure_Internet_Tunnel MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_3678 Logische Operation I_Secure_Internet_Tunnel::send_secure_IP_Internet**

Die Schnittstelle I_Secure_Internet_Tunnel MUSS die logische Operation send_secure_IP_Internet implementieren.

Tabelle 152: Operation send_secure_IP_Internet

I_Secure_Internet_Tunnel					Berechtigung: TIP
send_secure_IP_Internet	Parameter				V, I, A
	In	Data	Binary	IM101	NA/NA/NA
	Out	Data	Binary	IM101	NA/NA/NA
Diese Operation ermöglicht das Senden und Empfangen von IP-Paketen in das und aus dem Internet über einen sicheren Kanal und bietet den sicheren Internetzugang.					
Verfügbarkeit: N, Nichtabstreitbarkeit: NA					

⌫

ENTWURF

5.6.3.2 Zugang_Fremdnetze

5.6.3.2.1 I_Secure_Access_Bestandsnetz (Provided)

⌦ **TIP1-A_2383 Schnittstelle I_Secure_Access_Bestandsnetz**

Die Schnittstelle I_Secure_Access_Bestandsnetz MUSS alle zugehörigen logischen Operationen implementieren.⌫

⌦ **TIP1-A_2384 Logische Operation I_Secure_Access_Bestandsnetz::send_IP_Packet**

Die Schnittstelle I_Secure_Access_Bestandsnetz MUSS die logische Operation send_IP_Packet implementieren.

Tabelle 153: Operation send_IP_Packet

I_Secure_Access_Bestandsnetz					Berechtigung: TIP
send_IP_Packet	Parameter				V, I, A
	In	Data	Binary	IM101	NA/NA/NA
	Out	Data	Binary	IM101	NA/NA/NA
Diese Operation ermöglicht das Senden von IP-Paketen in Richtung angebundener ~~Bestandsnetze~~ Netze des Gesundheitswesens mit aAdG-NetG sowie das Empfangen von IP-Paketen bei bereits bestehender Verbindung. Performancewerte können nicht erhoben werden, da große Teile der Operation außerhalb der TI-Plattform erbracht werden.					
Verfügbarkeit: N, Nichtabstreitbarkeit: NA					

⌫

5.7 Prozess-Interfaces der TI-Plattform

Im folgenden Kapitel werden organisatorische Schnittstellen aufgeführt, über welche organisatorische Prozesse an die Produkttypen ankoppeln.

5.7.1 P_Cert_Provisioning (Provided)

⌦ **TIP1-A_2385 Organisatorische Schnittstelle P_Cert_Provisioning**

Die organisatorische Schnittstelle P_Cert_Provisioning MUSS alle zugehörigen Festlegungen erfüllen.

Tabelle 154: Schnittstelle P_Cert_Provisioning

P_Cert_Provisioning	Berechtigung: LE, Kartenherausgeber
Organisatorische Schnittstelle zur Veranlassung einer X.509-Zertifikatserzeugung durch den berechtigten Akteur mit anschließender Bereitstellung des Zertifikats durch die CA.	
Verfügbarkeit: M, Nichtabstreitbarkeit: SH	

⌫

5.7.2 P_Cert_Revocation (Provided)

⌦ **TIP1-A_2386 Organisatorische Schnittstelle P_Cert_Revocation**

ENTWURF

Die organisatorische Schnittstelle P_Cert_Revocation MUSS alle zugehörigen Festlegungen erfüllen.

Tabelle 155: Schnittstelle P_Cert_Revocation

P_Cert_Revocation	Berechtigung: LE, Kartenherausgeber
Organisatorische Schnittstelle zur Veranlassung der Sperrung eines X.509-Zertifikats durch den berechtigten Akteur.	
Verfügbarkeit: H, Nichtabstreitbarkeit: SH	

⌫

5.7.3 P_Trust_Approval (Provided)

⌦ **TIP1-A_2387 Organisatorische Schnittstelle P_Trust_Approval**

Die organisatorische Schnittstelle P_Trust_Approval MUSS alle zugehörigen Festlegungen erfüllen.

Tabelle 156: Schnittstelle P_Trust_Approval

P_Trust_Approval	Berechtigung: TIP
Organisatorische Schnittstelle zur Aufnahme, zur Änderung und zum Löschen eines Trust Service Provider X.509 und/oder einer Sub-CA eines TSP in den Vertrauensraum der TI (TSL).	
Verfügbarkeit: M, Nichtabstreitbarkeit: SH	

⌫

5.7.4 P_Sub_CA_Certification_CVC (Provided)

⌦ **TIP1-A_2388 Organisatorische Schnittstelle P_Sub_CA_Certification_CVC**

Die organisatorische Schnittstelle P_Sub_CA_Certification_CVC MUSS alle zugehörigen Festlegungen erfüllen.

Tabelle 157: Schnittstelle P_Sub_CA_Certification_CVC

P_Sub_CA_Certification_CVC	Berechtigung: TSP CVC
Organisatorische Schnittstelle zur Veranlassung der Ausstellung eines CVC-Sub-CA-Zertifikats für Kartenherausgeber bzw. deren Beauftragte, mit dem diese dann berechtigt sind, CV-Zertifikate für Smartcards der TI zu erzeugen.	
Verfügbarkeit: N, Nichtabstreitbarkeit: H	

⌫

5.7.5 P_Sub_CA_Certification_X.509 (Provided)

⌦ **TIP1-A_2470 Organisatorische Schnittstelle P_Sub_CA_Certification_X.509**

Die organisatorische Schnittstelle P_Sub_CA_Certification_X.509 MUSS alle zugehörigen Festlegungen erfüllen.

Tabelle 158: Schnittstelle P_Sub_CA_Certification_X.509

P_Sub_CA_Certification_X.509	TSP X.509nonQES
Organisatorische Schnittstelle zur Veranlassung der Ausstellung eines X.509-Sub-CA-Zertifikats oder für dessen Sperrung	
Verfügbarkeit: N, Nichtabstreitbarkeit: H	

⌫

ENTWURF

5.7.6 P_CVC_Provisioning (Provided)

⌦ **TIP1-A_2389 Organisatorische Schnittstelle P_CVC_Provisioning**

Die organisatorische Schnittstelle P_CVC_Provisioning MUSS alle zugehörigen Festlegungen erfüllen.

Tabelle 159: Schnittstelle P_CVC_Provisioning

P_CVC_Provisioning	Berechtigung: Kartenherausgeber
Organisatorische Schnittstelle zur Beauftragung eines CV-Zertifikates mit den spezifizierten Rollenattributen durch einen berechtigten Kartenherausgeber. Die Schnittstelle deckt den Prozessweg ab vom Kartenherausgeber über den Kartenhersteller bis zur CVC-CA, die als Response das CV-Zertifikat zur Kartenproduktion bereitstellt.	
Verfügbarkeit: M, Nichtabstreitbarkeit: SH	

⌫

5.7.7 P_DNS_Name_Entry_Announcement (Provided)

⌦ **TIP1-A_2390 Organisatorische Schnittstelle P_DNS_Name_Entry_Announcement**

Die organisatorische Schnittstelle P_DNS_Name_Entry_Announcement MUSS alle zugehörigen Festlegungen erfüllen.

Tabelle 160: Schnittstelle P_DNS_Name_Entry_Announcement

P_DNS_Name_Entry_Announcement	Berechtigung: FAD, SÜV, TIP, WA
Über diese Prozessschnittstelle können fachanwendungsspezifische Dienste und Zentrale Dienste der TI-Plattform Informationen zur Auflösung von FQDN in IP-Adressen ihres Dienstes bekanntgeben	
Verfügbarkeit: H, Nichtabstreitbarkeit: H	

⌫

5.7.8 P_DNS_Zone_Delegation (Provided)

⌦ **TIP1-A_2391 Organisatorische Schnittstelle P_DNS_Zone_Delegation**

Die organisatorische Schnittstelle P_DNS_Zone_Delegation MUSS alle zugehörigen Festlegungen erfüllen.

Tabelle 161: Schnittstelle P_DNS_Zone_Delegation

P_DNS_Zone_Delegation	Berechtigung: FAD, TIP, SÜV
Delegation von Teilen von Namensräumen (Subdomains) an andere DNS-Server	
Verfügbarkeit: H, Nichtabstreitbarkeit: H	

⌫

5.7.9 P_DNSSEC_Key_Distribution (Provided)

⌦ **TIP1-A_2392 Organisatorische Schnittstelle P_DNSSEC_Key_Distribution**

Die organisatorische Schnittstelle P_DNSSEC_Key_Distribution MUSS alle zugehörigen Festlegungen erfüllen.

Tabelle 162: Schnittstelle P_DNSSEC_Key_Distribution

ENTWURF

P_DNSSEC_Key_Distribution	Berechtigung: FAD, TIP, SÜV
Über diese Prozessschnittstelle wird der Key Signing Key des TI Trust Anchors bereitgestellt. Im Rahmen eines Schlüsselwechsels ausgetauschte Schlüssel werden endgültig gesperrt und dürfen nicht reaktiviert werden. Der Schlüssel muss in regelmäßigen Abständen mindestens alle 6 Jahre aktualisiert werden.	
Verfügbarkeit: H, Nichtabstreitbarkeit: N	

⌫

5.7.10 P_DNS_Service_Entry_Announcement (Provided)

⌦ **TIP1-A_2393 Organisatorische Schnittstelle P_DNS_Service_Entry_Announcement**

Die organisatorische Schnittstelle P_DNS_Service_Entry_Announcement MUSS alle zugehörigen Festlegungen erfüllen.

Tabelle 163: Schnittstelle P_DNS_Service_Entry_Announcement

P_DNS_Service_Entry_Announcement	Berechtigung: FAD, SÜV, WA
Über diese Prozessschnittstelle können fachanwendungsspezifische Dienste und zentrale Dienste der TI-Plattform Informationen zur Lokalisierung ihres Dienstes bekanntgeben	
Verfügbarkeit: NA, Nichtabstreitbarkeit: H	

⌫

5.7.11 P_KSRS_Maintenance (Provided)

⌦ **TIP1-A_2394 Organisatorische Schnittstelle P_KSRS_Maintenance**

Die organisatorische Schnittstelle P_KSRS_Maintenance MUSS alle zugehörigen Festlegungen erfüllen.

Tabelle 164: Schnittstelle P_KSRS_Maintenance

P_KSRS_Maintenance	Berechtigung: TIP
Über diese Schnittstelle können Aktualisierungspakete im KSR-Server bereitgestellt und verwaltet werden.	
Verfügbarkeit: M, Nichtabstreitbarkeit: H	

⌫

5.7.12 P_~~Directory~~Data_Maintenance (Provided)

⌦ **TIP1-A_5818 Organisatorische Schnittstelle P_~~Directory~~Data_Maintenance**

Die organisatorische Schnittstelle P_~~Directory~~Data_Maintenance MUSS alle zugehörigen Festlegungen erfüllen.

Tabelle 165: Schnittstelle P_~~Directory~~Data_Maintenance

P_~~Directory~~Data_Maintenance	Berechtigung: LE
Wenn die Karte mit der entsprechenden Telematik_ID nicht mehr existiert oder ungültig geworden ist können Leistungserbringer über diese Schnittstelle Verzeichniseinträge mit der alten Telematik_ID entfernen. Das ist z.B. bei einem Wechsel der Telematik_ID möglich.	

ENTWURF

Verfügbarkeit: H, Nichtabstreitbarkeit: H

⌫

5.7.13 P_Directory_Application_Registration (Provided)

⌦ **TIP1-A_5819 Organisatorische Schnittstelle P_Directory_Application_ Registration**

Die organisatorische Schnittstelle P_Directory_Application_Registration MUSS alle zugehörigen Festlegungen erfüllen.

Tabelle 166: Schnittstelle P_Directory_Application_Registration

P_Directory_Application_Registration	Berechtigung: FAD, SÜV
Diese Prozessschnittstelle ermöglicht • FA-Anbieter können sich beim Verzeichnisdienst registrieren. Nach Registrierung können fachanwendungsspezifische Daten in den Verzeichniseinträgen über die Schnittstelle I_Directory_Application_Maintenance gepflegt werden. Bei der Registrierung gibt der FA-Anbieter an o TLS-Client-Identität seines Fachdienstes (ID.FD.TLS-C), o Name der Fachanwendung o Name/Identität des Fachdienstes • FA-Anbieter können sich beim Verzeichnisdienst deregistrieren. Der Zugang über die Schnittstelle I_Directory_Application_Maintenance ist danach nicht mehr möglich und alle Daten dieses FA-Anbieters werden aus dem Verzeichnisdienst entfernt.	
Verfügbarkeit: N, Nichtabstreitbarkeit: H	

⌫

~~5.7.14 P_Directory_Administration_Registration (Provided)~~

~~**TIP1-A_5924 Organisatorische Schnittstelle P_Directory_Administration_ Registration**~~

~~Die organisatorische Schnittstelle P_Directory_Administration_Registration MUSS alle zugehörigen Festlegungen erfüllen.~~

~~**Tabelle 167: Schnittstelle P_Directory_Administration_Registration**~~

~~P_Directory_Administration_Registration~~	~~Berechtigung: FAD, SÜV~~
~~Diese Prozessschnittstelle ermöglicht~~ ~~• FA-Anbieter können sich beim Verzeichnisdienst registrieren. Nach dieser Registrierung können Basisdaten im Verzeichniseintrag eines Teilnehmers über die Schnittstelle I_Directory_Maintenance erstellt, gepflegt und gelöscht werden. Bei der Registrierung gibt der FA-Anbieter an~~ ~~o TLS-Client-Identität seines Fachdienstes (ID.FD.TLS-C),~~ ~~o Telematik-ID des Verzeichniseintrags, für den er sich registriert~~ ~~o Nachweis der Berechtigung zur Datenadminstration durch den Betroffenen (Inhaber des HBA oder der SMC-B)~~ ~~o Name/Identität des Fachdienstes~~ ~~• FA-Anbieter können sich beim Verzeichnisdienst deregistrieren. Der Zugang über die Schnittstelle I_Directory_Maintenance ist danach für den betroffenen Verzeichniseintrag nicht mehr möglich.~~	
~~Verfügbarkeit: N, Nichtabstreitbarkeit: H~~	

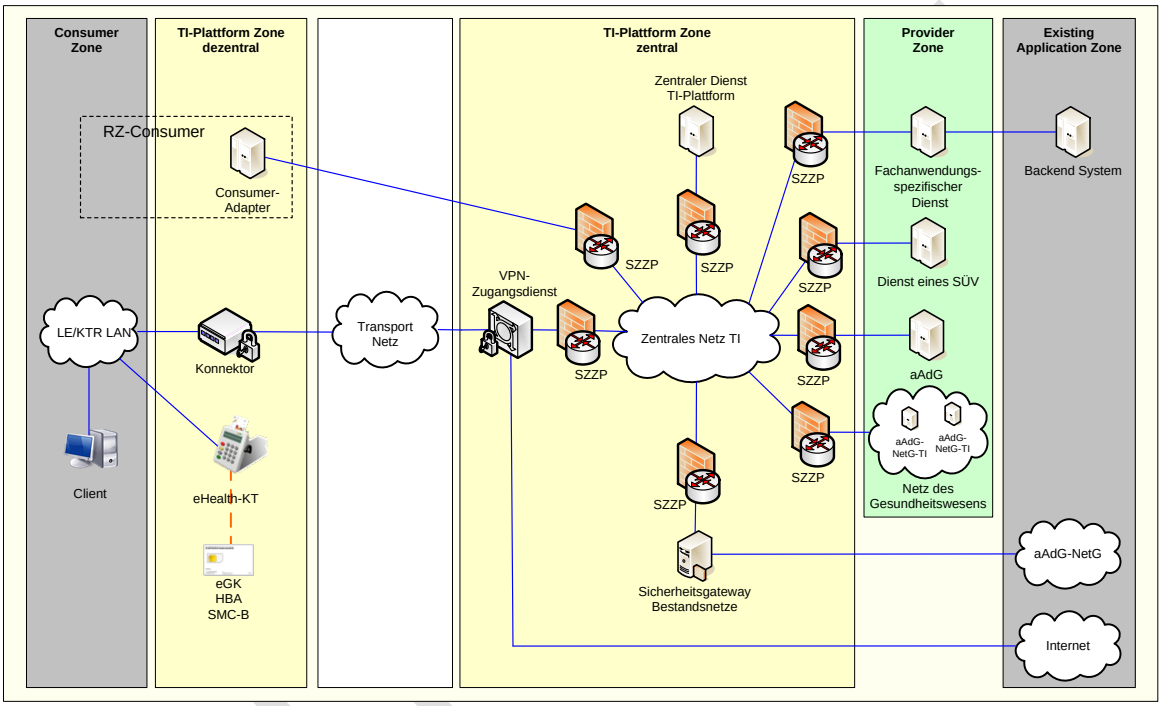
ENTWURF

3268

ENTWURF

6 Das Netzwerk der TI-Plattform

Zur Darstellung und zum Verständnis der Netzwerktopologie der TI-Plattform ist UML nur bedingt geeignet. Daher werden in diesem Kapitel zum besseren Verständnis das Zusammenwirken von Produkttypen zusätzlich als Netzwerkdiagramme abgebildet. Mögliche Redundanz- und Hochverfügbarkeitsansätze werden hier nicht thematisiert.



SZZP: Sicherer Zentraler Zugangspunkt

Abbildung 12: Netzwerktopologie der TI

Die Abbildung 12 zeigt eine schematische Übersicht zur Netzwerktopologie der TI, die sich an den in der Gesamtarchitektur definierten Zonen orientiert. Die Kardinalitäten der Produkttypen wird hier nicht dargestellt.

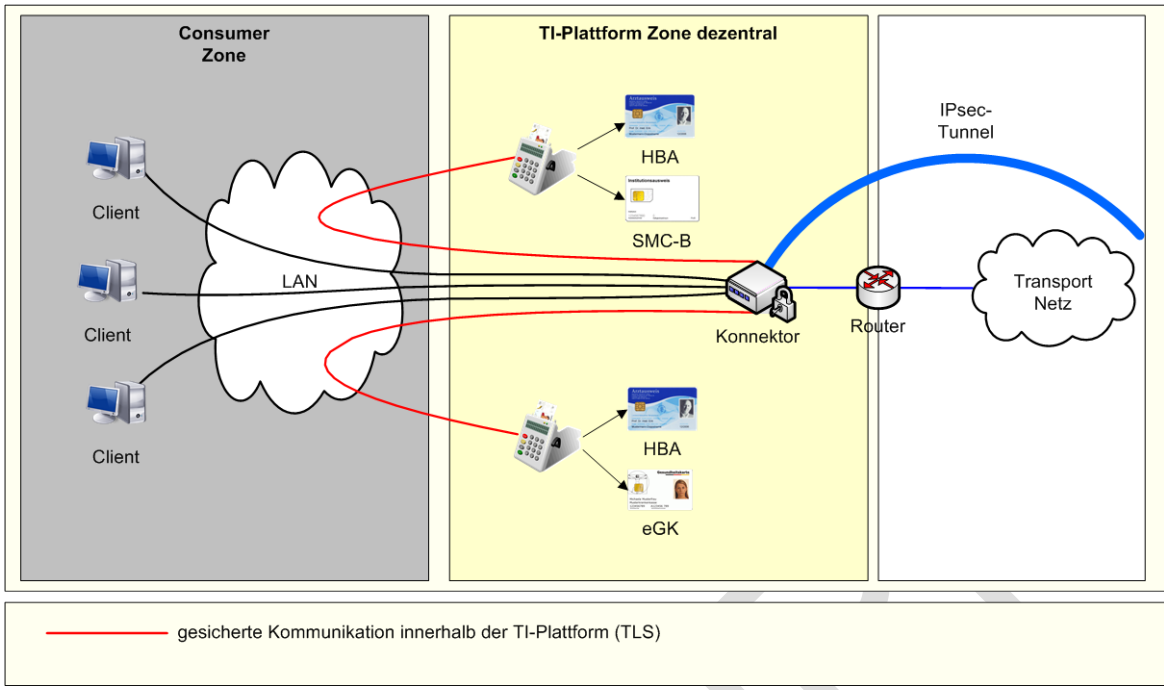


Abbildung 13: Netzwerkverbindungen dezentral

In Abbildung 13 werden die Netzwerkverbindungen im dezentralen Bereich noch einmal hervorgehoben, um die Heterogenität dieser Umgebung bewusst zu machen. Die Darstellung ist aber nur exemplarisch zu verstehen, da es nicht möglich ist alle Varianten in den verschiedenen Einsatzumgebungen (Arztpraxis, Krankenhaus, Kostenträgergeschäftsstelle, Leistungserbringerorganisation usw.) zu erfassen.

6.1.1 Zugangsnetz

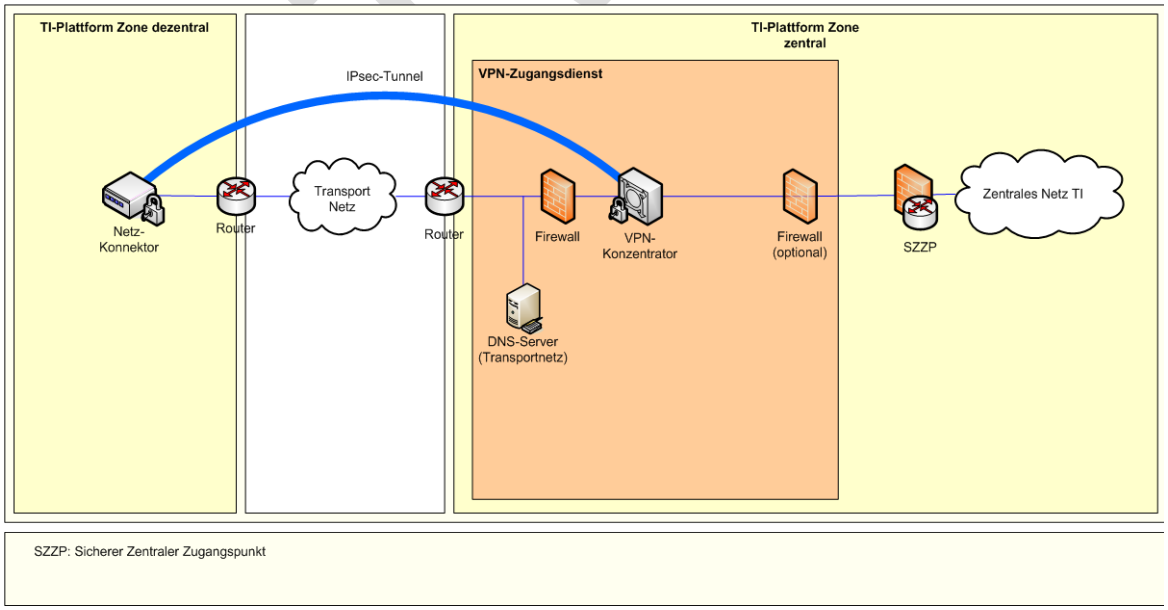


Abbildung 14: Netztopologie Zugangsnetz

In der Abbildung 14 ist exemplarisch der Aufbau des Zugangsnetzes dargestellt. Die Funktionalität wird im Wesentlichen vom Konnektor im dezentralen Bereich und dem VPN-Konzentrator auf zentraler Seite bereitgestellt. Der IPsec-Tunnel zwischen diesen

Komponenten wird über ein beliebiges IP-fähiges Transportnetz aufgebaut. Als Transportnetz kann das Internet verwendet werden. Ein vorhandener Internetanschluss bei Leistungserbringern kann nachgenutzt werden. Das unsichere Transportnetz wird mit einer Stateful Inspection Firewall gegenüber der TI-Plattform abgeschottet.

Der Adressraum der TI ist über den Nameserver für den Namensraum TI des VPN-Zugangsdienstes erreichbar. Die Auswahl dieses Nameservers erfolgt durch die DNS-Forwarding-Funktion im Konnektor.

⌦ **TIP1-A_3679 Produkttyp Konnektor, Zugang TI**

Der Produkttyp Konnektor MUSS, um die Dienste der TI oder die angeschlossenen weiteren Anwendungen des Gesundheitswesens mit Zugriff auf zentrale Dienste (aAdG und aAdG-NetG-TI) zu erreichen, den IPSec-Tunnel zu einem VPN-Konzentrator des VPN-Zugangsdienstes mit der Identität ID.VPNK.VPN verwenden.⌫

6.1.2 Zentrales Netz

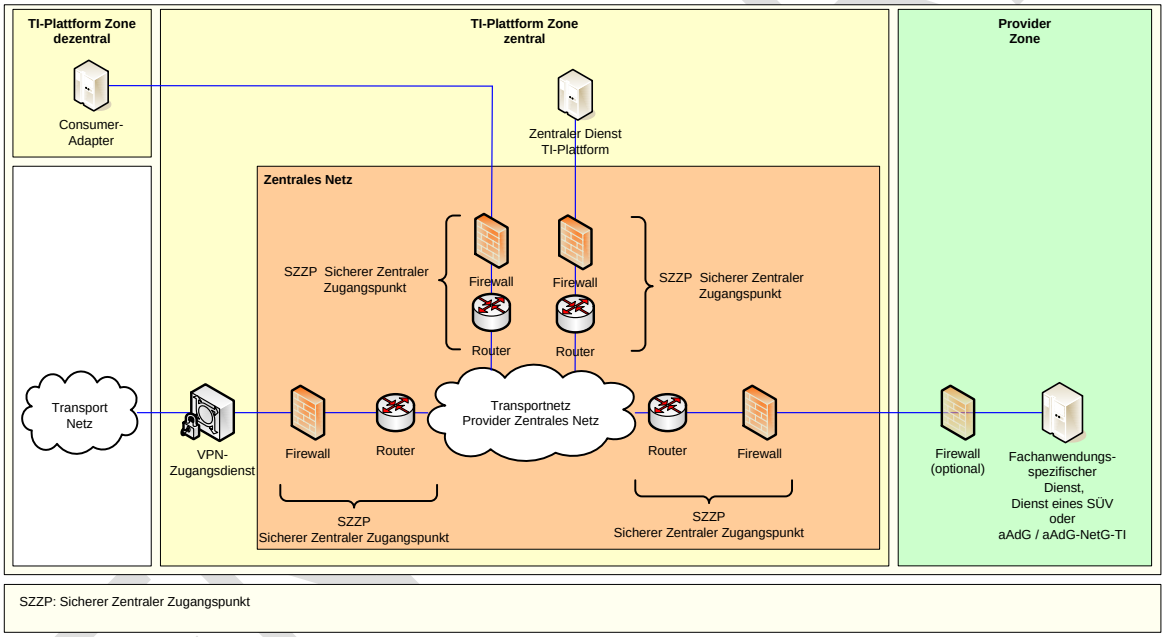


Abbildung 15: Netztopologie Zentrales Netz

Die Abbildung 15 zeigt die wesentlichen Bestandteile des zentralen Netzes der TI. Die fachdienstspezifischen Dienste, der VPN-Zugangsdienst, der Consumer Adapter im RZ-Consumer und die zentralen Dienste der TI-Plattform sind über einen sicheren zentralen Zugangspunkt (SZZP) an die Transportplattform des Netzproviders angeschlossen. In dieser Darstellung sind die beiden Funktionen des SZZP beispielhaft über die beiden separaten Komponenten Firewall und Router umgesetzt. Die Implementierung dieser Funktionen kann auch in einem einzelnen System erfolgen.

6.1.3 Sicherheitsgateway Bestandsnetze

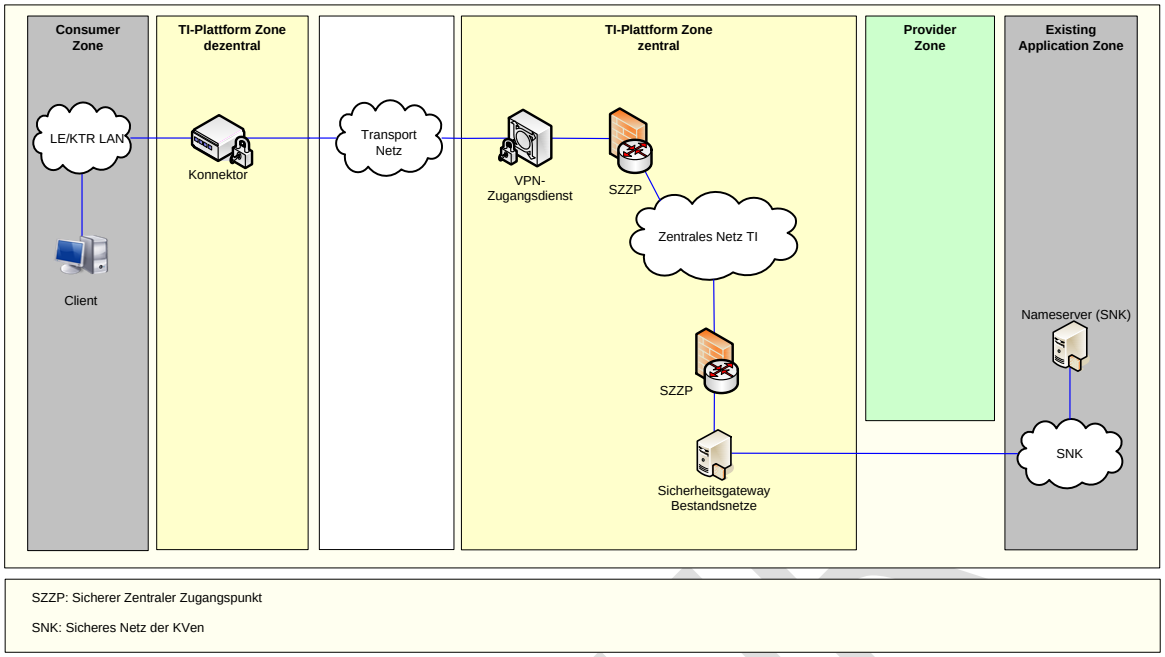


Abbildung 16: Netztopologie Sicherheitsgateway Bestandsnetze

In der Abbildung 16 ist der Zugang zu ~~Bestandsnetzen~~ einem angeschlossenen Netz des Gesundheitswesens mit anderen Anwendungen des Gesundheitswesens ohne Zugriff auf zentrale Dienste (aAdG-NetG) am Beispiel des sicheren Netzes der KVen (SNK) dargestellt.

Das Backbone des SNK wird transparent auf Netzwerkebene an die TI angebunden. Der Adressraum des SNK ist über das zentrale Netz der TI direkt erreichbar. Ein Sicherheitsgateway leitet in der Funktion eines Stateful Paketfilters am Übergang zwischen TI und SNK den Datenverkehr Richtung SNK weiter. Aus dem SNK in Richtung TI wird kein Verbindungsaufbau zugelassen.

Die Auflösung des Namensraumes SNK erfolgt durch interne Nameserver im SNK-Backbone. Die Auswahl der für den jeweiligen Namensraum zuständigen Nameserver erfolgt durch die DNS-Forwarding-Funktion im Konnektor.

Es findet kein Zonentransfer oder Zone-Delegation zwischen Nameservern der TI und des SNK statt.

Für die Anbindung des SNK werden über die Bereitstellung des Sicherheitsgateways hinaus keine weiteren spezifischen Sicherheitsleistungen durch die TI-Plattform erbracht.

⌦ **TIP1-A_3680 Produkttyp Konnektor, Zugang ~~Bestandsnetze~~ angeschlossene Netze des Gesundheitswesens mit aAdG-NetG**

Der Produkttyp Konnektor MUSS, um die Dienste angeschlossener ~~Bestandsnetze~~ Netze des Gesundheitswesens mit aAdG-NetG zu erreichen, den IPSec-Tunnel zu einem VPN-Konzentrator des VPN-Zugangsdienstes mit der Identität ID.VPNK.VPN verwenden.⌫

6.1.4 Sicherer Internetzugang

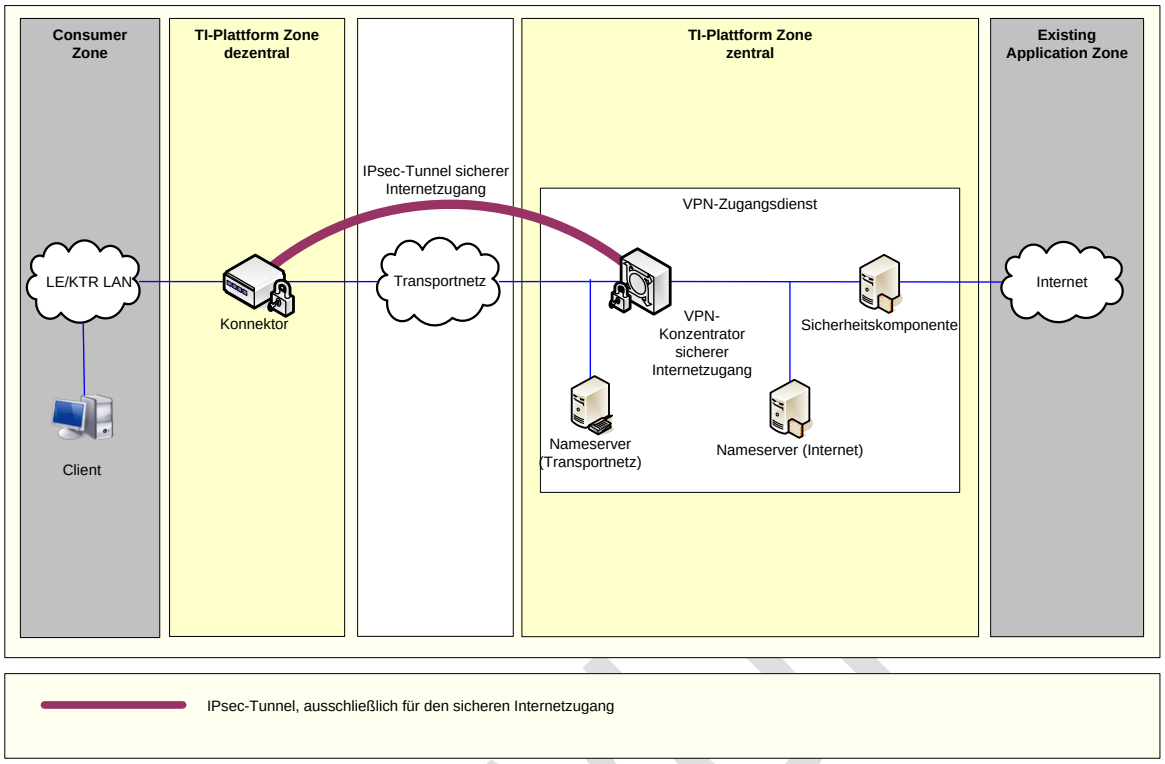


Abbildung 17: Netztopologie Sicherer Internetzugang

In der Abbildung 17 ist der Zugang für Clients in das Internet über den sicheren Internetzugang dargestellt.

Der Client sendet Daten zum Konnektor, um Dienste im Internet zu nutzen. Der Konnektor baut einen separaten IPSec-Tunnel für den Internet-Datenverkehr zu einem VPN-Konzentrator des VPN-Zugangsdienstes. Vom VPN-Konzentrator wird der Datenverkehr an eine Sicherheitskomponente weitergeleitet und gelangt danach zu den Diensten im Internet. Auf dem Rückweg der Verbindung wird der Datenverkehr aus dem Internet nach einer Sicherheits-Policy geprüft und gefiltert. Aus dem Internet in Richtung Client wird kein Verbindungsaufbau zugelassen.

Der IPsec-Tunnel wird ausschließlich für den sicheren Zugang ins Internet genutzt. Im Produkttyp VPN-Zugangsdienst sind die Komponenten für den Zugang ins Internet informationstechnisch von den Komponenten für den Zugang zur TI getrennt.

Der Adressraum des Internet ist über den Nameserver für den Namensraum Internet des VPN-Zugangsdienstes erreichbar. Die Auswahl dieses Nameservers erfolgt durch die DNS-Forwarding-Funktion im Konnektor.

⌦ **TIP1-A_3681 Produkttyp Konnektor, sicherer Internet-Zugang**

Der Produkttyp Konnektor MUSS, um die Dienste im Internet über den sicheren Internet-Zugang zu erreichen, den IPsec-Tunnel zu einem VPN-Konzentrator des VPN-Zugangsdienstes mit der Identität ID.VPNK.VPN-SIS verwenden.⌫

⌦ **TIP1-A_3682 Produkttyp Konnektor, keine netzwerktechnische Erreichbarkeit zwischen IPSec-Tunneln**

Der Produkttyp Konnektor MUSS sicherstellen, dass keine netzwerktechnische Erreichbarkeit zwischen dem IPsec-Tunnel TI und dem IPsec-Tunnel sicherer Internetzugang sowie der hinter den IPsec-Tunneln liegenden Netzwerken besteht.⌫

6.1.5 Weiternutzung Internet

Ein vorhandener Internetanschluss kann bei der Anbindung an die TI weiterhin für den Zugriff auf Anwendungen und Dienste im Internet genutzt werden. I.d.R. findet die Weiternutzung Internet alternativ zum Sicheren Internetzugang statt (siehe Kapitel 6.1.4).

Der TI-Konnektor leitet Anfragen aus dem LAN des Nutzers in Richtung Internet an die bereits vorhandene Infrastruktur (ISP-Router, Firewall, lokaler Router) weiter, die den Weitertransport über den vorhandenen Internetanschluss sicherstellen.

Die Auflösung des Namensraumes erfolgt durch die ISP-Nameserver im Internet. Die Auswahl der für den jeweiligen Namensraum zuständigen Nameserver erfolgt im Regelfall durch die DNS-Forwarding-Funktion im TI-Konnektor. In diesem Fall werden die Anfragen zur Auflösung des Internetnamensraumes durch den Konnektor an die statisch konfigurierte IP-Adresse des ISP-Routers gesendet. Alternativ können auch vorhandene lokale Nameserver genutzt werden, die dann eine Auflösung der Namensräume TI und Bestandnetz (z.B. über DNS-Forwarding Einträge) sicherstellen müssen.

Für die Weiternutzung des Internets werden keine spezifischen Sicherheitsleistungen durch die TI-Plattform erbracht. Der Leistungserbringer ist für die Absicherung des Interzugangs selbst verantwortlich, kann allerdings durch externe Anbieter angebotene, zusätzliche Sicherheitsleistungen (z. B. Anti-Malware, Content-Filter, Proxys) nutzen, die den lokalen Schutz der IT-Systeme unterstützen. Diese Angebote sind durch den Leistungserbringer frei wählbar und unterliegen nicht der Regelungshoheit der TI.

Ggf. ist zu prüfen ob die Eigenschaften (z. B. Bandbreite, SLA) des bisher genutzten Internetanschlusses weiterhin den Anforderungen genügen oder eine entsprechende Anpassung notwendig ist.

ENTWURF

6.1.6 Volumenerfassung im Netzwerk der TI-Plattform

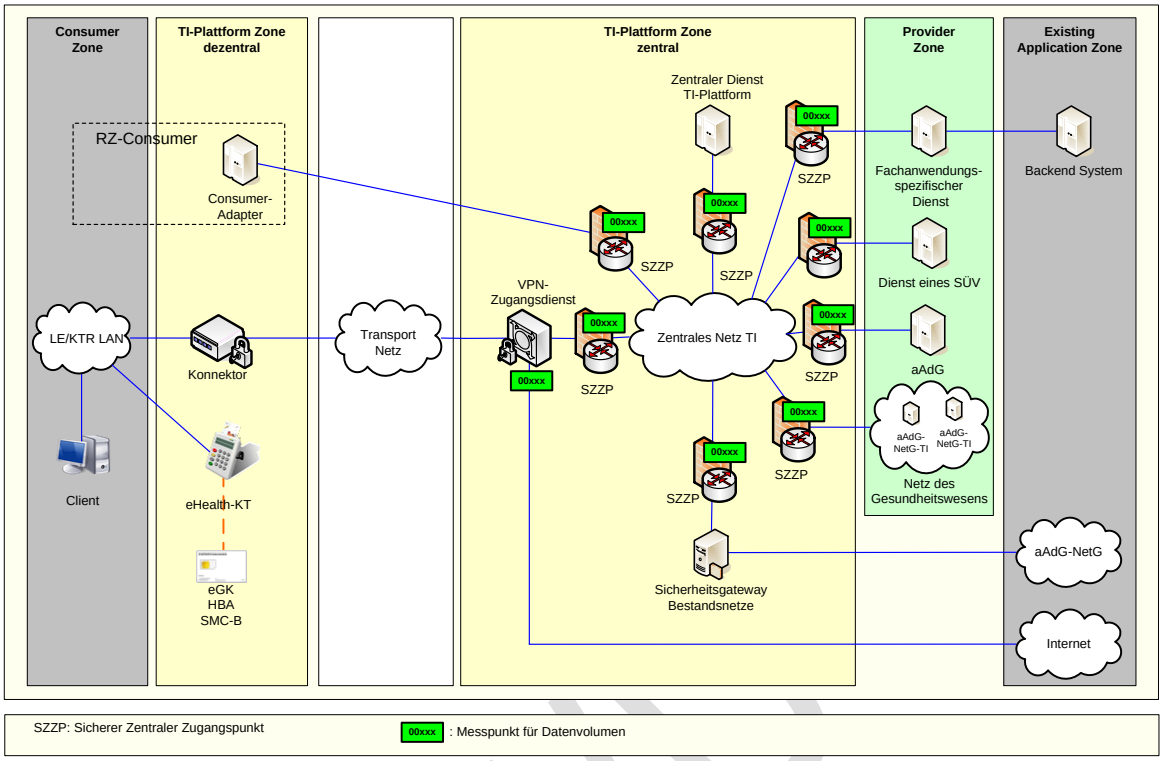


Abbildung 18: Messpunkte des Datenvolumens im Netzwerk der TI-Plattform

Um das Volumenmodell des Netzwerks der TI-Plattform ggf. anpassen zu können, werden an verschiedenen Komponenten des Netzwerks Volumenmessung vorgenommen. Die erfassten Daten werden in das betriebliche Reporting integriert und nachfolgend dazu genutzt das Volumenmodell des Netzwerks der TI-Plattform zu bestätigen oder ggf. anzupassen.

⌦ **TIP1-A_5080 Produkttyp Zentrales Netz, Volumenmessung im SZZP**

Der Produkttyp Zentrales Netz MUSS an seinen SZZPs das Volumen der übertragenen Daten erfassen. An SZZPs, über die zentrale Dienste, Dienste sicherer Übermittlungsverfahren, weitere Anwendungen des Gesundheitswesens oder fachanwendungsspezifische Dienste angeschlossen sind, MUSS die Erfassung für einzelne Dienste getrennt erfolgen.⌫

⌦ **TIP1-A_5081 Produkttyp VPN-Zugangsdienst, Volumenmessung im SIS**

Der SIS des Produkttyps VPN-Zugangsdienst MUSS das Gesamtvolumen der übertragenen Daten über den sicheren Internetzugang erfassen.⌫

6.2 Festlegungen zu Adressierung, Routing und Priorisierung

Die TI-Plattform stellt die anwendungsunabhängigen dezentralen Komponenten und zentralen Dienste bereit, die von den einzelnen Fachanwendungen genutzt werden. Es muss eine Netzwerkinfrastruktur zum Transport von Daten zwischen dezentralen Systemen, fachanwendungsspezifischen Diensten und zentralen Diensten der TI-Plattform bereitgestellt werden. Um die Interoperabilität auf der Netzwerkebene (OSI-Schicht 3) zu gewährleisten, werden übergreifende Vorgaben und Regelungen zur Adressierung, zur

Erreichbarkeit (Routing) und zu den Übertragungsprotokollen benötigt. In diesem Kapitel werden hierzu die notwendigen Festlegungen getroffen.

6.2.1 Festlegungen zum einzusetzenden IP-Protokoll

Für die Adressierung auf Netzwerkebene wird in der TI das IP-Protokoll verwendet. Langfristiges Ziel ist der ausschließliche Einsatz des IP-Protokolls in der Version 6 (IPv6). Da ein kurzfristige Ablösung des IP-Protokolls in der Version 4 (IPv4) insbesondere bei den Leistungserbringern oder Kostenträgern einen unvertretbar hohen Aufwand an Investitionskosten und Personal bedeutet, muss IPv4 noch weiterhin von der TI-Plattform unterstützt werden. Aus diesem Grund sollen Produkttypen der TI-Plattform beide IP-Versionen parallel unterstützten (Dual-Stack).

⌦ **TIP1-A_2399 Produkttypen der TI-Plattform, Unterstützung von IPv4**

Produkttypen der TI-Plattform, die über eine Netzwerkverbindung mit anderen Produkttypen der TI-Plattform oder mit Clientsystemen und fachanwendungsspezifischen Diensten kommunizieren MÜSSEN IPv4 unterstützen.⌫

Die Kriterien, ob eine Komponente oder ein Dienst IPv6-fähig ist, sind im Dokument „RIPE-501 - Requirements For IPv6 in ICT Equipment“ des RIPE[15] zusammengefasst, das damit eine Hilfestellung für Ausschreibungen darstellt. Die Vorgaben aus diesem Dokument werden in der übergreifenden Netzwerkspezifikation für die TI konkretisiert und angepasst.

Umgebung Leistungserbringer und Kostenträgergeschäftsstellen:

Leistungserbringer und Kostenträgergeschäftsstellen betreiben Clientsysteme (insbesondere Primärsysteme und deren Betriebssysteme) sowie Komponenten (Internetrouter, Switch, medizinische Geräte) wie bisher (mit IPv4/IPv6).

Konnektor und eHealth-Kartenterminal:

⌦ **TIP1-A_2400 Produkttyp Konnektor, IPv4 und IPv6 Dual-Stack-Modus**

Der Konnektor KANN IPv4 und IPv6 parallel unterstützen (Dual-Stack-Modus).⌫

⌦ **TIP1-A_2401 Produkttyp Konnektor, Hardwareunterstützung für IPv6**

Der Konnektor MUSS ohne Anpassung der Hardware IPv6 im Dual-Stack-Modus unterstützen können.⌫

⌦ **TIP1-A_2402 Produkttyp Konnektor, NAT-Unterstützung**

Der Konnektor MUSS zur Umsetzung von IPv4-Adressen Network Address Translation (NAT) unterstützen.⌫

⌦ **TIP1-A_2403 Produkttyp eHealth-Kartenterminal, IPv4 und IPv6 Dual-Stack-Modus**

[15] Réseaux IP Européens: RIPE ist ein 1989 gegründetes multinationales Forum, das für jedermann, der Interesse an der Weiterentwicklung des Internet hat, offensteht. Das Ziel von RIPE ist die Sicherstellung der Administration und der technischen Koordination, die notwendig ist, das Internet aufrechtzuerhalten und zu verbessern.

ENTWURF

eHealth-Kartenterminals SOLLEN IPv4 und IPv6 parallel unterstützen (Dual-Stack-Modus).⌫

Zentrales Netz, zentrale Dienste und VPN-Zugangsdienst:

⌦ **TIP1-A_2404 Zentrale TI-Plattform, IPv4 und IPv6 Dual-Stack-Modus**

Produkttypen in der zentralen TI-Plattform MÜSSEN IPv4 und IPv6 parallel unterstützen (Dual-Stack-Modus).⌫

6.2.2 Festlegungen zu Adressräumen

Im Folgenden werden die zu nutzenden Adressräume für die jeweilige Protokollversion festgelegt.

⌦ **TIP1-A_2405 TI, Einsatz eines IPv6-Prefix mit Global Address Scope**

Für den Einsatz von IPv6 in der TI MUSS ein IPv6-Prefix aus dem Global Address Scope [RFC 4007] genutzt werden. Hierdurch wird sichergestellt, dass die in der TI verwendeten Adressen weltweit eindeutig sind.⌫

⌦ **TIP1-A_2406 TI, keine Nutzung des IPv6-Prefix außerhalb der TI**

Der IPv6-Prefix der TI DARF NICHT außerhalb der TI (z. B. im Internet) genutzt werden.⌫

Den LE- und KTR-GS-Umgebungen wird jeweils ein separater IPv6-Prefix zugewiesen um eine Ende-zu-Ende-Kommunikation (ohne NAT) zu ermöglichen. Die Zuweisung der damit verbundenen Adressen erfolgt parallel zu evtl. bereits genutzten IPv6-Adressen. Diese Adressen werden ausschließlich zur Kommunikation mit der TI genutzt.

⌦ **TIP1-A_2407 TI, Verwendung festgelegter Adressräume für IPv4 und IPv6**

Für die Verwendung von IPv4 und IPv6 in der TI MÜSSEN die festgelegten Adressräume genutzt werden.

Tabelle 168: Festlegungen zu Adressräumen

Einsatzbereich	Adressraum IPv4	Adressraum IPv6
LE- und KTR-GS-Umgebung	keine Vorgabe	IPv6-Prefix der TI Optional zusätzlich eigene IPv6-Prefixe des LE bzw. der KTR-GS
Dezentrale Komponenten der TI-Plattform	IPv4-Adressen gemäß [RFC6598], bereitgestellt durch TI-Plattform	IPv6-Prefix der TI
Konnektor (Schnittstelle zum Transportnetz)	bereitgestellt durch ISP	bereitgestellt durch ISP
VPN-Server des VPN-Zugangsdienstes (Schnittstelle zum Transportnetz)	bereitgestellt durch Betreiber des VPN-Zugangsdienstes	bereitgestellt durch Betreiber des VPN-Zugangsdienstes
Zentrale Dienste der TI-Plattform	IPv4-Adressen gemäß [RFC6598], bereitgestellt durch TI-Plattform	IPv6-Prefix der TI
Fachanwendungsspezifische Dienste	IPv4-Adressen gemäß [RFC6598], bereitgestellt durch TI-Plattform	IPv6-Prefix der TI
~~Bestandsnetze~~ aAdG-NetG	Öffentliche IPv4-Adressen, bereitgestellt durch die ~~Bestandsnetze~~ aAdG-NetG	bereitgestellt durch die ~~Bestandsnetze~~ aAdG-NetG, zur Zeit nicht genutzt

ENTWURF

Einsatzbereich	Adressraum IPv4	Adressraum IPv6
aAdG und aAdG-NetG-TI	IPv4-Adressen gemäß [RFC6598], bereitgestellt durch TI-Plattform	IPv6-Prefix der TI
Dienst eines sicheren Übermittlungsverfahrens	IPv4-Adressen gemäß [RFC6598], bereitgestellt durch TI-Plattform	IPv6-Prefix der TI

⌫

⌦ **TIP1-A_2408 TI, Verwendung festgelegter TCP/UDP Ports**

Für die Kommunikation auf TCP- und UDP-Ebene in der TI MÜSSEN die festgelegten Ports genutzt werden.⌫

6.2.3 Festlegungen zum Routing

Die TI-Plattform MUSS eine Netzwerkinfrastruktur bereitstellen, in der die netzwerktechnische Erreichbarkeit von Komponenten und Diensten auf Netzwerkebene (Routing) sichergestellt ist. Hierfür sind an den Netzwerkübergabepunkten zwischen betroffenen Produkttypen Vorgaben zu definieren.

⌦ **TIP1-A_2409 Produkttyp Zentrales Netz, Ermöglichung einer Any-to-Any-Kommunikation**

Der Produkttyp Zentrales Netz MUSS zwischen den Netzwerkanschlusspunkten der Transportplattform eine Any-to-Any-Kommunikation ermöglichen.⌫

⌦ **TIP1-A_2410 TI-Plattform, statisches Routing zwischen Produkttypen**

An den Netzwerkanschlusspunkten zwischen Produkttypen der TI-Plattform SOLL der Austausch von Routing-Informationen statisch erfolgen.⌫

⌦ **TIP1-A_2411 Definition von Routing-Verfahren und Routing-Protokollen**

In der Netzwerkspezifikation MÜSSEN Vorgaben zu einzusetzenden Routing-Verfahren und Routing-Protokollen definiert werden.⌫

6.2.4 Festlegungen zu Namensräumen

Zur Kommunikation zwischen Komponenten und Diensten der TI werden anstatt IP-Adressen logische Bezeichner (Fully Qualified Domain Names - FQDN) verwendet. Diese ermöglichen eine hierarchische Ordnung der Systeme, eine bessere Lesbarkeit sowie eine leichtere Anpassung an die zugrundeliegende Adressierung. Der Namensdienst stellt die Funktion der Auflösung von FQDN in IP-Adressen bereit. Hierfür sind die Definition von Namensräumen und deren Einsatzbereich notwendig.

⌦ **TIP1-A_2412 TI, festgelegte Namensräume**

In der TI MÜSSEN die festgelegten Namensräume genutzt werden.

Tabelle 169: Festlegungen zu Namensräumen

Einsatzbereich	Namensraum
LE- und KTR-GS-Umgebung	keine Vorgaben
Dezentrale Komponenten der TI-Plattform	keine Vorgaben

ENTWURF

Einsatzbereich	Namensraum
Konnektor (Schnittstelle zum Transportnetz)	keine Vorgaben
VPN-Server des VPN-Zugangsdienstes (Schnittstelle zum Transportnetz)	Namensraum Transportnetz; dedizierte Subdomain des Betreibers VPN-Zugangsdienst
Zentrale Dienste der TI-Plattform	Geschlossener Namensraum TI
Fachanwendungsspezifische Dienste	Geschlossener Namensraum TI
aAdG und aAdG-NetG-TI	Geschlossener Namensraum TI
Dienst eines sicheren Übermittlungsverfahrens	Geschlossener Namensraum TI

⌫

⌦ **TIP1-A_2413 Produkttyp Namensdienst, Auflösung von FQDN nach IPv4 und IPv6**

Der Produkttyp Namensdienst MUSS für alle definierten Namensräume der TI eine Auflösung von FQDN nach IPv4 und IPv6 ermöglichen.⌫

⌦ **TIP1-A_2414 Produkttyp Namensdienst, Nutzung der Namensräume der TI**

Für die Lokalisierung von Diensten MUSS der Produkttyp Namensdienst die definierten Namensräume der TI nutzen.⌫

6.2.5 Festlegungen zum TLS-Protokoll

⌦ **TIP1-A_2415 TI-Plattform, Festlegungen zum TLS-Protokoll**

Die TI-Plattform MUSS die Version sowie die spezifische Konfiguration des TLS-Protokolls festlegen, um Sicherheit und Interoperabilität bei der Kommunikation mittels TLS innerhalb der TI zu gewährleisten.⌫

6.2.6 Festlegungen zur Priorisierung auf Netzwerkebene

Um eine potentielle Ressourcenknappheit bei den durch die TI-Plattform verantworteten Diensten und Komponenten zu vermeiden, müssen diese entsprechend der bekannten Performanceanforderungen ausgelegt werden und eine bedarfsgerechte Skalierung unterstützen. Bei Diensten und Komponenten die eine gleichzeitige Nutzung von Ressourcen vorsehen, besteht ein höheres Risiko der Überlastung durch kurzzeitige Lastspitzen. Bei der Anbindung von Leistungserbringern oder Kostenträgern an den VPN-Zugangsdienst der TI-Plattform gibt es nur begrenzte Möglichkeiten zur Auswahl und Skalierung des benötigten Netzwerkanschlusses. Auch im zentralen Netz der TI sind kurzzeitig auftretende Überlastsituationen bei der Nutzung einer Vielzahl von Anwendungen und Diensten nicht auszuschließen. Aus diesem Grund müssen für die Netzwerkkommunikation Maßnahmen zur Priorisierung umgesetzt werden.

⌦ **TIP1-A_2416 TI-Plattform, Festlegungen zu Priorisierungsverfahren auf Netzwerkebene**

Die übergreifende Netzwerkspezifikation MUSS festlegen, welche Verfahren zur Priorisierung auf Netzwerkebene eingesetzt werden.⌫

⌦ **TIP1-A_2417 TI-Plattform, Festlegungen zum Einsatz von Netzwerkpriorisierung in Produkttypen**

ENTWURF

Die übergreifende Netzwerkspezifikation MUSS festlegen, welche Produkttypen Verfahren zur Priorisierung auf Netzwerkebene umsetzen müssen.⌫

ENTWURF

7 Abhängigkeiten zwischen Produkttypen der TI-Plattform

Die Abhängigkeiten zwischen Produkttypen werden in einer Innen- und einer Außensicht dargestellt. In der Innensicht werden die Abläufe zwischen Produkttypen innerhalb der TI-Plattform beschrieben. Die Außensicht definiert Abläufe in fachanwendungsspezifischen Diensten und zwischen diesen Diensten und der TI-Plattform, in denen Vorgaben für die Umsetzung von Diensten der TI-Plattform festgelegt sind.

7.1 Prozessabläufe in fachanwendungsspezifischen Diensten

In dieser Außensicht werden die Abläufe dargestellt, die für fachanwendungsspezifische Dienste relevant sind. Es enthält weitere Informationen, die von den Architekten der Fachanwendungen benötigt werden, um die Architektur ihrer Fachanwendung festlegen zu können. Da eine Kapselung von logischen Diensten nur für Clientsysteme und Fachmodule erfolgt, müssen fachanwendungsspezifische Dienste diese Dienste selber realisieren. Die hier dargestellten Abläufe sind informativ und sollen die fachanwendungsspezifischen Dienste unterstützen.

7.1.1 Erstellung und Prüfung von digitalen Signaturen (Erstellung_Prüfung_Signatur)

7.1.1.1 Erstellung von digitalen Signaturen

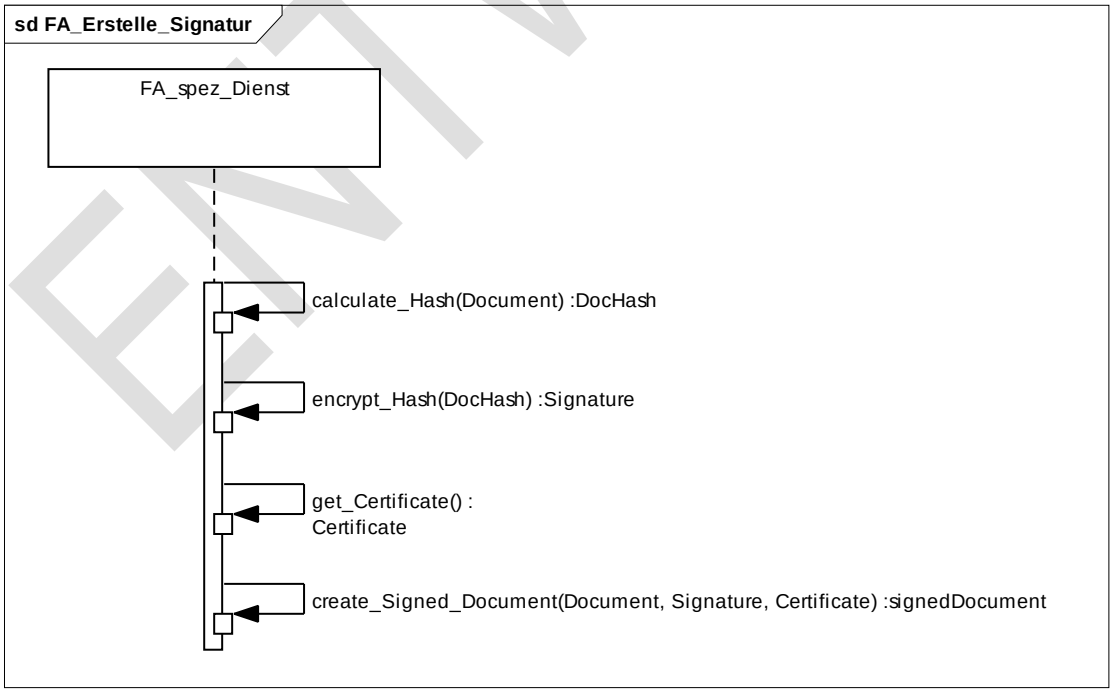


Abbildung 19: Ablauf: Erstellung digitale Signatur

ENTWURF

Abbildung 19 zeigt den Ablauf bei Erstellung einer digitalen Signatur. Für die Erstellung dieser Signatur werden keine weiteren Infrastrukturdienste der TI-Plattform benötigt.

Für das zu signierende Dokument wird unter Verwendung einer Hash-Funktion ein Hash-Wert gebildet, der nachfolgend unter Verwendung eines privaten Schlüssels verschlüsselt und zusammen mit dem X.509-Zertifikat der genutzten kryptographischen Identität in das signierte Dokument eingefügt wird. Die zu verwendende Hash-Funktion und der Verschlüsselungsalgorithmus werden über die TI-Plattform vorgegeben.

7.1.1.2 Prüfung von digitalen Signaturen

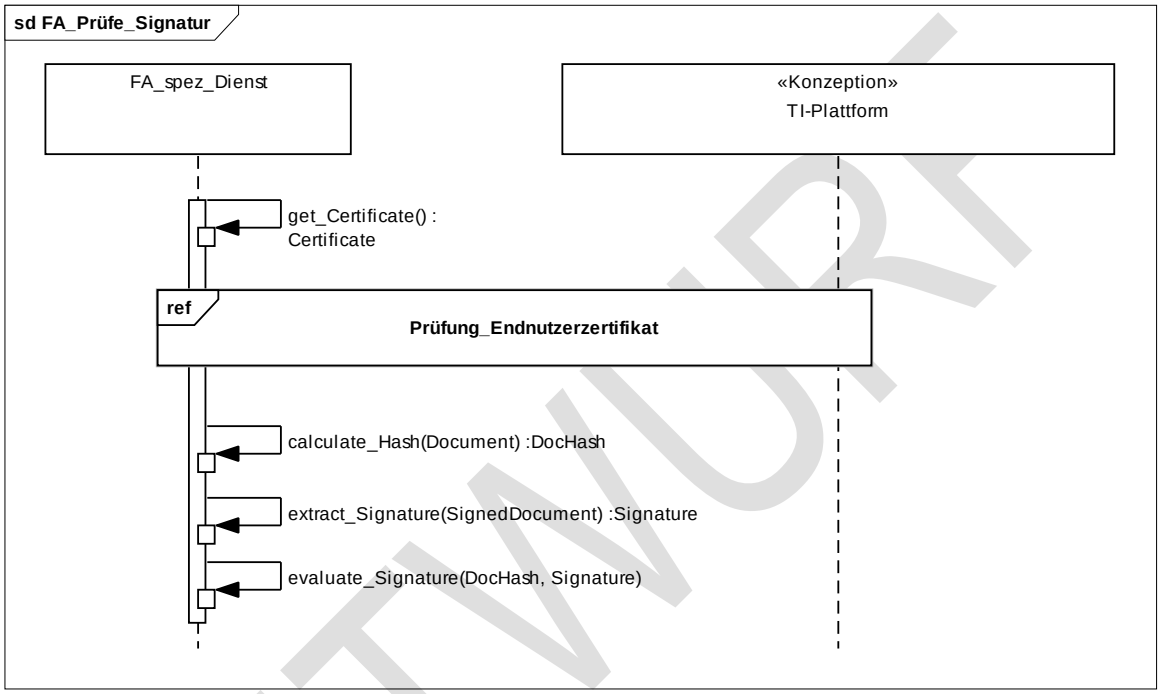


Abbildung 20: Ablauf: Prüfung digitale Signatur

Abbildung 20 zeigt den Ablauf bei Prüfung einer digitalen Signatur. Dabei wird der in Kapitel 7.1.2.2 beschriebene Ablauf für die Prüfung eines X.509-Zertifikats einbezogen.

Das X.509-Zertifikat der Identität, welche das Dokument signiert hat, wird geholt. Diese kann z. B. in das signierte Dokument eingebettet sein. Nach Prüfung des Zertifikats wird die Signatur des Dokuments unter Verwendung eines lokal für das Dokument erzeugten Hash-Werts evaluiert.

Die zu verwendende Hash-Funktion und der Entschlüsselungsalgorithmus werden über die TI-Plattform vorgegeben.

ENTWURF

7.1.2 Prüfung von X.509-Zertifikaten (Prüfung_Zertifikat)

7.1.2.1 TSL-Validierung

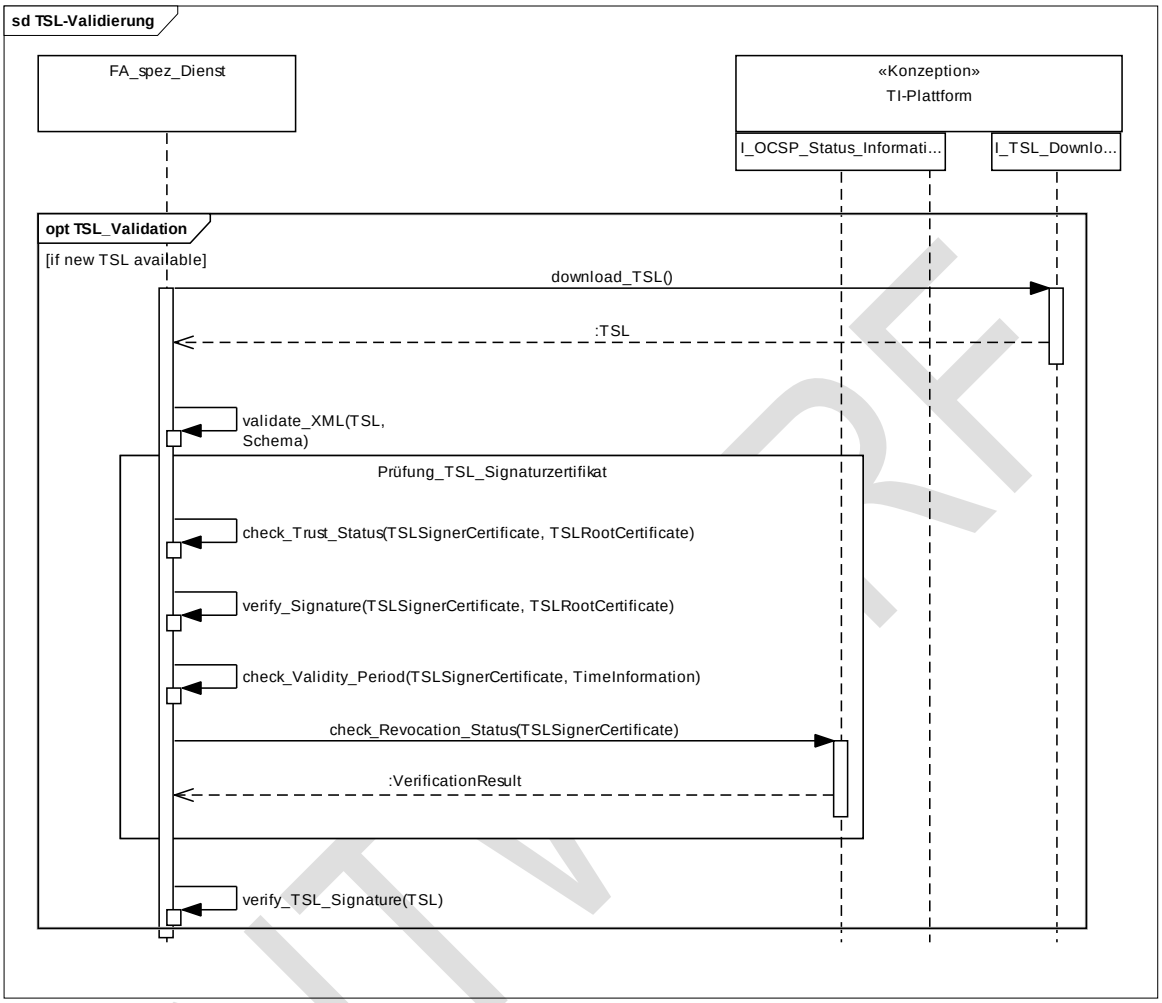


Abbildung 21: Ablauf: TSL-Validierung

Die Prüfung von X.509-Zertifikaten beinhaltet zwei getrennte Schritte. Vorbedingung für die Zertifikatsprüfung ist, dass eine aktuelle TSL ausgewertet ist und in Form eines Trust Stores vorliegt, damit die Vertrauenskette geprüft werden kann. Losgelöst von der Zertifikatsprüfung, die direkt auf Anforderung geschieht, erfolgt die TSL-Validierung in regelmäßigen Zyklen gemäß der u. g. Schritte:

1. Download der aktuellen Liste vom relevanten Downloadpunkt
2. Validierung gegen das XML-Schema der TSL
3. Prüfung des TSL-Signaturzertifikats (Prüfschritte analog der in Abbildung 22 dargestellten Schritte, wobei der Vertrauensstatus gegen ein sicher verwahrtes TSL-Signer-CA-Zertifikat erfolgt)
4. Prüfung der XML-Signatur

7.1.2.2 Prüfung von X.509-Zertifikaten

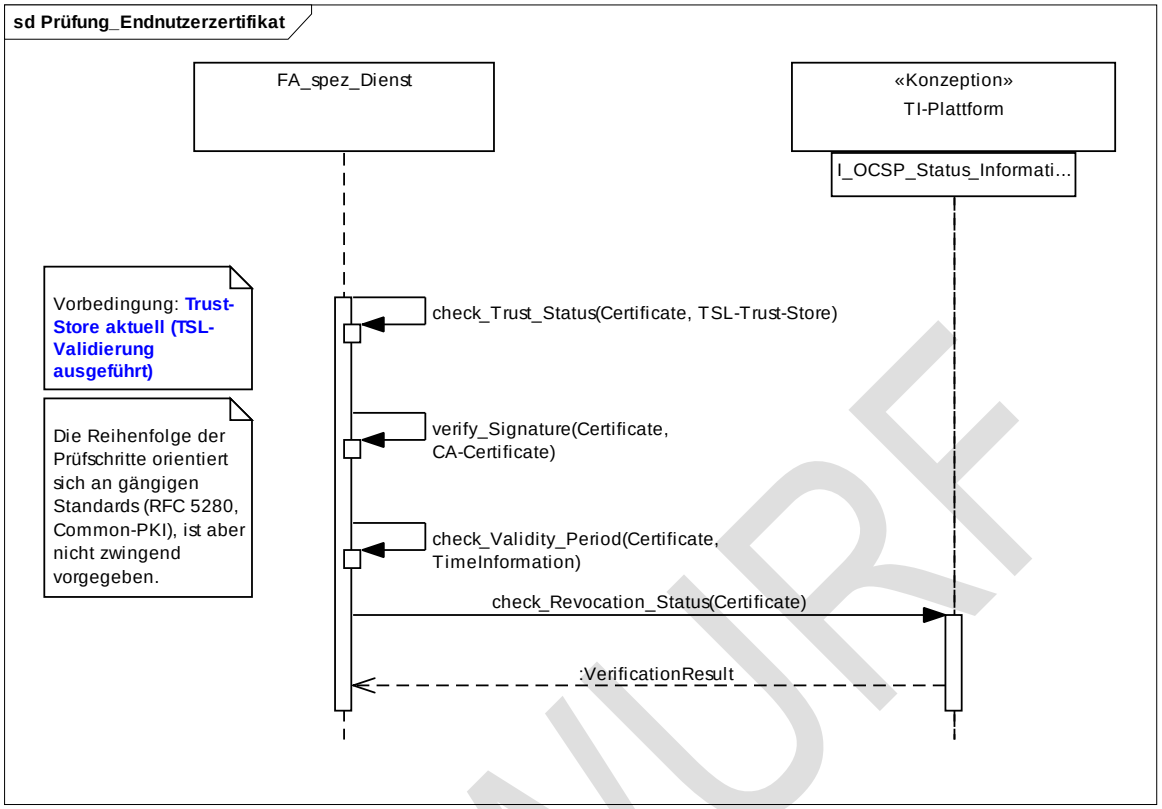


Abbildung 22: Ablauf: Prüfung von X.509-Zertifikaten

Die Prüfung von X.509-Zertifikaten kann nur erfolgen, wenn eine validierte TSL im Trust Store der prüfenden Komponente verfügbar ist. Folgende Schritte müssen beim Prüfen ausgeführt werden:

1. Prüfung des Vertrauensstatus der Aussteller-CA anhand der im Trust Store hinterlegten CA-Zertifikate
2. mathematische Prüfung der Zertifikatssignatur
3. Prüfung der zeitlichen Gültigkeit des Zertifikats
4. Prüfung des Revocation Status durch Abfrage des relevanten OCSP-Responders

Die Reihenfolge ist empfohlen z. B. hinsichtlich wirtschaftlicher Umsetzbarkeit (Offline-Schritte vor Online-Schritten), aber nicht zwingend vorgegeben.

Neben dem Ergebnis der Zertifikatsprüfung wird als weiterer Rückgabeparameter die im Zertifikat hinterlegte Rolle an das aufrufende System zurück geliefert.

7.2 Prozessabläufe zwischen Produkttypen der TI-Plattform

Dieses Kapitel dokumentiert die Abhängigkeiten verschiedener Produkttypen zueinander. Es ist somit normativ bei der Spezifikation der verschiedenen Produkttypen zu berücksichtigen.

ENTWURF

Die Festlegungen beschreiben ausschließlich die Abläufe im „Gut-Fall“. Festlegungen für die Reaktion auf Fehlerfälle in den Abläufen werden erst auf Ebene der Spezifikation getroffen.

7.2.1 Benutzerinteraktion_KT

7.2.1.1 Ablauf Benutzerinteraktion am Kartenterminal

⌦ TIP1-A_2418 Ablauf Benutzerinteraktion am Kartenterminal

Alle am Ablauf „Benutzerinteraktion am Kartenterminal“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

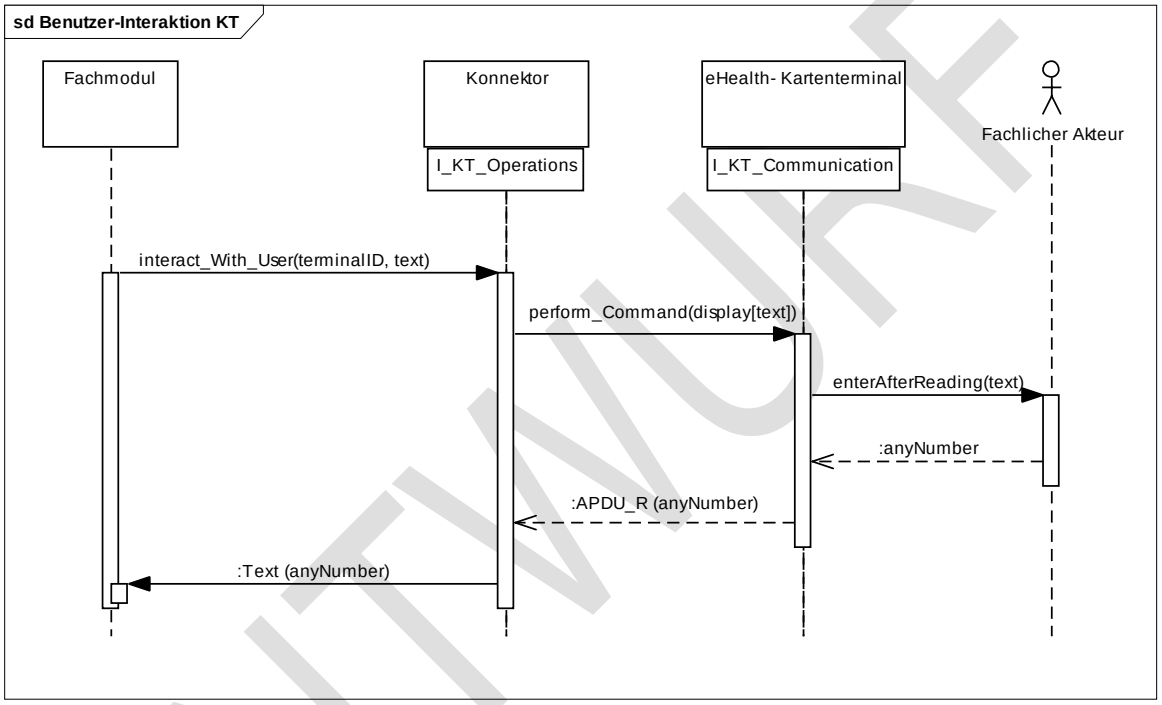


Abbildung 23: Ablauf: Benutzerinteraktion am Kartenterminal

Zwischen Konnektor und eHealth-Kartenterminal wird eine TLS-Verbindung mit gegenseitiger Authentisierung und einem Pairing genutzt. Der Konnektor authentisiert sich dabei mit ID.SAK.AUT, das Kartenterminal mit ID.SMKT.AUT.⌫

7.2.2 Erstellung_Prüfung_QES

7.2.2.1 Ablauf QES erzeugen

⌦ TIP1-A_2419 Ablauf QES erzeugen

Alle am Ablauf „QES erzeugen“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

ENTWURF

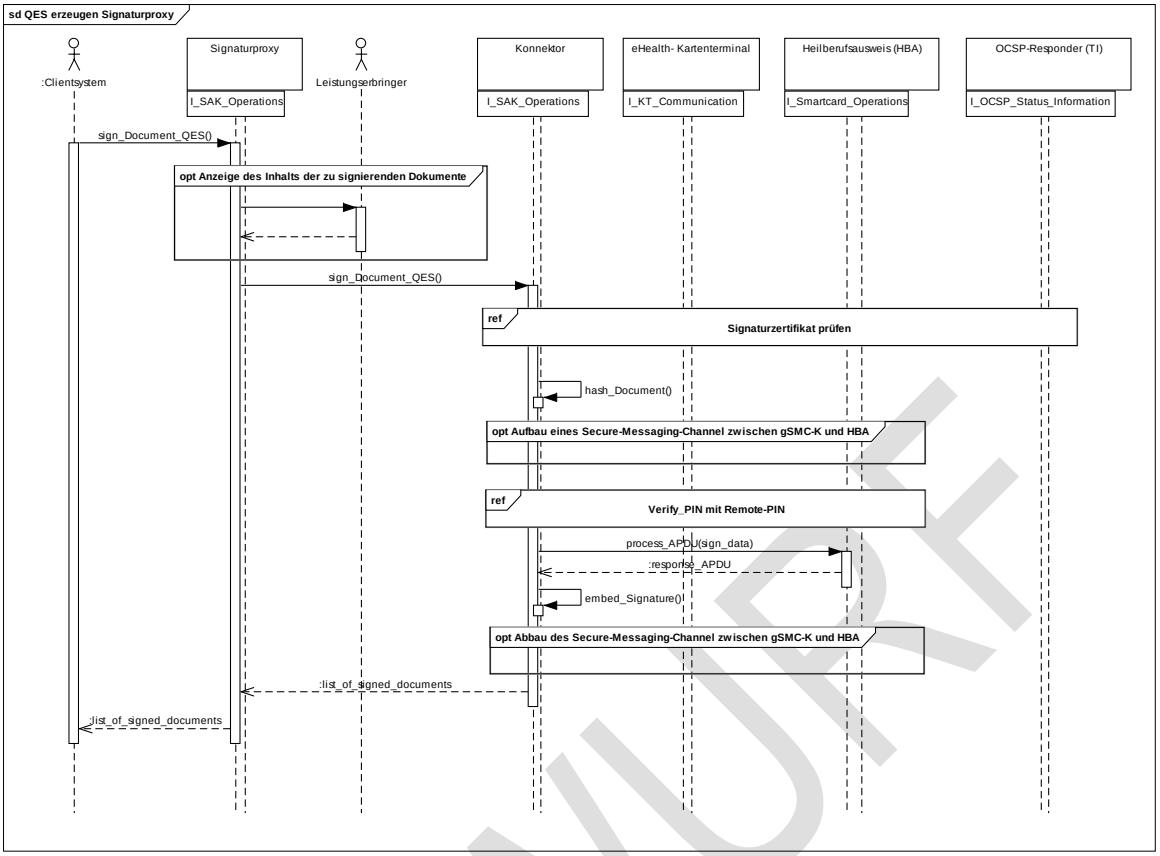


Abbildung 24: Ablauf: QES erzeugen

Abbildung 24 stellt den Ablauf zur Erzeugung einer QES am Beispiel des Produkttyps Konnektor dar.

Falls keine Stapel- sondern eine Einzelsignatur durchgeführt werden soll, kann die Kommunikation zum HBA auch ohne Aufbau eines Secure-Messaging-Channels erfolgen. Der Secure-Messaging-Channels erfüllt die Vorgaben der Technischen Richtlinie [BSI-TR-03114].

Die Operationsaufrufe innerhalb des Produkttyps Konnektor (wie z. B. hash_Document) sind hier nur zur besseren Verständlichkeit des Ablaufs dargestellt.

Die Komponente Signaturproxy wird durch den Produkttyp Konnektor bereitgestellt, ist aber auf den Systemen des Leistungserbringers installiert und deshalb in Abbildung 24 separat dargestellt.

Alternativ zur Darstellung in der Abbildung kann das Clientsystem auch direkt die Operation des Konnektors aufrufen. In diesem Fall kann keine Anzeige der Inhalte erfolgen.⌧

7.2.2.2 Ablauf QES prüfen

⌦ TIP1-A_2420 Ablauf QES prüfen

Alle am Ablauf „QES prüfen“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

ENTWURF

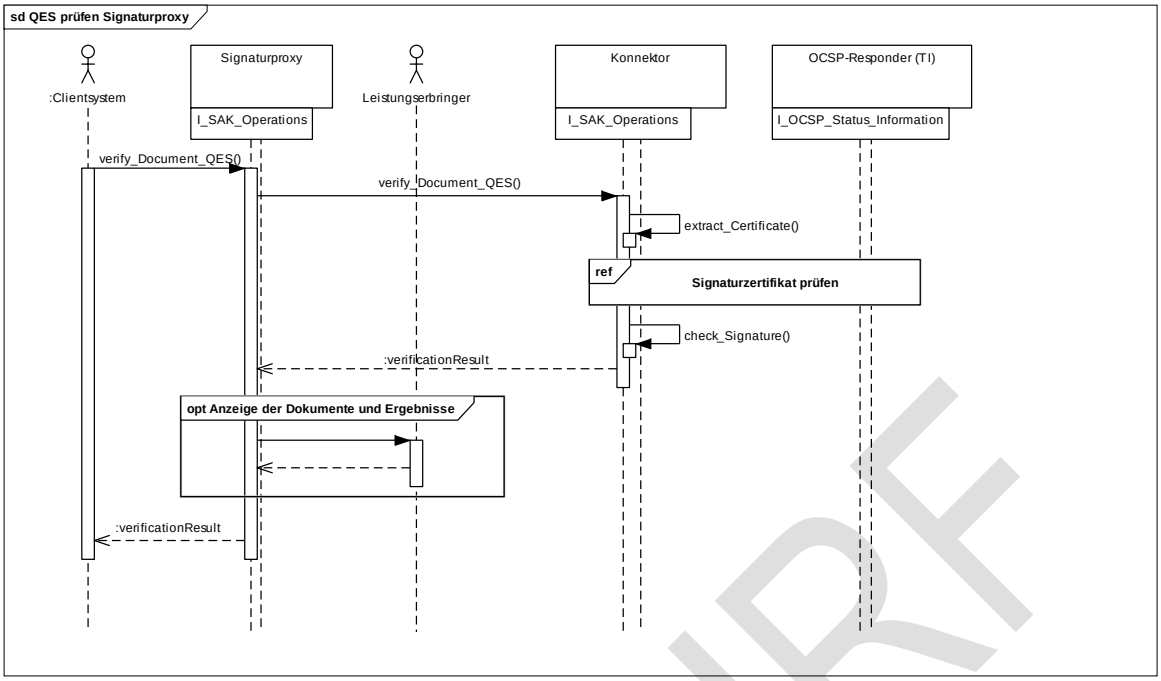


Abbildung 25: Ablauf: QES prüfen

Abbildung 25 stellt den Ablauf zur Prüfung einer QES am Beispiel des Produkttyps Konnektor dar. Die Operationsaufrufe innerhalb des Produkttyps Konnektor (z. B. extract_Certificate) sind nicht normativ und hier nur zur besseren Verständlichkeit des Ablaufs dargestellt.

Die Komponente Signaturproxy wird durch den Produkttyp Konnektor bereitgestellt, ist aber auf den Systemen des Leistungserbringers installiert und deshalb in Abbildung 25 separat dargestellt.

Alternativ zur Darstellung in der Abbildung kann das Clientsystem auch direkt die Operation des Konnektors aufrufen. In diesem Fall kann keine Anzeige der Inhalte und Ergebnisse erfolgen.⌫

7.2.3 Information_Systemzustände

7.2.3.1 Ablauf Anmeldung zur Notifikation und Notifikation

⌦ **TIP1-A_2421 Ablauf Anmeldung zur Notifikation und Notifikation**

Alle am Ablauf „Anmeldung zur Notifikation und Notifikation“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

ENTWURF

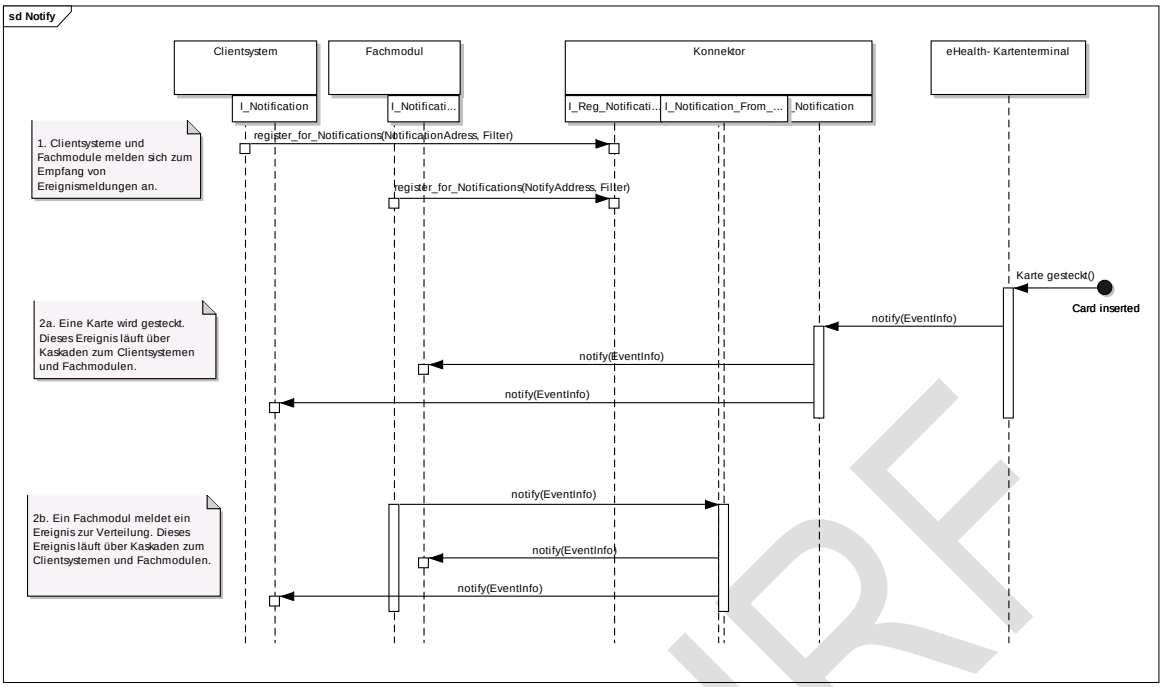


Abbildung 26: Ablauf: Anmeldung zur Notifikation und anschließende Notifikation durch Kartenevent, bzw. Fachmodulmeldung

Der Notifikationsmechanismus des Dienstes Information_Systemzustände besteht aus zwei Schritten:

1. Clientsysteme und Fachmodule melden sich via register_for_Notification mit Ihren Benachrichtigungsadressen beim Konnektor an und abonnieren damit zukünftige Meldungen über Events. Über den Filterparameter kann die Liste der Events, die bei Auftreten an sie gemeldet werden sollen, eingeschränkt werden.

2a. Ein Event in der dezentralen TI-Plattform tritt auf, hier als Beispiel das Stecken einer Karte in ein Kartenterminal. Das Kartenterminal sendet ein notify an den Konnektor, welcher aus dem internen Plattformereignis eine Eventinformation bildet und dieses an alle registrierten Clientsysteme und Fachmodule sendet, die sich über ihren bei der Registrierung übergebenen Filter für diese Art der Meldung abonniert haben.

2b. Ein Fachmodul möchte ein fachspezifisches Event zur Verteilung melden. Es ruft dazu notify des Konnektors auf. Dieser sendet diese Eventinformation an alle registrierten Clientsysteme und Fachmodule, die sich über ihren bei der Registrierung übergebenen Filter für diese Art der Meldung abonniert haben.

Alle Aufrufe im Kontext des PUSH-Mechanismus des Dienstes sind asynchron. Es erfolgt keine Quittung oder Protokollierung, ob eine Event-Meldung erfolgreich zugestellt werden konnte.⌫

7.2.3.2 Ablauf Sammeln der Umgebungsinformationen und Abfrage RessourcenInfo

⌦ **TIP1-A_2422 Ablauf Sammeln der Umgebungsinformationen und Abfrage RessourcenInfo**

ENTWURF

Alle am Ablauf „Sammeln der Umgebungsinformationen und Abfrage RessourcenInfo“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

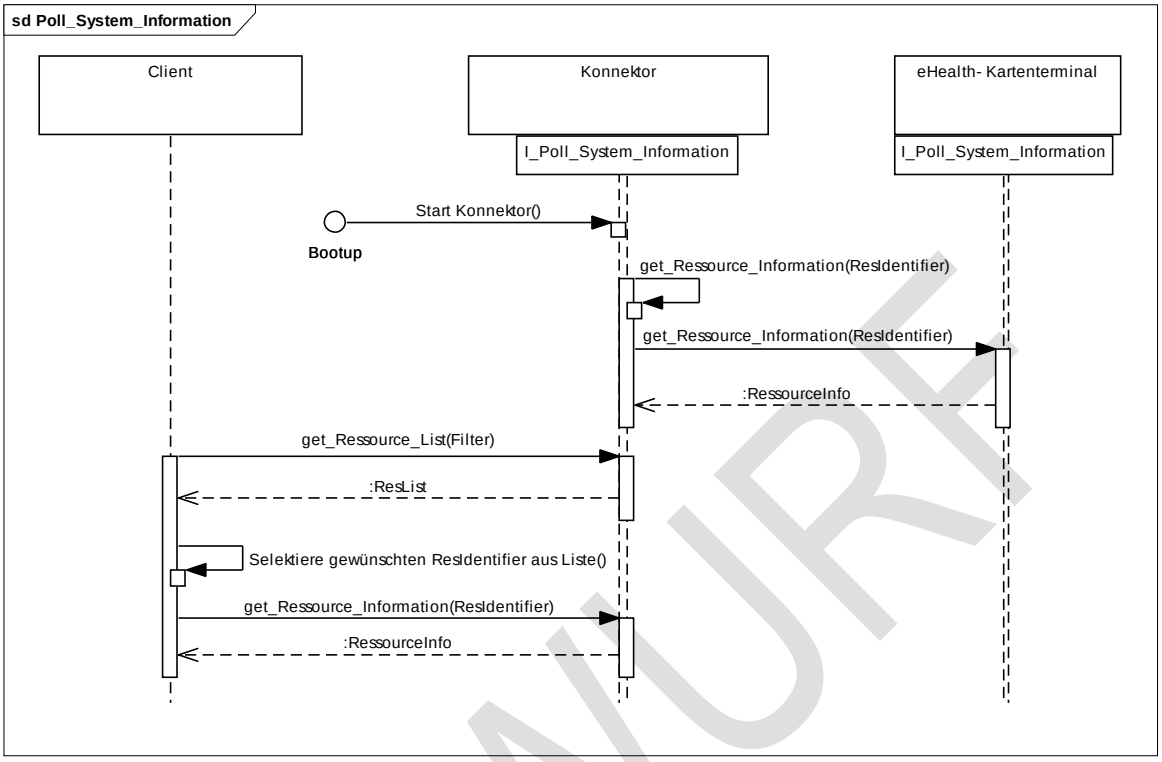


Abbildung 27: Ablauf: Sammeln der Umgebungsinformationen und anschließende Abfrage RessourcenInfo durch Clientsystem

Während der Startup-Phase des Konnektors füllt dieser seinen Informationsspeicher über die von ihm verwalteten anderen dezentralen Komponenten eHealth-Kartenterminals und dort gesteckter Karten. Via get_Ressource_Information fragt er bei diesen Komponenten alle Details ab, die diese von sich liefern können (Herstellername, Versionsnummer, VPN-Status, Anzahl Slots, gesteckte Karten etc.) und speichert sie zwischen. Diese im Konnektor vorgehaltenen Statusinformationen der verwalteten dezentralen Komponenten werden kontinuierlich durch eintreffende Eventinformationen aktualisiert (hier nicht modelliert).

Zu jeder Zeit nach dem initialen Befüllen der gesammelten Statusinformationen, können Clientsysteme (oder Fachmodule, hier nicht modelliert) per get_Ressource_List vom Konnektor Listen über verwaltete dezentrale Komponenten anfordern. Über den Filterparameter können die Einträge der Liste beschränkt werden (bsp.: Nur Kartenterminals zurückliefern). Sofern das Clientsystem oder Fachmodul Details zu einer spezifischen Komponente haben möchte (beispielsweise zu einer gesteckten Karte), durchsucht sie die zurückgelieferte Liste nach Ordnungskriterien, über die sie die gewünschte Komponente in der Liste identifizieren kann. Der in der Liste dieser Komponente zugeordnete ResIdentifier wird im Folgeaufruf der Operation get_Ressource_Information verwendet, um alle zu dieser so eindeutig identifizierten Komponente verfügbaren Detailinformation zu erhalten.⌫

ENTWURF

7.2.4 Konfigurations- und Software Repository (KSR)

7.2.4.1 Ablauf Anzeigen verfügbarer Aktualisierungen

⌦ TIP1-A_2423 Ablauf Anzeigen verfügbarer Aktualisierungen

Alle am Ablauf „Anzeigen verfügbarer Aktualisierungen“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

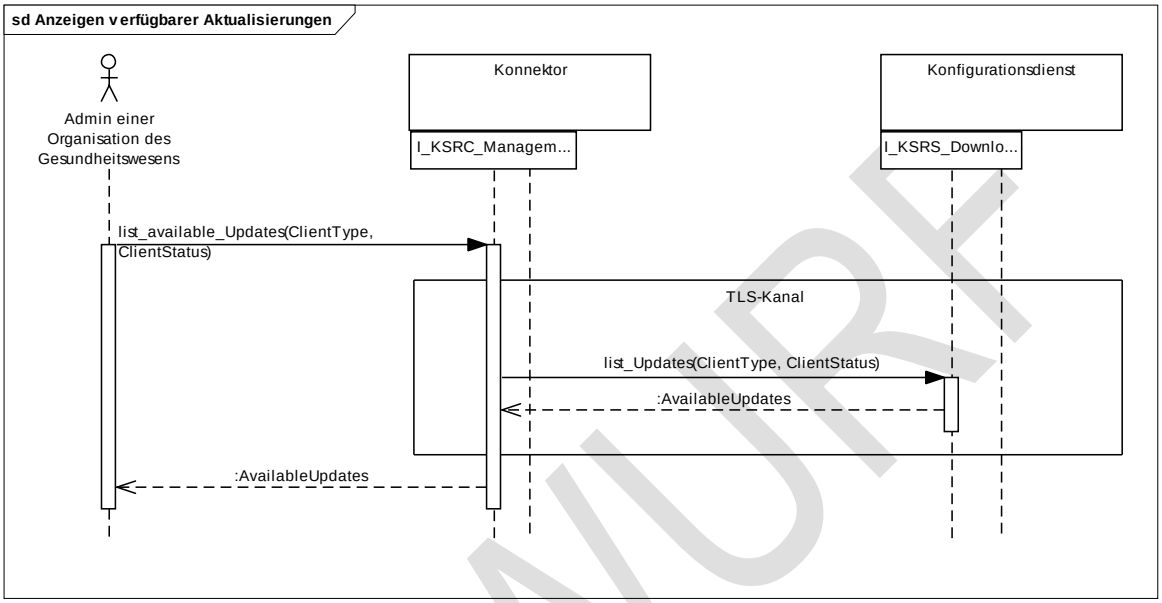


Abbildung 28: Ablauf: Anzeigen verfügbarer Aktualisierungen

Der Administrator kann sich mit der Operation list_Available_Updates des Produkttyps Konnektor verfügbare Aktualisierungen anzeigen lassen.

Zwischen Konnektor und Konfigurationsdienst wird eine TLS-Verbindung mit einseitiger Authentisierung aufgebaut. Zur Serverauthentisierung wird das X.509-Zertifikat mit der TLS-Server-Identität des Konfigurationsdienstes (ID.ZD.TLS_S) genutzt.⌫

7.2.4.2 Ablauf Software oder Konfigurationen aus KSR aktualisieren

⌦ TIP1-A_2424 Ablauf Software oder Konfigurationen über KSR aktualisieren

Alle am Ablauf „Software oder Konfigurationen über KSR aktualisieren“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

ENTWURF

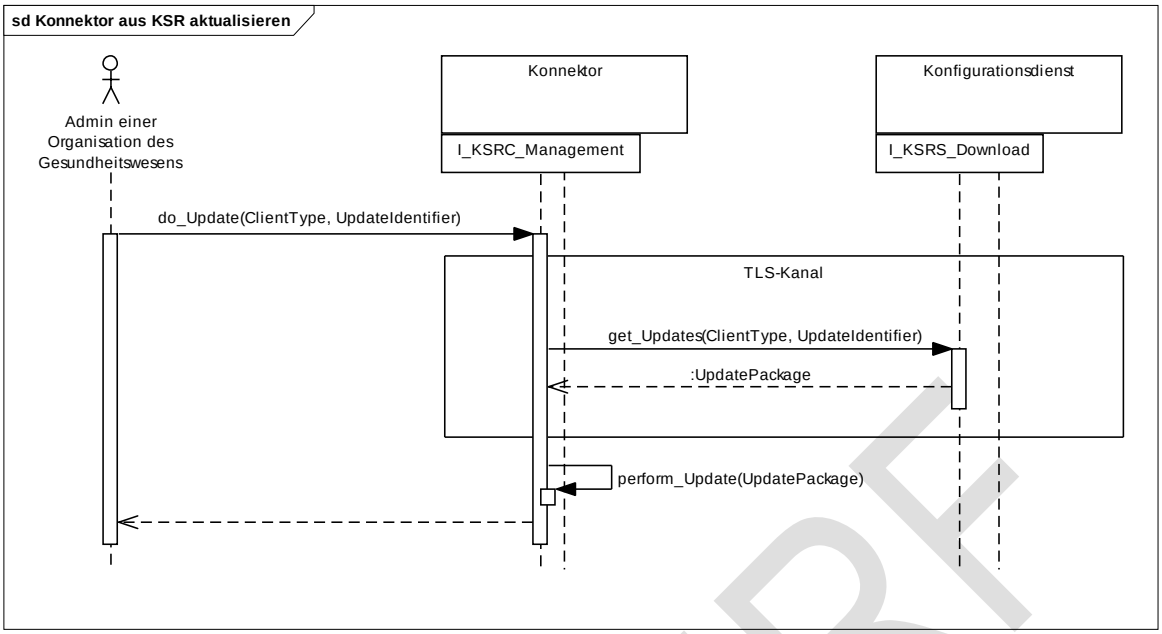


Abbildung 29: Ablauf: Konnektor aus Konfigurationsdienst aktualisieren

Abbildung 29 zeigt die Aktualisierung des Konnektors aus dem Konfigurationsdienst. Die Realisierung des Schritts perform_update innerhalb des Produkttyps Konnektor ist nicht normativ.

Zwischen Konnektor und Konfigurationsdienst wird eine TLS-Verbindung unter Nutzung der kryptographischen Identität ID.ZD.TLS_S zur Serverauthentisierung aufgebaut.

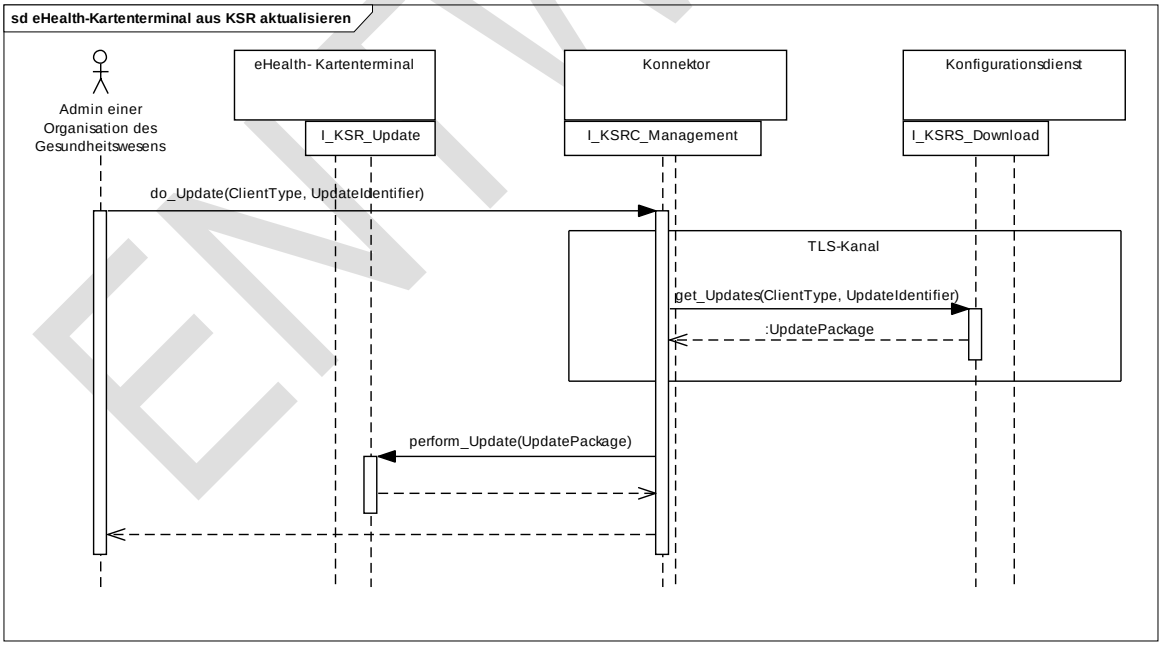


Abbildung 30: Ablauf: eHealth-Kartenterminal aus Konfigurationsdienst aktualisieren

Abbildung 30 stellt die Aktualisierung des Produkttyps eHealth-Kartenterminal aus dem Konfigurationsdienst dar.

ENTWURF

Zwischen Konnektor und Konfigurationsdienst wird eine TLS-Verbindung unter Nutzung der kryptographischen Identität ID.ZD.TLS_S zur Serverauthentisierung aufgebaut.

Zwischen Konnektor und eHealth-Kartenterminal wird eine TLS-Verbindung mit gegenseitiger Authentisierung und einem Pairing genutzt. Der Konnektor authentisiert sich dabei mit ID.SAK.AUT, das Kartenterminal mit ID.SMKT.AUT. ⌫

7.2.4.3 Ablauf ~~Bestands~~Netzkonfigurationen aAdG-NetG aktualisieren

⌦ TIP1-A_5116 Ablauf ~~Bestands~~Netzkonfigurationen aAdG-NetG aktualisieren

Alle am Ablauf „~~Bestands~~Netzkonfigurationen aAdG-NetG aktualisieren“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

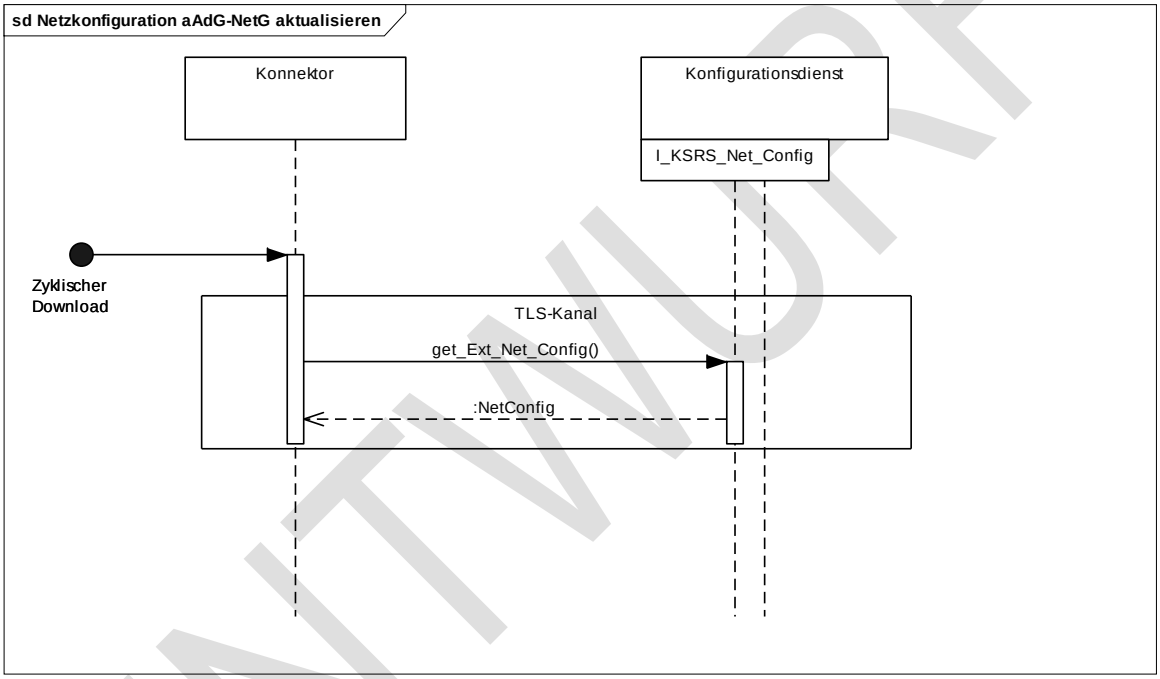


Abbildung 31: Ablauf: ~~Bestands~~Netzkonfigurationen aAdG-NetG aktualisieren

Der Konnektor lädt zyklisch die aktuelle Konfigurationsdatei mit den nötigen ~~Bestandsnetzparametern~~ Netzwerkparametern der angeschlossenen Netze des Gesundheitswesens mit aAdG-NetG vom Konfigurationsdienst. Im Fall einer Änderung der Parameter passt der Konnektor seine Konfigurationsmöglichkeiten dementsprechend an.

Neu angeschlossene ~~Bestandsnetze~~ Netze des Gesundheitswesens mit aAdG-NetG sind im Konnektor grundsätzlich freigeschaltet und ihre Konfiguration wird umgehend angewendet. Die Freischaltung eines ~~Bestandsnetzes~~ angeschlossenen Netzes des Gesundheitswesens mit aAdG-NetG kann durch den Administrator aber widerrufen werden. In diesem Fall wird die entsprechende Konfiguration gelöscht und das ~~Bestandsnetze~~ Netz des Gesundheitswesens mit aAdG-NetG ist durch angeschlossene Clientsysteme nicht mehr erreichbar.

Die Konfiguration entfallener ~~Bestandsnetze~~ Netze des Gesundheitswesens mit aAdG-NetG wird im Konnektor automatisch gelöscht.

ENTWURF

Zwischen Konnektor und Konfigurationsdienst wird eine TLS-Verbindung mit einseitiger Authentisierung aufgebaut. Zur Serverauthentisierung wird das X.509-Zertifikat mit der TLS-Server-Identität des Konfigurationsdienstes (ID.ZD.TLS_S) genutzt.⌫

7.2.4.4 Ablauf Anzeigen verfügbarer Pakete für Fachmodul

⌦ TIP1-A_6056 Ablauf Anzeigen verfügbarer Pakete für Fachmodul

Alle am Ablauf „Anzeigen verfügbarer Pakete für Fachmodul“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

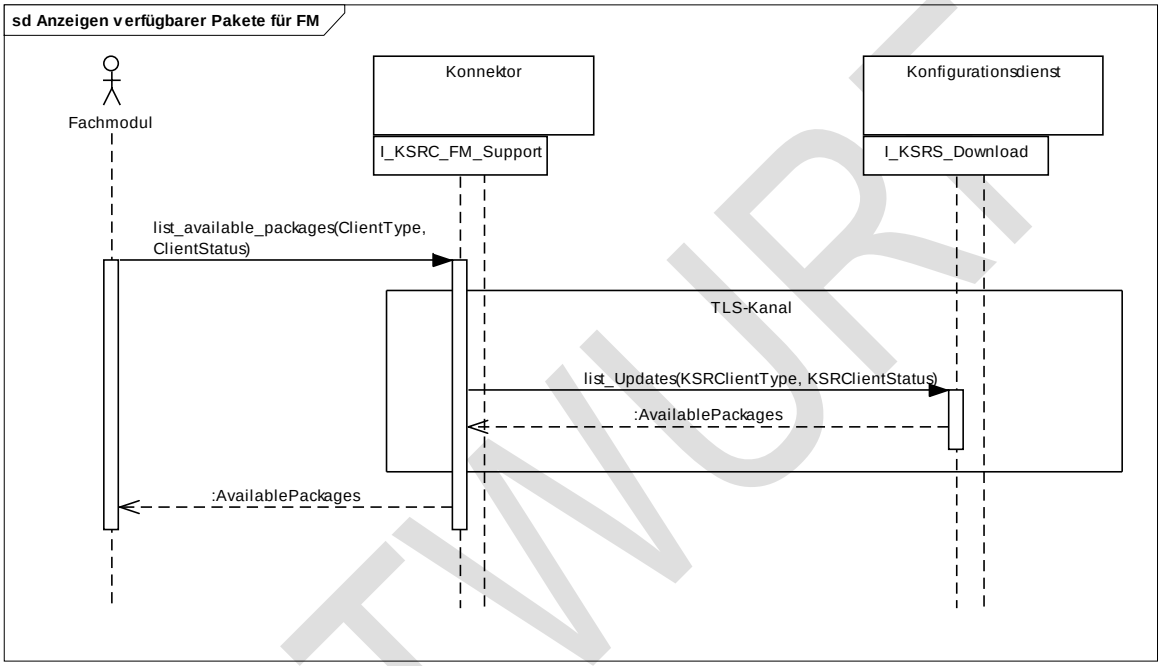


Abbildung 32: Ablauf: Anzeigen verfügbarer Pakete für Fachmodul

Das Fachmodul kann sich mit der Operation list_Available_Packages des Produkttyps Konnektor verfügbare Pakete anzeigen lassen.

Zwischen Konnektor und Konfigurationsdienst wird eine TLS-Verbindung mit einseitiger Authentisierung aufgebaut. Zur Serverauthentisierung wird das X.509-Zertifikat mit der TLS-Server-Identität des Konfigurationsdienstes (ID.ZD.TLS_S) genutzt.⌫

7.2.4.5 Ablauf Paket für Fachmodul aus KSR laden

⌦ TIP1-A_6057 Ablauf Paket für Fachmodul aus KSR laden

Alle am Ablauf „Paket für Fachmodul aus KSR laden“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

ENTWURF

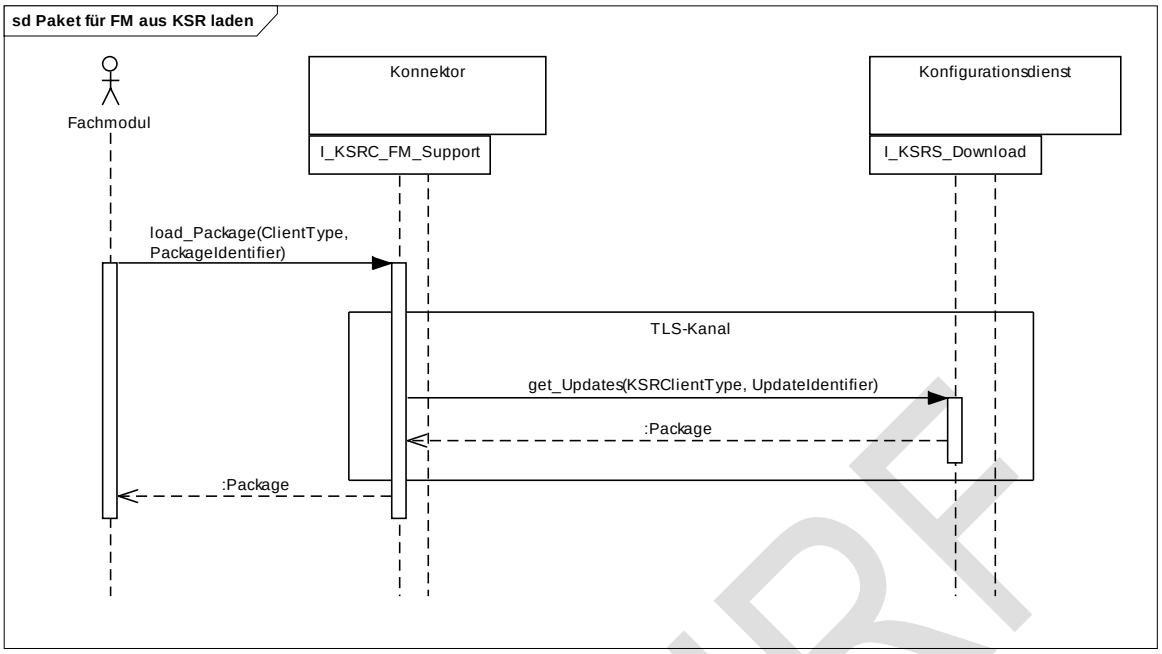


Abbildung 33: Ablauf: Paket für Fachmodul aus KSR laden

Das Fachmodul kann sich mit der Operation load_Package des Produkttyps Konnektor ein bestimmtes Paket laden.

Zwischen Konnektor und Konfigurationsdienst wird eine TLS-Verbindung mit einseitiger Authentisierung aufgebaut. Zur Serverauthentisierung wird das X.509-Zertifikat mit der TLS-Server-Identität des Konfigurationsdienstes (ID.ZD.TLS_S) genutzt. ⌫

7.2.5 Aktualisierung von TSL und Vertrauensliste der BNetzA in Produkttypen

7.2.5.1 Ablauf Aktualisierung der TSL über die TI-Plattform

⌦ **TIP1-A_3683 Ablauf Aktualisierung der TSL über die TI-Plattform**

Alle am Ablauf „Aktualisierung der TSL über die TI-Plattform“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

ENTWURF

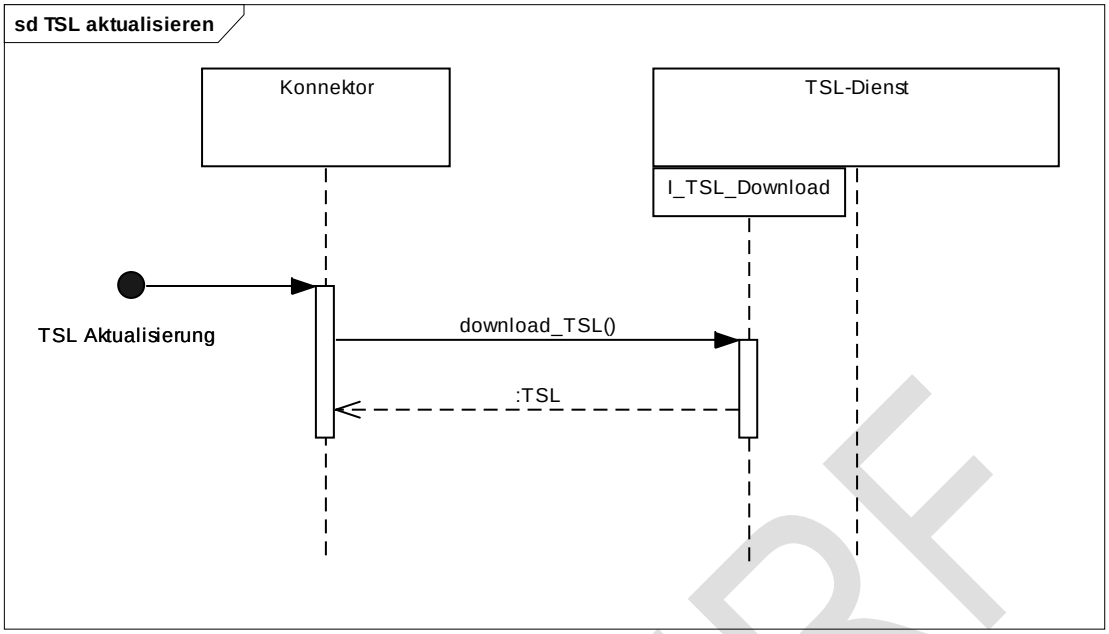


Abbildung 34: Ablauf: Aktualisierung der TSL über die TI-Plattform

Der am Beispiel Konnektor gezeigte Ablauf trifft auch für alle Produkttypen, die Zertifikate der TI prüfen zu. ⌫

7.2.5.2 Ablauf Aktualisierung der Vertrauensliste der BNetzA über die TI-Plattform

⌦ **TIP1-A_6774 Ablauf Aktualisierung der BNetzA-VL über die TI-Plattform**

Alle am Ablauf „Aktualisierung der BNetzA-VL über die TI-Plattform“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

ENTWURF

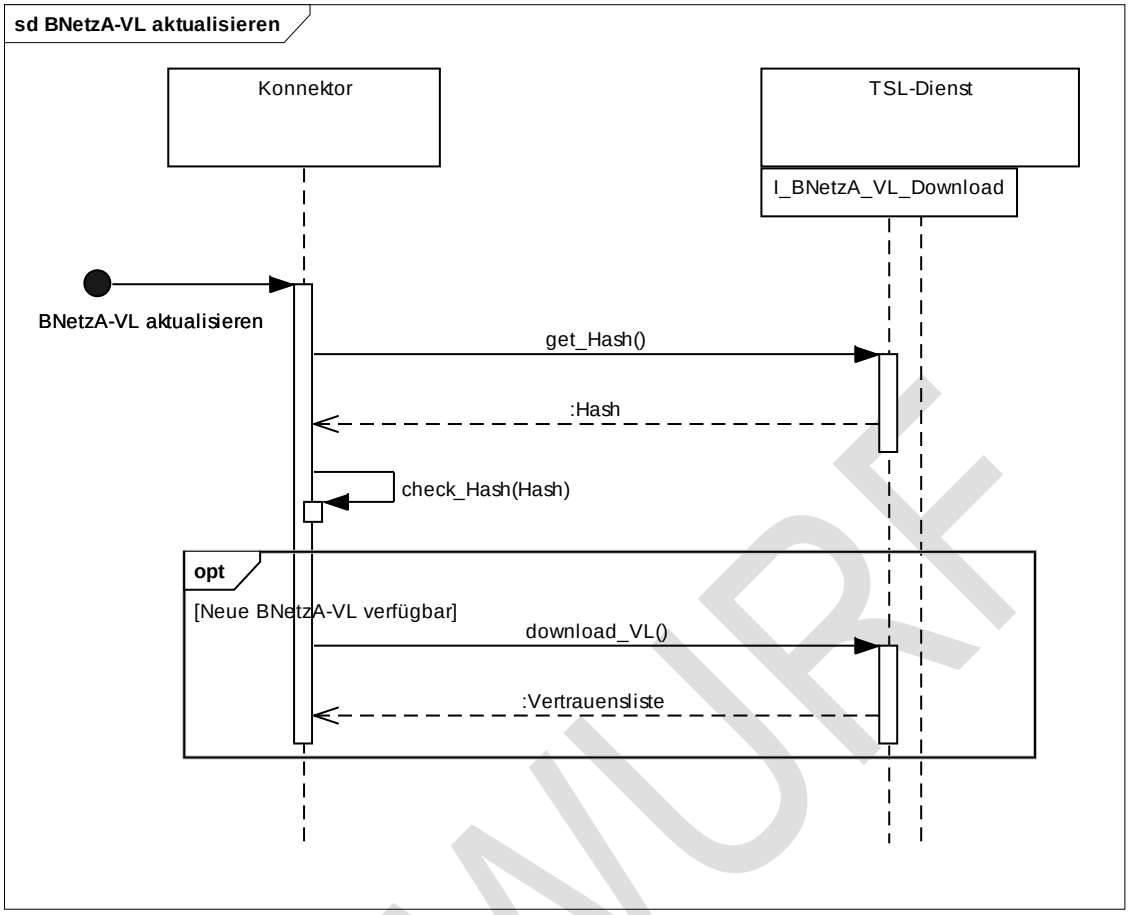


Abbildung 35: Ablauf: Aktualisierung der BNetzA-VL über die TI-Plattform

Dieses Diagramm beschreibt den Ablauf einer Aktualisierung der Vertrauensliste der BNetzA innerhalb der TI.

Bevor der Konnektor die Vertrauensliste lädt prüft er, ob eine neue Vertrauensliste verfügbar ist. Dafür lädt er vom TSL-Dienst den Hash der aktuell bereitgestellten Vertrauensliste und vergleicht diesen mit dem Hash der aktuell im Konnektor gespeicherten Vertrauensliste. Nur wenn die beiden Hashes nicht übereinstimmen wird die neue Vertrauensliste vom TSL-Dienst bezogen.

Zwischen Konnektor und TSL-Dienst wird eine TLS-Verbindung mit Server-Authentisierung aufgebaut. Der TSL-Dienst authentisiert sich dabei mit ID.ZD.TLS_S.⌫

7.2.6 Aktualisierung der CRL im Konnektor

7.2.6.1 Ablauf Aktualisierung der CRL im Konnektor

⌦ TIP1-A_4463 Ablauf Aktualisierung der CRL im Konnektor

Alle am Ablauf „Aktualisierung der CRL im Konnektor“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

ENTWURF

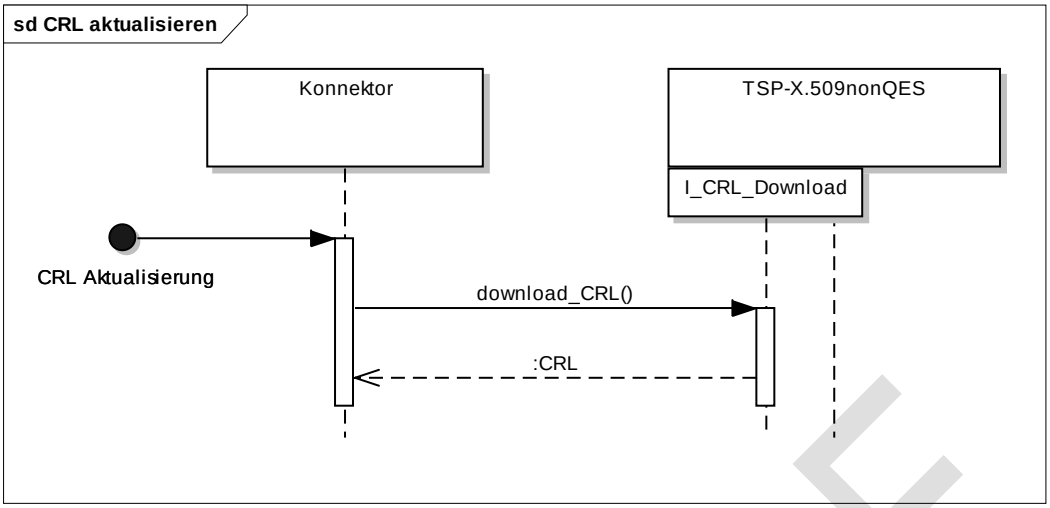


Abbildung 36: Ablauf: Aktualisierung der CRL im Konnektor

Die CRL wird am CDP über HTTP Version 1.1 bereitgestellt. ⌫

7.2.7 Prüfung von X.509-Zertifikaten (Prüfung_Zertifikat)

7.2.7.1 Ablauf Initialisierung Trust Store

⌦ **TIP1-A_2425 Ablauf Initialisierung Trust Store**

Alle am Ablauf „Initialisierung Trust Store“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

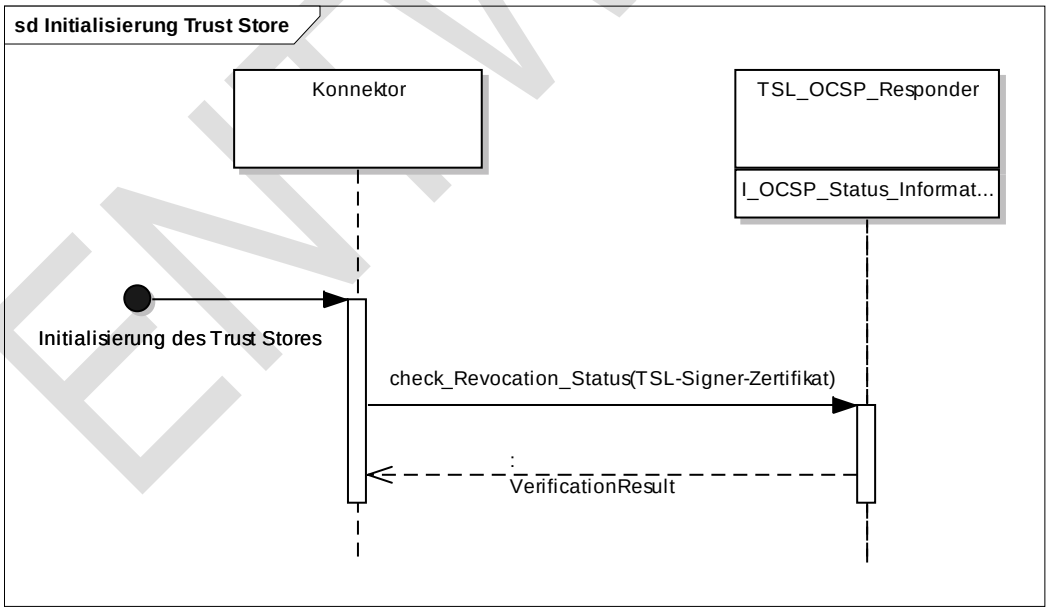


Abbildung 37: Ablauf: Initialisierung Trust Store

Bei Initialisierung oder Aktualisierung des Trust Stores wird im Rahmen der Validierung der TSL auch eine Zertifikatsprüfung des TSL-Signaturzertifikats durchgeführt. Außer für den Produkttyp Konnektor im Offline-Modus wird immer als Teilschritt dieser Zertifikatsprüfung der Status des Zertifikats ermittelt; dazu wird eine OCSP-Abfrage an den OCSP-Responder des TSL-Service-Providers gestellt.

ENTWURF

Falls die OCSP-Abfrage nicht möglich ist oder der Status des Zertifikats „revoked“ ist, darf die TSL nicht aktiviert werden. Eine vorhandene TSL muss in diesem Fall weiter verwendet werden.

Der am Beispiel Konnektor gezeigte Ablauf trifft auch für alle Produkttypen, die Zertifikate der TI prüfen zu.

Für Konnektoren im Offline-Modus findet die Zertifikatsprüfung (siehe [gemKPT_PKI_TIP#6.5.2]) ohne Prüfung des Sperrstatus statt. In diesem Fall ist eine Aktivierung der TSL auch ohne Prüfung des Sperrstatus möglich.⌫

7.2.7.2 Ablauf Zertifikat prüfen

⌦ TIP1-A_2426 Ablauf Zertifikat prüfen

Alle am Ablauf „Zertifikat prüfen“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

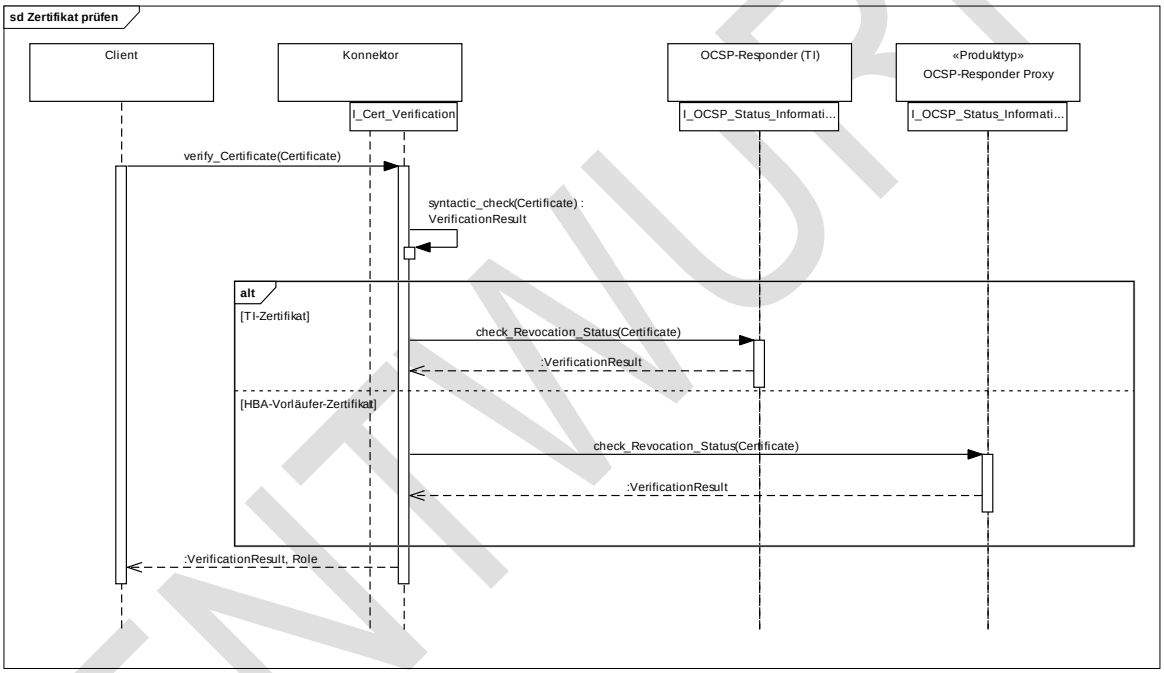


Abbildung 38: Ablauf: Zertifikat prüfen

Im Rahmen der Zertifikatsprüfung muss im Online-Fall der Zertifikatsstatus des zu prüfenden Zertifikats ermittelt werden, um festzustellen ob das Zertifikat nicht bereits gesperrt wurde. Für jedes zu prüfende Zertifikat ist über die TSL die Adresse des relevanten OCSP-Responders hinterlegt. Zur Steigerung der Verfügbarkeit sind Backup-Responder möglich, deren Adressen dann ebenfalls in der TSL hinterlegt sein müssen. Weitere Informationen zur Zertifikatsprüfung sind in [gemKPT_PKI_TIP#6.5] zu finden. Der am Beispiel Konnektor gezeigte Ablauf trifft auch für alle Produkttypen, die Zertifikate der TI prüfen zu. ⌫

7.2.8 Verzeichnis_Identitäten

7.2.8.1 Ablauf Abfrage des Verzeichnisses

⌦ TIP1-A_5821 Ablauf Abfrage des Verzeichnisses

ENTWURF

Alle am Ablauf „Abfrage des Verzeichnisses“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

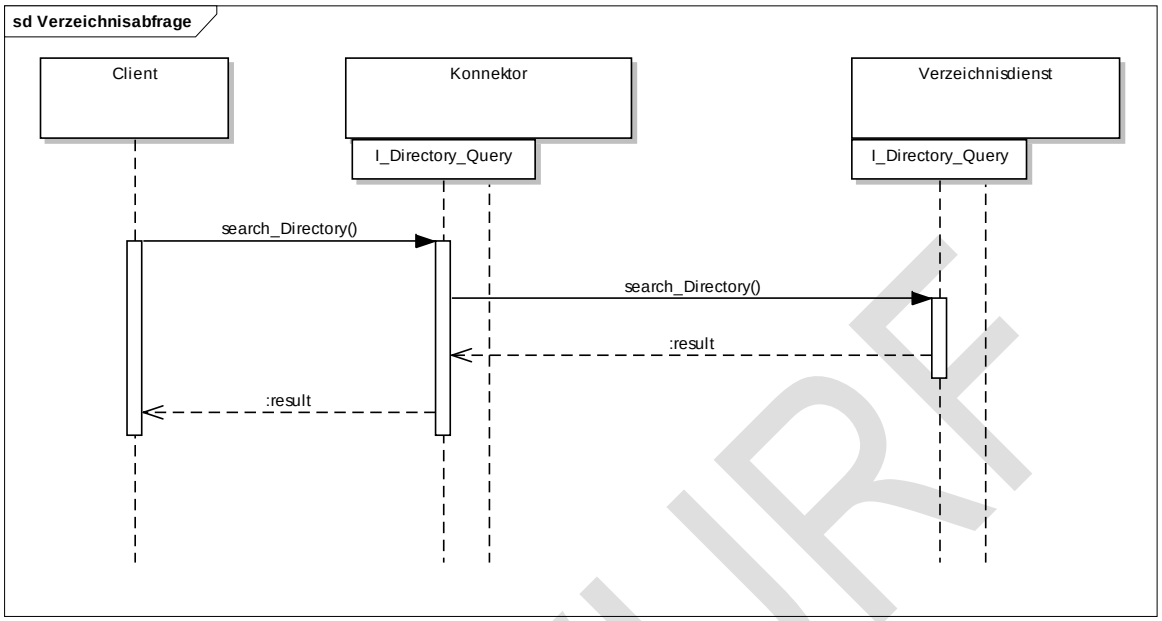


Abbildung 39: Abfrage des Verzeichnisses durch Clientsysteme und Fachmodule

Dieses Diagramm beschreibt den Aufbau einer Abfrage des Verzeichnisdienstes.

Mit einer Suchanfrage an den Verzeichnisdienst können Informationen aus dem Datenbestand des Verzeichnisdienstes ermittelt werden. Die Verzeichnisdienstabfrage (search_Directory) enthält einen Suchfilter. Der Konnektor leitet die Verzeichnisdienstanfrage unverändert weiter. Der Verzeichnisdienst sendet die Antwort mit den gefundenen Einträgen an den Konnektor welcher sie an den Aufrufer zurückgibt.

Das Protokoll zur Verzeichnisabfrage entspricht LDAP (RFC4511).

Zwischen Konnektor und Verzeichnisdienst wird eine TLS-Verbindung mit Server-Authentisierung aufgebaut. Der Verzeichnisdienst authentisiert sich dabei mit ID.ZD.TLS_S.

Der am Beispiel Konnektor gezeigte Ablauf trifft auch für den Consumer-Adapter der TI-Plattform im RZ-Consumer zu. ⌫

7.2.9 Namensauflösung

7.2.9.1 Ablauf FQDN des TI-Namensraums auflösen

⌦ TIP1-A_2427 Ablauf FQDN des TI-Namensraums auflösen

Alle am Ablauf „FQDN des TI-Namensraums auflösen“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

Abhängig von der Deployment-Variante kann die Namensauflösung nach einem der beiden folgenden Muster ablaufen:

ENTWURF

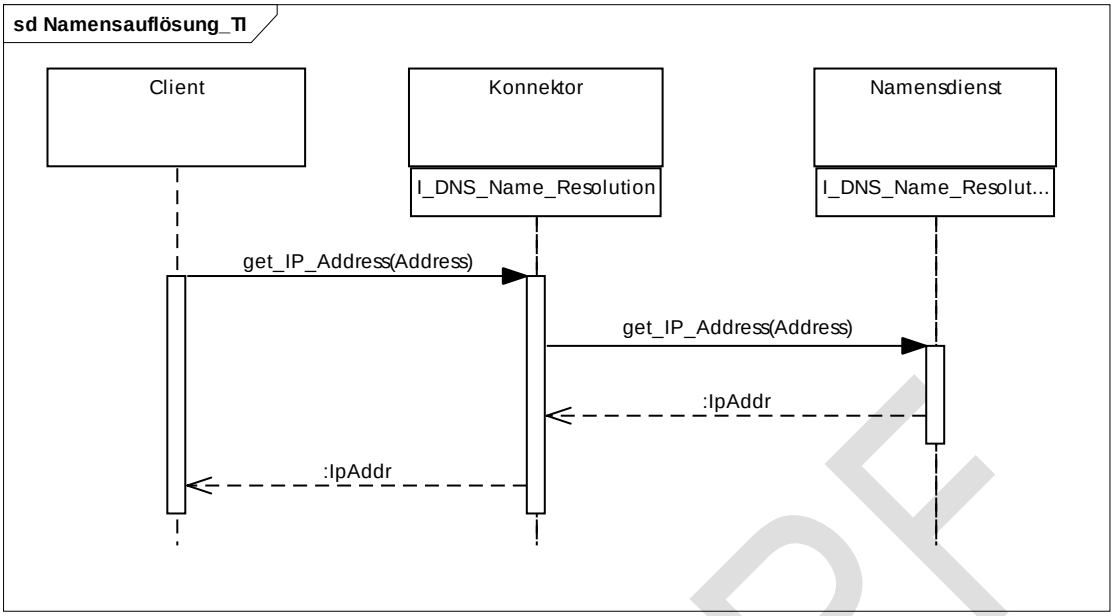


Abbildung 40: Ablauf: Namensauflösung

An der Auflösung eines Namens sind die Komponenten DNS-Client (Resolver) und DNS-Forwarder im Konnektor und der Namensdienst beteiligt. DNS-Forwarder und Namensdienst bieten jeweils die Schnittstelle I_DNS_Name_Resolution an und implementieren sie komponenten- bzw. dienstspezifisch. Der DNS-Client bietet die Schnittstelle I_DNS_Name_Information an. Der Produkttyp Konnektor enthält sowohl den DNS-Client als auch den DNS-Forwarder.

(Das Sequenzdiagramm kann die Komponenten nicht gleichzeitig mit den Schnittstellen und Produkttypen anzeigen, daher muss die Zuordnung der Schnittstellen zu den Komponenten hier verbal ergänzt werden.)

Der allgemeine Ablauf ist folgender: Ein Produkttyp der TI-Plattform baut eine Verbindung zu einem anderen Produkttyp der TI-Plattform auf und muss dazu den FQDN dieses Produkttypen in eine IP-Adresse auflösen. Der DNS-Client (Resolver) des Produkttypen sendet eine DNS-Abfrage mit dem aufzulösenden FQDN als Parameter an den DNS-Nameserver (Namensraum TI) des Namensdienstes. Der Namensdienst sendet eine DNSSEC-signierte Antwort, mit den zum angefragten FQDN passenden IP-Adressen an den anfragenden Produkttyp zurück. ~~Der DNS-Client muss die Antwort auf Authentizität und Integrität (DNSSEC) prüfen.~~ Jede Antwort auf eine Anfrage wird im Cache gespeichert.

Der am Beispiel Konnektor gezeigte Ablauf trifft auch für folgende Produkttypen zu, d. h. sie nutzen die Operation get_IP_Address am Interface I_DNS_Name_Resolution des Produkttypen Namensdienst:

- Konnektor
- Konfigurationsdienst
- OCSP-Responder Proxy
- Trust Service Provider
- gematik Root-CA

ENTWURF

- TSL-Dienst
- VPN-Zugangsdienst
- Zeitdienst
- Sicherheitsgateway Bestandsnetze
- Störungsampel
- Verzeichnisdienst
- Consumer-Adapter der TI-Plattform im RZ-Consumer ⌫

7.2.9.2 Ablauf FQDN für sichere Online-Anbindung auflösen

⌦ **TIP1-A_2428 Ablauf FQDN für sichere Online-Anbindung auflösen**

Alle am Ablauf „FQDN für sichere Online-Anbindung auflösen“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

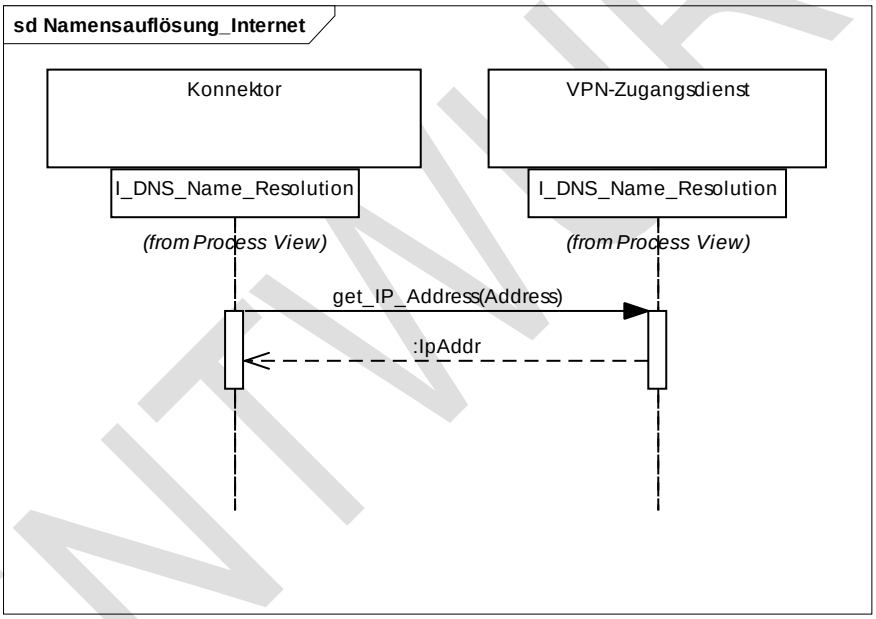


Abbildung 41: Ablauf: Namensauflösung Internet

Um eine Verbindung mit der TI aufbauen zu können muss der Konnektor den Namen des VPN-Servers beim VPN-Zugangsdienst auflösen. Der Konnektor sendet eine DNS-Abfrage mit dem aufzulösenden FQDN als Parameter an den DNS-Nameserver (Namensraum Transportnetz des VPN-Zugangsdienstes. Der DNS-Nameserver (Namensraum Transportnetz) des VPN-Zugangsdienstes sendet eine Antwort, mit den zum angefragten FQDN passenden IP-Adressen, an den Konnektor zurück. Jede Antwort auf eine Anfrage wird im Cache gespeichert.⌫

7.2.9.3 Ablauf FQDN aus ~~Bestandsnetzen~~ Netzen des Gesundheitswesens mit aAdG-NetG auflösen

⌦ **TIP1-A_2473 Ablauf FQDN aus ~~Bestandsnetzen~~ Netzen des Gesundheitswesens mit aAdG-NetG auflösen**

ENTWURF

Alle am Ablauf „FQDN aus ~~Bestandsnetzen~~ Netzen des Gesundheitswesens mit aAdG-NetG auflösen“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

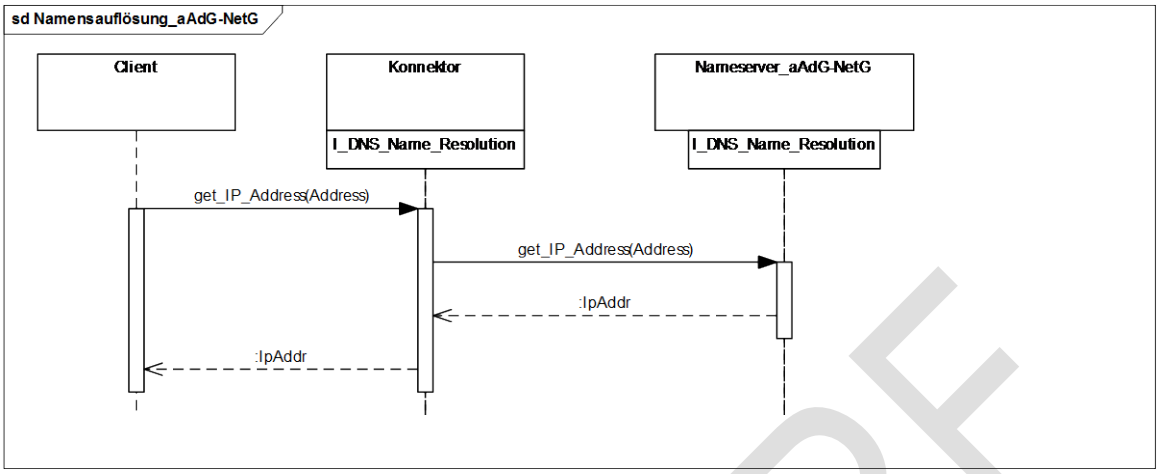


Abbildung 42: Ablauf: Namensauflösung ~~Bestandsnetz~~ Netzen des Gesundheitswesens mit aAdG-NetG

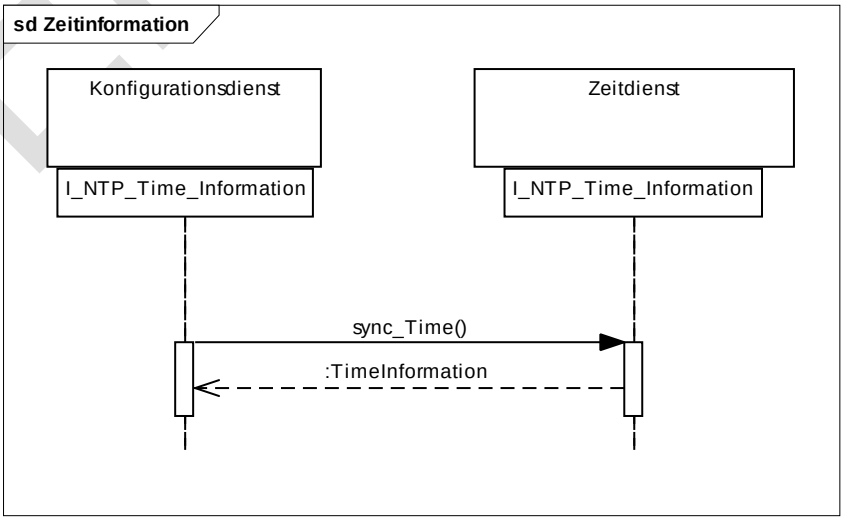
Um einen Dienst in einem ~~Bestandsnetz~~ Netz des Gesundheitswesens mit aAdG-NetG zu erreichen muss ein Client über den Konnektor den entsprechenden FQDN auflösen. Der Konnektor sendet eine DNS-Abfrage mit dem aufzulösenden FQDN als Parameter an den DNS-Nameserver (Namensraum ~~Bestandsnetz~~ Netz des Gesundheitswesens mit aAdG-NetG) des ~~Bestandsnetzes~~ Netzes des Gesundheitswesens mit aAdG-NetG. Der DNS-Nameserver sendet eine Antwort, mit den zum angefragten FQDN passenden IP-Adressen, an den Konnektor zurück. Jede Antwort auf eine Anfrage wird im Cache gespeichert.⌫

7.2.10 Zeitinformation

7.2.10.1 Ablauf Zeitinformation der TI abfragen

⌦ TIP1-A_2429 Ablauf Zeitinformation der TI abfragen

Alle am Ablauf „Zeitinformation der TI abfragen“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.



ENTWURF

Abbildung 43: Ablauf: Zeitinformation abfragen

Die Synchronisation mit dem Zeitdienst erfolgt nach den Regeln von NTP regelmäßig in festen oder variablen Zeitintervallen. Der NTP-Client des aufrufenden Produkttypen sendet ein NTP-Paket an den Zeitdienst. Der Zeitdienst sendet ein NTP-Paket an den NTP-Client zurück. Der Client errechnet einen Korrekturwert auf Basis der ausgetauschten Zeitstempel und korrigiert seine Systemzeit.

Folgende Produkttypen nutzen die Operation sync_Time am Interface I_NTP_Time_Information des Produkttypen Zeitdienst:

- Konfigurationsdienst
- OCSP-Responder Proxy
- Trust Service Provider X.509 QES
- Trust Service Provider X.509 nonQES
- gematik Root-CA
- TSL-Dienst
- VPN-Zugangsdienst
- Störungsampel
- Sicherheitsgateway Bestandsnetze
- Consumer-Adapter der TI-Plattform im RZ-Consumer

Der VPN-Zugangsdienst stellt ebenfalls die Schnittstelle I_NTP_Time_Information bereit, die vom Konnektor genutzt wird.

Der Konnektor stellt die Schnittstelle I_NTP_Time_Information den Clientsystemen bereit.

Die Synchronisation zwischen den Zeitservern von VPN-Zugangsdienst mit denen des Zeitdienstes sowie vom Konnektor mit den Zeitservern des VPN-Zugangsdienstes erfolgt ebenfalls über die Schnittstelle I_NTP_Time_Information. ⌫

7.2.11 Kartenzugriff

7.2.11.1 Ablauf generische Kartenoperation

⌦ **TIP1-A_2430 Ablauf generische Kartenoperation**

Alle am Ablauf „Generische Kartenoperation“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

ENTWURF

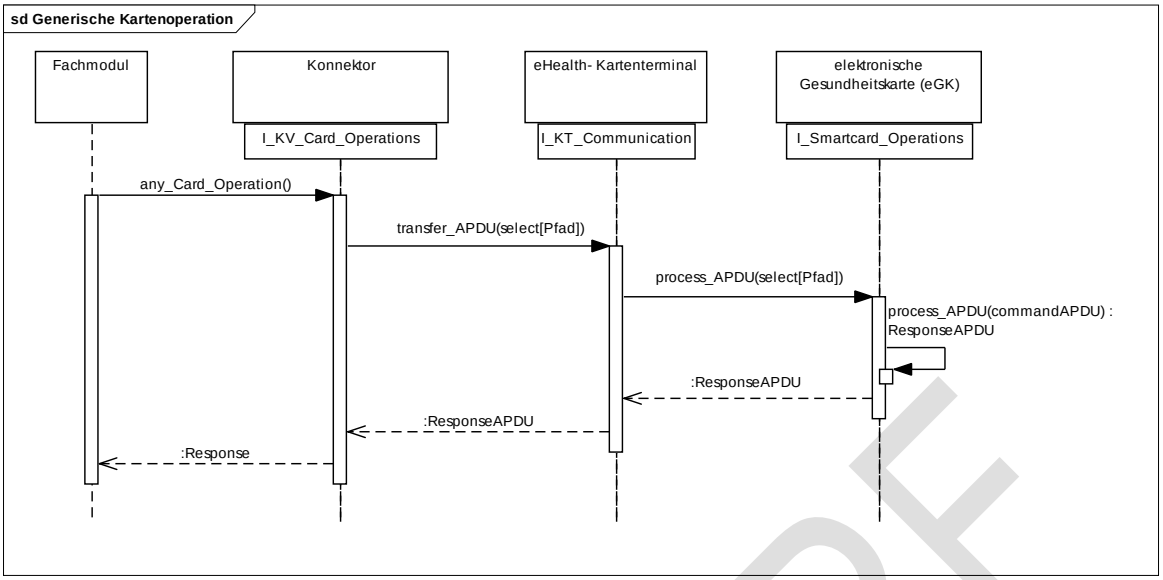


Abbildung 44: Ablauf: Generische Kartenoperation

Dieses Diagramm beschreibt den typischen Ablauf bei der Nutzung einer Kartenfunktion. Auslösender Akteur ist hier ein Fachmodul. Es ruft eine der Operationen aus dem Interface I_KV_Card_Operations auf, hier stellvertretend für alle any_Card_Operation genannt. Der Konnektor konstruiert daraus ein Kartenkommando (APDU) und sendet es über eine sichere Kommunikations-strecke an das Kartenterminal. Dieses erkennt, dass das Kommando für eine der gesteckten Karten bestimmt ist und leitet es dorthin weiter. Die Karte verarbeitet das Kommando und liefert eine Antwort zurück.

Zwischen Konnektor und eHealth-Kartenterminal wird eine TLS-Verbindung mit gegenseitiger Authentisierung und einem Pairing genutzt. Der Konnektor authentisiert sich dabei mit ID.SAK.AUT, das Kartenterminal mit ID.SMKT.AUT.

Der am Beispiel eGK gezeigte Ablauf trifft auch für die Produkttypen HBA, SMC-B und HSM-B zu.

Die Kommunikation zum HSM-B erfolgt nicht über das eHealth-Kartenterminal sondern über die Schnittstelle I_HSM_Operations direkt zwischen Konnektor und HSM-B.

HINWEIS: Die Übertragungsstrecke zwischen eHealth-Kartenterminal und Karte wird nicht über technische Mechanismen gesichert.⌫

⌦ **TIP1-A_5421 Ablauf generische Kartenoperation mit MobKT**

Alle am Ablauf „generische Kartenoperation mit MobKT“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

ENTWURF

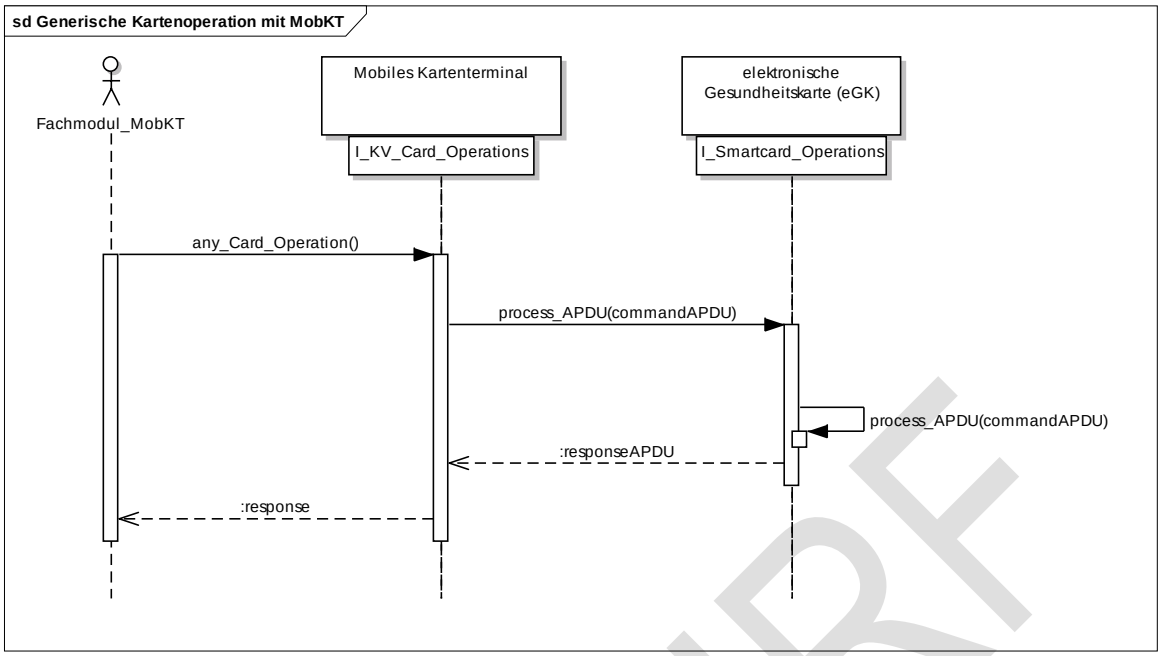


Abbildung 45: Ablauf: Generische Kartenoperation mit MobKT

Dieses Diagramm beschreibt den typischen Ablauf bei der Nutzung einer Kartenfunktion über das Mobile Kartenterminal. Auslösender Akteur ist ein Fachmodul für Mobile Kartenterminals. Es ruft eine der Operationen aus dem Interface I_KV_Card_Operations auf, hier stellvertretend für alle any_Card_Operation genannt. Das Mobile Kartenterminal konstruiert daraus ein Kartenkommando (APDU) und sendet es an die Karte. Die Karte verarbeitet das Kommando und liefert eine Antwort zurück.

Der am Beispiel eGK gezeigte Ablauf trifft auch für die Produkttypen HBA und SMC-B zu.

HINWEIS: Die Übertragungsstrecke zwischen Mobilem Kartenterminal und Karte wird nicht über technische Mechanismen gesichert.⌫

7.2.11.2 Ablauf PIN-Eingabe direkt

⌦ **TIP1-A_2431 Ablauf PIN-Eingabe direkt**

Alle am Ablauf „PIN-Eingabe direkt“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

ENTWURF

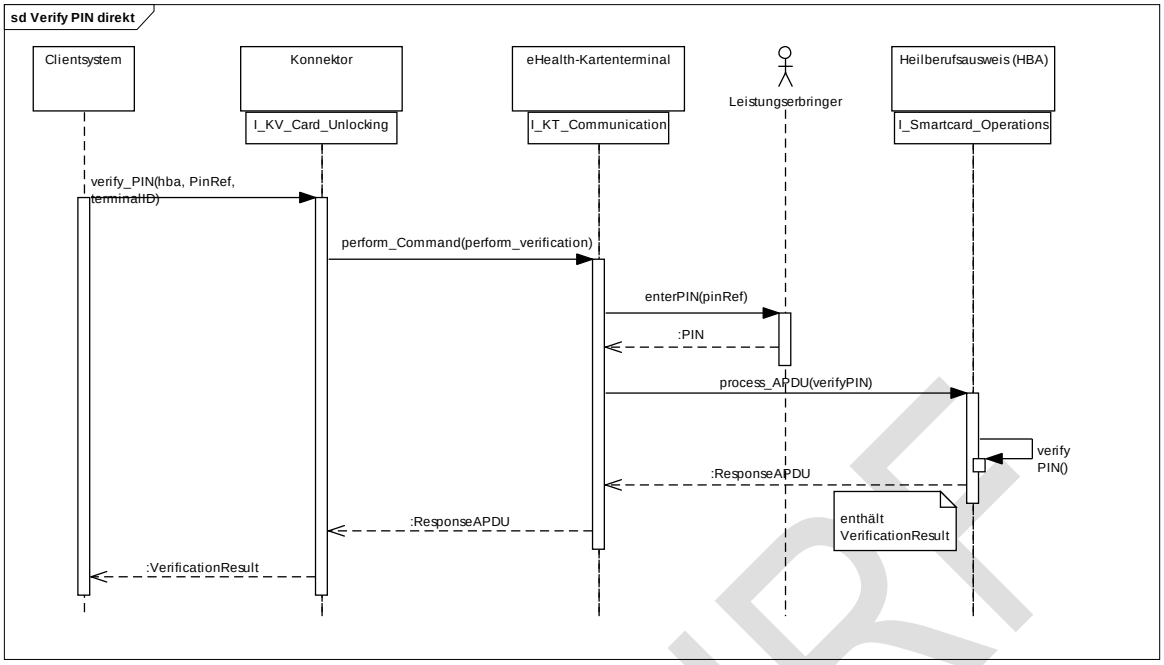


Abbildung 46: Ablauf: Verify PIN direkt

Bei der direkten PIN-Eingabe wird die PIN an demselben Kartenterminal abgefragt, in dem auch die Karte steckt. Der Konnektor konstruiert ein Kartenterminalkommando, das seinerseits ein Kartenkommando enthält, und sendet es an das angegebene Kartenterminal. Dieses erfragt die PIN beim Anwender, fügt sie in das eingebettete Kartenkommando ein und sendet es an die Karte weiter. Die Karte prüft die PIN und liefert das Ergebnis zurück.

Zwischen Konnektor und eHealth-Kartenterminal wird eine TLS-Verbindung mit gegenseitiger Authentisierung und einem Pairing genutzt. Der Konnektor authentisiert sich dabei mit ID.SAK.AUT, das Kartenterminal mit ID.SMKT.AUT.

Der am Beispiel HBA gezeigte Ablauf trifft auch für die Produkttypen SMC-B und HSM-B zu.

Die Kommunikation zum HSM-B erfolgt nicht über das eHealth-Kartenterminal sondern über die Schnittstelle I_HSM_Operations direkt zwischen Konnektor und HSM-B.

Die PIN-Eingabe für ein HSM-B erfolgt nicht über das eHealth-Kartenterminal, sondern am HSM-B direkt.

HINWEIS: Die Übertragungsstrecke zwischen eHealth-Kartenterminal und Karte wird nicht über technische Mechanismen gesichert.⌫

⌦ **TIP1-A_5422 Ablauf PIN-Eingabe mit MobKT**

Alle am Ablauf „PIN-Eingabe mit MobKT“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

ENTWURF

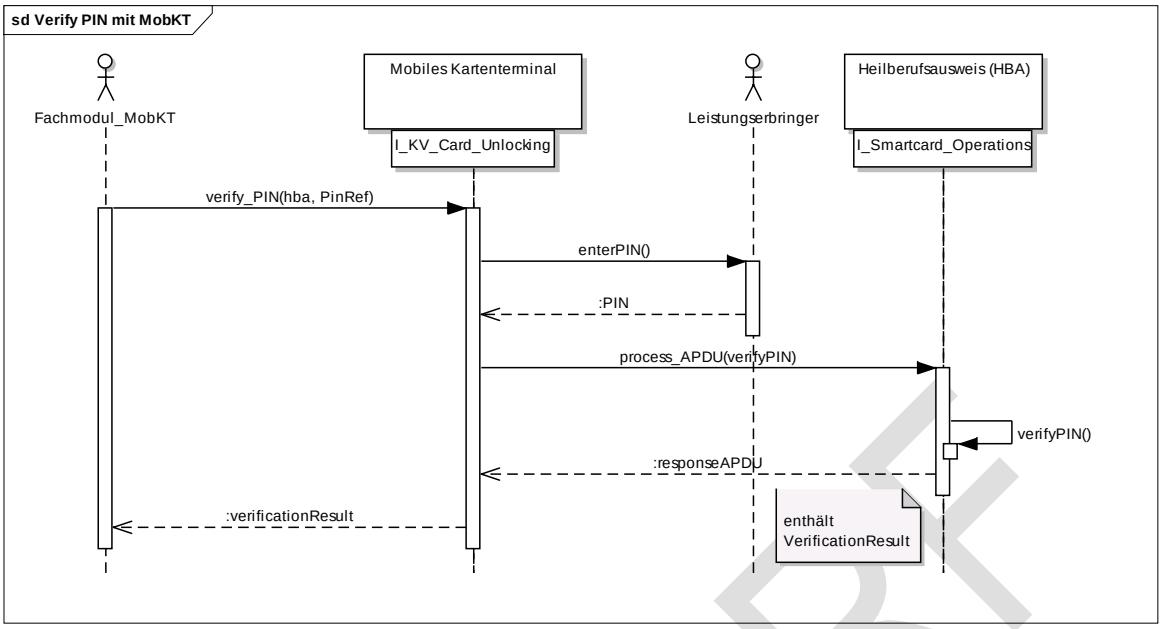


Abbildung 47: Ablauf: Verify PIN mit MobKT

Das Mobile Kartenterminal erfragt die PIN beim Anwender, fügt sie in das Kartenkommando ein und sendet es an die Karte weiter. Die Karte prüft die PIN und liefert das Ergebnis zurück.

Der am Beispiel HBA gezeigte Ablauf trifft auch für den Produkttyp SMC-B zu.

HINWEIS: Die Übertragungsstrecke zwischen Mobilem Kartenterminal und Karte wird nicht über technische Mechanismen gesichert.⌫

7.2.11.3 Ablauf PIN-Eingabe mit Remote_PIN

⌦ **TIP1-A_2432 Ablauf PIN-Eingabe mit Remote_PIN**

Alle am Ablauf „PIN-Eingabe mit Remote_PIN“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

ENTWURF

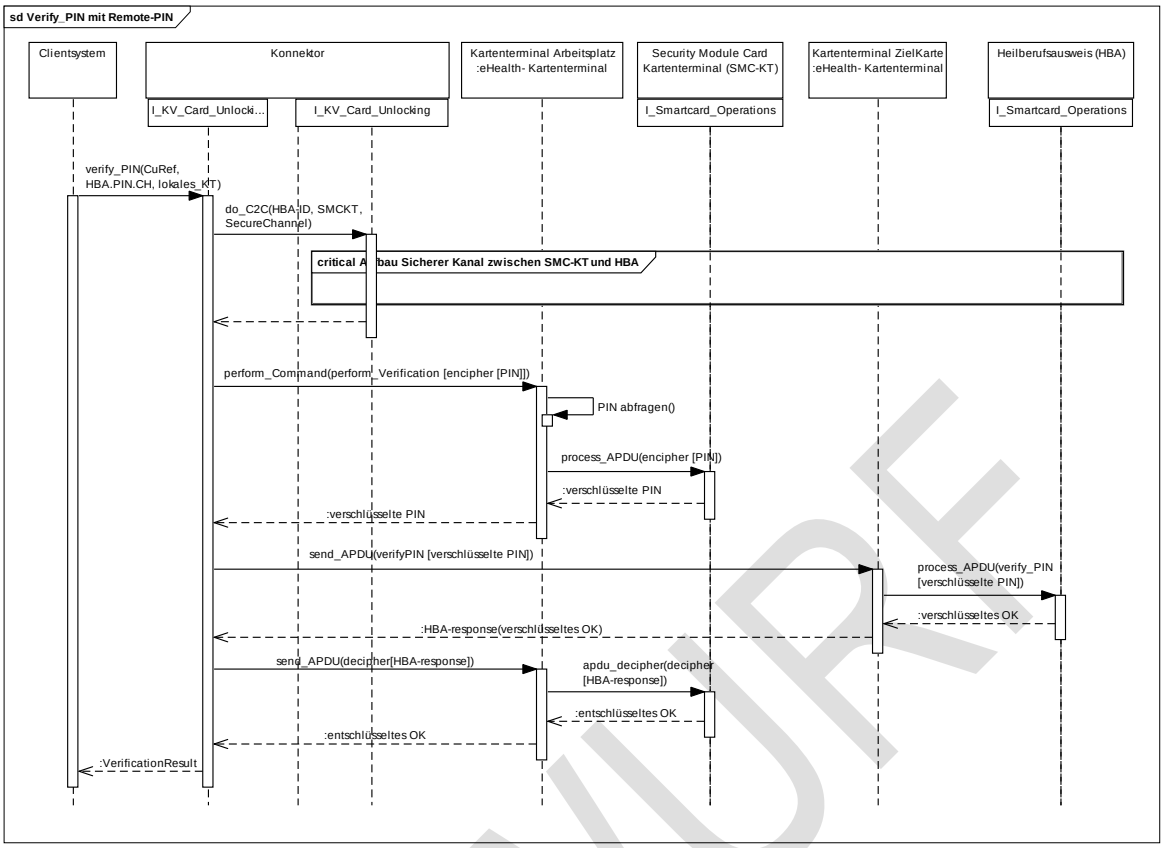


Abbildung 48: Ablauf: PIN-Eingabe mit Remote_PIN

Für eine PIN-Eingabe per Remote-PIN muss ein Aufrufer außer der Karte, die die PIN prüfen soll (Remote-PIN-Empfänger), und der PIN-Reference auch ein Kartenterminal angeben, das die PIN-Eingabe entgegennehmen soll – im Diagramm als „Kartenterminal Arbeitsplatz“ bezeichnet, da es am Arbeitsplatz des Leistungserbringers oder Kostenträgers steht. Es wird vorausgesetzt, dass in diesem Kartenterminal immer eine Karte mit einem CV-Zertifikat steckt, die die Rolle „Remote-PIN-Sender“ übernehmen kann. Die Karte in der Rolle des Remote-PIN-Empfängers kann in einem beliebigen Kartenterminal im LAN des Leistungserbringers oder Kostenträgers stecken.

Nach dem Aufbau eines Sicheren Kanals zwischen dem Remote-PIN-Sender im lokalen Terminal und dem Remote-PIN-Empfänger (d.h. Aushandeln eines gemeinsamen symmetrischen Schlüssels zwischen diesen beiden Karten) wird der Nutzer zur Eingabe der PIN am lokalen Terminal aufgefordert. Das Kartenterminal übergibt die PIN an den Remote-PIN-Sender, der sie in verschlüsselter Form über den Konnektor an die Zielkarte zum Entschlüsseln und Prüfen sendet. Schließlich muss das verschlüsselte Verifikationsergebnis noch vom Remote-PIN-Sender entschlüsselt und dann vom Kartenterminimal an den Konnektor übergeben werden.

Zwischen Konnektor und den eHealth-Kartenterminals werden TLS-Verbindungen mit gegenseitiger Authentisierung und einem Pairing genutzt. Der Konnektor authentisiert sich dabei mit ID.SAK.AUT, die Kartenterminals mit ID.SMKT.AUT.

Der am Beispiel HBA gezeigte Ablauf trifft auch für die Produkttypen SMC-B und HSM-B zu.

ENTWURF

Die Kommunikation zum HSM-B erfolgt nicht über das eHealth-Kartenterminal, sondern direkt zwischen Konnektor und HSM-B.

HINWEIS: Die Übertragungsstrecke zwischen eHealth-Kartenterminals und Karten wird nicht über technische Mechanismen gesichert.⌫

7.2.12 Sichere Online-Anbindung

7.2.12.1 Ablauf Aufbau eines sicheren Kanals zur Anbindung an die zentrale TI-Plattform

⌦ **TIP1-A_2433 Ablauf Aufbau eines sicheren Kanals zur Anbindung an die zentrale TI-Plattform**

Alle am Ablauf „Aufbau eines sicheren Kanals zur Anbindung an die zentrale TI-Plattform“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

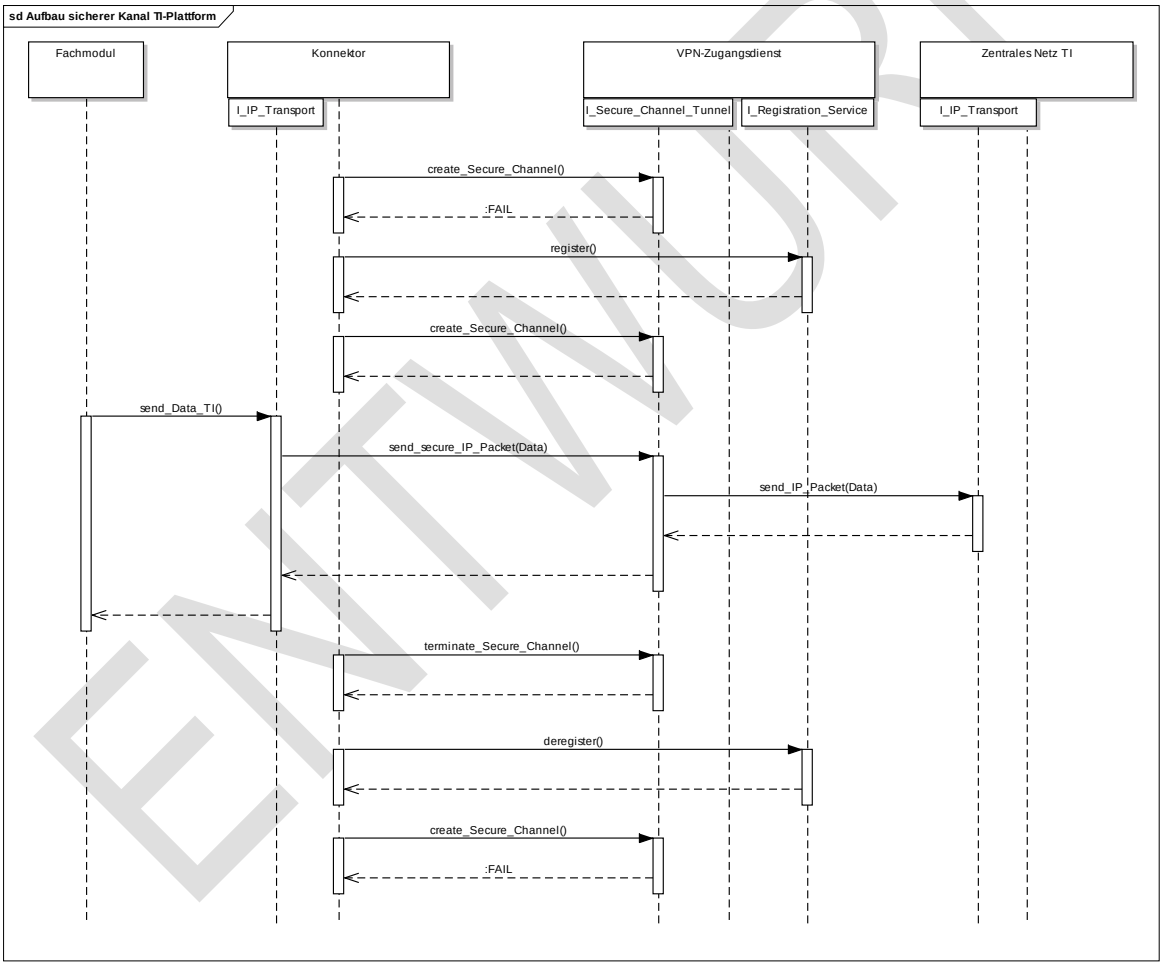


Abbildung 49: Ablauf: Aufbau eines sicheren Kanals zur Anbindung an die Zentrale TI-Plattform

Dieses Diagramm beschreibt den Aufbau eines sicheren Kanals (Secure Channel) zwischen Konnektor und dem VPN-Zugangsdienst.

Der sichere Kanal wird auf Basis von IPsec unter Nutzung von IKEv2 im Tunnel-Modus mit gegenseitiger Authentisierung aufgebaut. Der VPN-Zugangsdienst

ENTWURF

verwendet dabei die Identität ID.VPNK.VPN, der Konnektor die Identität ID.NK.VPN.

Der Zertifikatsstatus der Identität ID.VPNK.VPN wird über eine CRL geprüft.

Zur Nutzung der Schnittstelle I_Registration_Service wird zwischen Konnektor und VPN-Zugangsdienst eine TLS-Verbindung mit gegenseitiger Authentisierung aufgebaut. Der Konnektor authentisiert sich dabei mit ID.HCI.AUT der am Registrierungsprozess beteiligten SMC-B, der VPN-Zugangsdienst mit ID.ZD.TLS-S.

Für das Zertifikat ID.ZD.TLS-S wird beim Aufbau dieser Verbindung auf eine Statusprüfung verzichtet.

Die Operationen register und deregister müssen nur einmalig genutzt werden, um einen Konnektor bei Inbetriebnahme für die Kommunikation in das zentrale Netz freizuschalten oder wieder zu sperren, wenn dieser außer Betrieb genommen wird.⌫

7.2.13 Sicherer Internetzugang

7.2.13.1 Ablauf Aufbau eines sicheren Kanals zur Anbindung des sicheren Internetzugangs

⌦ **TIP1-A_3684 Ablauf Aufbau eines sicheren Kanals zur Anbindung des sicheren Internetzugangs**

Alle am Ablauf „Aufbau eines sicheren Kanals zur Anbindung des sicheren Internetzugangs“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

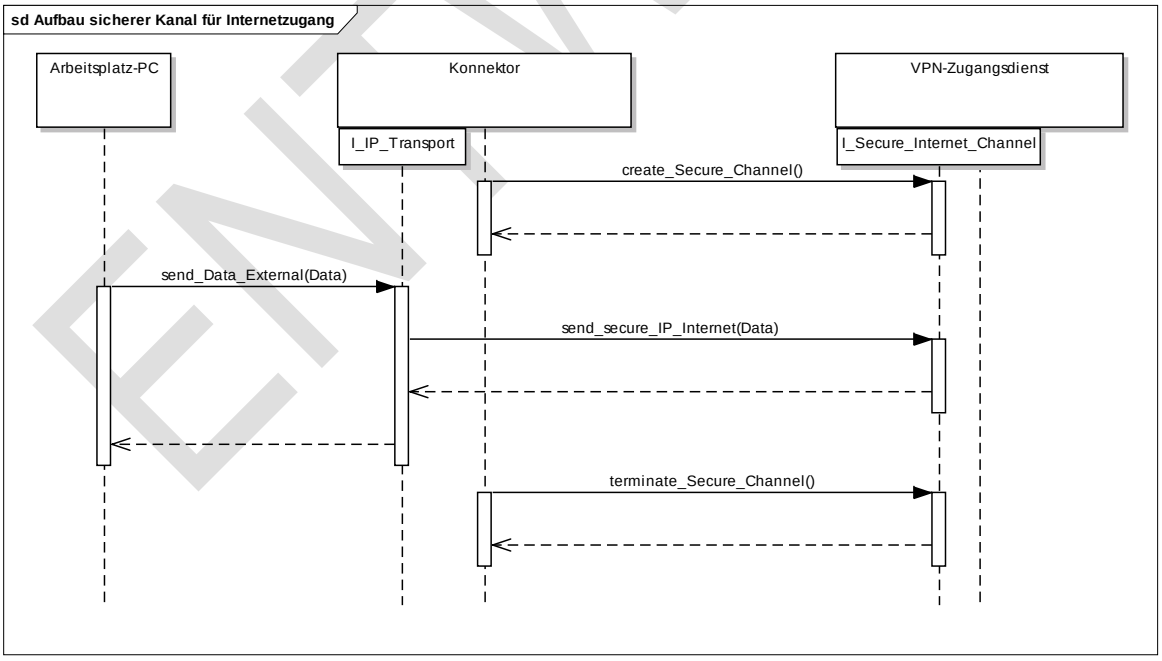


Abbildung 50: Ablauf: Aufbau eines sicheren Kanals zur Anbindung des sicheren Internetzugangs

Dieses Diagramm beschreibt den Aufbau eines sicheren Kanals (Secure Channel) zwischen Konnektor und dem VPN-Zugangsdienst.

ENTWURF

Der sichere Kanal wird auf Basis von IPsec unter Nutzung von IKEv2 im Tunnel-Modus mit gegenseitiger Authentisierung aufgebaut. Der VPN-Zugangsdienst verwendet dabei die Identität ID.VPNK.VPN-SIS, der Konnektor die Identität ID.NK.VPN.

Der Zertifikatsstatus der Identität ID.VPNK.VPN-SIS wird über eine CRL geprüft. ⌫

ENTWURF

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
A	Administrator
aAdG	andere Anwendungen des Gesundheitswesens (mit Zugriff auf Dienste der TI)
aAdG-NetG	andere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens
aAdG-NetG-TI	andere Anwendungen des Gesundheitswesens mit Zugriff auf Dienste der TI aus angeschlossenen Netzen des Gesundheitswesens
APDU	Application Protocoll Data Unit
AUT	Authentication
BNetzA	Bundesnetzagentur
C2C	Card to Card
CA	Certificate Authority
CMS	Card Management Service
CS	Clientsystem
CVC	Card Verifiable Certificate
DNS	Domain Name Service
DNSSEC	Domain Name System Security Extensions
eGK	elektronische Gesundheitskarte
FAD	fachanwendungsspezifischer Dienst
FM	Fachmodul
FQDN	Fully Qualified Domain Name
GA	Gesamtarchitektur
GS	Geschäftsstelle
GUI	Graphical User Interface
HBA	Heilberufsausweis
HCA	
HSM	Hardware Security Module
ID	Identifier
IP	Internet Protocol
ISP	Internet Service Provider
KSR	Konfigurations- und Software-Repository

ENTWURF

Kürzel	Erläuterung
KT	Kartenterminal
KTR	Kostenträger
KV	Krankenversicherung
LAN	Local Area Network
LE	Leistungserbringer
LH	Lastenheft
MFM	Fachmodul MobKT
NAT	Network Adress Translation
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OSI	Open Systems Interconnection
P	Provider Zone
PIN	Personal Identification Number
PKI	Public Key Infrastructure
QES	qualifizierte elektronische Signatur
SAK	Signaturanwendungskomponente
SC	Secure Consumer Zone
SIS	Secure Internet Service
SM	Sicherheitsmodul
SMC	Security Module Card
SNK	Sicheres Netz der KVen
SSEE	sichere Signaturerstellungseinheit
SÜV	sicheres Übermittlungsverfahren
TCP	Transmission Control Protocol
TI	Telematikinfrastruktur
TI_D	TI-Plattform Zone dezentral
TI_Z	TI-Plattform Zone zentral
TIP	Telematikinfrastruktur-Plattform
TLS	Transport Layer Security
TSL	Trust-service Status List
TSP	Trust Service Provider
UDP	User Datagram Protocol
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus

ENTWURF

Kürzel	Erläuterung
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
ZN	zentrales Netz

A2 – Glossar

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

Abbildung 1: Dienst-Kategorien der TI-Plattform 13
Abbildung 2: Anwendungskategorien von weiteren Anwendungen 15
Abbildung 3: Modellierung der TI mittels Produkttypen, Produkten und Produktinstanzen 16
Abbildung 4: Logische Architekturschichten (Zonen) und Building Blocks 17
Abbildung 5: Außensicht der TI-Plattform 30
Abbildung 6: Domänenmodell Karten der TI 33
Abbildung 7: CardUsageReference 41
Abbildung 8: Beteiligte Komponenten beim Remote-PIN-Verfahren 44
Abbildung 9: Übersicht des Gesamtsystems der TI 49
Abbildung 10: Produkttypsicht 50
Abbildung 11: Datenmodell Verzeichnisdienst 69
Abbildung 12: Netzwerktopologie der TI 143
Abbildung 13: Netzwerkverbindungen dezentral 144
Abbildung 14: Netztopologie Zugangsnetz 144
Abbildung 15: Netztopologie Zentrales Netz 145
Abbildung 16: Netztopologie Sicherheitsgateway Bestandsnetze 146
Abbildung 17: Netztopologie Sicherer Internetzugang 147
Abbildung 18: Messpunkte des Datenvolumens im Netzwerk der TI-Plattform 149
Abbildung 19: Ablauf: Erstellung digitale Signatur 155
Abbildung 20: Ablauf: Prüfung digitale Signatur 156
Abbildung 21: Ablauf: TSL-Validierung 157
Abbildung 22: Ablauf: Prüfung von X.509-Zertifikaten 158
Abbildung 23: Ablauf: Benutzerinteraktion am Kartenterminal 159
Abbildung 24: Ablauf: QES erzeugen 160
Abbildung 25: Ablauf: QES prüfen 161

ENTWURF

Abbildung 26: Ablauf: Anmeldung zur Notifikation und anschließende Notifikation durch Kartenevent, bzw. Fachmodulmeldung 162

Abbildung 27: Ablauf: Sammeln der Umgebungsinformationen und anschließende Abfrage RessourcenInfo durch Clientsystem 163

Abbildung 28: Ablauf: Anzeigen verfügbarer Aktualisierungen 164

Abbildung 29: Ablauf: Konnektor aus Konfigurationsdienst aktualisieren 165

Abbildung 30: Ablauf: eHealth-Kartenterminal aus Konfigurationsdienst aktualisieren ..165

Abbildung 31: Ablauf: ~~Bestands~~Netzkonfigurationen aAdG-NetG aktualisieren....166

Abbildung 32: Ablauf: Anzeigen verfügbarer Pakete für Fachmodul....167

Abbildung 33: Ablauf: Paket für Fachmodul aus KSR laden....168

Abbildung 34: Ablauf: Aktualisierung der TSL über die TI-Plattform....169

Abbildung 35: Ablauf: Aktualisierung der BNetzA-VL über die TI-Plattform....170

Abbildung 36: Ablauf: Aktualisierung der CRL im Konnektor....171

Abbildung 37: Ablauf: Initialisierung Trust Store....171

Abbildung 38: Ablauf: Zertifikat prüfen 172

Abbildung 39: Abfrage des Verzeichnisses durch Clientsysteme und Fachmodule....173

Abbildung 40: Ablauf: Namensauflösung 174

Abbildung 41: Ablauf: Namensauflösung Internet 175

Abbildung 42: Ablauf: Namensauflösung ~~Bestandsnetz~~ Netzen des Gesundheitswesens mit aAdG-NetG 176

Abbildung 43: Ablauf: Zeitinformation abfragen....177

Abbildung 44: Ablauf: Generische Kartenoperation....178

Abbildung 45: Ablauf: Generische Kartenoperation mit MobKT....179

Abbildung 46: Ablauf: Verify PIN direkt 180

Abbildung 47: Ablauf: Verify PIN mit MobKT....181

Abbildung 48: Ablauf: PIN-Eingabe mit Remote_PIN....182

Abbildung 49: Ablauf: Aufbau eines sicheren Kanals zur Anbindung an die Zentrale TI-Plattform 183

Abbildung 50: Ablauf: Aufbau eines sicheren Kanals zur Anbindung des sicheren Internetzugangs....184

Abbildung 51: Informationsmodell der TI-Plattform 204

A4 – Tabellenverzeichnis

Tabelle 1: Kommunikationsmatrix TI (Zonen)....18

Tabelle 2: Zugriffsberechtigter Personenkreis (PK) nach §291a SGB V....22

Tabelle 3: Personenkreis ohne Zugriffsberechtigung nach §291a SGB V 23

Tabelle 4: Fachliche Rollen....23

ENTWURF

Tabelle 5: Tab_ArchTIP_002 Rollenmodell in der Außensicht der TI-Plattform 23
Tabelle 6: Betriebliche Rollen 24
Tabelle 7: Technische Rollen 25
Tabelle 8: Smartcards in der TI 31
Tabelle 9: Karten-Objekttypen und Domänen-Mapping 37
Tabelle 10: Operationen auf Karten der TI 38
Tabelle 11: Mapping logische Smartcard- zu Konnektor-Schnittstellen 39
Tabelle 12: Schnittstellen und Prozesse des Produkttyps eGK 53
Tabelle 13: Schnittstellen und Prozesse des Produkttyps HBA 54
Tabelle 14: Schnittstellen und Prozesse des Produkttyps SMC-B 54
Tabelle 15: Schnittstellen und Prozesse des Produkttyps HSM-B 55
Tabelle 16: Schnittstellen und Prozesse des Produkttyps gSMC-KT 56
Tabelle 17: Schnittstellen und Prozesse des Produkttyps gSMC-K 56
Tabelle 18: Schnittstellen und Prozesse des Produkttyps eHealth-Kartenterminal 57
Tabelle 19: Schnittstellen und Prozesse des Produkttyps Mobiles Kartenterminal 59
Tabelle 20: Schnittstellen und Prozesse des Produkttyps Konnektor 61
Tabelle 21: Schnittstellen und Prozesse des Produkttyps Zentrales Netz TI 65
Tabelle 22: Schnittstellen und Prozesse des Produkttyps Zeitdienst 66
Tabelle 23: Schnittstellen und Prozesse des Produkttyps Namensdienst 67
Tabelle 24: Schnittstellen und Prozesse des Produkttyps Verzeichnisdienst 68
Tabelle 25: Schnittstellen und Prozesse des Produkttyps TSL-Dienst 71
Tabelle 26: Schnittstellen und Prozesse des Produkttyps Konfigurationsdienst 72
Tabelle 27: Schnittstellen und Prozesse des Produkttyps VPN-Zugangsdienst 73
Tabelle 28: Schnittstellen und Prozesse des Produkttyps Sicherheitsgateway Bestandsnetze 75
Tabelle 29: Schnittstellen und Prozesse des Produkttyps Trust Service Provider X.509 nonQES 76
Tabelle 30: Schnittstellen und Prozesse des Produkttyps Trust Service Provider X.509 QES 77
Tabelle 31: Schnittstellen und Prozesse des Produkttyps Trust Service Provider CVC 78
Tabelle 32: Schnittstellen und Prozesse des Produkttyps CVC-Root 78
Tabelle 33: Schnittstellen und Prozesse des Produkttyps OCSP-Responder Proxy 78
Tabelle 34: Schnittstellen und Prozesse des Produkttyps Störungsampel 79
Tabelle 35: Schnittstellen und Prozesse des Produkttyps Service Monitoring 80
Tabelle 36: Legende zu den Abkürzungen in den Operationstabellen 82
Tabelle 37: Operation interact_with_User 83
Tabelle 38: Operation sign_Document 83

ENTWURF

Tabelle 39: Operation verify_Document 84
Tabelle 40: Operation external_Authenticate 85
Tabelle 41: Operation get_Certificate 85
Tabelle 42: Operation sign_Document_QES 86
Tabelle 43: Operation verify_Document_QES 87
Tabelle 44: Operation get_Metadata 88
Tabelle 45: Operation issue_Identity_Assertion 88
Tabelle 46: Operation renew_Identity_Assertion 89
Tabelle 47: Operation cancel_Identity_Assertion 89
Tabelle 48: Operation signin 90
Tabelle 49: Operation signout 90
Tabelle 50: Operation sign_Token 91
Tabelle 51: Operation get_Ressource_List 91
Tabelle 52: Operation get_Ressource_Information 92
Tabelle 53: Operation notify 92
Tabelle 54: Operation notify 93
Tabelle 55: Operation register_for_Notifications 94
Tabelle 56: Operation list_available_Updates 94
Tabelle 57: Operation do_Update 95
Tabelle 58: Operation list_available_Packages 95
Tabelle 59: Operation load_Package 96
Tabelle 60: Operation do_local_Update 96
Tabelle 61: Operation perform_Update 96
Tabelle 62: Operation get_Card_Usage_Reference 97
Tabelle 63: Operation discard_Card_Usage_Reference 97
Tabelle 64: Operation handle_Session 98
Tabelle 65: Operation verify_PIN 99
Tabelle 66: Operation unblock_PIN 99
Tabelle 67: Operation initialize_PIN 100
Tabelle 68: Operation change_PIN 100
Tabelle 69: Operation enable_PIN 100
Tabelle 70: Operation disable_PIN 101
Tabelle 71: Operation get_PIN_Status 101
Tabelle 72: Operation do_C2C 101
Tabelle 73: Operation send_Secure 102
Tabelle 74: Operation verify_Certificate 103

ENTWURF

Tabelle 75: Operation encrypt_Document 103
Tabelle 76: Operation decrypt_Document 104
Tabelle 77: Operation encrypt_Document_Symmetric 105
Tabelle 78: Operation decrypt_Document_Symmetric 105
Tabelle 79: Operation get_Role 106
Tabelle 80: Operation search_Directory 106
Tabelle 81: Operation read_Data 107
Tabelle 82: Operation erase_Data 107
Tabelle 83: Operation write_Data 107
Tabelle 84: Operation get_Data 108
Tabelle 85: Operation put_Data 108
Tabelle 86: Operation get_Data 108
Tabelle 87: Operation put_Data 109
Tabelle 88: Operation show_Data 109
Tabelle 89: Operation type_Data 109
Tabelle 90: Operation print_Document 110
Tabelle 91: Operation configure_MobKT 110
Tabelle 92: Operation get_Service_Information 111
Tabelle 93: Operation get_IP_Address 111
Tabelle 94: Operation get_IP_Address 112
Tabelle 95: Operation sync_Time 112
Tabelle 96: Operation get_Time 113
Tabelle 97: Operation set_System_Time 113
Tabelle 98: Operation extract_card_data 113
Tabelle 99: Operation read_Card_Data 114
Tabelle 100: Operation read_KVK 114
Tabelle 101: Operation write_Card_Data 114
Tabelle 102: Operation erase_Card_Data 115
Tabelle 103: Operation verify_eGK 115
Tabelle 104: Operation write_eGK_Protocol 115
Tabelle 105: Operation read_eGK_Protocol 116
Tabelle 106: Operation decrypt_Data 116
Tabelle 107: Operation sign_Data 116
Tabelle 108: Operation get_Random 117
Tabelle 109: Operation send_APDU 117
Tabelle 110: Operation do_Reset 117

ENTWURF

Tabelle 111: Operation configure_KTs 118
Tabelle 112: Operation perform_Command 118
Tabelle 113: Operation transfer_APDU 119
Tabelle 114: Operation write_Data 119
Tabelle 115: Operation read_Data 119
Tabelle 116: Operation erase_Data 120
Tabelle 117: Operation send_Data_TI 120
Tabelle 118: Operation send_Data_External 121
Tabelle 119: Operation set_CS_Access_Mode 121
Tabelle 120: Operation add_Clientsystem 122
Tabelle 121: Operation remove_Clientsystem 122
Tabelle 122: Operation list_Updates 122
Tabelle 123: Operation get_Updates 123
Tabelle 124: Operation send_Secure 123
Tabelle 125: Operation register 124
Tabelle 126: Operation deregister 124
Tabelle 127: Operation get_Status 124
Tabelle 128: Operation search_Directory 125
Tabelle 129: Operation add_Directory_Entry 126
Tabelle 130: Operation read_Directory_Entry 126
Tabelle 131: Operation modify_Directory_Entry 127
Tabelle 132: Operation delete_Directory_Entry 127
Tabelle 133: Operation add_Directory_FA-Attributes 128
Tabelle 134: Operation delete_Directory_FA-Attributes 128
Tabelle 135: Operation modify_Directory_FA-Attributes 128
Tabelle 136: Operation get_Service_Location 129
Tabelle 137: Operation get_IP_Address 130
Tabelle 138: Operation get_FQDN 130
Tabelle 139: Operation check_Revocation_Status 131
Tabelle 140: Operation download_TSL 131
Tabelle 141: Operation download_VL 131
Tabelle 142: Operation get_Hash 132
Tabelle 143: Operation provide_Certificate 132
Tabelle 144: Operation revoke_Certificate 133
Tabelle 145: Operation download_CRL 133
Tabelle 146: Operation sync_Time 134

ENTWURF

Tabelle 147: Operation update_Information 134
Tabelle 148: Operation update_Information 134
Tabelle 149: Operation get_Ext_Net_Config 135
Tabelle 150: Operation send_Data 135
Tabelle 151: Operation send_secure_IP_Packet 136
Tabelle 152: Operation send_secure_IP_Internet 136
Tabelle 153: Operation send_IP_Packet 137
Tabelle 154: Schnittstelle P_Cert_Provisioning 137
Tabelle 155: Schnittstelle P_Cert_Revocation 138
Tabelle 156: Schnittstelle P_Trust_Approval 138
Tabelle 157: Schnittstelle P_Sub_CA_Certification_CVC 138
Tabelle 158: Schnittstelle P_Sub_CA_Certification_X.509 138
Tabelle 159: Schnittstelle P_CVC_Provisioning 139
Tabelle 160: Schnittstelle P_DNS_Name_Entry_Announcement 139
Tabelle 161: Schnittstelle P_DNS_Zone_Delegation 139
Tabelle 162: Schnittstelle P_DNSSEC_Key_Distribution 139
Tabelle 163: Schnittstelle P_DNS_Service_Entry_Announcement 140
Tabelle 164: Schnittstelle P_KSRS_Maintenance 140
Tabelle 165: Schnittstelle P_~~Directory~~Data_Maintenance 140
Tabelle 166: Schnittstelle P_Directory_Application_Registration 141
~~Tabelle 167: Schnittstelle P_Directory_Administration_Registration~~ 141
Tabelle 168: Festlegungen zu Adressräumen 151
Tabelle 169: Festlegungen zu Namensräumen 152
Tabelle 170: Tab_ArchTIP_001 Kryptographische Endnutzer-Identitäten und deren Einsatz in der TI-Plattform 196
Tabelle 171: Datentypen und ihre Bedeutung 201

A5 – Referenzierte Dokumente

A5.1 – Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer entnehmen Sie bitte der aktuellsten, auf der Internetseite der gematik veröffentlichten Dokumentenlandkarte, in der die vorliegende Version aufgeführt wird.

ENTWURF

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_PKI_TIP]	gematik: Konzept PKI der TI-Plattform
[gemSpec_OM]	gematik: Operations und Maintenance Spezifikation
[gemKPT_Test]	gematik: Testkonzept
[gemKPT_Betr]	gematik: Spezifisches Betriebskonzept
[gemRL_NvTIwA]	gematik: Richtlinie Nutzungsvoraussetzungen der TI für weitere Anwendungen des Gesundheitswesens sowie für die Gesundheitsforschung

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI-TR-03114]	BSI TR-03114 (22.10.2007) Stapelsignatur mit dem Heilberufsausweis
[BSI-SiGw]	BSI (2005): Konzeption von Sicherheitsgateways, Version 1.0 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Konz_SiGw_pdf.pdf
[ISO/IEC27001]	ISO/IEC 27001:2005 Specification for an Information Security Management System, ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques
[RFC6598]	RFC6598 (April 2012): IANA-Reserved IPv4 Prefix for Shared Address Space http://tools.ietf.org/html/rfc6598
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2109
[RFC4007]	RFC4007 (März 2005): IPv6 Scoped Address Architecture http://tools.ietf.org/html/rfc4007
[SGB V]	BGBl. I S.2477 (20.12.1988): Sozialgesetzbuch, Fünftes Buch Zuletzt geändert durch Art. 4 G v. 14.4.2010 I 410 Gesetzliche Krankenversicherung
[eIDAS]	Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
[Common-PKI]	T7 & TeleTrust (20.01.2009): Common PKI Spezifikation, Version 2.0 http://www.t7ev.org/themen/entwickler/common-pki-v20-spezifikation.html
[RFC2560]	RFC 2560 (Juni 1999): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP http://tools.ietf.org/html/rfc2560

ENTWURF

Anhang B – Kryptographische Endnutzer-Identitäten und deren Einsatz in der TI-Plattform

Tabelle 170: Tab_ArchTIP_001 Kryptographische Endnutzer-Identitäten und deren Einsatz in der TI-Plattform

Identitätsbezeichnung	Verwendungszweck	Zertifikatstyp	zugeordnete Karten / Sicherheitsmodule	fachliche / technische Rolle	Architekturschicht (Zone)	Herausgeber	Eingesetzt in
Krypto-Identitäten zu qualifizierten Zertifikaten für eGK und HBA							
ID.CH.QES (opt.)	QES	X.509	eGK	Versicherter	---	Kostenträger (KTR)	---
ID.HP.QES	QES	X.509	HBA	Leistungserbringer	TI-Plattform dezentral	Leistungserbringer-organisation (LEO)	Erstellung_Prüfung_QES
eGK							
ID.CH.AUT	Authentisierung	X.509	eGK	Versicherter	TI-Plattform dezentral	KTR	Erstellung_Prüfung_Signatur
ID.CH.ENC	Ver-/Entschlüsselung	X.509	eGK	Versicherter	TI-Plattform dezentral	KTR	Verschlüsselung_Entschlüsselung
ID.CH.AUTN	Authentisierung	X.509	eGK	Versicherter	TI-Plattform dezentral	KTR	Erstellung_Prüfung_Signatur (pseudonym)
ID.CH.ENCV	Ver-/Entschlüsselung	X.509	eGK	Versicherter	TI-Plattform dezentral	KTR	Verschlüsselung_Entschlüsselung (pseudonym)
ID.eGK.AUT_CVC	C2C-Authentisierung	CVC	eGK	Versicherter	TI-Plattform dezentral	KTR	Kartenfreischaltung

ENTWURF

Identitätsbezeichnung	Verwendungszweck	Zertifikatstyp	zugeordnete Karten / Sicherheitsmodule	fachliche / technische Rolle	Architekturschicht (Zone)	Herausgeber	Eingesetzt in
ID.CAMS_HPA.AUT_CVC (opt.)	HPA/CAMS-Authentisierung	X.509	eGK	Versicherter	---	KTR	---
HBA							
ID.HP.AUT	TLS-Authentisierung	X.509	HBA	Leistungserbringer	TI-Plattform dezentral	LEO	Komm_Transport
ID.HP.ENC	Ver-/Entschlüsselung	X.509	HBA	Leistungserbringer	TI-Plattform dezentral	LEO	Verschlüsselung_Entschlüsselung
ID.HP.AUTO (opt.)	Authentisierung	X.509	HBA	Leistungserbringer	---	---	---
ID.HPC.AUTR_CVC	Rollenauthentisierung	CVC	HBA	Leistungserbringer	TI-Plattform dezentral	LEO	Kartenfreischaltung
ID.HPC.AUTD_SUK_CVC	Geräteauthentisierung	CVC	HBA	Leistungserbringer	TI-Plattform dezentral	LEO	Remote-PIN
ID.CAMS_HPC.AUT_CVC (opt.)	HPC/CAMS-Authentisierung	CVC	HBA	Leistungserbringer	---	LEO	---
SMC-B, HSM-B							
ID.HCI.OSIG	Institutions-Signatur	X.509	SMC-B, HSM-B	Leistungserbringer, Mitarbeiter Gesellschafterorganisation oder Mitarbeiter Kostenträger	TI-Plattform dezentral	LEO, KTR	Erstellung_Prüfung_Signatur
ID.HCI.AUT	Authentisierung	X.509	SMC-B,	Leistungserbringer, Mitarbeiter	TI-Plattform	LEO, KTR	Komm_Transport

ENTWURF

Identitätsbezeichnung	Verwendungszweck	Zertifikatstyp	zugeordnete Karten / Sicherheitsmodule	fachliche / technische Rolle	Architekturschicht (Zone)	Herausgeber	Eingesetzt in
			HSM-B	Gesellschafterorganisation oder Mitarbeiter Kostenträger	dezentral		
ID.HCI.ENC	Ver-/Entschlüsselung	X.509	SMC-B, HSM-B	Leistungserbringer, Mitarbeiter Gesellschafterorganisation oder Mitarbeiter Kostenträger	TI-Plattform dezentral	LEO, KTR	Verschlüsselung_Entschlüsselung
ID.SMC.AUTR_CVC	Rollenauthentisierung	CVC	SMC-A/B, HSM-B	Leistungserbringer, Mitarbeiter Gesellschafterorganisation oder Mitarbeiter Kostenträger	TI-Plattform dezentral	LEO, KTR	Kartenfreischaltung
ID.SMC.AUTD_RPE_CVC	Geräteauthentisierung	CVC	SMC-B, HSM-B	TI-Plattform	TI-Plattform dezentral	LEO, KTR	Remote-PIN
ID.CAMS_SMC.AUT_CVC (opt.)	SMC/CAMS-Authentisierung	CVC	SMC-A/B, HSM-B	Leistungserbringer, Mitarbeiter Gesellschafterorganisation oder Mitarbeiter Kostenträger	---	LEO, KTR	---
Konnektor (inkl. SAK)							

ENTWURF

Identitätsbezeichnung	Verwendungszweck	Zertifikatstyp	zugeordnete Karten / Sicherheitsmodule	fachliche / technische Rolle	Architekturschicht (Zone)	Herausgeber	Eingesetzt in
ID.NK.VPN	IPSec-Authentisierung	X.509	gSMC-K	TI-Plattform	TI-Plattform dezentral	TI-Plattform	Sichere_Online_Anbindung
ID.SAK.AUTD_CVC	Geräteauthentisierung	CVC	gSMC-K	TI-Plattform	TI-Plattform dezentral	TI-Plattform	Erstellung_Prüfung_QES
ID.SAK.AUT	Authentisierung	X.509	gSMC-K	TI-Plattform	TI-Plattform dezentral	TI-Plattform	Erstellung_Prüfung_QES
ID.AK.AUT	Authentisierung	X.509	gSMC-K	TI-Plattform	TI-Plattform dezentral	TI-Plattform	Sichere_Anbindung_Client
Kartenterminal							
ID.SMKT.AUT	Authentisierung	X.509	gSMC-KT	TI-Plattform	TI-Plattform dezentral	TI-Plattform	Kartenfreischaltung Kartennutzung Kartenterminalverwaltung
ID.SMC.AUTD_RPS_CVC	Geräteauthentisierung	CVC	gSMC-KT	TI-Plattform	TI-Plattform dezentral	TI-Plattform	Remote-PIN
Vertrauensraum der TI							
ID.TSL.SIG	Signatur	X.509	HSM	TI-Plattform	TI-Plattform zentral	TI-Plattform	PKI
Fachanwendungsspezifische Dienste							

ENTWURF

Identitätsbezeichnung	Verwendungszweck	Zertifikatstyp	zugeordnete Karten / Sicherheitsmodule	fachliche / technische Rolle	Architekturschicht (Zone)	Herausgeber	Eingesetzt in
ID.FD. TLS-C	Client-Authentisierung (Fachdienste)	X.509	Keystore / Software-Token	Fachanwendungsspezifischer Dienst	Provider	von gematik beauftragter Dienstleister	Dienst-zu-Dienst-Kommunikation
ID.FD. TLS-S	Server-Authentisierung (Fachdienste)	X.509	Keystore / Software-Token	Fachanwendungsspezifischer Dienst	Provider	von gematik beauftragter Dienstleister	Komm_Transport
ID.CM.TLS-CS	Client-/ Serverauthentisierung (Clientmodul)	X.509	Keystore / Software-Token	Clientmodul	Consumer	von gematik beauftragter Dienstleister	Kommunikation zwischen Clientmodul und fachanwendungsspezifischem Dienst bzw. Clientmodul zu Clientsystemen
Zentrale Dienste							
ID.VPNK.VPN	IPSec-Authentisierung	X.509	Keystore / Software-Token	TI-Plattform	TI-Plattform zentral	TI-Plattform	Sichere_Online_Anbindung
ID.VPNK.VPN-SIS	IPSec-Authentisierung	X.509	Keystore / Software-Token	TI-Plattform	TI-Plattform zentral	TI-Plattform	Sicherer Internetzugang
ID.ZD.TLS-S	Server-Authentisierung (zentrale Dienste)	X.509	Keystore / Software-Token	TI-Plattform	TI-Plattform zentral	von gematik beauftragter Dienstleister	Verbindung zu zentralen Diensten oder zum Konnektor

ENTWURF

Anhang C – Datentypen der TI-Plattform

Tabelle 171: Datentypen und ihre Bedeutung

Datentyp	Bedeutung
AccessProtocolEntry	Eintrag in Zugriffsprotokolldatei der eGK
APDU_K	CommandAPDU
APDU_R	ResponseAPDU
Binary	Binäre Anwendungsdaten
C2CType	Aufzähltyp bezeichnet einseitige, gegenseitige Authentisierung, C2C mit Aushandeln von Session- oder Introductionkeys
CallContext	Aufrufkontext einer Kartenoperation, bestehend aus personenbezogenen und systembezogenen Informationsanteilen wie z. B. Mandant bzw. aufrufendes System
CardDataDetails	Position und Länge der Daten in einer Datei auf der Smartcard oder Recordnummer
CardDataPath	Lokalisierung von Daten auf der Karte (DF, EF)
CardInfo	Merkmale einer Karte, mit der sie beim Anmelden der Kartennutzung identifiziert werden kann (Terminal, Slot, ICCSN o.ä.)
CardUsageReference	Verweis auf ein n-Tupel aus RessourceIdentifier und Parametern, die eine Gruppe von Nutzern mit gleichen Rechten zum Zugriff auf die Karte charakterisieren. Der Verweis hat eine ausreichend hohe Entropie, so dass er nicht erraten werden kann.
CertificateReference	Identifikator für X.509- Zertifikate auf den Karten, z.B. EF.C.CH.AUTN. Realisierung als Aufzähltyp oder als Navigationspfad. Wenn Navi, dann auch in extract_card_data verwendbar.
CertificateX.509	X.509-Zertifikat
ClientsystemIdentifier	Identifiziert ein Clientsystem. Technische Umsetzung noch offen (X.509, IP-Adresse, MAC etc.)
ConfigurationData	Konfigurationsdaten
CSAccessMode	Enumeration der erlaubten Anbindungsvarianten von Clientsystemen: - SecuredOnly - Unsecured
DataType	Enumeration des Datentyps, der über die Hostschnittstelle des MobKT übertragen wird.
DirectoryAttributes	Die Attribute eines Verzeichniseintrags.
DirectoryEntryVariant	Gibt an welche Daten automatisch in den Verzeichniseintrag übernommen werden.

ENTWURF

Datentyp	Bedeutung
DirectoryQuery	Filter für eine Suchanfrage an den Verzeichnisdienst.
DirectoryQueryResult	Antwort auf eine Suchanfrage an den Verzeichnisdienst.
DocumentType	Format des Documents - PDF/A - TEXT - TIFF - XML - MIME - Binär
EncBinary	Verschlüsselte Version von binären Anwendungsdaten
EncDocumentType	Verschlüsselte Version eines Dokuments vom Typ: - PDF/A - XML - MIME - Binär
EventInformation	Informationen über ein eingetretenes Ereignis (komplexe Struktur mit näheren Informationen zum Ereignis)
FQDN	FQDN eines fachanwendungsspezifische Dienstes
InfoElementIDType	Identifikator für Informationselemente von Karten des Gesundheitswesens, vor allem aus Zertifikaten. Evtl. Aufzähltyp oder Navigationspfad
IpAddress	IP-Adresse eines fachanwendungsspezifische Dienstes
KeyReference	Referenz auf den privaten Schlüssel, mit dem signiert oder entschlüsselt werden soll. Die gültigen Werte für KeyReference bzw. Mechanismen, diese abzufragen, werden in den Spezifikationen der TI-Plattform festgelegt.
KSRClientType	Beschreibt die dezentralen Komponenten, für die aktuell verfügbare Updates abgefragt werden sollen.
KSRClientStatus	Update-Status der abfragenden dezentralen Komponente
MFMType	Identifikation des bei Operationen auf der MobKT-Plattform adressierten Fachmoduls bzw. der MobKT-Plattform (wenn diese durch get_Data oder put_Data adressiert wird). Mögliche Werte sind: - VSDM
NotificationAddress	Adresse, an die eintretende Ereignisse gesendet werden sollen
OnOffType	Beginn / Ende eines Zustandes
OperationMode	Modus von unblock_PIN
PINReference	Aufzähltyp für PIN-Referenzen der Karten
PINStatus	Status der durch PINReference bezeichneten PIN einer gewählten Karte.
QESConfirmationData	Bestätigung der Signaturauslösung für QES
RessourceDetails	komplexer Datentyp zur Aufnahme aller statischen und dynamischen Informationen einer dezentralen Komponente. Der Datentyp fasst Informationen über die Produkttypen KT, Karte,

ENTWURF

Datentyp	Bedeutung
	MobKT. Enthält unter anderem: - RessourceIdentifier - CardInfo - Status Online/Offline - Betriebszustand der Komponente (OK=Normal, Warnung=Admin-Interaktion sinnvoll, Kritisch=Fachlich eingeschränkt, Admin-Interaktion erforderlich) - verfügbaren technischen Zertifikate (zur Ermittlung der verbleibenden Gültigkeitsdauer) - Versionsinformationen
RessourceIdentifier	Identifikator für ein Gerät oder einer Identität einer bestimmten Smartcard bestehend aus einer eindeutigen ID und einer Typkennung.
RessourceList	Eine Liste von Elementen, je bestehend aus: - RessourceIdentifier - RessourceName - RessourceType
RessourceName	frei vergebener Name einer Dezentralen Komponente im lokalen Netz des LE
RessourceType	(Produkt-)Enumeration-Typ einer Dezentralen Komponente im lokalen Netz des LE.
SignedBinary	Signierte Version von binären Anwendungsdaten
SignedDocumentType	Signierte Version eines Dokuments vom Typ: - PDF/A - TEXT - TIFF - XML - MIME - Binär
SymmetricKey	Symmetrischer Schlüssel
Text	alphanumerische Zeichenkette
Telematik_ID	Identifikation eines Leistungserbringers oder einer Organisation des Gesundheitswesens
TimeInformation	aktuelle Zeitinformation vom NTP-Server (zentral).
UpdateIdentifier	Identifikation eines Softwareupdates bzw. eines Konfigurationsupdates
UpdatePackage	Software-Update-Paket oder Konfigurationsdaten-Paket
URI	URI eines Fachdienstes
VerificationResultType	das Ergebnis einer Prüfung, z. B. einer Zertifikatsprüfung, einer Signatur- oder QES-Prüfung
XML	XML-Format (z.B. TSL)
XmlSchema	Schema eines XML-Dokuments

ENTWURF

Anhang D – Informationsmodell der TI-Plattform

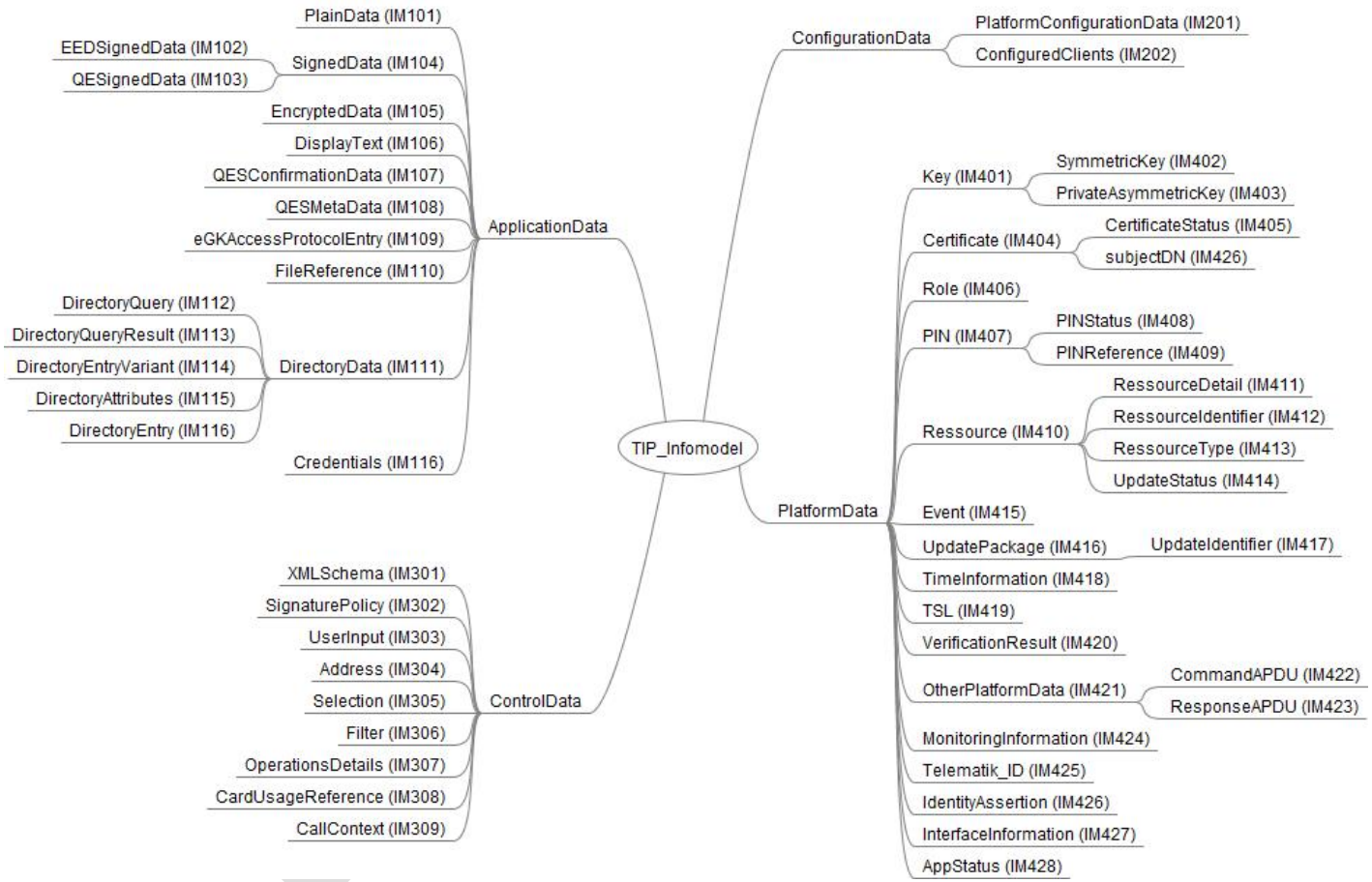


Abbildung 51: Informationsmodell der TI-Plattform