

## Einführung der Gesundheitskarte

# Konzept

# Architektur der TI-Plattform

Version: 1.10.0  
Revision: \main\rel\_online\rel\_ors1\rel\_opb1\51  
Stand: 20.04.2017  
Status: freigegeben  
Klassifizierung: öffentlich  
Referenzierung: gemKPT\_Arch\_TIP

---

## Dokumentinformationen

---

### Änderungen zur Vorversion

Anpassung für Kartengeneration 2.1, Änderungsliste

### Dokumentenhistorie

| Version | Stand    | Kap./<br>Seite     | Grund der Änderung, besondere Hinweise   | Bearbeitung |
|---------|----------|--------------------|--|-------------|
| 0.12.0  | 13.06.12 |                    | Überarbeitung für Vergabeverfahren   | gematik     |
| 0.14.0  | 26.06.12 |                    | Überarbeitung für Vergabeverfahren   | gematik     |
|         | 09.07.12 | 5.5.1.10           | einzelne Korrekturen   | P77         |
| 0.15.0  | 16.07.12 | 3.8, 5, 6<br>und 7 | Einarbeitung CR0029 – Sicherer Internetzugang  | P77         |
| 0.16.0  | 31.08.12 |                    | Einarbeitung von Änderungen aus dem<br>Kommentierungsverfahren   | P77         |
| 1.0.0   | 15.10.12 |                    | Korrekturen  | gematik     |
| 1.1.0   | 12.11.12 |                    | Einarbeitung Kommentare aus der<br>übergreifenden Konsistenzprüfung  | gematik     |
| 1.2.0   | 06.06.13 |                    | Einarbeitung durch die PL bestätigter<br>Korrekturen, Umbenennung des Produkttyps<br>OCSP-Responder BnetzA-Proxy in OCSP-<br>Responder Proxy, Einarbeitung Kommentare LA | gematik     |
| 1.3.0   | 15.08.13 |                    | Einarbeitung gemäß Änderungsliste  | gematik     |
| 1.4.0   | 21.02.14 |                    | Losübergreifende Synchronisation   | gematik     |
| 1.5.0   | 17.07.15 |                    | Einarbeitung CR KOM-LE und Errata-Inhalte in<br>ORS1   | P77         |
| 1.6.0   | 03.05.16 |                    | Anpassungen zum Online-Produktivbetrieb (Stufe<br>1)   | gematik     |
| 1.7.0   | 13.07.16 |                    | Einarbeitung von Änderungen aus dem<br>Kommentierungsverfahren   |             |
| 1.8.0   | 16.10.16 |                    | Aufnahme SMC-B für Organisationen der<br>Gesellschafter, Anpassungen gemäß<br>Änderungsliste   | gematik     |
| 1.9.0   | 06.02.17 |                    | Überarbeitung bzgl. eIDAS und Signaturproxy  | gematik     |
|         | 22.03.17 |                    | Anpassung für Kartengeneration 2.1,<br>Änderungsliste  | gematik     |
| 1.10.0  | 20.04.17 |                    | freigegeben  | gematik     |

---

## Inhaltsverzeichnis

---

|  |           |
|--|-----------|
| <b>Dokumentinformationen .....</b>                             | <b>2</b>  |
| <b>Inhaltsverzeichnis .....</b>                                | <b>3</b>  |
| <b>1 Einordnung des Dokuments .....</b>                        | <b>10</b> |
| 1.1 Zielsetzung .....  | 10        |
| 1.2 Zielgruppe .....   | 10        |
| 1.3 Geltungsbereich .....                                      | 10        |
| 1.4 Abgrenzung des Dokuments .....                             | 10        |
| 1.5 Methodik .....   | 11        |
| <b>2 Grundlagen der Architektur der TI-Plattform .....</b>     | <b>12</b> |
| 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        |
| 2.1.2 Produkttypen, Produkte und Produktinstanzen .....        | 15        |
| 2.1.3 Logische Architekturschichten (Zonen) .....              | 16        |
| 2.1.4 Kontrolle der Kommunikationswege .....                   | 17        |
| 2.2 Betrieb und Wartung (Operation and Maintenance) .....      | 18        |
| 2.3 Bedarfsgerechte Leistungsfähigkeit (Performance) .....     | 19        |
| 2.4 Sicherheitsleistung der TI-Plattform .....                 | 19        |
| 2.4.1 Abgrenzung zwischen TI-Plattform und Fachanwendung ..... | 19        |
| 2.4.2 Sicherheitsleistung der Produkttypen .....               | 20        |
| 2.5 Parallelbetrieb eGK-Generationen 1 und 2 .....             | 20        |
| 2.6 Rollen der TI-Plattform .....                              | 21        |
| 2.6.1 Personenkreise der Telematikinfrastruktur .....          | 21        |
| 2.6.2 Rollen .....   | 22        |
| <b>3 Leistungen der TI-Plattform in der Außensicht .....</b>   | <b>24</b> |
| 3.1 Qualifizierte elektronische Signatur .....                 | 24        |
| 3.2 Einfache digitale elektronische Signatur .....             | 24        |
| 3.3 Ver- und Entschlüsselung .....                             | 24        |
| 3.4 Public Key Infrastructure (PKI) .....                      | 24        |
| 3.5 Smartcards des Gesundheitswesens .....                     | 25        |

|         |   |    |
|---------|---|----|
| 3.6     | Anbindung an das geschlossene Netzwerk der TI .....                                   | 25 |
| 3.7     | Zugang zu Bestandsnetzen.....   | 25 |
| 3.8     | Sicherer Internetzugang.....  | 25 |
| 3.9     | Außensicht der TI-Plattform im Ganzen .....   | 25 |
| 4       | Lösungen der Architektur der TI-Plattform .....                                       | 27 |
| 4.1     | Zugriff auf Karten.....   | 27 |
| 4.2     | Mandantenfähigkeit .....  | 28 |
| 4.3     | Remote-PIN .....  | 30 |
| 4.4     | Mobile Szenarien .....  | 32 |
| 5       | Produkttypen der TI-Plattform .....   | 34 |
| 5.1     | Übersicht des Gesamtsystems.....  | 34 |
| 5.2     | Festlegungen zu Produkttypen der TI-Plattform .....                                   | 34 |
| 5.3     | Produkttypen der Zone TI-Plattform dezentral .....                                    | 38 |
| 5.3.1   | Produkttyp elektronische Gesundheitskarte (eGK) .....                                 | 38 |
| 5.3.2   | Produkttyp Heilberufsausweis (HBA) .....  | 39 |
| 5.3.3   | Produkttyp Security Module Card Organisationen des Gesundheitswesens (SMC-B) 39       |    |
| 5.3.4   | Produkttyp Hardware Security Module Organisationen des Gesundheitswesens (HSM-B)..... | 40 |
| 5.3.5   | Produkttyp Security Module Card Kartenterminal (gSMC-KT).....                         | 41 |
| 5.3.6   | Produkttyp Security Module Card Konnektor (gSMC-K).....                               | 41 |
| 5.3.7   | Produkttyp eHealth-Kartenterminal (KT) .....  | 42 |
| 5.3.8   | Produkttyp Mobiles Kartenterminal (MobKT).....  | 43 |
| 5.3.9   | Produkttyp Konnektor .....  | 44 |
| 5.3.9.1 | Konfigurationsmodell des Konnektors.....  | 45 |
| 5.3.9.2 | Logische Trennung innerhalb des Konnektors.....                                       | 46 |
| 5.3.9.3 | Anforderungen an den Konnektor.....   | 47 |
| 5.4     | Produkttypen der Zone TI-Plattform zentral .....                                      | 50 |
| 5.4.1   | Produkttyp Zentrales Netz TI (Zentrales Netz) .....                                   | 50 |
| 5.4.2   | Produkttyp Zeitdienst .....   | 51 |
| 5.4.3   | Produkttyp Namensdienst.....  | 51 |
| 5.4.4   | Produkttyp Verzeichnisdienst.....   | 52 |
| 5.4.5   | Produkttyp TSL-Dienst.....  | 55 |
| 5.4.6   | Produkttyp Konfigurationsdienst (Konfigdienst).....                                   | 56 |
| 5.4.7   | Produkttyp VPN-Zugangsdienst (Zugangsdienst) .....                                    | 57 |
| 5.4.8   | Produkttyp Sicherheitgateway Bestandsnetze (SG-BNet) .....                            | 59 |
| 5.4.9   | Produkttyp Trust Service Provider X.509 nonQES (TSP-X.509nonQES) ...                  | 60 |
| 5.4.10  | Produkttyp Trust Service Provider X.509 QES (TSP-X.509QES).....                       | 60 |
| 5.4.11  | Produkttyp gematik Root-CA .....  | 61 |
| 5.4.12  | Produkttyp Trust Service Provider CVC (TSP-CVC) .....                                 | 61 |
| 5.4.13  | Produkttyp CVC-Root .....   | 62 |
| 5.4.14  | Produkttyp OCSP-Responder Proxy (OCSP-Proxy) .....                                    | 62 |
| 5.4.15  | Produkttyp Störungsampel.....   | 63 |

|            |  |           |
|------------|--|-----------|
| <b>5.5</b> | <b>Interfaces der TI-Plattform Dezentral .....</b> | <b>64</b> |
| 5.5.1      | Basisdienste .....                                 | 65        |
| 5.5.1.1    | <i>Benutzerinteraktion_KT</i> .....                | 65        |
| 5.5.1.1.1  | I_KT_Operations (Provided) .....                   | 65        |
| 5.5.1.2    | <i>Erstellung_Prüfung_Signatur</i> .....           | 66        |
| 5.5.1.2.1  | I_Sign_Operations (Provided) .....                 | 66        |
| 5.5.1.3    | <i>Erstellung_Prüfung_QES</i> .....                | 68        |
| 5.5.1.3.1  | I_SAK_Operations (Provided) .....                  | 68        |
| 5.5.1.4    | <i>Information_Systemzustände</i> .....            | 70        |
| 5.5.1.4.1  | I_Poll_System_Information (Provided) .....         | 70        |
| 5.5.1.4.2  | I_Notification (Required) .....                    | 72        |
| 5.5.1.4.3  | I_Notification_From_FM .....                       | 72        |
| 5.5.1.4.4  | I_Reg_Notification (Provided) .....                | 73        |
| 5.5.1.5    | <i>KSR</i> .....                                   | 73        |
| 5.5.1.5.1  | I_KSRC_Management (Provided) .....                 | 73        |
| 5.5.1.5.2  | I_KSRC_Local_Management (Provided) .....           | 74        |
| 5.5.1.5.3  | I_KSR_Update (Provided) .....                      | 75        |
| 5.5.1.6    | <i>Kartenverwaltung</i> .....                      | 75        |
| 5.5.1.6.1  | I_KV_Card_Handling (Provided) .....                | 75        |
| 5.5.1.6.2  | I_KV_Card_Reservation (Provided) .....             | 76        |
| 5.5.1.7    | <i>Kartenfreischaltung</i> .....                   | 77        |
| 5.5.1.7.1  | I_KV_Card_Unlocking (Provided) .....               | 77        |
| 5.5.1.8    | <i>Komm_Transport</i> .....                        | 80        |
| 5.5.1.8.1  | I_TLS_Client (Provided) .....                      | 80        |
| 5.5.1.9    | <i>Prüfung_Zertifikat</i> .....                    | 80        |
| 5.5.1.9.1  | I_Cert_Verification (Provided) .....               | 80        |
| 5.5.1.10   | <i>Verschlüsselung_Entschlüsselung</i> .....       | 81        |
| 5.5.1.10.1 | I_Crypt_Operations (Provided) .....                | 81        |
| 5.5.1.10.2 | I_Symm_Crypt_Operations (Provided) .....           | 83        |
| 5.5.1.11   | <i>Verzeichnis_Identitäten</i> .....               | 84        |
| 5.5.1.11.1 | I_Directory_Query (Provided) .....                 | 84        |
| 5.5.1.12   | <i>Mobile_Offline_Dienste</i> .....                | 84        |
| 5.5.1.12.1 | I_MobKT_Temp_Storage (Provided) .....              | 84        |
| 5.5.1.12.2 | I_MobKT_FMAccess (Provided) .....                  | 85        |
| 5.5.1.12.3 | I_MobKT_CommFM (Required) .....                    | 86        |
| 5.5.1.12.4 | I_MobKT_GUI (Provided) .....                       | 87        |
| 5.5.1.12.5 | I_MobKT_Printer (Provided) .....                   | 88        |
| 5.5.1.12.6 | I_MobKT_Management (Provided) .....                | 88        |
| 5.5.2      | Infrastrukturdienste .....                         | 89        |
| 5.5.2.1    | <i>Dienstlokalisierung</i> .....                   | 89        |

|            |  |           |
|------------|--|-----------|
| 5.5.2.1.1  | I_DNS_Service_Information (Provided)                                   | 89        |
| 5.5.2.2    | <i>Namensauflösung</i>   | 89        |
| 5.5.2.2.1  | I_DNS_Name_Information (Provided)                                      | 89        |
| 5.5.2.2.2  | I_DNS_Name_Resolution (Provided)                                       | 90        |
| 5.5.2.3    | <i>Zeitinformation</i>   | 90        |
| 5.5.2.3.1  | I_NTP_Time_Information (Provided)                                      | 90        |
| 5.5.2.3.2  | I_Synchronised_System_Time (Provided)                                  | 91        |
| 5.5.2.3.3  | I_Change_System_Time (Provided)  | 91        |
| 5.5.2.4    | <i>Kartennutzung</i>   | 92        |
| 5.5.2.4.1  | I_KV_Card_Operations (Provided)  | 92        |
| 5.5.2.5    | <i>Kartenterminalverwaltung</i>  | 95        |
| 5.5.2.5.1  | I_KTV_Management (Provided)  | 95        |
| 5.5.2.5.2  | I_KT_Communication (Provided)  | 96        |
| 5.5.3      | Netzwerkdienste  | 96        |
| 5.5.3.1    | <i>Datentransport/Sichere Online-Anbindung/Sicherer Internetzugang</i> | 96        |
| 5.5.3.1.1  | I_IP_Transport (Provided)  | 96        |
| 5.5.3.2    | <i>Sichere Anbindung Client</i>  | 97        |
| 5.5.3.2.1  | I_Facade_Access_Configuration  | 97        |
| <b>5.6</b> | <b>Interfaces der TI-Plattform Zentral</b>                             | <b>99</b> |
| 5.6.1      | Basisdienste   | 99        |
| 5.6.1.1    | <i>KSR</i>   | 99        |
| 5.6.1.1.1  | I_KSRS_Download (Provided)   | 99        |
| 5.6.1.2    | <i>Komm_Transport</i>  | 100       |
| 5.6.1.2.1  | I_TLS (Required)   | 100       |
| 5.6.1.3    | <i>Konnektorregistrierung</i>  | 100       |
| 5.6.1.3.1  | I_Registration_Service (Provided)                                      | 100       |
| 5.6.1.4    | <i>Verzeichnis_Identitäten</i>   | 101       |
| 5.6.1.4.1  | I_Directory_Query (Provided)   | 101       |
| 5.6.1.4.2  | I_Directory_Maintenance (Provided)                                     | 102       |
| 5.6.1.4.3  | I_Directory_Application_Maintenance (Provided)                         | 104       |
| 5.6.2      | Infrastrukturdienste   | 105       |
| 5.6.2.1    | <i>Dienstlokalisierung</i>   | 105       |
| 5.6.2.1.1  | I_DNS_Service_Localization (Provided)                                  | 105       |
| 5.6.2.2    | <i>Namensauflösung</i>   | 106       |
| 5.6.2.2.1  | I_DNS_Name_Resolution (Provided)                                       | 106       |
| 5.6.2.3    | <i>PKI</i>   | 107       |
| 5.6.2.3.1  | I_OCSP_Status_Information (Provided)                                   | 107       |
| 5.6.2.3.2  | I_TSL_Download (Provided)  | 107       |
| 5.6.2.3.3  | I_BNetzA_VL_Download (Provided)  | 108       |
| 5.6.2.3.4  | I_Cert_Provisioning  | 108       |

|            |   |            |
|------------|---|------------|
| 5.6.2.3.5  | I_Cert_Revocation.....  | 109        |
| 5.6.2.3.6  | I_CRL_Download (Provided) .....   | 109        |
| 5.6.2.4    | <i>Zeitinformation</i> .....  | 110        |
| 5.6.2.4.1  | I_NTP_Time_Information (Provided) .....                                   | 110        |
| 5.6.2.5    | <i>Monitoring des Betriebszustandes</i> .....                             | 110        |
| 5.6.2.5.1  | I_Monitoring_Update (Provided) .....                                      | 110        |
| 5.6.2.5.2  | I_Monitoring_Read (Provided) .....  | 111        |
| 5.6.2.6    | <i>Konfiguration von Bestandsnetzen</i> .....                             | 111        |
| 5.6.2.6.1  | I_KSRS_Net_Config (Provided).....   | 111        |
| 5.6.3      | Netzwerkdienste .....   | 112        |
| 5.6.3.1    | <i>Datentransport/Sichere Online-Anbindung/Sicherer Internetzugang</i> .. | 112        |
| 5.6.3.1.1  | I_IP_Transport (Provided) .....   | 112        |
| 5.6.3.1.2  | I_Secure_Channel_Tunnel (Provided).....                                   | 112        |
| 5.6.3.1.3  | I_Secure_Internet_Tunnel (Provided) .....                                 | 113        |
| 5.6.3.2    | <i>Zugang_Fremdnetze</i> .....  | 113        |
| 5.6.3.2.1  | I_Secure_Access_Bestandsnetz (Provided) .....                             | 113        |
| <b>5.7</b> | <b>Prozess-Interfaces der TI-Plattform.....</b>                           | <b>114</b> |
| 5.7.1      | P_Cert_Provisioning (Provided).....                                       | 114        |
| 5.7.2      | P_Cert_Revocation (Provided) .....  | 114        |
| 5.7.3      | P_Trust_Approval (Provided).....  | 114        |
| 5.7.4      | P_Sub_CA_Certification_CVC (Provided) .....                               | 115        |
| 5.7.5      | P_Sub_CA_Certification_X.509 (Provided).....                              | 115        |
| 5.7.6      | P_CVC_Provisioning (Provided) .....                                       | 115        |
| 5.7.7      | P_DNS_Name_Entry_Announcement (Provided) .....                            | 115        |
| 5.7.8      | P_DNS_Zone_Delegation (Provided) .....                                    | 116        |
| 5.7.9      | P_DNSSEC_Key_Distribution (Provided) .....                                | 116        |
| 5.7.10     | P_DNS_Service_Entry_Announcement (Provided) .....                         | 116        |
| 5.7.11     | P_KSRS_Maintenance (Provided).....  | 117        |
| 5.7.12     | P_Directory_Maintenance (Provided) .....                                  | 117        |
| 5.7.13     | P_Directory_Application_Registration (Provided) .....                     | 117        |
| 5.7.14     | P_Directory_Administration_Registration (Provided) .....                  | 118        |
| <b>6</b>   | <b>Das Netzwerk der TI-Plattform.....</b>                                 | <b>119</b> |
| 6.1.1      | Zugangsnetz.....  | 120        |
| 6.1.2      | Zentrales Netz .....  | 121        |
| 6.1.3      | Sicherheitsgateway Bestandsnetze .....                                    | 122        |
| 6.1.4      | Sicherer Internetzugang .....   | 123        |
| 6.1.5      | Weiternutzung Internet .....  | 124        |
| 6.1.6      | Volumenerfassung im Netzwerk der TI-Plattform .....                       | 125        |
| <b>6.2</b> | <b>Festlegungen zu Adressierung, Routing und Priorisierung .....</b>      | <b>125</b> |
| 6.2.1      | Festlegungen zum einzusetzenden IP-Protokoll .....                        | 126        |
| 6.2.2      | Festlegungen zu Adressräumen .....  | 127        |
| 6.2.3      | Festlegungen zum Routing.....   | 128        |
| 6.2.4      | Festlegungen zu Namensräumen .....  | 128        |
| 6.2.5      | Festlegungen zum TLS-Protokoll.....                                       | 129        |



|            |  |            |
|------------|--|------------|
| 6.2.6      | Festlegungen zur Priorisierung auf Netzwerkebene.....                                    | 129        |
| <b>7</b>   | <b>Abhängigkeiten zwischen Produkttypen der TI-Plattform .....</b>                       | <b>131</b> |
| <b>7.1</b> | <b>Prozessabläufe in fachanwendungsspezifischen Diensten .....</b>                       | <b>131</b> |
| 7.1.1      | Erstellung und Prüfung von digitalen Signaturen<br>(Erstellung_Prüfung_Signatur) .....   | 131        |
| 7.1.1.1    | Erstellung von digitalen Signaturen.....   | 131        |
| 7.1.1.2    | Prüfung von digitalen Signaturen.....  | 132        |
| 7.1.2      | Prüfung von X.509-Zertifikaten (Prüfung_Zertifikat) .....                                | 133        |
| 7.1.2.1    | TSL-Validierung.....   | 133        |
| 7.1.2.2    | Prüfung von X.509-Zertifikaten .....   | 134        |
| <b>7.2</b> | <b>Prozessabläufe zwischen Produkttypen der TI-Plattform.....</b>                        | <b>134</b> |
| 7.2.1      | Benutzerinteraktion_KT .....   | 135        |
| 7.2.1.1    | Ablauf Benutzerinteraktion am Kartenterminal.....  | 135        |
| 7.2.2      | Erstellung_Prüfung_QES.....  | 135        |
| 7.2.2.1    | Ablauf QES erzeugen .....  | 135        |
| 7.2.2.2    | Ablauf QES prüfen.....   | 136        |
| 7.2.3      | Information_Systemzustände .....   | 137        |
| 7.2.3.1    | Ablauf Anmeldung zur Notifikation und Notifikation.....                                  | 137        |
| 7.2.3.2    | Ablauf Sammeln der Umgebungsinformationen und Abfrage<br>RessourcenInfo .....            | 138        |
| 7.2.4      | Konfigurations- und Software Repository (KSR) .....                                      | 140        |
| 7.2.4.1    | Ablauf Anzeigen verfügbarer Aktualisierungen .....                                       | 140        |
| 7.2.4.2    | Ablauf Software oder Konfigurationen aus KSR aktualisieren.....                          | 140        |
| 7.2.4.3    | Ablauf Bestandsnetzkonfigurationen aktualisieren.....                                    | 142        |
| 7.2.5      | Aktualisierung von TSL und Vertrauensliste der BNetzA in Produkttypen .....              | 143        |
| 7.2.5.1    | Ablauf Aktualisierung der TSL über die TI-Plattform .....                                | 143        |
| 7.2.5.2    | Ablauf Aktualisierung der Vertrauensliste der BNetzA über die TI-<br>Plattform .....     | 143        |
| 7.2.6      | Aktualisierung der CRL im Konnektor .....  | 144        |
| 7.2.6.1    | Ablauf Aktualisierung der CRL im Konnektor .....   | 144        |
| 7.2.7      | Prüfung von X.509-Zertifikaten (Prüfung_Zertifikat) .....                                | 145        |
| 7.2.7.1    | Ablauf Initialisierung Trust Store .....   | 145        |
| 7.2.7.2    | Ablauf Zertifikat prüfen.....  | 146        |
| 7.2.8      | Verzeichnis_Identitäten .....  | 146        |
| 7.2.8.1    | Ablauf Abfrage des Verzeichnisses .....  | 146        |
| 7.2.9      | Namensauflösung.....   | 147        |
| 7.2.9.1    | Ablauf FQDN des TI-Namensraums auflösen.....   | 147        |
| 7.2.9.2    | Ablauf FQDN für sichere Online-Anbindung auflösen .....                                  | 149        |
| 7.2.9.3    | Ablauf FQDN aus Bestandsnetzen auflösen .....  | 149        |
| 7.2.10     | Zeitinformation.....   | 150        |
| 7.2.10.1   | Ablauf Zeitinformation der TI abfragen.....  | 150        |
| 7.2.11     | Kartenzugriff .....  | 151        |
| 7.2.11.1   | Ablauf generische Kartenoperation.....   | 151        |
| 7.2.11.2   | Ablauf PIN-Eingabe direkt .....  | 153        |
| 7.2.11.3   | Ablauf PIN-Eingabe mit Remote_PIN .....  | 155        |
| 7.2.12     | Sichere Online-Anbindung.....  | 157        |
| 7.2.12.1   | Ablauf Aufbau eines sicheren Kanals zur Anbindung an die zentrale TI-<br>Plattform ..... | 157        |
| 7.2.13     | Sicherer Internetzugang .....  | 158        |



|   |            |
|---|------------|
| 7.2.13.1 Ablauf Aufbau eines sicheren Kanals zur Anbindung des sicheren Internetzugangs .....       | 158        |
| <b>Anhang A – Verzeichnisse.....</b>  | <b>160</b> |
| A1 – Abkürzungen.....   | 160        |
| A2 – Glossar .....  | 162        |
| A3 – Abbildungsverzeichnis.....   | 162        |
| A4 – Tabellenverzeichnis.....   | 163        |
| A5 – Referenzierte Dokumente.....   | 167        |
| A5.1 – Dokumente der gematik.....   | 167        |
| A5.2 – Weitere Dokumente.....   | 168        |
| <b>Anhang B – Kryptographische Endnutzer-Identitäten und deren Einsatz in der TI-Plattform.....</b> | <b>169</b> |
| <b>Anhang C – Datentypen der TI-Plattform .....</b>   | <b>174</b> |
| <b>Anhang D – Informationsmodell der TI-Plattform.....</b>  | <b>177</b> |

---

## 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.

### 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 und Betrieb dieses Systems (siehe hier [gemKPT\_Test] und [gemKPT\_Betr]).

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.

---

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

---

### **2.1 Architekturmerkmale**

#### **2.1.1 TI-Plattform als Basis der Fachanwendungen**

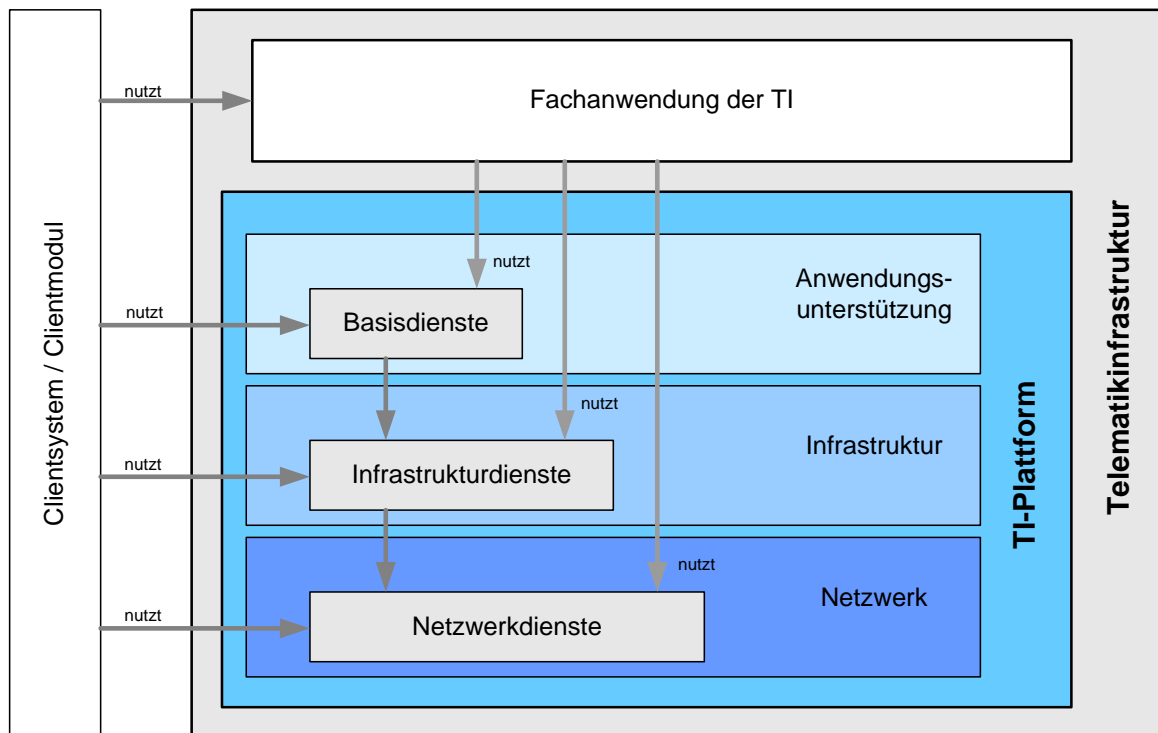
Die Trennung von TI-Plattform und Fachanwendungen ist als dediziertes Ziel der TI-Plattform festgelegt worden und darin die Entkopplung der Systeme TI-Plattform und Fachanwendungen gefordert. Dabei ist es unerheblich, ob es sich um eine Fachanwendung der Telematikinfrastruktur oder um eine unbekannte 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



**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 Verantwortungsbe-  
reichen, die jeweils aufeinander aufbauen. Die oberste Ebene bilden die Fachanwen-  
dungen, die sich der Funktionalitäten der von der TI-Plattform bereitgestellten darunter-  
liegenden Schichten (Basisdienste, Infrastrukturdienste, Netzwerkdienste) bedienen.

Dabei sind die Dienste, welche die TI-Plattform den Fachanwendungen anbietet, grund-  
sätzlich 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 – Än-  
derungen 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 Fach-  
anwendung entweder eine Erweiterung des Dienstangebots der TI-Plattform  
motivieren oder eine eigene Alternativlösung einsetzen.

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

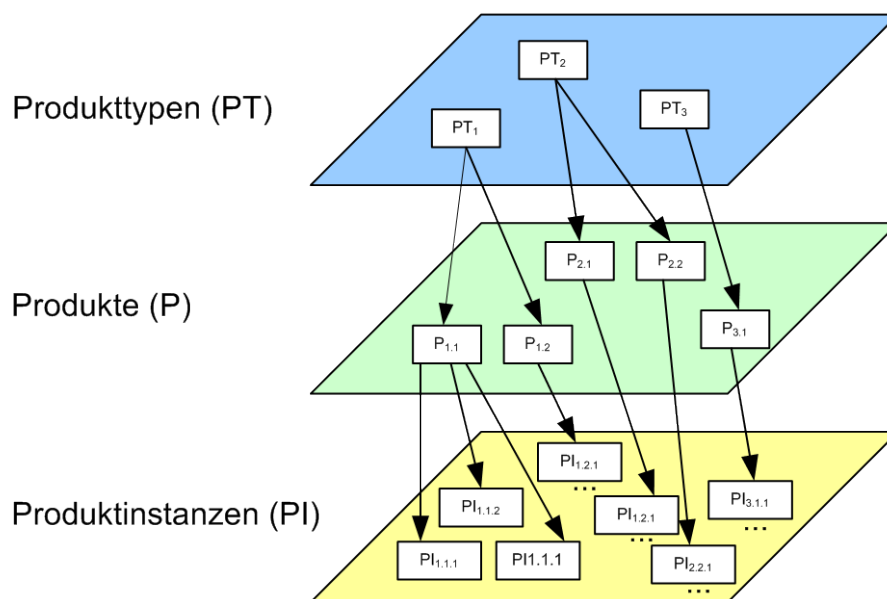
So entsteht insgesamt ein Dienstbaukasten, aus dem sich die Fachanwendungen nach  
Bedarf bedienen können.

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

### 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.

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 2: 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.

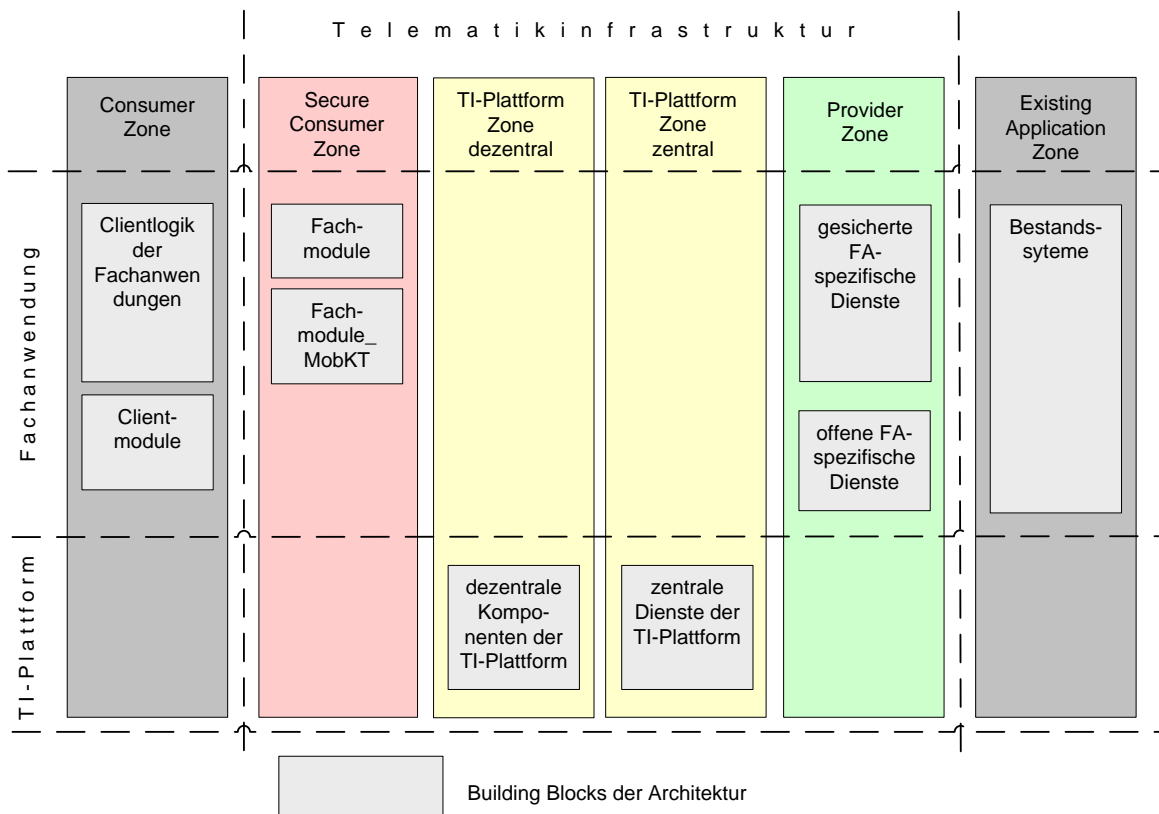
Ein großer Freiheitsgrad in den Produktinstanzkardinalitäten unterstützt das Prinzip des diskriminierungsfreien Wettbewerbs:

- Die Anbindung verschiedener Instanzen von fachanwendungsspezifischen Diensten der gleichen Anwendung ist grundsätzlich möglich. Sie wird durch Ausgestaltung der Netzwerkdienste und der Dienstlokalisierung 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 3 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.



**Abbildung 3: 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 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, 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 und die fachlichen Schnittstellen der fachanwendungsspezifischen Dienste 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<sup>1</sup> zugegriffen werden.

Die Existing Application Zone umfasst die Bestandssysteme der Fachanwendungen (z. B. CMS). Auch Bestandsnetze ist hier eingeordnet.

#### 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)**

|                                    | Consumer Zone<br>(C) | Secure Consumer Zone<br>(SC) | TI-Plattform-Zone dezentral<br>(TI_D) | TI-Plattform-Zone zentral<br>(TI_Z) | Provider Zone<br>(P) | Existing Application Zone<br>(EA) |
|------------------------------------|----------------------|------------------------------|---------------------------------------|-------------------------------------|----------------------|-----------------------------------|
| Consumer Zone (C)                  | -- <sup>2</sup>      | X                            | X                                     | --                                  | X                    | X <sup>3</sup>                    |
| Secure Consumer Zone (SC)          | X <sup>4</sup>       | --                           | X                                     | --                                  | X                    | --                                |
| TI-Plattform-Zone dezentral (TI_D) | X <sup>4</sup>       | X <sup>4</sup>               | X                                     | X                                   | --                   | --                                |

<sup>1</sup> Die Dienst-zu-Dienst-Kommunikation zwischen fachanwendungsspezifischen Diensten über das zentrale Netz muss für jede Verbindung explizit freigeschaltet werden.

<sup>2</sup> Die Kommunikation innerhalb der Consumer Zone unterliegt nicht der Regelungshoheit der Telematikinfrastruktur.

<sup>3</sup> Diese Kommunikation beschränkt sich auf die Anbindung des SNK bzw. anderer angeschlossener Bestandsnetze und den sicheren Internetzugang.

<sup>4</sup> Diese Kommunikation ist nur erlaubt, wenn nach dem Publish-Subscribe Pattern zuvor eine Registrierung vorgenommen wurde.

|                                  | Consumer Zone<br>(C) | Secure Consumer Zone<br>(SC) | TI-Plattform-Zone dezentral<br>(TI_D) | TI-Plattform-Zone zentral<br>(TI_Z) | Provider Zone<br>(P) | Existing Application Zone<br>(EA) |
|----------------------------------|----------------------|------------------------------|---------------------------------------|-------------------------------------|----------------------|-----------------------------------|
| TI-Plattform-Zone zentral (TI_Z) | --                   | --                           | --                                    | X                                   | --                   | --                                |
| Provider Zone (P)                | --                   | --                           | --                                    | X                                   | X                    | X                                 |
| Existing Application Zone (EA)   | --                   | --                           | --                                    | --                                  | X <sup>5</sup>       | --                                |

Um den Fachanwendungen die Möglichkeit zu bieten, fachanwendungsspezifische Dienste in einen auf Netzwerkebene geschützten Bereich zu platzieren, wird zusätzlich zu den Zonenregeln dafür gesorgt, dass „gesicherte Fachanwendungsspezifische Dienste“ nur über Fachmodule erreicht werden können, während „offene Fachanwendungsspezifische Dienste“ auch durch Clientsysteme oder Clientmodule erreichbar sind.

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) möglich sind. ☒

In der TI-Plattform zentral ist die Kommunikation in Richtung aller zugelassenen Dienste und angeschlossenen Bestandsnetze im Rahmen des Test- und Zulassungsverfahrens freizuschalten. Im dezentralen Bereich ist die Kommunikation zu Pflichtanwendungen gemäß §291a SGB V [SGB V] immer erlaubt. Die Kommunikation in Richtung eines Bestandsnetzes muss durch den Administrator explizit freigeschaltet werden. Dabei wird immer das Bestandsnetz als Ganzes und nicht einzelne Dienste im Bestandsnetz 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

<sup>5</sup> Diese Kommunikation darf nicht aus dem SNK bzw. anderen angeschlossenen Bestandsnetzen erfolgen.

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 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<sup>6</sup>.

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.

### 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.

---

<sup>6</sup> Dies gilt auch für Fachdaten, die auf der eGK oder dem mobilen Kartenterminal gespeichert werden. Die Container der eGK bzw. die Speicherbereiche des mobilen Kartenterminals, in denen diese Daten abgelegt werden, gelten als Speicherort der Fachanwendungen.

## 2.6 Rollen der TI-Plattform

### 2.6.1 Personenkreise der Telematikinfrastuktur

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 zugriffsberechtigten 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. | Zugriffsberechtigter 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                              |

Obwohl nicht namentlich benannt, erstreckt sich der Personenkreis 5 ebenfalls auf berufsmäßige Gehilfen von psychologischen Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten.

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 Telematikinfrastuktur nutzen oder mit ihr interagieren. Tabelle 3 benennt diese Personenkreise.

**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 | Im § 291a SGB V nicht erwähnt, jedoch im SGB V.   |

| PK-Nr. | Personenkreis ohne Zugriffsberechtigung nach §291a SGB V   | Abgrenzung zu §291a SGB V |
|--------|--|---------------------------|
|        | Organisationen.<br>Teilnehmender Personenkreis der TI gemäß.<br>Gesellschafterbeschluss der gematik. |                           |

## 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<br>Gesellschafterorganisation | Mitarbeiter von Gesellschaftern der gematik und denen durch sie vertretenen Organisationen. Nicht enthalten sind Mitarbeiter, die gemäß §291 SGB V tätig sind     | 11  |

**Tabelle 5: Betriebliche Rollen**

| Rolle                                      | Beschreibung   | PK nach §291a SGB V (siehe Tabelle 2 und Tabelle 3) |
|--|--|---|
| Kartenherausgeber eGK                      | Herausgeber 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         | 10  |



| Rolle         | Beschreibung  | PK nach §291a SGB V<br>(siehe Tabelle 2 und<br>Tabelle 3) |
|---------------|---|---|
|               | der TI zuständig  |   |
| Administrator | Fachpersonal zum Aufbau und Betrieb der Telematikinfrastruktur und der vorhandenen Primär- und Backend-Systeme. Es wird unterschieden zwischen:<br>a) Administrator einer Organisation des Gesundheitswesens<br>b) Administrator eines zentralen Dienstes | 10  |
| gematik       | Mitarbeiter gematik   | 10  |

Tabelle 6: Technische Rollen

| Rolle                             | Beschreibung   | PK nach §291a SGB V<br>(siehe Tabelle 2 und<br>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   |
| Fachanwendungsspezifischer 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.  | 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   |

---

## **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 5.5.1.10 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.

### 3.5 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.

### 3.6 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.

### 3.7 Zugang zu Bestandsnetzen

Neben der Telematikinfrastruktur existieren im deutschen Gesundheitswesen verschiedene andere Bestandsnetze, die Leistungserbringern Fachanwendungen bereitstellen. Die TI-Plattform ermöglicht es Leistungserbringern, die Fachanwendungen angeschlossener Bestandnetze über die TI-Plattform erreichen und nutzen zu können.

### 3.8 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.

### 3.9 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 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 im Projektauftrag der Basis-TI der Stufe 1 geforderten 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.

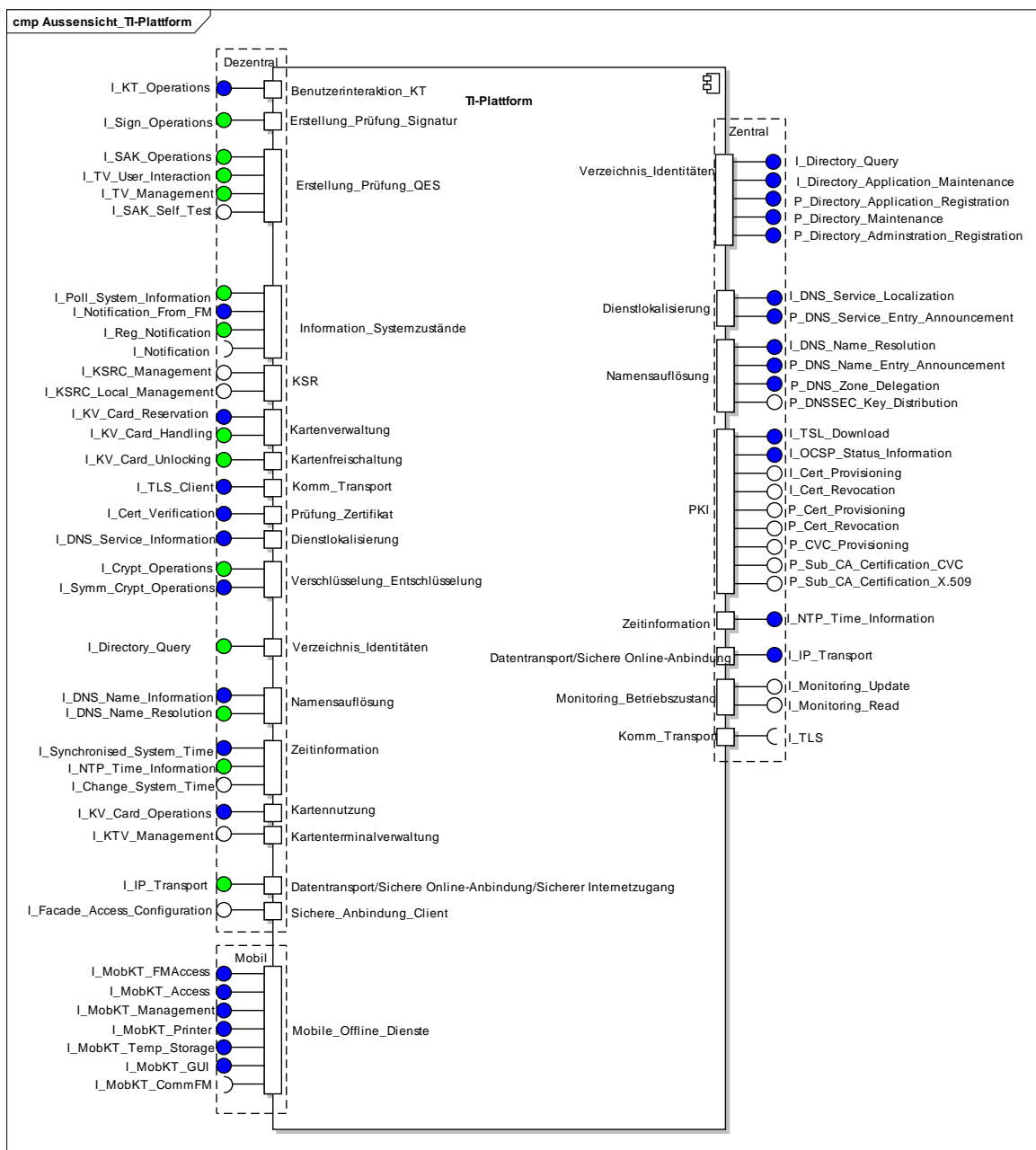


Abbildung 4: Außensicht der TI-Plattform

---

## 4 Lösungen der Architektur der TI-Plattform

---

### 4.1 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 berechnigte Anwender diesen erhöhten Sicherheitszustand der Karte nutzen können. Welche Anwender berechnigt sind, hängt vom Kartentyp ab. Bei organisations-/institutionsbezogenen Karten dürfen alle berechnigten 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 Ressourceldentifizier adressiert. Vor der Nutzung von direkten Kartenoperationen und solchen Operationen, die Kartenzugriffe implizieren, wie Signieren oder Entschlüsseln, muss der Aufrufer den Ressourceldentifizier der Karte zusammen mit dem Aufrufkontext einmalig an die TI-Plattform übermitteln. Aus der Kombination von Ressourceldentifizier 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 modellieren zu können. Wie der spätere tatsächliche technische Mechanismus ausgestaltet werden wird, der die obigen Anforderungen (Abgrenzung der Sicherheitszustände von verschiedenen Aufrufem) umsetzt, wird auf Spezifikationsebene unter Berücksichtigung von Sicherheitsaspekten entschieden.

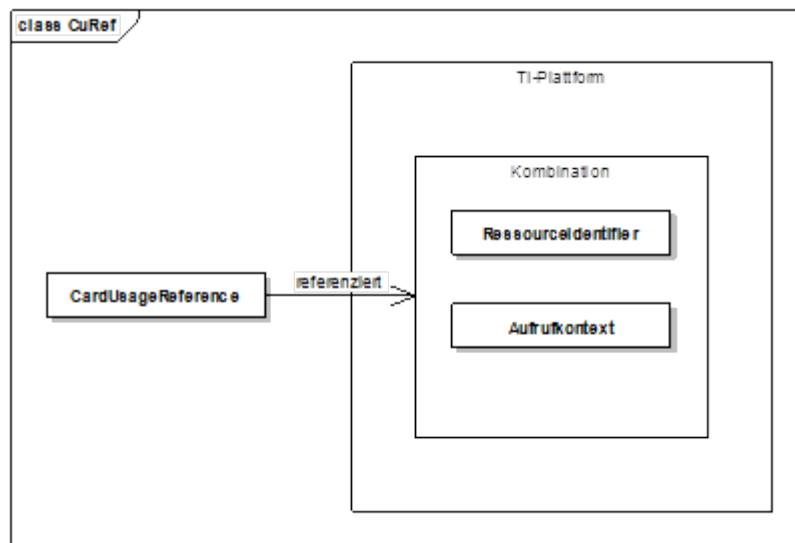


Abbildung 5: CardUsageReference

## 4.2 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

#### 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.



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.

### 4.3 Remote-PIN

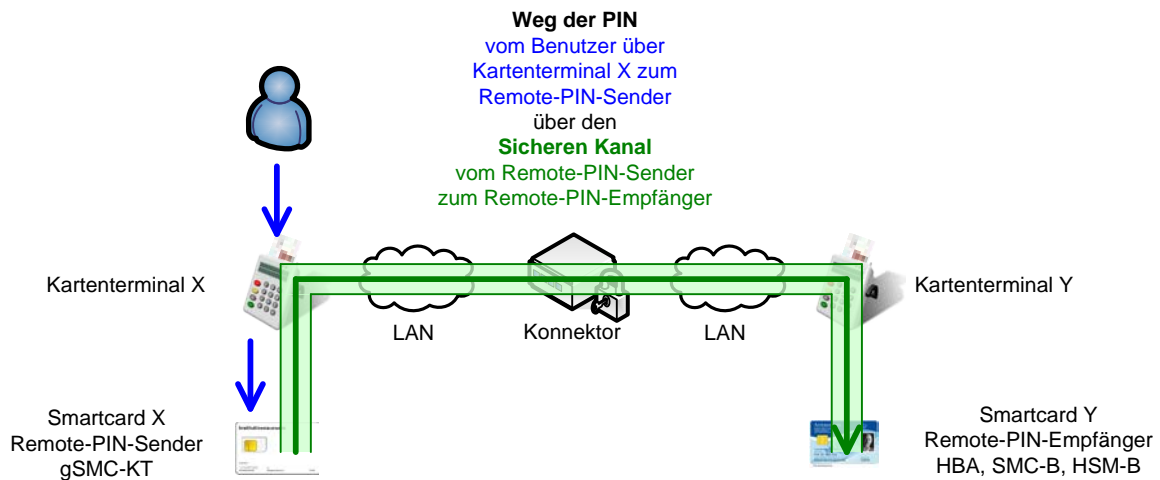
Die Telematikinfrastruktur ermöglicht dem Anwender für alle angebotenen Funktionen, die PIN-Eingaben an HBAs oder an SMC-B/HSM-B benötigen, die für diese Funktion nötige PIN wahlweise lokal einzugeben oder per Remote-PIN-Eingabe durchzuführen.

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.

Die beteiligten Komponenten des Remote-PIN-Verfahrens skizziert Abbildung 6:



**Abbildung 6: 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:

- 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. Der in der technischen Richtlinie genannte Akteur SMC-A ist nicht verbindlich und wird durch die festgelegten Remote-PIN-Sender ersetzt. ☒

## 4.4 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.

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.

## 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 7 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.

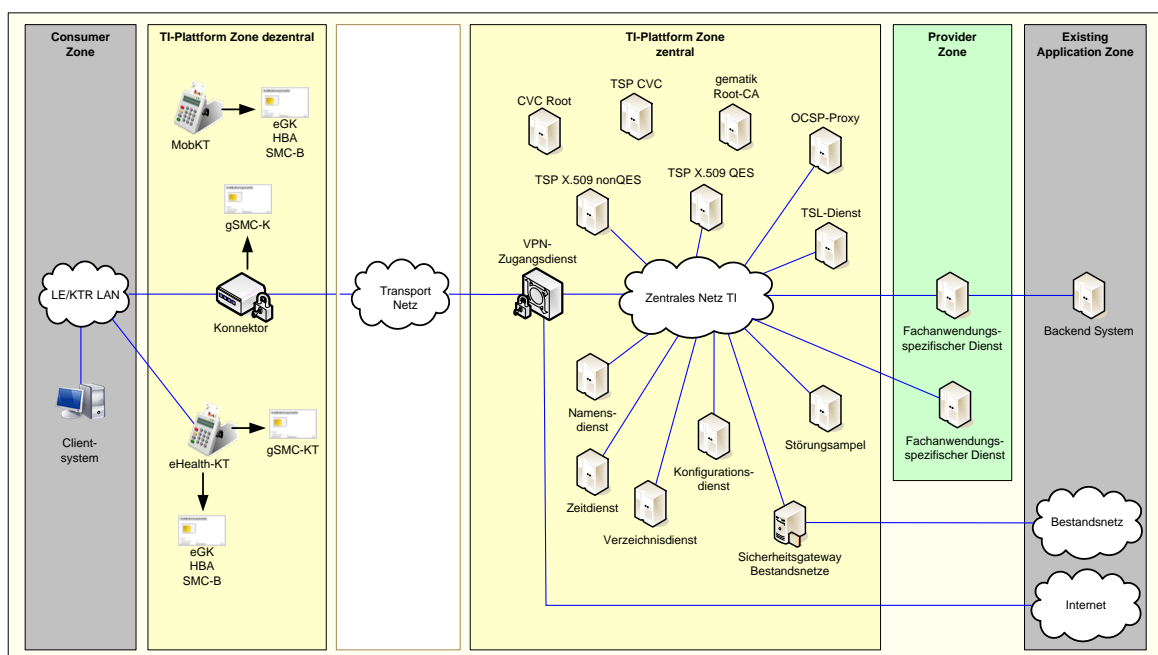


Abbildung 7: Übersicht des Gesamtsystems der TI

### 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.

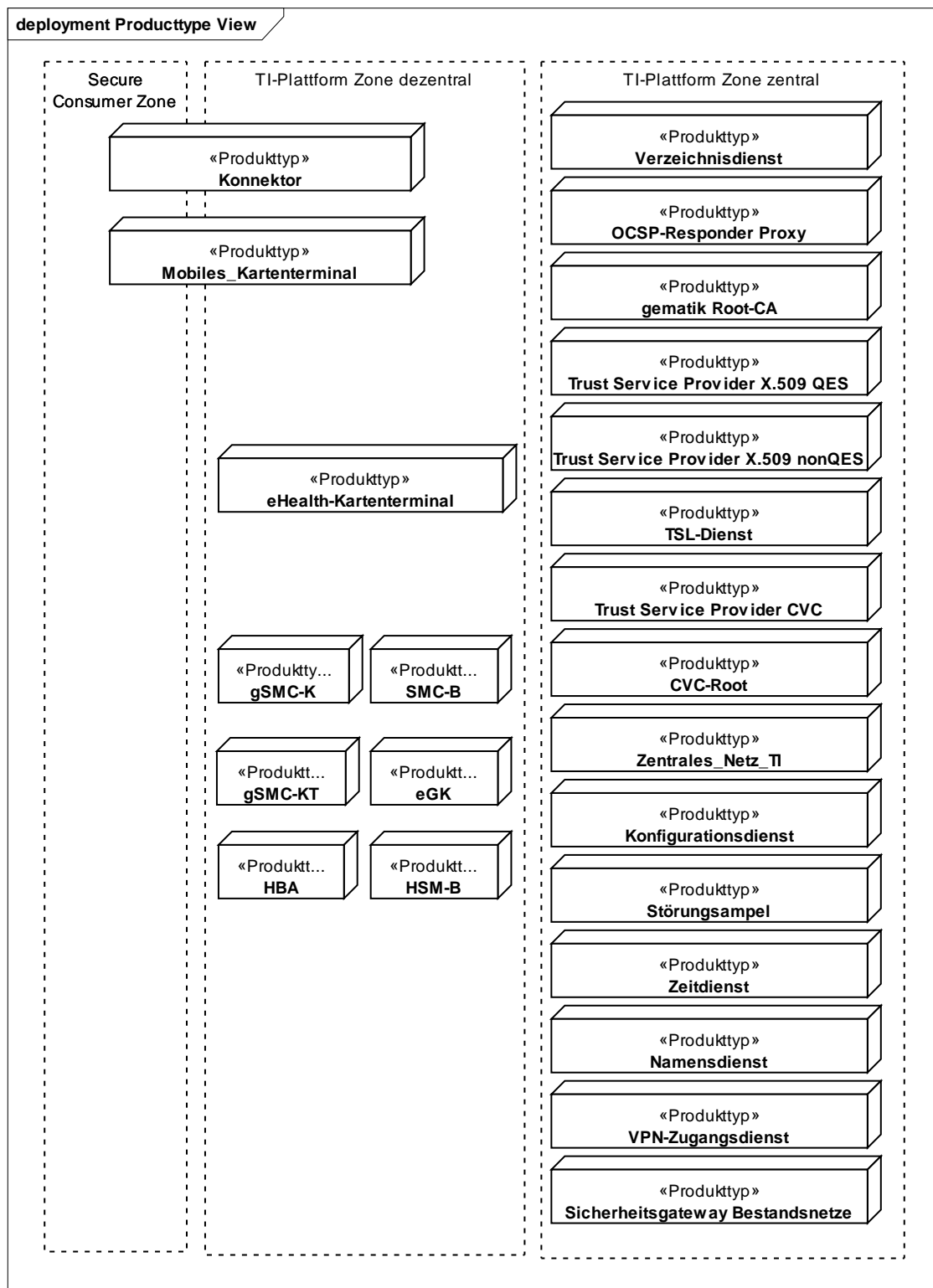


Abbildung 8: Produkttypsicht



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\_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 nach zehnmöglicher Nutzung (unabhängig von der richtigen oder falschen Eingabe) der PUK, die Karte gesperrt bleibt. ☒

☒ **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. ☒

☒ **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.

### 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 Verschlüsselung von Daten des Versicherten eingesetzt. Zusätzlich können auf der eGK in begrenztem Umfang Daten der Fachanwendungen 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 7: 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_Smartcard_Operations         | Konnektor                     | Aufgrund des bestehenden Bestandsschutzes erfolgt in diesem Dokument keine weitere Beschreibung dieser Schnittstelle. |
| 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. ☒

### 5.3.2 Produkttyp Heilberufsausweis (HBA)

Der HBA ist eine Smartcard und wird zur Authentisierung des Leistungserbringers in der TI sowie zur Signatur und Verschlüsselung 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 8: 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_Smartcard_Operations         | Konnektor                     | Aufgrund des bestehenden Bestandsschutzes erfolgt in diesem Dokument keine weitere Beschreibung dieser Schnittstelle. |
| Benötigte Schnittstellen       |                               |   |
|                                |                               |   |
| Fachliche Prozesse             | Bedingungen                   |   |
|                                |                               |   |

☒

### 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 bzw. der Leistungserbringerinstitution in der TI sowie zur Signatur und Verschlüsselung 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 9: 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_Smartcard_Operations         | Konnektor                     | Aufgrund des bestehenden Bestandsschutzes erfolgt in diesem Dokument keine weitere Beschreibung dieser Schnittstelle. |
| Benötigte Schnittstellen       |                               |   |

| Fachliche Prozesse | Bedingungen |
|--------------------|-------------|
|                    |             |



- ☒ **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)

Das HSM-B ist ein spezielles HSM und wird zur Authentisierung von Organisationen des Gesundheitswesens in der TI sowie zur Signatur und Verschlüsselung 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 10: 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 ersetzen 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**

Der Produkttyp HSM-B MUSS vollständig alle Funktionen einer oder mehrerer 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 11: Schnittstellen und Prozesse des Produkttyps gSMC-KT**

| gSMC-KT                        |             |   |
|--------------------------------|-------------|---|
| Bereitgestellte Schnittstellen | Nutzer      | Bedingungen   |
|                                |             | Da dieser Produkttyp eng an den Produkttyp eHealth-Kartenterminal gebunden ist und dort innerhalb des Gerätes verbaut wird, wurde auf eine weitere konzeptionelle Betrachtung der nötigen Schnittstellen und derer Nutzer verzichtet. |
| Benötigte Schnittstellen       |             |   |
|                                |             |   |
| Fachliche Prozesse             | Bedingungen |   |
|                                |             |   |

☒

### 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 12: Schnittstellen und Prozesse des Produkttyps gSMC-K**

| gSMC-K                         |             |  |
|--------------------------------|-------------|--|
| Bereitgestellte Schnittstellen | Nutzer      | Bedingungen  |
|                                |             | Da dieser Produkttyp eng an den Produkttyp Konnektor gebunden ist und dort innerhalb des Gerätes verbaut wird, wurde auf eine weitere konzeptionelle Betrachtung der nötigen Schnittstellen und derer Nutzer verzichtet. |
| Benötigte Schnittstellen       |             |  |
|                                |             |  |
| Fachliche Prozesse             | Bedingungen |  |
|                                |             |  |

☒

### 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 13: 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 Bestandsschutz des eHealth-Kartenterminals, da sie entweder die Firmware des KT's betreffen oder durch Vorgaben der Arbeitsgruppe „Einsatzumgebung Kartenterminal“<sup>7</sup> 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**

<sup>7</sup> 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.

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.

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 14: 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                                |  |
| <b>Benötigte Schnittstellen</b>  |  |  |
| I_ICC_Contacts, I_Notification, PrinterConnector (repräsentiert den Anschluss eines externen Druckers, optional), I_MobKT_CommFM |  |  |
| <b>Fachliche Prozesse</b>  | <b>Nutzer</b>                                  | <b>Bedingungen</b>   |
|  |  |  |



#### ☒ 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. ☒

#### ☒ 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 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)**

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.

Neben dem Standalone-Szenario (siehe auch § 291 Abs. 2b Satz 2 SGB V) mit einer physischen Trennung der Umgebung der Clientsysteme und der zentralen TI-Plattform, und dem damit verbunden Einsatz von 2 Konnektoren und 2 eHealth-Kartenterminals, muss entsprechend (LH-BasisTI-A\_1981) zusätzlich ein Modus der logischen Trennung ermöglicht werden, in dem lediglich ein Konnektor benötigt wird. In diesem Modus wird durch den Konnektor sichergestellt, dass keine Daten zwischen Clientsystem und der zentralen TI-Plattform oder den fachanwendungsspezifischen Diensten fließen. Die Sicherheitseigenschaft dieser logischen Trennung im Konnektor wird nach einheitlichen Kriterien gemäß Common Criteria (CC) evaluiert und zertifiziert.

##### **5.3.9.2 Logische Trennung innerhalb des Konnektors**

Für den Konnektor werden nur eingeschränkt Vorgaben zur internen Architektur der Konnektor-Hardware und -Firmware getroffen. Bei derzeitiger Konnektorarchitektur wird das Sicherheitsniveau der logischen Trennung nicht durch den Einsatz zusätzlicher logischer Software-Komponenten (z. B. zwei Fachmodule VSDM zur Unterstützung der logischen Trennung) erhöht. Daher ist es ausreichend, die Konnektorleistungen zur Unterstützung der logischen Trennung an der Außensicht des Konnektor zu definieren. Auch der Einsatz von 2 Kartenterminals zur Separierung von Anwendungsfällen mit Online-Nutzung der TI und rein lokal ablaufenden Anwendungsfällen erhöht das Sicherheitsniveau nicht.

##### ☒ **TIP1-A\_2462 Logische Trennung im Konnektor**

Der Konnektor MUSS zur Unterstützung des Standalone-Szenarios einen Modus der logischen Trennung zwischen Clientsystemen und der zentralen TI-Plattform unterstützen.

Folgende Eigenschaften sind für den Modus der logischen Trennung zu berücksichtigen:

- Der Modus der logischen Trennung MUSS durch den Administrator über eine Konfigurationseinstellung aktivierbar und deaktivierbar sein.
- Im Modus der logischen Trennung MUSS der Konnektor alle vorgesehenen Funktionen auch mit einem einzelnen angeschlossenen Kartenterminal anbieten. Ausgenommen davon sind nur Funktionen deren Erbringung zwei oder mehrere Kartenterminals benötigt, wie z. B. Remote-PIN.

- Der Konnektor MUSS jeglichen direkten Netzwerkverkehr zwischen Clientsystemen und der TI unterbinden (Dies schließt speziell auch die Kommunikation zwischen Clientsystemen und Bestandsnetzen ein).
- Es MÜSSEN folgende Funktionen (und die hierfür notwendigen Netzwerk- und Infrastrukturdienste) im Konnektor unterstützt werden, die einen Zugriff vom Konnektor auf die zentrale TI-Plattform haben:
  - VPN-Verbindung in die zentrale TI-Plattform (I\_Secure\_Channel\_Tunnel)
  - Download der TSL (I\_TSL\_Download)
  - alle Anwendungsfälle der Fachanwendung VSDM und die hierfür nötigen Leistungen der TI-Plattform (z.B. Zertifikatsprüfung)
  - Unterstützung des Basisdienstes KSR

Alle anderen Funktionen des Konnektors sowie alle weiteren Fachanwendungen MÜSSEN derart bereitgestellt werden, als wäre keine Online-Anbindung vorhanden. ☒

### 5.3.9.3 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 15: 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_KSRC_Local_Management        | Admin einer Organisation des Gesundheitswesens |  |
| I_KSRC_Management              | Admin einer Organisation des Gesundheitswesens |  |
| 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,<br>Fachmodul                           |                                       |
| I_Reg_Notification   | Clientsystem,<br>Fachmodul                           |                                       |
| I_SAK_Operations   | Clientsystem,<br>Fachmodul                           |                                       |
|  |  |                                       |
| I_Sign_Operations  | Clientsystem,<br>Fachmodul                           |                                       |
| I_Synchronised_System_Time   | Fachmodul  |                                       |
| I_KV_Card_Unlocking  | Clientsystem,<br>Fachmodul                           |                                       |
|  |  |                                       |
|  |  |                                       |
| I_KT_Operations  | Fachmodul  |                                       |
| I_KTV_Management   | Admin einer<br>Organisation des<br>Gesundheitswesens |                                       |
| I_Change_System_Time   | Admin einer<br>Organisation des<br>Gesundheitswesens | Ist nur im Offline-Fall zu verwenden. |
| I_KV_Card_Reservation  | Fachmodul,   |                                       |
| I_Notification   | eHealth-<br>Kartenterminal                           |                                       |
| I_Directory_Query  | Clientsystem,<br>Fachmodul                           |                                       |
| <b>Benötigte Schnittstellen</b>  |  |                                       |
| I_Smartcard_Operations <sup>1)</sup> , I_KVK_Read <sup>1)</sup> , I_HSM_Operations (optional) <sup>2)</sup> , I_Notification,<br>I_Poll_System_Information, I_OCSP_Status_Information, I_DNS_Name_Resolution,<br>I_NTP_Time_Information, I_KSR_Update, I_KSRS_Download, I_KT_Communication,<br>I_DNS_Service_Localization, I_Secure_Channel_Tunnel, I_TLS, I_TSL_Download,<br>I_BNetA_VL_Download, I_Secure_Internet_Tunnel, I_CRL_Download, I_Registration_Service,<br>I_KSRS_Net_Config, I_Directory_Query |  |                                       |
| <sup>1)</sup> Aufgrund des bestehenden Bestandsschutzes erfolgt in diesem Dokument keine weitere<br>Beschreibung dieser Schnittstelle  |  |                                       |
| <sup>2)</sup> Optional benötigte Schnittstelle, da die Unterstützung eines HSM-B durch den Konnektor optional<br>ist   |  |                                       |
| <b>Fachliche Prozesse</b>  | <b>Nutzer</b>  | <b>Bedingungen</b>                    |
|  |  |                                       |



☒ **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 Klinik-einrichtungen 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**

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\_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.

### 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 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. Ein Verbindungsaufbau in die TI aus Fremdnetzen wird verhindert. Nur Clientsysteme aus der Consumer Zone dürfen auf Fremdnetze 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 16: Schnittstellen und Prozesse des Produkttyps Zentrales Netz TI**

| Zentrales Netz TI              |  |             |
|--------------------------------|--|-------------|
| Bereitgestellte Schnittstellen | Nutzer   | Bedingungen |
| I_IP Transport                 | FA_spez_Dienst,<br>Zeitdienst,<br>Namensdienst,<br>TSL-Dienst,<br>Konfigurationsdienst,<br>VPN-Zugangsdienst,<br>Trust Service Provider<br>X.509 nonQES,<br>Trust Service Provider<br>X.509 QES,<br>Störungssampel |             |
| Benötigte Schnittstellen       |  |             |
|                                |  |             |
| Fachliche Prozesse             | Nutzer   | Bedingungen |
|                                |  |             |





☒ **TIP1-A\_2519 Produkttyp Zentrales Netz-TI, nur zugelassene Fachdienste anbinden**

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 17: Schnittstellen und Prozesse des Produkttyps Zeitdienst**

| Zeitdienst                            |  |             |
|---------------------------------------|--|-------------|
| Bereitgestellte Schnittstellen        | Nutzer   | Bedingungen |
| I_NTP_Time_Information                | FA_spez_Dienst,<br>Namensdienst,<br>TSL-Dienst,<br>Konfigurationsdienst,<br>VPN-Zugangsdienst,<br>Trust Service Provider |             |
| 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 Namens-

raumes (Subdomains) kann an andere Dienstbetreiber delegiert werden (DNS-Zone-Delegation).

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 18: Schnittstellen und Prozesse des Produkttyps Namensdienst**

| Namensdienst                           |  |   |
|--|--|---|
| Bereitgestellte Schnittstellen         | Nutzer   | Bedingungen                               |
| I_DNS_Name_Resolution                  | FA_spez_Dienst,<br>Zentrales Netz TI,<br>Zeitdienst,<br>TSL-Dienst,<br>Konfigurationsdienst,<br>VPN-Zugangsdienst,<br>Trust Service Provider,<br>Konnektor |   |
| 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,<br>Zentrales Netz TI,<br>Zeitdienst,<br>TSL-Dienst,<br>Konfigurationsdienst,<br>VPN-Zugangsdienst,<br>Trust Service Provider               | inklusive Änderung und<br>Deregistrierung |
| P_DNSSEC_Key_Distribution              | FA_spez_Dienst,<br>VPN-Zugangsdienst,<br>Zeitdienst,<br>TSL-Dienst,<br>Konfigurationsdienst,<br>Trust Service Provider                                     |   |
| P_DNS_Service_Entry_Announcement       | FA_spez_Dienst,<br>VPN-Zugangsdienst,<br>Zeitdienst,<br>TSL-Dienst,<br>Konfigurationsdienst,<br>Trust Service Provider                                     | inklusive Änderung und<br>Deregistrierung |
| P_DNS_Zone_Delegation                  | FA_spez_Dienst,<br>VPN-Zugangsdienst,<br>Zeitdienst,<br>TSL-Dienst,<br>Konfigurationsdienst,<br>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.

**Tabelle 19: Schnittstellen und Prozesse des Produkttyps Verzeichnisdienst**

| Verzeichnisdienst  |   |   |
|--|---|---|
| <b>Beschreibung</b>  | 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 berechnigte fachanwendungs spezifische Dienste geändert, hinzugefügt und gelöscht werden. |   |
| Bereitgestellte Schnittstellen   | Nutzer  | Bedingungen   |
| I_Directory_Query  | TIP,<br>FA_spez_Dienst  |   |
| I_Directory_Maintenance  | FA_spez_Dienst  | Die Schnittstelle wird über TLS mit beidseitiger Authentifizierung bereitgestellt |
| 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 |   |   |
| Fachliche Prozesse   | Nutzer  | Bedingungen   |
| P_Directory_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:

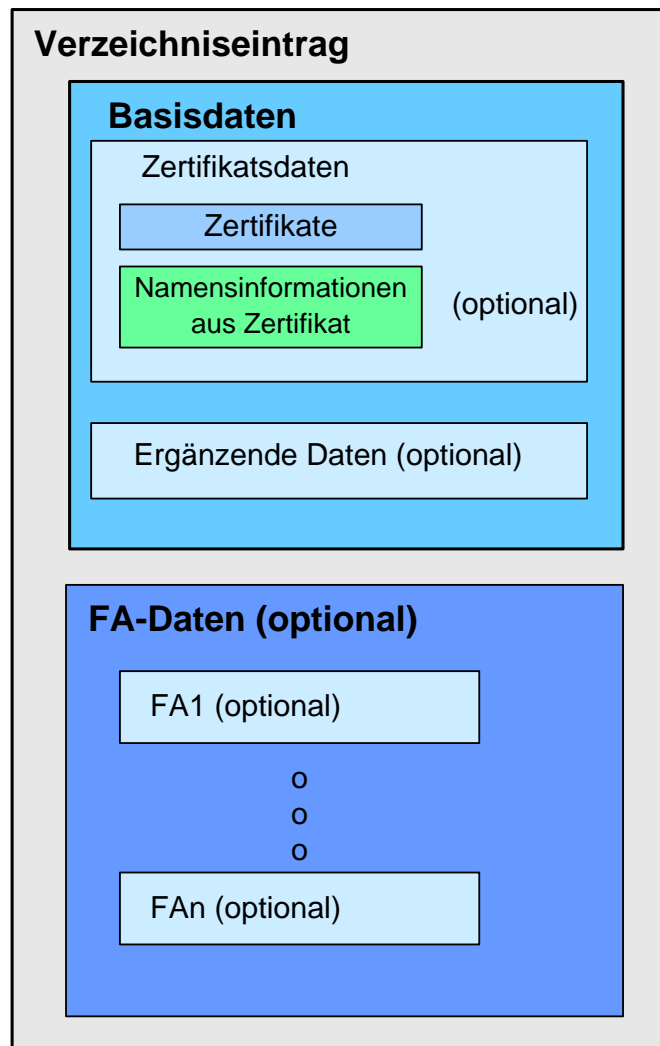


Abbildung 9: Datenmodell Verzeichnisdienst

**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 Verzeichnisdienstes MUSS die Telematik-ID als Ordnungskriterium für das Datenmodell verwenden. ☒

☒ **TIP1-A\_5778 Produkttyp Verzeichnisdienst, Löschen Basiseintrag Verzeichnisdienst**

Der Produkttyp Verzeichnisdienstes 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. ☒

### 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.

☒ **TIP1-A\_2238 Produkttyp TSL-Dienst, Schnittstellen und Prozesse**

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

**Tabelle 20: Schnittstellen und Prozesse des Produkttyps TSL-Dienst**

| TSL-Dienst                     |   |             |
|--------------------------------|---|-------------|
| Bereitgestellte Schnittstellen | Nutzer  | Bedingungen |
| I_OCSP_Status_Information      | FA_spez_Dienst,<br>Konnektor,<br>VPN-Zugangsdienst  |             |
| I_TSL_Download                 | FA_spez_Dienst,<br>Konnektor,<br>VPN-Zugangsdienst, |             |
| 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<br>X.509 nonQES,<br>Trust Service Provider<br>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-Karten-terminal 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 21: 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 |             |

☒

☒ **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 Gesamtbetriebsverantwortlichen der TI zyklisch bereitgestellt werden. ☒

### 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 22: 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 |
|   |        |             |

☒

☒ **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. ☒

☒ **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 Sicherheitgateway Bestandsnetze (SG-BNet)

Der Produkttyp Sicherheitgateway Bestandsnetze ermöglicht den Clientsystemen die Nutzung von Diensten in Bestandsnetzen, wie dem sicheren Netz der KVen (SNK).

Jedes Bestandsnetz wird über eine eigene Instanz des Produkttyps Sicherheitgateway Bestandsnetze an die TI angebunden.

Um die TI vom SNK bzw. anderen Bestandsnetzen abzuschotten, werden an diesen Netzübergängen Sicherheitgateways eingesetzt werden.

☒ **TIP1-A\_2241 Produkttyp Sicherheitgateway Bestandsnetze, Schnittstellen und Prozesse**

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

**Tabelle 23: Schnittstellen und Prozesse des Produkttyps Sicherheitgateway Bestandsnetze**

| Sicherheitgateway 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 Sicherheitgateway Bestandsnetze, Sicherung ggü. dem Bestandsnetz**

Der Produkttyp Sicherheitgateway Bestandsnetze MUSS Richtung Bestandsnetze durch Stateful Inspection Firewalls und ein Applikation Level Gateway gesichert werden. ☒

☒ **TIP1-A\_2533 Produkttyp Sicherheitgateway Bestandsnetze, kein Verbindungsaufbau aus Bestandsnetzen**

Der Produkttyp Sicherheitsgateway Bestandsnetze MUSS den Verbindungsaufbau aus Bestandsnetzen 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 berechnigte 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 24: 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,<br>Betreiber_ZD,<br>Betreiber_FD       |  |
| I_Cert_Revocation   | Hersteller,<br>Betreiber_ZD,<br>Betreiber_FD       |  |
| I_OCSP_Status_Information   | FA_spez_Dienst,<br>Konnektor,<br>VPN-Zugangsdienst | 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,<br>Kartenherausgeber                           |  |
| P_Cert_Revocation   | LE,<br>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 berechnigte 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 25: 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 berechnigte 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 berechnigte Personen (HBA, eGK) und Organisationen/Institutionen (SM-B).

##### ☒ TIP1-A\_2243 Produkttyp Trust Service Provider CVC, Schnittstellen und Prozesse

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

**Tabelle 26: 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 27: 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 28: 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. |
| <b>Benötigte Schnittstellen</b>                               |               |                    |
| I_NTP_Time_Information, I_DNS_Name_Resolution, I_IP Transport |               |                    |
| <b>Fachliche Prozesse</b>                                     | <b>Nutzer</b> | <b>Bedingungen</b> |
|   |               |                    |



☒ **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 29: Schnittstellen und Prozesse des Produkttyps Störungsampel**

| <b>Störungsampel</b>  |                               |  |
|---|-------------------------------|--|
| <b>Bereitgestellte Schnittstellen</b>                         | <b>Nutzer</b>                 | <b>Bedingungen</b>   |
| I_Monitoring_Update   | Betreiber_ZD,<br>Betreiber_FD |  |
| I_Monitoring_Read   |                               | <p>Diese Schnittstelle MUSS im Internet für die nachfolgenden Nutzer angeboten werden.</p> <ul style="list-style-type: none"> <li>• Anbieter in ihrer Rolle als betriebsverantwortliche Instanz,</li> <li>• die Supportdienstleistenden,</li> <li>• die Servicebetriebsverantwortlichen der TI,</li> <li>• die gematik als gesamtbetriebsverantwortliche Instanz.</li> </ul> |
| <b>Benötigte Schnittstellen</b>                               |                               |  |
| I_NTP_Time_Information, I_DNS_Name_Resolution, I_IP Transport |                               |  |
| <b>Fachliche Prozesse</b>                                     | <b>Nutzer</b>                 | <b>Bedingungen</b>   |
|   |                               |  |



#### ☒ **TIP1-A\_2540 Produkttyp Störungsampel, Generierung Gesamtfunktionsstatus**

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. ☒

## 5.5 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**) 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 30 werden die für die Dokumentation verwendeten Abkürzungen erklärt.



Tabelle 30: 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 47 verwendet.

Die aus Kapitel 4.2 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.

## 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 31: Operation interact\_with\_User

| I_KT_Operations   |           |          |                       |       | Berechtigung: FM |
|---|-----------|----------|-----------------------|-------|------------------|
| interact_with_User  | Parameter |          |                       |       | V, I, A          |
|   | In        | KT_Ident | Ressourceldentifizier | 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 32: 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               |

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 33: 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



#### ⊗ TIP1-A\_5075 Logische Operation I\_Sign\_Operations::external\_Authenticate

Die Schnittstelle I\_Sign\_Operations MUSS die logische Operation external\_Authenticate implementieren.

**Tabelle 34: Operation external\_Authenticate**

| I_Sign_Operations     |           |            |                    |       | Berechtigung:<br>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 35: Operation get\_Certificate**

| I_Sign_Operations | Berechtigung:<br>CS, FM |
|-------------------|-------------------------|
|-------------------|-------------------------|

| get_Certificate  | Parameter |             |                        |       | V, I, A  |
|--|-----------|-------------|------------------------|-------|----------|
|  | In        | ResID       | Ressourcenidentifizier | IM412 | M/H/H    |
|  | In        | CuRef       | CardUsageReference     | IM308 | SH/SH/SH |
|  | Out       | Certificate | CertificateX.509       | IM404 | M/M/M    |
| <p>Die Operation liefert ein X.509-Zertifikat von einer gesteckten Karte.<br/>         Anhand der CardUsageReference (<i>CuRef</i>) wird die zu verwendende Karte adressiert und werden die Zugriffsrechte geprüft. Das konkrete Zertifikat wird durch die Resource-ID (<i>ResID</i>) referenziert und im Ergebnis (<i>Certificate</i>) zurück geliefert.<br/>         Abrufbar sind alle X.509-Zertifikate von</p> <ul style="list-style-type: none"> <li>HBA (zeitlich begrenzt auch die HBA-Vorläuferkarten HBA-qSig und ZOD-2.0) und SMC-B für Clientsysteme</li> <li>eGK, HBA und SMC-B für Fachmodule</li> </ul> <p>Verfügbarkeit: NA, Nichtabstreitbarkeit: NA1.3.0</p> |           |             |                        |       |          |



### 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

Die Schnittstelle I\_SAK\_Operations MUSS die logische Operation sign\_Document\_QES implementieren.

**Tabelle 36: Operation sign\_Document\_QES**

| I_SAK_Operations   |           |                |                            |       | Berechtigung:<br>CS, FM                       |
|--|-----------|----------------|----------------------------|-------|---|
| sign_Document_QES  | Parameter |                |                            |       | V, I, A                                       |
|  | In        | DataToBeSigned | List of DocumentType       | IM101 | SH/SH/SH<br>(Dokument)<br>SH/SH/SH<br>(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<br>(Dokument)<br>SH/SH/SH<br>(Liste)   |
| <p>Mit dieser Operation wird eine qualifizierte elektronische Signatur (QES) gemäß [eIDAS] für jedes der übergebenen Dokumente (<i>DataToBeSigned</i>) 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 (<i>CuRef</i>) geprüft.</p> <p>Es wird die Übereinstimmung der Eigenschaften der Dokumente mit den Vorgaben der übergebenen Policies (<i>Policies</i>) 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.<br/>         Des Weiteren muss vor Erstellung der Signatur geprüft werden, ob die Gültigkeitsdauer des Signaturzertifikats überschritten ist.<br/>         Die Verwendung von Attributzertifikaten wird unterstützt.</p> |           |                |                            |       |   |

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.

#### Eigenschaften der Stapelsignatur

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.
- Die Stapelsignatur kann bis zum Auslösen der qualifizierten elektronischen Signaturen (PIN-Eingabe) und während der Stapelbearbeitung 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 37: Operation verify\_Document\_QES**

| I_SAK_Operations    |           |                    |                        |       | Berechtigung<br>: 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



#### 5.5.1.4 Information\_Systemzustände

##### 5.5.1.4.1 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\_Resource\_List

Die Schnittstelle I\_Poll\_System\_Information MUSS die logische Operation get\_Resource\_List implementieren.



Tabelle 38: 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                     |
| <p>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“).</p> <p>Die zurückgegebene Liste enthält pro Listenelement die Informationen Ressourceldentifizier, RessourceType und RessourcenName.</p> <p>Unterschiedliche dezentrale Komponenten liefern unterschiedliche Inhalte:</p> <ul style="list-style-type: none"> <li>➤ Ein MobKT listet: Slots, gesteckte Karten, Drucker</li> <li>➤ Eine Kartenterminalverwaltung listet die verwalteten KTs</li> <li>➤ Eine Kartenverwaltung liefert eine Liste der verwalteten Karten</li> <li>➤ Eine Kartenterminal listet seine Funktionalen Einheiten (Display, PIN-Pad, Slots)</li> </ul> |           |         |               |       |                           |
| 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 39: Operation get\_Ressource\_Information

| I_Poll_System_Information   |           |                 |                       |       | Berechtigung: CS, FM, MFM |
|---|-----------|-----------------|-----------------------|-------|---------------------------|
| get_Ressource_Information   | Parameter |                 |                       |       | V, I, A                   |
|   | In        | ResIdentifizier | Ressourceldentifizier | IM412 | M/H/H                     |
|   | Out       | ResDetail       | RessourceDetails      | IM411 | M/H/H                     |
| <p>Die Operation liefert statische und dynamische Informationen der dezentralen Komponente, die über ResIdentifizier selektiert wird. Die Liste aller aktuell verfügbaren ResIdentifizier ist über get_Ressource_List abrufbar.</p> <p>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):</p> <ul style="list-style-type: none"> <li>- Ressourceldentifizier</li> <li>- CardInfo</li> <li>- Status Online/Offline</li> <li>- Betriebszustand der Komponente (OK=Normal, Warnung=Admin-Interaktion sinnvoll, Kritisch=Fachlich eingeschränkt, Admin-Interaktion erforderlich)</li> <li>- verfügbare technische Zertifikate (zur Ermittlung der verbleibenden Gültigkeitsdauer)</li> <li>- Versionsinformationen</li> </ul> <p>Unterschiedliche dezentrale Komponenten liefern unterschiedliche Inhalte:</p> <ul style="list-style-type: none"> <li>➤ Eine Systeminformation liefert die Informationen, die sie von den erreichbaren Komponenten erhalten kann (MobKT, Kartenterminalverwaltung, Kartenverwaltung, VPN-Client, Kartenterminal).</li> <li>➤ Ein MobKT liefert alle Statusinformationen des gesamten Geräts (User eingeloggt, welche Karten gesteckt, Status der Karten, Freier Speicher des Zwischenspeichers etc.).</li> <li>➤ 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.</li> <li>➤ Eine Kartenverwaltung liefert Informationen zu einer Karte (Eigenschaften der Karte: Kartentyp, Version, PIN-Status etc.).</li> <li>➤ Ein Kartenterminal liefert Informationen über seine funktionalen Einheiten (Display, PIN-Pad, Slots, etc.) und seiner aktuellen Zuständen (Gerätestatus, welche Slots sind belegt etc.).</li> </ul> |           |                 |                       |       |                           |
| Verfügbarkeit: NA, Nichtabstreitbarkeit: NA   |           |                 |                       |       |                           |





#### 5.5.1.4.2 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 40: Operation notify**

| I_Notification   |           |           |                  |       | Berechtigung: TIP |
|--|-----------|-----------|------------------|-------|-------------------|
| notify   | Parameter |           |                  |       | V, I, A           |
|  | In        | EventInfo | EventInformation | IM415 | M/H/H             |
| <p>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).</p> <p>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:</p> <ul style="list-style-type: none"> <li>- Betriebszustandswechsel</li> <li>- Wechsel in den verfügbaren Karten</li> <li>- Bedarf einer PIN-Verifikation</li> <li>- Fortschrittsfeedback (bei lang andauernden Operationen)</li> <li>- Informationen über Interaktionsbedarf</li> </ul> <p>Unterschiedliche dezentrale Komponenten liefern unterschiedliche Inhalte:</p> <ul style="list-style-type: none"> <li>➤ 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).</li> <li>➤ Ein MobKT meldet Statusänderungen des gesamten Geräts (User angemeldet, Karte gesteckt, Kartenstatus verändert etc.).</li> <li>➤ Eine Kartenterminalverwaltung meldet Ereignisse, die an sie von den von ihr verwalteten KTs gesendet wurden</li> <li>➤ Eine Kartenverwaltung meldet Zustandsänderungen an den von ihr verwalteten Karten (gesteckt, gezogen, PIN-Status verändert, PIN-Eingabe erwartet etc.).</li> <li>➤ Ein Kartenterminal meldet eingetretene Ereignisse der Art: Ankündigung eines terminalseitig initiierten Verbindungsabbruchs, Slotstatusänderungen (Karte gesteckt, Karte entfernt), Tastaturreignis etc.</li> </ul> |           |           |                  |       |                   |
| Verfügbarkeit: N, Nichtabstreitbarkeit: NA   |           |           |                  |       |                   |



#### 5.5.1.4.3 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 41: 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  |           |           |                  |       |                       |



#### 5.5.1.4.4 I\_Reg\_Notification (Provided)

##### ☒ TIP1-A\_2271 Schnittstelle I\_Reg\_Notification

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 42: 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  |           |               |                     |       |                            |



#### 5.5.1.5 KSR

##### 5.5.1.5.1 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 43: Operation list\_available\_Updates**

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



### ☒ TIP1-A\_2275 Logische Operation I\_KSRC\_Management::do\_Update

Die Schnittstelle I\_KSRC\_Management MUSS die logische Operation do\_Update implementieren.

**Tabelle 44: Operation do\_Update**

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



#### 5.5.1.5.2 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 45: 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 ( <i>updatePackage</i> ) auf einem lokalen Datenträger bereitstellen. |           |               |               |       |                 |
| Verfügbarkeit: N, Nichtabstreitbarkeit: H   |           |               |               |       |                 |



#### 5.5.1.5.3 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 46: 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 ( <i>UpdatePackage</i> ) aus.<br>Das eHealth-Kartenterminal nutzt hierfür die Standard-SICCT-Schnittstelle für das Update des SICCT-Kartenterminals. |           |               |               |       |                   |
| Verfügbarkeit: N, Nichtabstreitbarkeit: H   |           |               |               |       |                   |



#### 5.5.1.6 Kartenverwaltung

##### 5.5.1.6.1 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 Ressourceldentifizier 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 47: Operation `get_Card_Usage_Reference`**

| I_KV_Card_Handling   |           |         |                       |       | Berechtigung:<br>CS, FM, MFM |
|--|-----------|---------|-----------------------|-------|------------------------------|
| get_Card_Usage_Reference   | Parameter |         |                       |       | V, I, A                      |
|  | In        | ResID   | Ressourceldentifizier | IM412 | M/H/H                        |
|  | In        | CallCon | CallContext           | IM309 | SH/SH/SH                     |
|  | Out       | CuRef   | CardUsageReference    | IM308 | SH/SH/SH                     |
| <p>Die Operation <code>get_Card_Usage_Reference</code> liefert zu einer gewählten Karte (<i>ResID</i>) und einem Aufrufkontext (<i>CallCon</i>) eine <i>CardUsageReference</i> zurück (<i>CuRef</i>). Die <i>CardUsageReference</i> wird innerhalb dieser Operation neu angelegt, wenn für diese Karte und zu diesem Aufrufkontext noch keine vorhanden ist. Die erzeugte <i>CardUsageReference</i> hat eine ausreichend hohe Entropie, so dass sie nicht erraten werden kann und nicht zufällig auf eine andere Kombination von Ressourceldentifizier und Aufrufkontext in der Kartenverwaltung zeigen kann.</p> <p>Die gewählte Karte wird anhand der <i>ResID</i> identifiziert, die ein User aus der Ergebnisliste der Operation <code>get_Ressource_List</code> selektiert hat.</p> <p>In die <i>CardUsageReference</i> 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 <i>CardUsageReference</i> bekommen und einen eventuell erhöhten Sicherheitszustand gemeinsam nutzen.</p> <p>Die <i>CardUsageReference</i> wird in allen folgenden Operationsaufrufen von CS, FM und MFM als Verweis auf die Karte verwendet, mit der die Operation durchgeführt werden soll.</p> <p>Verfügbarkeit: NA, Nichtabstreitbarkeit: NA</p> |           |         |                       |       |                              |



#### ✖ **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 48: Operation `discard_Card_Usage_Reference`**

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



#### 5.5.1.6.2 `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 49: 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                 |
| <p>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.</p> <p>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.</p> <p>Im Rahmen einer QES muss diese Operation nicht explizit vom Fachmodul aufgerufen werden, da die SAK sich um die Exklusivität der Kartennutzung kümmert.</p> |           |            |                    |       |                       |
| Verfügbarkeit: NA, Nichtabstreitbarkeit: NA   |           |            |                    |       |                       |



### 5.5.1.7 Kartenfreischaltung

#### 5.5.1.7.1 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 können 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 50: 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  | Ressourceldentifizier | IM412 | M/M/M                     |
|  | In        | UsageInformation | Text                  | IM101 | SH/SH/SH                  |
| <p>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.</p> |           |                  |                       |       |                           |

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::unlock\_PIN

Die Schnittstelle I\_KV\_Card\_Unlocking MUSS die logische Operation unlock\_PIN implementieren.

**Tabelle 51: Operation unlock\_PIN**

| I_KV_Card_Unlocking  |           |               |                       |       | Berechtigung: CS, FM, MFM |
|--|-----------|---------------|-----------------------|-------|---------------------------|
| unlock_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      | Ressourceldentifizier | IM412 | M/M/M                     |
| Die Operation unlock_PIN veranlasst das Entsperren einer blockierten PIN. Dabei fordert das Kartenterminal den Nutzer zur Eingabe eines PUK auf und je nach <i>OperationMode</i> zur Eingabe einer neuen PIN. 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

Die Schnittstelle I\_KV\_Card\_Unlocking MUSS die logische Operation initialize\_PIN implementieren.

**Tabelle 52: 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           | Ressourceldentifizier  | 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 53: 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     | Ressourceldentifizier | 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 seiner alten PIN 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\_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 54: 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 <i>PinReference</i> bezeichneten PIN einer gewählten Karte. Der PIN-Status enthält Angaben zum Sicherheitszustand, 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 55: 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:

- einseitig, gegenseitig
- mit oder ohne Aushandlung von Schlüsseln für einen sicheren Kanal
- Authentisierungsart wie z.B. Rollenaauthentisierung 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



### 5.5.1.8 Komm\_Transport

#### 5.5.1.8.1 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 56: Operation `send_Secure`**

| I_TLS_Client   |           |          |                        |       | Berechtigung: FM |
|--|-----------|----------|------------------------|-------|------------------|
| send_Secure  | Parameter |          |                        |       | V, I, A          |
|  | In        | Address  | URI                    | IM304 | M/M/M            |
|  | In        | Identity | Ressourcenidentifizier | IM412 | M/M/M            |
|  | In        | InData   | Binary                 | IM101 | H/H/H            |
|  | Out       | OutData  | Binary                 | IM101 | H/H/H            |
| <p><code>I_TLS_Client</code> ist die Schnittstelle, über die mit der logischen Operation <code>send_Secure</code> eine durch SM-B authentifizierte TLS-Verbindung zu einem fachanwendungsspezifischen Dienst aufgebaut und genutzt werden kann, um beliebige fachliche Nachrichten zu übertragen.</p> <p>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 <code>ID.FD.TLS-S</code>. Diese Identität wird durch die Operation beim Verbindungsaufbau geprüft.</p> |           |          |                        |       |                  |
| Verfügbarkeit: H, Nichtabstreitbarkeit: H  |           |          |                        |       |                  |



### 5.5.1.9 Prüfung\_Zertifikat

#### 5.5.1.9.1 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**

Die Schnittstelle I\_Cert\_Verification MUSS die logische Operation verify\_Certificate implementieren.

**Tabelle 57: Operation verify\_Certificate**

| I_Cert_Verification   |           |                    |                        |       | Berechtigung:<br>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                        |
| <p>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.</p> <p>Neben dem Ergebnis der Zertifikatsprüfung wird als weiterer Rückgabeparameter die im Zertifikat hinterlegte Rolle an das aufrufende System zurück geliefert.</p> <p>HINWEIS: im Offline-Szenario des mobilen Kartenterminals kann eine Prüfung des Revocation-Status durch Online-Abfrage des relevanten OCSP-Responders nicht erfolgen.</p> <p>Die verbindliche Beschreibung der Schritte erfolgt in [gemKPT_PKI_TIP#6.5].</p> <p>Die Beschreibung der Prüfschritte der QES-Zertifikatsprüfung erfolgt in [gemKPT_PKI_TIP#6.6].</p> <p>Der Prüfungsvorgang selbst kann abhängig von den einzelnen Prüfschritten folgende Status haben:</p> <ul style="list-style-type: none"> <li>- Prüfungsvorgang komplett durchgeführt</li> <li>- Prüfungsvorgang durchgeführt mit Einschränkungen (einzelne Prüfschritte konnten nicht durchgeführt werden)</li> <li>- Prüfungsvorgang fehlgeschlagen (kritische Prüfschritte konnten nicht durchgeführt werden)</li> </ul> <p>Als Prüfergebnis („VerificationResult“) eines durchgeführten Prüfungsvorgangs sind möglich:</p> <ul style="list-style-type: none"> <li>- Zertifikat ist gültig</li> <li>- Zertifikat ist gültig mit Einschränkung (Online-Prüfung des Gültigkeitsstatus konnte nicht durchgeführt werden)</li> <li>- Zertifikat ist nicht gültig</li> </ul> <p>Fehlgeschlagene Prüfungsvorgänge können kein Prüfergebnis liefern.</p> <p>Weitere Informationen zu Prüfungsvorgang, Abbruchbedingungen und deren Auswirkungen auf das Prüfergebnis siehe [gemKPT_PKI_TIP#6.7].</p> <p>Die Operation muss selbst entscheiden, welche Art der Prüfung (QES, nonQES) vorgenommen wird.</p> <p>Verfügbarkeit: M, Nichtabstreitbarkeit: NA</p> |           |                    |                        |       |                              |

☒

### 5.5.1.10 Verschlüsselung\_Entschlüsselung

#### 5.5.1.10.1 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 58: Operation encrypt\_Document**

| I_Crypt_Operations  |           |               |                          |       | Berechtigung:<br>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)<br>M/SH/SH (für die Liste) |
|   | Out       | EncryptedData | EncDocumentType          | IM105 | M/SH/SH   |
| <p>Diese Operation verschlüsselt das übergebene Dokument (<i>Data</i>) für alle in der übergebenen Zertifikatliste (<i>Certificates</i>) 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.</p> <p>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.</p> <p>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 (<i>EncryptedData</i>) im unten aufgeführten Format zurück. Das Dokument enthält das symmetrisch verschlüsselte Dokument und alle erzeugten hybriden Schlüssel.</p> <p>Es werden die nachfolgenden Dokumententypen mit dem jeweiligen Verschlüsselungsverfahren unterstützt:</p> <ul style="list-style-type: none"> <li>• Binär, PDF/A und MIME mit CMS</li> <li>• XML (einschließlich der WS-Trust Elemente X.509-Token und SAML-Token) mit XMLEnc</li> </ul> <p>Es werden die folgenden kryptographischen Identitäten unterstützt:</p> <ul style="list-style-type: none"> <li>• eGK: ID.CH.ENC, ID.CH.ENCV für Fachmodule</li> <li>• SMC-B: ID.HCI.ENC für Fachmodule und Clientsysteme</li> <li>• HBA: ID.HP.ENC für Fachmodule und Clientsysteme</li> </ul> <p>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.</p> <p>Zu nutzen sind zeitlich begrenzt auch die HBA-Vorläuferkarten HBA-qSig und ZOD-2.0 mit ihren für die Verschlüsselung vorgesehenen kryptographischen Identitäten.</p> <p>Die Operation unterstützt mindestens Dokumente bis zu einer Größe von 25 MB.</p> <p>Verfügbarkeit: NA, Nichtabstreitbarkeit: NA</p> |           |               |                          |       |   |



#### ⊗ TIP1-A\_2299 Logische Operation I\_Crypt\_Operations::decrypt\_Document

Die Schnittstelle I\_Crypt\_Operations MUSS die logische Operation decrypt\_Document implementieren.

**Tabelle 59: Operation decrypt\_Document**

| I_Crypt_Operations  |           |               |                    |       | Berechtigung:<br>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 ( <i>EncryptedData</i> ) 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.ENC.V für Fachmodule
- SMC-B: ID.HCI.ENC für Fachmodule und Clientsysteme
- HBA: ID.HP.ENC für Fachmodule und Clientsysteme

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



#### 5.5.1.10.2 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 60: 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         |
| <p>Diese Operation verschlüsselt das übergebene Dokument (<i>Data</i>) in binärer Darstellung unter Verwendung eines symmetrischen Schlüsselalgorithmus. Dabei kann der zu verwendende Schlüssel (<i>Key</i>) optional übergeben werden. Wird kein Schlüssel übergeben, so wird ein Schlüssel in ausreichender Qualität erzeugt (<i>NewKey</i>) und mit dem verschlüsselten Dokument (<i>EncryptedData</i>) zusammen zurück geliefert.</p> <p>Die Operation unterstützt mindestens Dokumente bis zu einer Größe von 25 MB.</p> <p>Verfügbarkeit: NA, Nichtabstreitbarkeit: NA</p> |           |               |              |       |                  |



##### ☒ 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 61: 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 ( <i>EncryptedData</i> ) in binärer Darstellung unter Verwendung eines symmetrischen Schlüsselalgorithmus. Der zu verwendende Schlüssel ( <i>Key</i> ) wird übergeben.<br>Die Operation liefert das entschlüsselte Dokument ( <i>Data</i> ) zurück.<br>Die Operation unterstützt mindestens Dokumente bis zu einer Größe von 25 MB.<br>Verfügbarkeit: NA, Nichtabstreitbarkeit: NA |           |               |                 |       |                  |



#### 5.5.1.11 Verzeichnis\_Identitäten

##### 5.5.1.11.1 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 62: 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).<br><br><i>Query</i> : Enthält den Filter für die Suchanfrage.<br><i>Result</i> : Enthält das Ergebnis der Verzeichnisabfrage.<br>Verfügbarkeit: H, Nichtabstreitbarkeit: N |           |        |                      |       |                      |



#### 5.5.1.12 Mobile\_Offline\_Dienste

##### 5.5.1.12.1 I\_MobKT\_Temp\_Storage (Provided)

##### ☒ TIP1-A\_2302 Schnittstelle `I_MobKT_Temp_Storage`

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 63: Operation read\_Data**

| I_MobKT_Temp_Storage   |           |          |          |       | Berechtigung: MFM |
|--|-----------|----------|----------|-------|-------------------|
| read_Data  | Parameter |          |          |       | V, I, A           |
|  | In        | MFM_ID   | MFMTType | 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 64: Operation erase\_Data**

| I_MobKT_Temp_Storage   |           |        |          |       | Berechtigung: MFM |
|--|-----------|--------|----------|-------|-------------------|
| erase_Data   | Parameter |        |          |       | V, I, A           |
|  | In        | MFM_ID | MFMTType | 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 65: Operation write\_Data**

| I_MobKT_Temp_Storage   |           |          |          |       | Berechtigung: MFM |
|--|-----------|----------|----------|-------|-------------------|
| write_Data   | Parameter |          |          |       | V, I, A           |
|  | In        | MFM_ID   | MFMTType | 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  |           |          |          |       |                   |



#### 5.5.1.12.2 I\_MobKT\_FMAccess (Provided)

### ☒ TIP1-A\_2309 Schnittstelle I\_MobKT\_FMAccess



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 66: Operation get\_Data**

| I_MobKT_FMAccess   |           |                  |           |       | Berechtigung: CS |
|--|-----------|------------------|-----------|-------|------------------|
| get_Data   | Parameter |                  |           |       | V, I, A          |
|  | In        | MFM_ID           | MFMTType  | IM421 | M/H/H            |
|  | In        | Data_Description | Data Type | IM101 | M/H/H            |
|  | Out       | Data             | Binary    | IM101 | SH/SH/SH         |
| Diese Operation ermöglicht dem Clientsystems das Lesen von Daten eines mobilen Fachmoduls.<br>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.<br>Die möglichen zulässigen Werte für Data_Description sind daher die Summe der erlaubten Werte, die seitens aller mobilen Fachanwendungen vorgegeben werden.<br>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 67: Operation put\_Data**

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

☒

### 5.5.1.12.3 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 68: Operation get\_Data

| 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 69: 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  |           |                  |          |       |                   |



#### 5.5.1.12.4 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 70: Operation show\_Data

| I_MobKT_GUI  |           |        |        |       | Berechtigung: MFM |
|--|-----------|--------|--------|-------|-------------------|
| show_Data  | Parameter |        |        |       | V, I, A           |
|  | In        | MFM_ID | MFMTyp | 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 71: Operation type\_Data**

| I_MobKT_GUI  |           |        |        |       | Berechtigung: MFM |
|--|-----------|--------|--------|-------|-------------------|
| type_Data  | Parameter |        |        |       | V, I, A           |
|  | In        | MFM_ID | MFMTyp | 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.<br>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  |           |        |        |       |                   |



#### 5.5.1.12.5 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 72: 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.<br>Ob das MobKT die Druckdaten sequenziell bearbeitet oder einen Druckerspooler bereitstellt ist herstellerspezifisch.<br>Sollte kein Drucker angeschlossen sein, meldet die Operation einen Fehler. |           |           |      |       |                   |
| Verfügbarkeit: NA, Nichtabstreitbarkeit: NA  |           |           |      |       |                   |



#### 5.5.1.12.6 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 73: 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. |           |         |                   |       |                 |
| 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 74: 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 75: 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.<br>Die Operation liefert eine per DNSSEC validierte Antwort. |           |         |           |       |                  |
| Verfügbarkeit: H, Nichtabstreitbarkeit: NA  |           |         |           |       |                  |



#### 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 76: 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.<br>Die Namensräume TI, angeschlossene Bestandsnetze und Internet müssen auflösbar sein. Die Namensräume angeschlossene Bestandsnetze und Internet werden nur aufgelöst, wenn die zuständigen DNS-Server bekannt sind.<br>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 77: 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

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 78: 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\_Change\_System\_Time MUSS die logische Operation set\_System\_Time implementieren.

Tabelle 79: 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 80: Operation extract\_card\_data

| I_KV_Card_Operations  |           |       |                    |       | Berechtigung: FM |
|---|-----------|-------|--------------------|-------|------------------|
| 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 ( <i>Data</i> ) zu einem ausgewählten Zertifikat der bestimmten Karte ( <i>CuRef</i> ). Welches Zertifikat für eine bestimmte Art von Karten genutzt wird, wird durch die TI-Plattform festgelegt.<br>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 81: 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 Smartcard, die durch die CardUsageReference ( <i>CuRef</i> ) 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 82: Operation read\_KVK

| I_KV_Card_Operations |           | Berechtigung: FM, MFM |
|----------------------|-----------|-----------------------|
| read_KVK             | Parameter | V, I, A               |



|   |     |       |                       |       |          |
|---|-----|-------|-----------------------|-------|----------|
|   | In  | ResID | Ressourceldentifizier | 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 83: Operation write\_Card\_Data**

| I_KV_Card_Operations   |           |                 |                    |       | Berechtigung:<br>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 Smartcard, die durch die CardUsageReference (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\_2341 Logische Operation I\_KV\_Card\_Operations::verify\_eGK

Die Schnittstelle I\_KV\_Card\_Operations MUSS die logische Operation verify\_eGK implementieren.

**Tabelle 84: Operation verify\_eGK**

| I_KV_Card_Operations  |           |                    |                        |       | Berechtigung:<br>FM, MFM |
|---|-----------|--------------------|------------------------|-------|--------------------------|
| verify_eGK  | Parameter |                    |                        |       | V, I, A                  |
|   | In        | ResID              | Ressourceldentifizier  | IM412 | M/H/H                    |
|   | Out       | VerificationResult | VerificationResultType | IM420 | M/H/H                    |
| Die Operation verify_eGK prüft, ob die über ResID identifizierte Karte in technischer Hinsicht gültig ist.  |           |                    |                        |       |                          |
| Die eGK ist gültig, wenn: <ul style="list-style-type: none"> <li>• der HCA-Container der eGK aktiv (nicht gesperrt) ist</li> <li>• das AUT-Zertifikat der eGK gültig ist. Dabei wird das AUT-Zertifikat durch die Operation verify_Certificate des Interfaces I_Cert_Verification geprüft.</li> </ul> |           |                    |                        |       |                          |
| 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 85: Operation write\_eGK\_Protocol**

| I_KV_Card_Operations |           |       |                    |       | Berechtigung:<br>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 benötigte Sicherheitszustand hergestellt wurde. |    |                     |                     |       |          |
| Verfügbarkeit: M, Nichtabstreitbarkeit: H   |    |                     |                     |       |          |



### ☒ 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 86: 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).<br>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 87: 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 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\_2345 Logische Operation I\_KV\_Card\_Operations::send\_APDU

Die Schnittstelle I\_KV\_Card\_Operations MUSS die logische Operation send\_APDU implementieren.

**Tabelle 88: 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.<br>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 89: 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.<br>Das Reset unterbricht ein eventuell mit dieser Karte laufendes C2C. |           |       |                    |       |                  |
| Verfügbarkeit: NA, Nichtabstreitbarkeit: NA  |           |       |                    |       |                  |



### 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 90: Operation configure\_KTs**

| I_KTV_Management  |           |          |                     |       | Berechtigung: A |
|---|-----------|----------|---------------------|-------|-----------------|
| configure_KTs   | Parameter |          |                     |       | V, I, A         |
|   | In        | Data     | ConfigurationData   | IM201 | M/M/M           |
|   | In        | KT_Ident | Ressourceldentifier | IM412 | M/M/M           |
| Die Operation configure_KTs ermöglicht einem Administrator die Verwaltung der Kartenterminals im Netz. Dazu gehört: <ul style="list-style-type: none"> <li>• Hinzufügen und Entfernen von Kartenterminals,</li> <li>• Durchführen des Pairings</li> <li>• Aktivieren / Deaktivieren von Kartenterminals</li> </ul> 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 91: 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

Die Schnittstelle I\_KT\_Communication MUSS die logische Operation transfer\_APDU implementieren.

Tabelle 92: 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  |           |        |              |       |                   |



## 5.5.3 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 93: 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                |
| <p>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.</p> <p>Es erfolgt eine Kontrolle und Filterung des Datenverkehrs über einen konfigurierbaren Paketfilter mit Stateful Inspection.</p> <p>Aufgrund der Nutzung von IPv4 erfolgt eine IP-Adressumsetzung (NAT).</p> <p>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).</p> |           |         |           |       |                      |
| 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.

**Tabelle 94: 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         |
| <p>Diese Operation ermöglicht das Senden und Empfangen von IP-Paketen zur Nutzung der Bestandsnetzanbindung, 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</p> <ul style="list-style-type: none"> <li>• den Internetverkehr verwirft, wenn kein sicherer Internetzugang konfiguriert ist oder</li> <li>• dem Client mitteilt, über welches Gateway er diesen Verkehr versenden kann, wenn ein solches Gateway verfügbar ist.</li> </ul> <p>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).</p> |           |         |           |       |                  |
| 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 95: 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 <ul style="list-style-type: none"> <li>über eine vertrauliche Server-authentisierte Verbindung (server-authenticated)</li> <li>über eine vertrauliche beidseitig authentifizierte Verbindung (mutual-authenticated)</li> <li>über eine nicht gesicherte Verbindung (unsecured)</li> </ul> auf die Schnittstellen des Produkttyps zugreifen dürfen.<br>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.<br>Bei einer Vertraulichen Verbindung authentisiert sich die TI-Plattform mit der Identität ID.AK.AUT.<br>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.

**Tabelle 96: Operation add\_Clientsystem**

| I_Facade_Access_Configuration   |           |    |                          |       | Berechtigung: A |
|---|-----------|----|--------------------------|-------|-----------------|
| add_Clientsystem  | Parameter |    |                          |       | V, I, A         |
|   | In        | CS | ClientsystemIdentifizier | 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 Identifizier 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.<br>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 97: Operation remove\_Clientsystem**

| I_Facade_Access_Configuration   |           |    |                          |       | Berechtigung: A |
|---|-----------|----|--------------------------|-------|-----------------|
| remove_Clientsystem   | Parameter |    |                          |       | V, I, A         |
|   | In        | CS | ClientsystemIdentifizier | 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).<br>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 98: 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)<br>M/H/H (für die Liste) |
| Die Operation listet die auf einem KSR-Server verfügbaren Updates (AvailableUpdates) für eine dezentrale Komponente der TI-Plattform (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 99: 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 (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 100: 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. ☒

##### ☒ TIP1-A\_5077 Logische Operation I\_Registration\_Service::register

Die Schnittstelle I\_Registration\_Service MUSS die logische Operation register implementieren.

**Tabelle 101: Operation register**

| I_Registration_Service  |           |                |                  |       | Berechtigung: TIP |
|---|-----------|----------------|------------------|-------|-------------------|
| 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 ( <i>KonCertificate</i> ) und eine vom VPN-Zugangsdienst bereitgestellte eindeutige Vertrags-ID ( <i>ContractID</i> ) 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 ( <i>RegStatus</i> ) und der Vertragstatus ( <i>ContractStatus</i> ) übermittelt. Es besteht auch die Möglichkeit weitere Informationen ( <i>AdditionalInfo</i> ) 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 102: Operation deregister**

| I_Registration_Service  |           |                |                  |       | Berechtigung: TIP |
|---|-----------|----------------|------------------|-------|-------------------|
| 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             |
| <p>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.</p> <p>Der Konnektor übermittelt das Zertifikat der Identität ID.NK.VPN (<i>KonCertificate</i>) und eine vom VPN-Zugangsdienst bereitgestellte eindeutige Vertrags-ID (<i>ContractID</i>) 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.</p> <p>Als Ergebnis der Operation werden der neue Registrierungsstatus (<i>RegStatus</i>) und der Vertragstatus (<i>ContractStatus</i>) übermittelt. Es besteht auch die Möglichkeit weitere Informationen (<i>AdditionalInfo</i>) in Textform zu übermitteln.</p> <p>Verfügbarkeit: H, Nichtabstreitbarkeit: NA</p> |           |                |                  |       |                   |



### ☒ TIP1-A\_5079 Logische Operation I\_Registration\_Service::get\_Status

Die Schnittstelle I\_Registration\_Service MUSS die logische Operation get\_Status implementieren.

**Tabelle 103: Operation get\_Status**

| I_Registration_Service   |           |                |                  |       | Berechtigung: TIP |
|--|-----------|----------------|------------------|-------|-------------------|
| 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             |
| <p>Die Operation ermöglicht die aktuellen Registrierungsinformationen eines Konnektors beim VPN-Zugangsdienst abzufragen.</p> <p>Der Konnektor übermittelt das Zertifikat der Identität ID.NK.VPN (<i>KonCertificate</i>) 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 (<i>RegStatus</i>) und der Vertragstatus (<i>ContractStatus</i>) übermittelt. Es besteht auch die Möglichkeit weitere Informationen (<i>AdditionalInfo</i>) in Textform zu übermitteln.</p> <p>Verfügbarkeit: KS, Nichtabstreitbarkeit: NA</p> |           |                |                  |       |                   |



## 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 104: Operation search\_Directory**

| I_Directory_Query   |           |        |                      |       | Berechtigung:<br>FAD, TIP |
|---|-----------|--------|----------------------|-------|---------------------------|
| 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). |           |        |                      |       |                           |
| <i>Query:</i> Enthält den Filter für die Suchanfrage.   |           |        |                      |       |                           |
| <i>Result:</i> Enthält das Ergebnis der Verzeichnisabfrage.   |           |        |                      |       |                           |
| Verfügbarkeit: H, Nichtabstreitbarkeit: N   |           |        |                      |       |                           |

☒

#### 5.6.1.4.2 I\_Directory\_Maintenance (Provided)

☒ **TIP1-A\_5806 Die Schnittstelle I\_Directory\_Maintenance**

Die Schnittstelle I\_Directory\_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\_Maintenance::add\_Directory\_Entry**

Die Schnittstelle I\_Directory\_Maintenance MUSS die logische Operation add\_Directory\_Entry implementieren.

**Tabelle 105: Operation add\_Directory\_Entry**

| I_Directory_Maintenance  |           |                          |                       |       | Berechtigung:<br>FAD |
|--|-----------|--------------------------|-----------------------|-------|----------------------|
| add_Directory_Entry  | Parameter |                          |                       |       | Vertr./Integr./Auth. |
|  | In        | Variant                  | DirectoryEntryVariant | IM114 | M/H/H                |
|  | In        | EncCertificate           | CertificateX.509      | IM404 | M/M/M                |
|  | In        | Attributes<br>(optional) | DirectoryAttributes   | IM115 | M/H/H                |
| Mit dieser Operation kann ein Verzeichniseintrag mit der im ENC-Zertifikat ( <i>EncCertifikat</i> ) enthaltenen Telematik_ID erzeugt oder erweitert werden.  |           |                          |                       |       |                      |
| <u>Variant = "full"</u><br>Eingangsparemeter: <i>Variant</i> ="full"<br>Das ENC-Zertifikat wird im Verzeichniseintrag gespeichert. Außerdem werden <ul style="list-style-type: none"> <li>• Telematik-ID und</li> <li>• Namensinformationen</li> </ul> aus dem Zertifikat im Verzeichniseintrag gespeichert. |           |                          |                       |       |                      |
| <u>Variant="minimal"</u><br>Eingangsparemeter: <i>Variant</i> ="minimal"<br>Das ENC-Zertifikat wird im Verzeichniseintrag gespeichert. Außerdem wird die <ul style="list-style-type: none"> <li>• Telematik-ID</li> </ul>  |           |                          |                       |       |                      |

aus dem Zertifikat im Verzeichniseintrag gespeichert.

Das *EncCertifikat* wird im Verzeichniseintrag hinterlegt.

Die zusätzlichen Attribute (*Attributes*) werden entsprechend ihren Werten mit einem neuen Wert überschrieben, gelöscht oder bleiben unverändert.

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\_Maintenance::read\_Directory\_Entry

Die Schnittstelle I\_Directory\_Maintenance MUSS die logische Operation read\_Directory\_Entry implementieren.

**Tabelle 106: Operation read\_Directory\_Entry**

| I_Directory_Maintenance  |           |             |                |       | Berechtigung:<br>FAD |
|--|-----------|-------------|----------------|-------|----------------------|
| read_Directory_Entry   | Parameter |             |                |       | Vertr./Integr./Auth. |
|  | In        | TelematikID | Telematik_ID   | IM424 | M/H/H                |
|  | Out       | Entry       | DirectoryEntry | IM116 | M/H/H                |
| Mit dieser Operation kann der vollständige Verzeichniseintrag ( <i>Entry</i> ) bestehend aus Telematik-ID, Basisdaten und FA-Daten mit der Telematik-ID ( <i>TelematikID</i> ) gelesen werden. |           |             |                |       |                      |
| Verfügbarkeit: M, Nichtabstreitbarkeit: N  |           |             |                |       |                      |



### ☒ TIP1-A\_5809 Die Schnittstelle I\_Directory\_Maintenance::modify\_Directory\_Entry

Die Schnittstelle I\_Directory\_Maintenance MUSS die logische Operation modify\_Directory\_Entry implementieren.

**Tabelle 107: Operation modify\_Directory\_Entry**

| I_Directory_Maintenance  |           |                |                       |       | Berechtigung:<br>FAD |
|--|-----------|----------------|-----------------------|-------|----------------------|
| modify_Directory_Entry   | Parameter |                |                       |       | Vertr./Integr./Auth. |
|  | In        | Variant        | DirectoryEntryVariant | IM114 | M/H/H                |
|  | In        | EncCertificate | CertificateX.509      | IM404 | M/M/M                |
|  | In        | Attributes     | DirectoryAttributes   | IM115 | M/H/H                |
| Mit dieser Operation können die optionalen Attribute der Basisdaten des Verzeichniseintrags mit der im ENC-Zertifikat enthaltenen Telematik_ID modifiziert werden.   |           |                |                       |       |                      |
| <u>Variant = "full"</u><br>Eingangsparameter: Variant="full"<br>Das ENC-Zertifikat wird zu den im Verzeichnisdienst gespeicherten Zertifikaten hinzugefügt, sofern sie dort noch nicht enthalten sind. Außerdem werden Namensinformationen aus dem Zertifikat im Verzeichniseintrag gespeichert. |           |                |                       |       |                      |
| <u>Variant="minimal"</u><br>Eingangsparameter: Variant="minimal"<br>Das ENC-Zertifikat wird zu den im Verzeichnisdienst gespeicherten Zertifikaten hinzugefügt, sofern es dort noch nicht enthalten ist.<br>Eventuell im Verzeichniseintrag vorhandene Namensinformationen werden gelöscht.      |           |                |                       |       |                      |
| Das <i>EncCertifikat</i> wird im Verzeichniseintrag hinterlegt.  |           |                |                       |       |                      |
| Für die Attribute ( <i>Attributes</i> ) 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\_Maintenance::delete\_Directory\_Entry**

Die Schnittstelle I\_Directory\_Maintenance MUSS die logische Operation delete\_Directory\_Entry implementieren.


**Tabelle 108: Operation delete\_Directory\_Entry**

|   |           |             |              |       |                      |
|---|-----------|-------------|--------------|-------|----------------------|
| I_Directory_Maintenance   |           |             |              |       | Berechtigung:<br>FAD |
| delete_Directory_Entry  | Parameter |             |              |       | Vertr./Integr./Auth. |
|   | In        | TelematikID | Telematik_ID | IM424 | M/H/H                |
| Mit dieser Operation kann der Verzeichniseintrag mit der Telematik-ID ( <i>TelematikID</i> ) gelöscht werden. |           |             |              |       |                      |
| Verfügbarkeit: H, Nichtabstreitbarkeit: H   |           |             |              |       |                      |



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 109: Operation add\_Directory\_FA-Attributes**

|   |           |               |                     |       |                      |
|---|-----------|---------------|---------------------|-------|----------------------|
| I_Directory_Application_Maintenance   |           |               |                     |       | Berechtigung:<br>FAD |
| 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 ( <i>TelematikID</i> ) fachanwendungsspezifische Attribute ( <i>FA-Attributes</i> ) hinzugefügt werden.<br>Hinzugefügt werden können die Attribute welche zu der Fachanwendung des aufrufenden Dienstes gehören.<br>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.<br>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 110: Operation delete\_Directory\_FA-Attributes

| I_Directory_Application_Maintenance  |           |             |              |       | Berechtigung:<br>FAD |
|--|-----------|-------------|--------------|-------|----------------------|
| delete_Directory_FA-Attributes   | Parameter |             |              |       | Vertr./Integr./Auth. |
|  | In        | TelematikID | Telematik_ID | IM424 | M/M/M                |
| <p>Mit dieser Operation werden alle fachanwendungsspezifischen Attribute - welche zu der Fachanwendung des aufrufenden Dienstes gehören - des Verzeichniseintrags mit der (<i>TelematikID</i>) gelöscht.</p> <p>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.</p> <p>Die Operation erlaubt nur die Verarbeitung der fachanwendungsspezifischen Daten des im TLS Verbindungsaufbaus identifizierten fachanwendungsspezifischen Fachdienstes.</p> <p>Verfügbarkeit: NA, Nichtabstreitbarkeit: H</p> |           |             |              |       |                      |



### **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 111: Operation modify\_Directory\_FA-Attributes

| I_Directory_Application_Maintenance   |           |               |                     |       | Berechtigung:<br>FAD |
|---|-----------|---------------|---------------------|-------|----------------------|
| modify_Directory_FA-Attributes  | Parameter |               |                     |       | Vertr./Integr./Auth. |
|   | In        | TelematikID   | Telematik_ID        | IM424 | M/M/M                |
|   | In        | FA-Attributes | DirectoryAttributes | IM115 | M/H/H                |
| <p>Mit dieser Operation können fachanwendungsspezifische Attribute (<i>FA-Attributes</i>) von einem Verzeichniseintrag mit der (<i>TelematikID</i>) modifiziert werden.</p> <p>Modifiziert werden können die Attribute welche zu der Fachanwendung des aufrufenden Dienstes gehören.</p> <p>Für die Attribute gibt es die Update-Optionen: Neuen Wert setzen, bestehenden Wert löschen, keine Änderung vornehmen.</p> <p>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.</p> <p>Die Operation erlaubt nur die Verarbeitung der fachanwendungsspezifischen Daten des im TLS Verbindungsaufbaus identifizierten fachanwendungsspezifischen Fachdienstes.</p> <p>Verfügbarkeit: NA, Nichtabstreitbarkeit: H</p> |           |               |                     |       |                      |



## 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 112: Operation get\_Service\_Location

| I_DNS_Service_Localization  |           |                  |         |       | Berechtigung: FAD |
|---|-----------|------------------|---------|-------|-------------------|
| 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 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)

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 113: Operation get\_IP\_Address

| I_DNS_Name_Resolution   |           |                  |           |       | Berechtigung: FAD, TIP |
|---|-----------|------------------|-----------|-------|------------------------|
| 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 114: Operation get\_FQDN

| I_DNS_Name_Resolution |           |                  |           |       | Berechtigung: FAD, TIP |
|-----------------------|-----------|------------------|-----------|-------|------------------------|
| 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

Die Schnittstelle I\_OCSP\_Status\_Information MUSS die logische Operation check\_Revocation\_Status implementieren.

**Tabelle 115: Operation check\_Revocation\_Status**

|  |           |                    |                        |       |                              |
|--|-----------|--------------------|------------------------|-------|------------------------------|
| I_OCSP_Status_Information  |           |                    |                        |       | Berechtigung:<br>FAD,<br>TIP |
| 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 <ul style="list-style-type: none"> <li>für alle X.509-Zertifikate (außer denen für eGK) gemäß [Common-PKI] unter obligatorischer Verwendung der CertHash-Erweiterung (Positive Statement),</li> <li>für alle X.509-Zertifikate der eGK gemäß [RFC2560].</li> </ul> |           |                    |                        |       |                              |
| 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 116: Operation download\_TSL**

|                |                    |
|----------------|--------------------|
| I_TSL_Download | Berechtigung: FAD, |
|----------------|--------------------|

|  |           |      |     |       |         |
|--|-----------|------|-----|-------|---------|
|  |           |      |     |       | TIP     |
| download_TSL   | Parameter |      |     |       | V, I, A |
|  | Out       | Data | XML | IM419 | N/M/M   |
| Die Operation lädt die TSL von einem TSL-Download-Punkt.<br>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 117: Operation download\_VL**

|   |           |                 |     |       |                   |
|---|-----------|-----------------|-----|-------|-------------------|
| I_BNetZA_VL_Download  |           |                 |     |       | Berechtigung: TIP |
| download_VL   | Parameter |                 |     |       | V, I, A           |
|   | Out       | Vertrauensliste | 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 118: 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 Vertrauensliste 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 119: Operation provide\_Certificate**

|   |           |                    |                  |       |   |
|---|-----------|--------------------|------------------|-------|---|
| I_Cert_Provisioning   |           |                    |                  |       | Berechtigung:<br>Hersteller,<br>Betreiber_ZD,<br>Betreiber_FD |
| 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. ☒

##### ☒ TIP1-A\_2377 Logische Operation I\_Cert\_Revocation::revoke\_Certificate

Die Schnittstelle I\_Cert\_Revocation MUSS die logische Operation revoke\_Certificate implementieren.

**Tabelle 120: Operation revoke\_Certificate**

|  |           |         |                      |       |   |
|--|-----------|---------|----------------------|-------|---|
| I_Cert_Revocation  |           |         |                      |       | Berechtigung:<br>Hersteller,<br>Betreiber_ZD,<br>Betreiber_FD |
| 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 121: 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.

**Tabelle 122: Operation sync\_Time**

| I_NTP_Time_Information   |           |                 |      |       | Berechtigung: FAD, TIP |
|--|-----------|-----------------|------|-------|------------------------|
| 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 123: Operation update\_Information**

| I_Monitoring_Update  |           |        |                       |       | Berechtigung: FAD, TIP |
|--|-----------|--------|-----------------------|-------|------------------------|
| update_Information   | Parameter |        |                       |       | V, I, A                |
|  | In        | status | MonitoringInformation | IM424 | M/M/M                  |
| Über diese Schnittstelle können Betreiber von fachanwendungsspezifischen Diensten und den zentralen Diensten der TI-Plattform die für die Dienstleistung 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 124: Operation update\_Information**

|   |           |        |                       |       |  |
|---|-----------|--------|-----------------------|-------|--|
| I_Monitoring_Read   |           |        |                       |       | Berechtigung:<br>Betreiber_ZD,<br>Betreiber_FD |
| 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 und den zentralen Diensten der TI-Plattform abfragen. |           |        |                       |       |  |
| Verfügbarkeit: M, Nichtabstreitbarkeit: N   |           |        |                       |       |  |



#### 5.6.2.6 Konfiguration von Bestandsnetzen

##### 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 125: Operation get\_Ext\_Net\_Config**

|  |           |           |                   |       |                      |
|--|-----------|-----------|-------------------|-------|----------------------|
| I_KSRS_Net_Config  |           |           |                   |       | Berechtigung:<br>TIP |
| get_Ext_Net_Config   | Parameter |           |                   |       | V, I, A              |
|  | Out       | netConfig | ConfigurationData | IM201 | M/H/H                |
| Diese Operation ermöglicht den Download einer Konfigurationsdatei ( <i>netConfig</i> ), in welcher alle durch den Konnektor benötigten Konfigurationsparameter der angeschlossenen Bestandsnetze 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 126: Operation send\_Data**

| I_IP_Transport  |           |         |           |       | Berechtigung: FAD, TIP |
|---|-----------|---------|-----------|-------|------------------------|
| 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 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 127: 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 128: 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   |           |      |        |       |                   |

☒

## 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 129: 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 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 130: Schnittstelle P\_Cert\_Provisioning**

|  |  |
|--|--|
| P_Cert_Provisioning  | Berechtigung: LE,<br>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

Die organisatorische Schnittstelle P\_Cert\_Revocation MUSS alle zugehörigen Festlegungen erfüllen.

**Tabelle 131: Schnittstelle P\_Cert\_Revocation**

|   |  |
|---|--|
| P_Cert_Revocation   | Berechtigung: LE,<br>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 132: 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 133: 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 134: 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   |                 |



#### 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 135: 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 136: Schnittstelle P\_DNS\_Name\_Entry\_Announcement**

| P_DNS_Name_Entry_Announcement  | Berechtigung: FAD, TIP |
|--|------------------------|
| 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 137: Schnittstelle P\_DNS\_Zone\_Delegation**

| P_DNS_Zone_Delegation  | Berechtigung: FAD, TIP |
|--|------------------------|
| 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 138: Schnittstelle P\_DNSSEC\_Key\_Distribution**

| P_DNSSEC_Key_Distribution  | Berechtigung: FAD, TIP |
|--|------------------------|
| 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 139: Schnittstelle P\_DNS\_Service\_Entry\_Announcement**

| P_DNS_Service_Entry_Announcement   | Berechtigung: FAD |
|--|-------------------|
| 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 140: 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\_Maintenance (Provided)

#### ☒ TIP1-A\_5818 Organisatorische Schnittstelle P\_Directory\_Maintenance

Die organisatorische Schnittstelle P\_Directory\_Maintenance MUSS alle zugehörigen Festlegungen erfüllen.

**Tabelle 141: Schnittstelle P\_Directory\_Maintenance**

| P_Directory_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. |                  |
| 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 142: Schnittstelle P\_Directory\_Application\_Registration**

| P_Directory_Application_Registration   | Berechtigung: FAD |
|--|-------------------|
| Diese Prozessschnittstelle ermöglicht <ul style="list-style-type: none"> <li>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 <ul style="list-style-type: none"> <li>TLS-Client-Identität seines Fachdienstes (ID.FD.TLS-C),</li> <li>Name der Fachanwendung</li> <li>Name/Identität des Fachdienstes</li> </ul> </li> <li>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.</li> </ul> |                   |
| 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 143: Schnittstelle P\_Directory\_Administration\_Registration**

| P_Directory_Administration_Registration   | Berechtigung: FAD |
|---|-------------------|
| <p>Diese Prozessschnittstelle ermöglicht</p> <ul style="list-style-type: none"> <li>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 <ul style="list-style-type: none"> <li>TLS-Client-Identität seines Fachdienstes (ID.FD.TLS-C),</li> <li>Telematik-ID des Verzeichniseintrags, für den er sich registriert</li> <li>Nachweis der Berechtigung zur Datenadministration durch den Betroffenen (Inhaber des HBA oder der SMC-B)</li> <li>Name/Identität des Fachdienstes</li> </ul> </li> <li>FA-Anbieter können sich beim Verzeichnisdienst deregistrieren. Der Zugang über die Schnittstelle I_Directory_Maintenance ist danach für den betroffenen Verzeichniseintrag nicht mehr möglich.</li> </ul> |                   |
| Verfügbarkeit: N, Nichtabstreitbarkeit: H   |                   |



## 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.

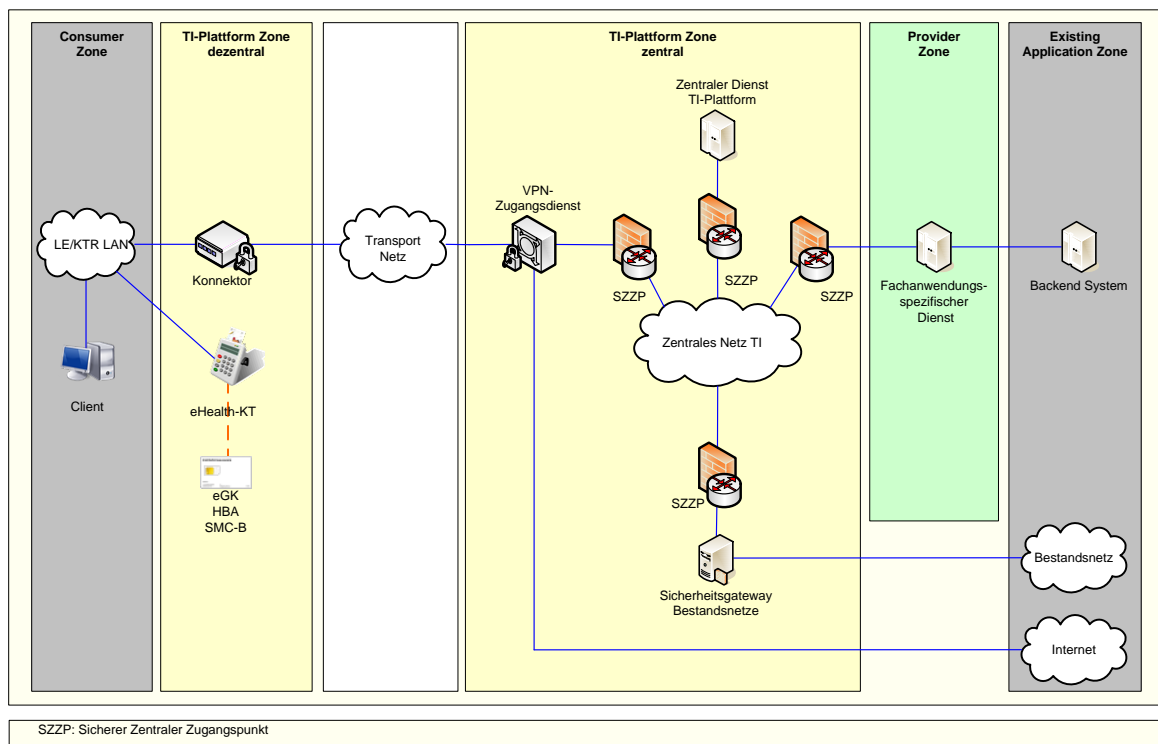
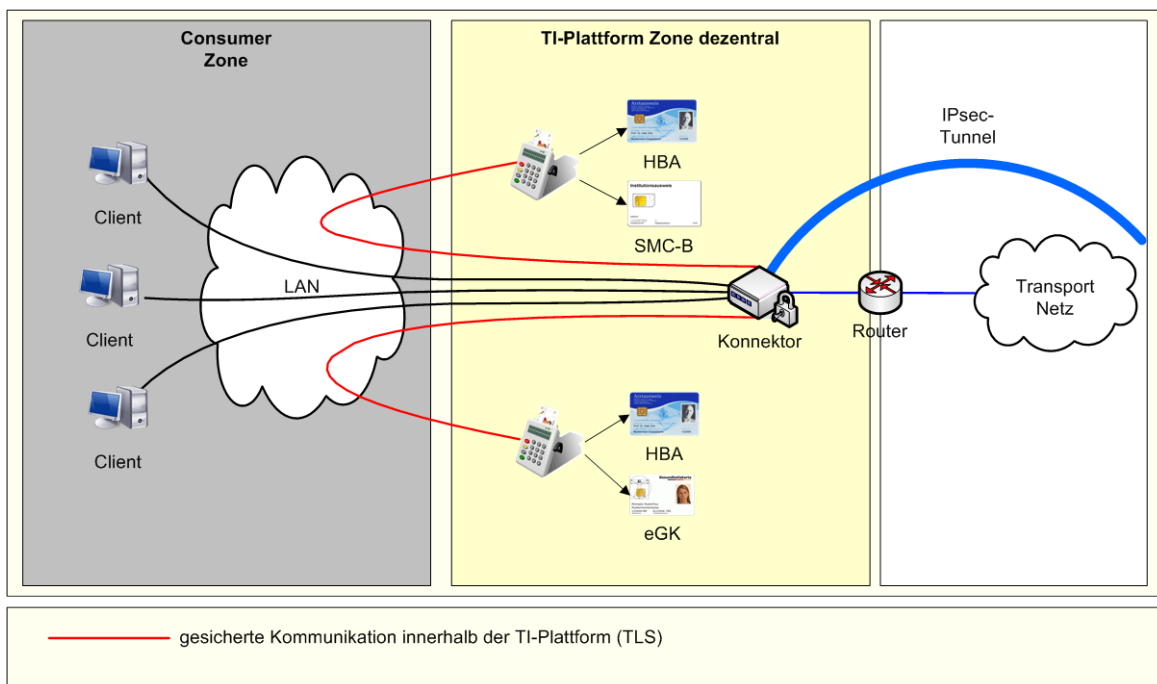


Abbildung 10: Netzwerktopologie der TI

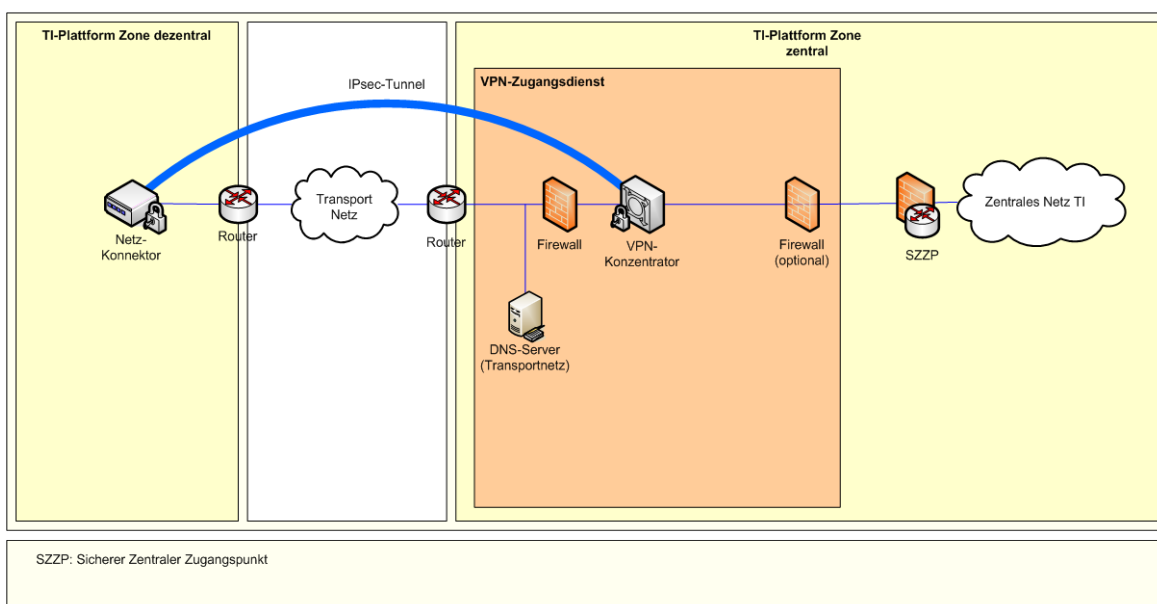
Die Abbildung 10 zeigt eine schematische Übersicht zur Netzwerktopologie der TI, die sich an den in der Gesamtarchitektur definierten Zonen orientiert. Die Kardinalitäten der Produkttypen wird hier nicht dargestellt.



**Abbildung 11: Netzwerkverbindungen dezentral**

In Abbildung 11 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, Kostenträgerschaft, Leistungserbringerorganisation usw.) zu erfassen.

### 6.1.1 Zugangsnetz



**Abbildung 12: Netztopologie Zugangsnetz**

In der Abbildung 12 ist exemplarisch der Aufbau des Zugangsnetzes dargestellt. Die Funktionalität wird im Wesentlichen vom Konnektor im dezentralen Bereich und dem



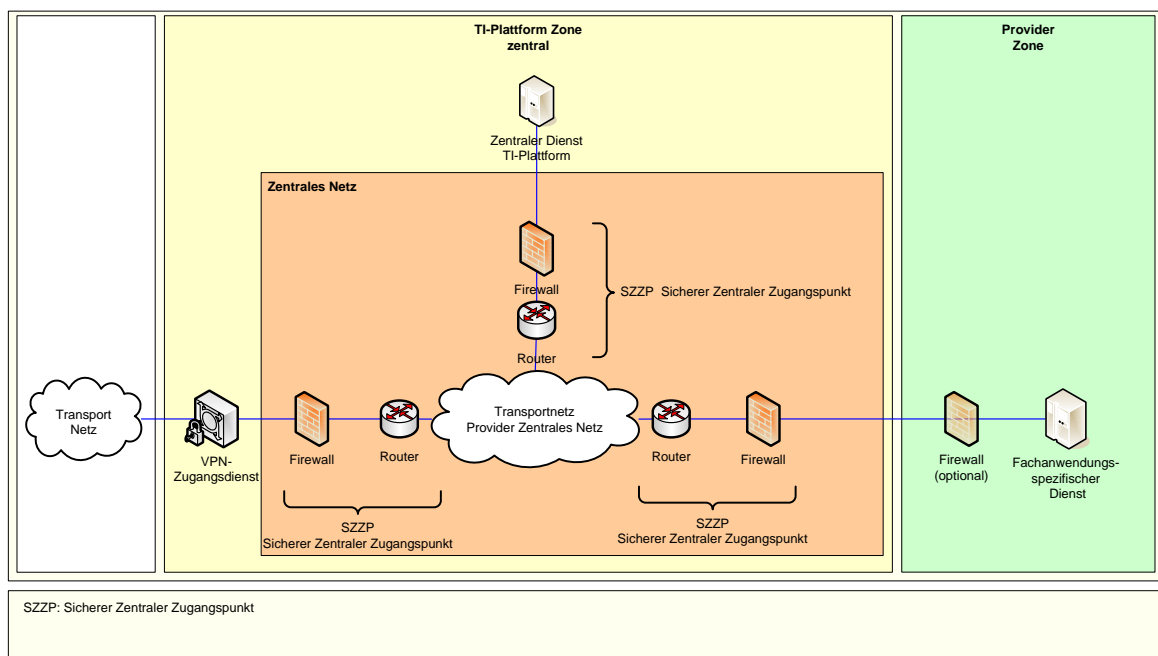
VPN-Konzentrator auf zentraler Seite bereitgestellt. Der IPsec-Tunnel zwischen diesen Komponenten wird über ein beliebiges IP-fähiges Transportnetz aufgebaut. Als Transportnetz kann das Internet verwendet werden. Ein vorhandener Internetanschluss bei Leistungserbringern kann nachgenutzt werden. Das unsichere 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 zu erreichen, den IPsec-Tunnel zu einem VPN-Konzentrator des VPN-Zugangsdienstes mit der Identität ID.VPNK.VPN verwenden. ☒

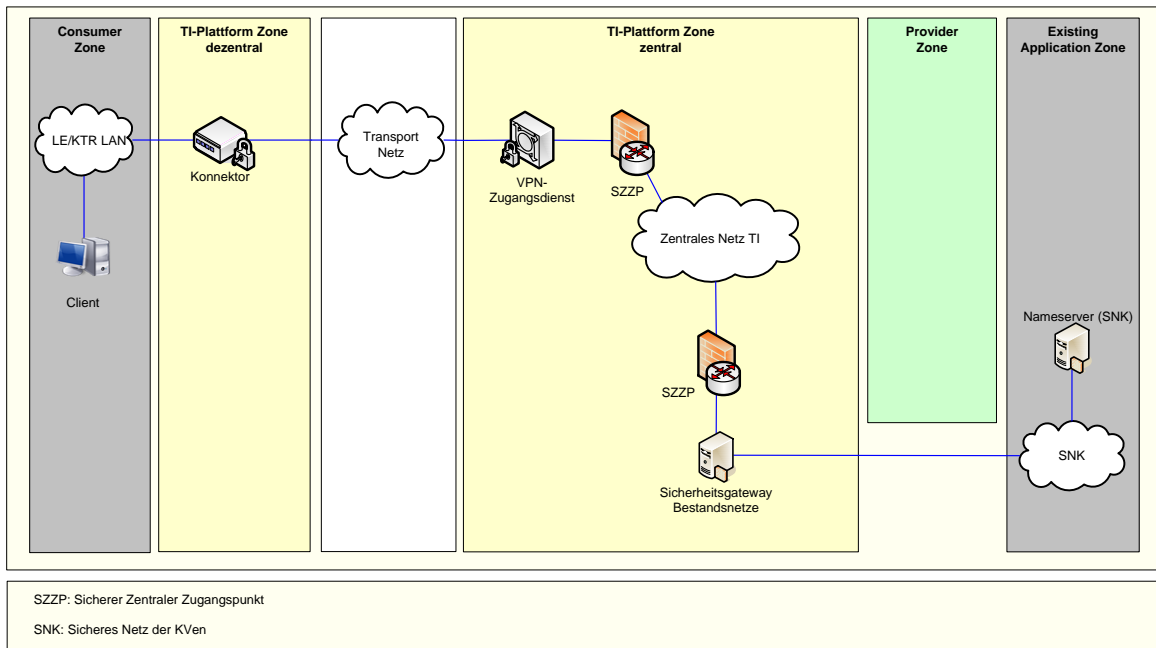
### 6.1.2 Zentrales Netz



**Abbildung 13: Netztopologie Zentrales Netz**

Die Abbildung 13 zeigt die wesentlichen Bestandteile des zentralen Netzes der TI. Die fachdienstspezifischen Dienste, der VPN-Zugangsdienst 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 14: Netztopologie Sicherheitsgateway Bestandsnetze**

In der Abbildung 14 ist der Zugang zu Bestandsnetzen 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.

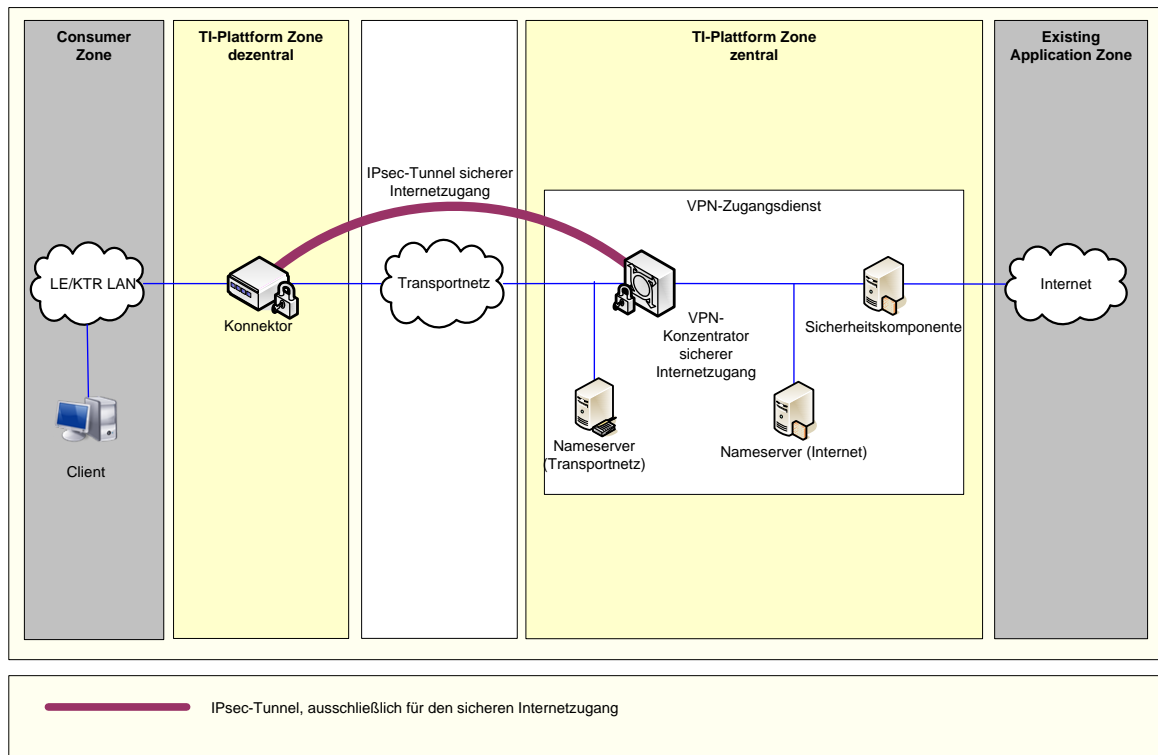
Es findet kein Zonentransfer oder Zone-Delegation zwischen Nameservern der TI und des SNK statt.

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**

Der Produkttyp Konnektor MUSS, um die Dienste angeschlossener Bestandsnetze 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 15: Netztopologie Sicherer Internetzugang**

In der Abbildung 15 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 Interzugang 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).

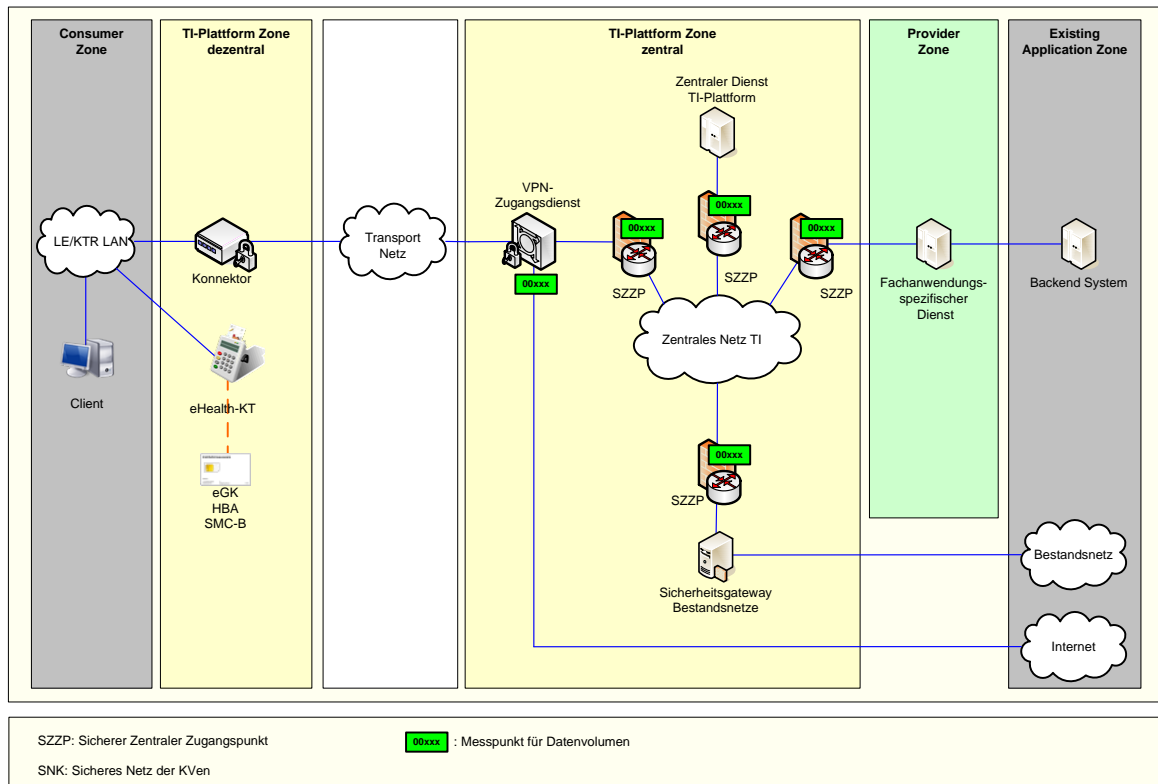
Der TI-Konnektor leitet Anfragen aus dem LAN des Nutzers in Richtung Internet an die bereits vorhandene Infrastruktur (ISP-Router, Firewall, lokaler Router) weiter, die den Weitertransport über den vorhandenen Internetanschluss sicherstellen.

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 Interzuges 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.

## 6.1.6 Volumenerfassung im Netzwerk der TI-Plattform



**Abbildung 16: 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 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 bereit-

gestellt 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 unvermeidbar 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 unterstützen (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<sup>8</sup> 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 Kostenträrgeschäftsstellen:**

Leistungserbringer und Kostenträrgeschäftsstellen 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. ☒

---

<sup>8</sup> 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.

☒ **TIP1-A\_2403 Produkttyp eHealth-Kartenterminal, IPv4 und IPv6 Dual-Stack-Modus**

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 144: Festlegungen zu Adressräumen**

| Einsatzbereich   | Adressraum IPv4  | Adressraum IPv6  |
|--|--|--|
| LE- und KTR-GS-Umgebung  | keine Vorgabe  | IPv6-Prefix der TI<br>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              | IPv6-Prefix der TI   |



| Einsatzbereich | Adressraum IPv4   | Adressraum IPv6  |
|----------------|---|--|
|                | TI-Plattform  |  |
| Bestandsnetze  | Öffentliche IPv4-Adressen, bereitgestellt durch die Bestandsnetze | bereitgestellt durch die Bestandsnetze, zur Zeit nicht genutzt |



#### ☒ 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 145: Festlegungen zu Namensräumen**

| Einsatzbereich                          | Namensraum     |
|---|----------------|
| LE- und KTR-GS-Umgebung                 | keine Vorgaben |
| Dezentrale Komponenten der TI-Plattform | keine Vorgaben |

| Einsatzbereich   | Namensraum  |
|--|---|
| Konnektor (Schnittstelle zum Transportnetz)                          | keine Vorgaben  |
| VPN-Server des VPN-Zugangsdienstes (Schnittstelle zum Transportnetz) | Namensraum Zugangsnetz; dedizierte Subdomain des Betreibers VPN-Zugangsdienst |
| Zentrale Dienste der TI-Plattform                                    | Geschlossener Namensraum TI   |
| Fachanwendungsspezifische Dienste                                    | 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

Die übergreifende Netzwerkspezifikation MUSS festlegen, welche Produkttypen Verfahren zur Priorisierung auf Netzwerkebene umsetzen müssen. ☒

## 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

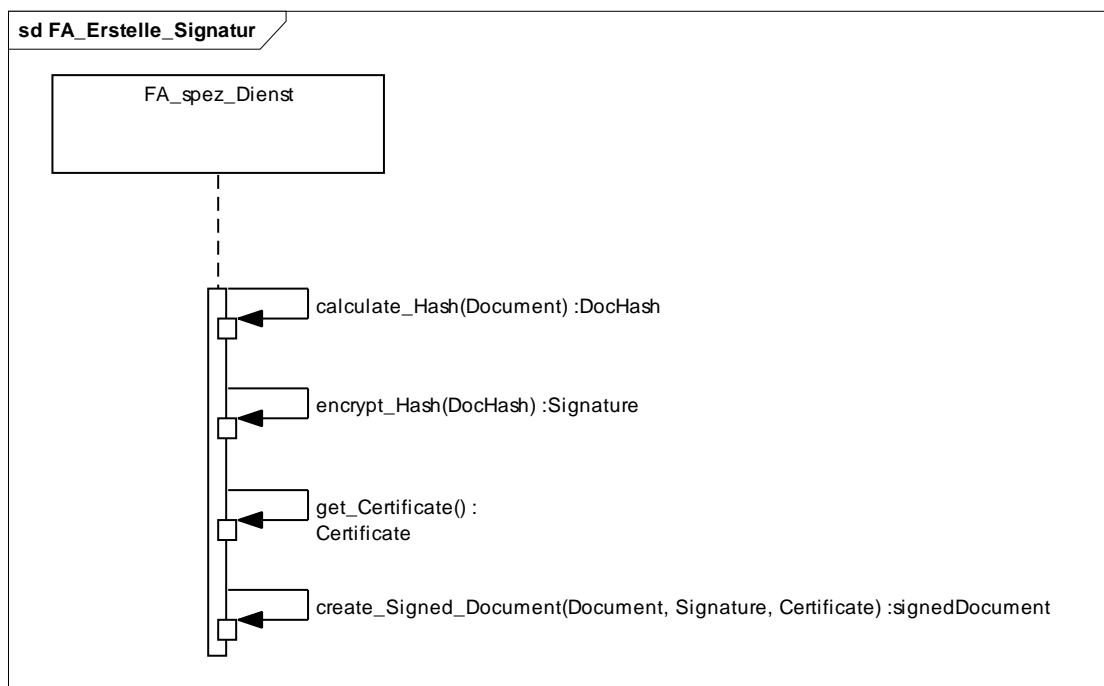
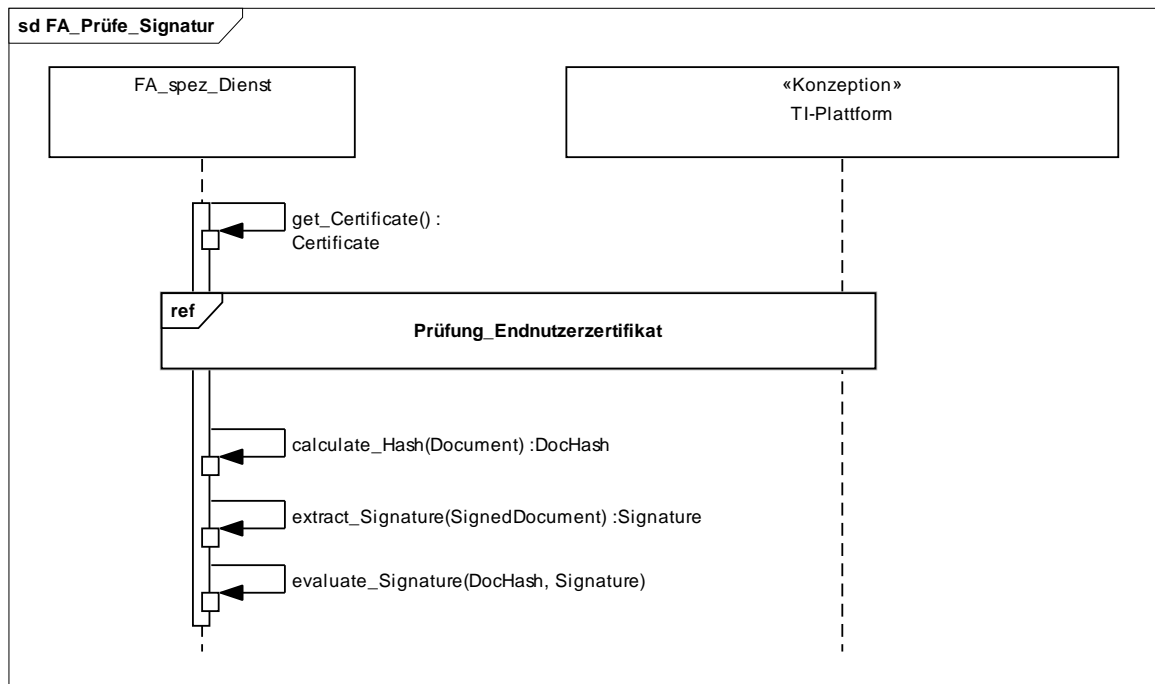


Abbildung 17: Ablauf: Erstellung digitale Signatur

Abbildung 17 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 18: Ablauf: Prüfung digitale Signatur**

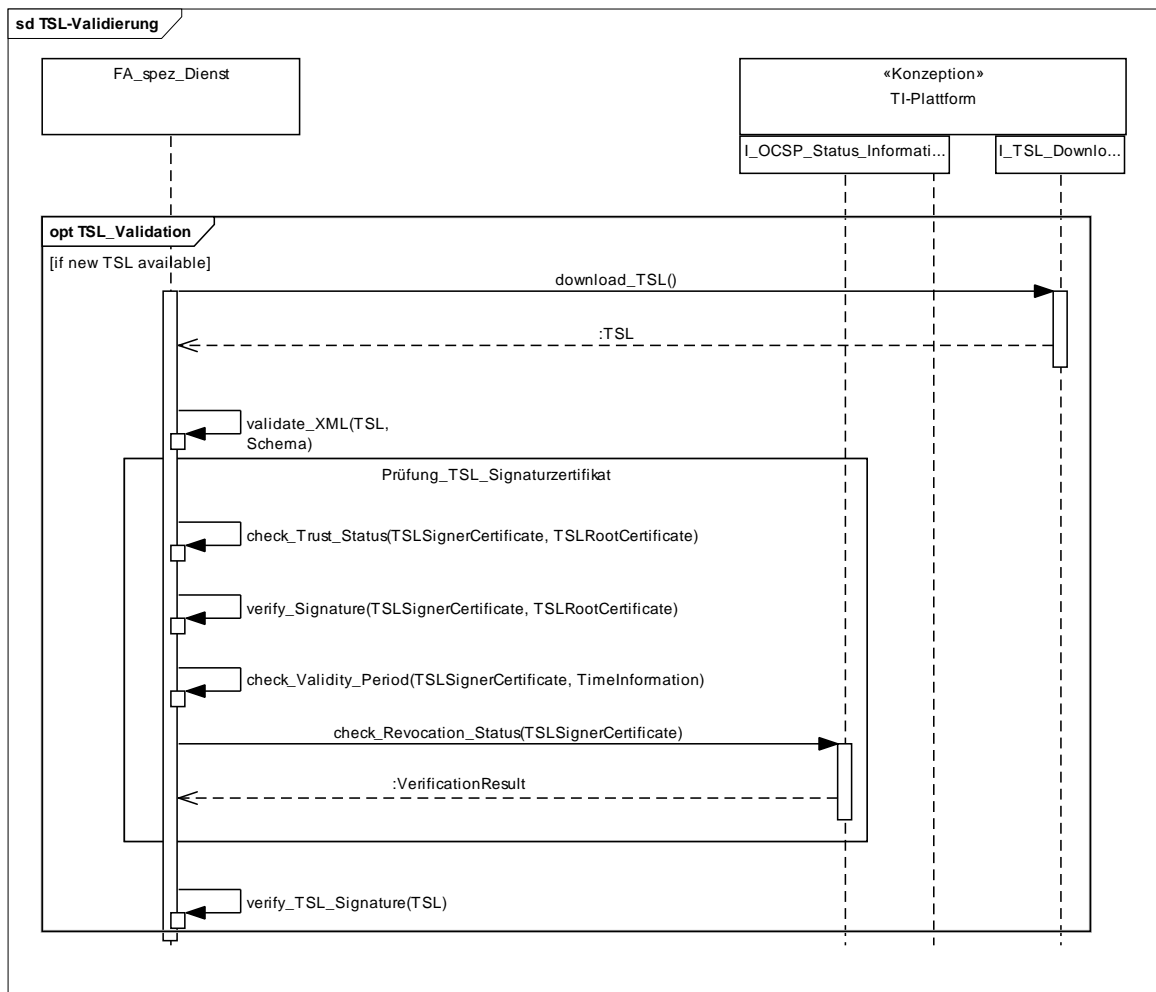
Abbildung 18 zeigt den Ablauf bei Prüfung einer digitalen Signatur. Dabei wird der in Kapitel 7.1.2.2 beschriebene Ablauf für die Prüfung eines X.509-Zertifikats einbezogen.

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.

## 7.1.2 Prüfung von X.509-Zertifikaten (Prüfung\_Zertifikat)

### 7.1.2.1 TSL-Validierung



**Abbildung 19: 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 20 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

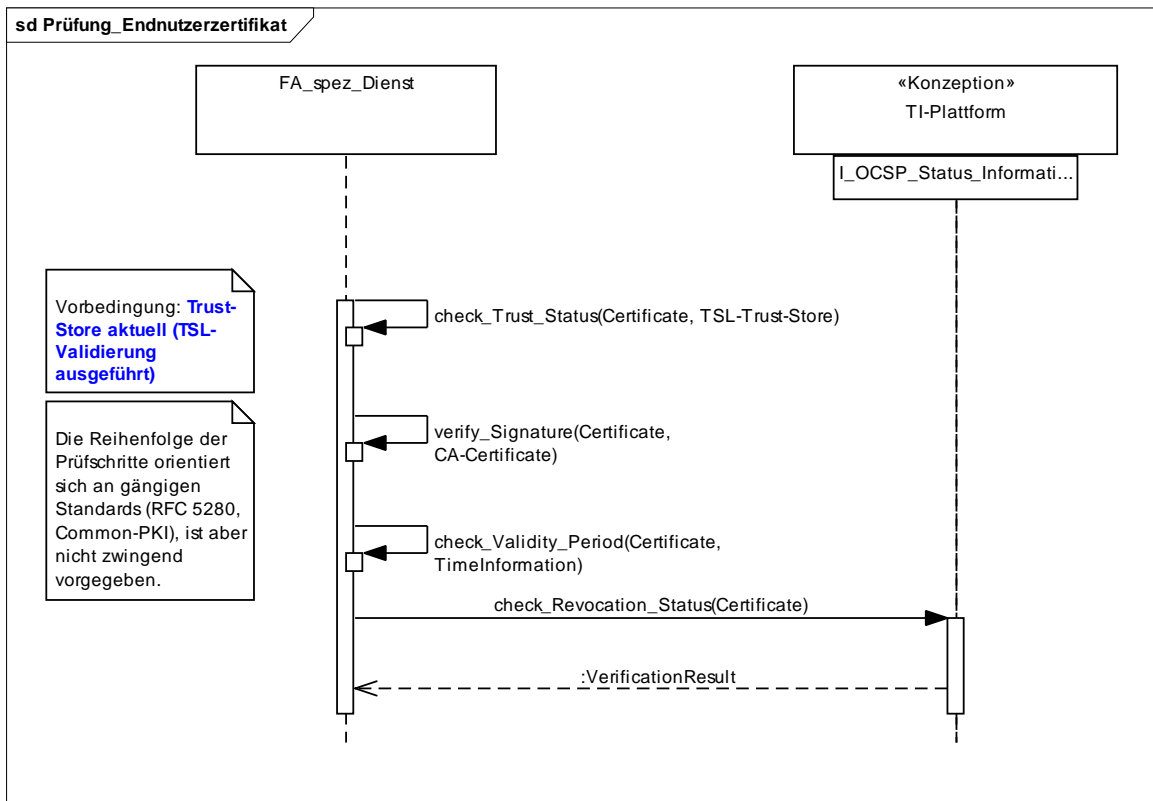


Abbildung 20: Ablauf: Prüfung von X.509-Zertifikaten

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.



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.

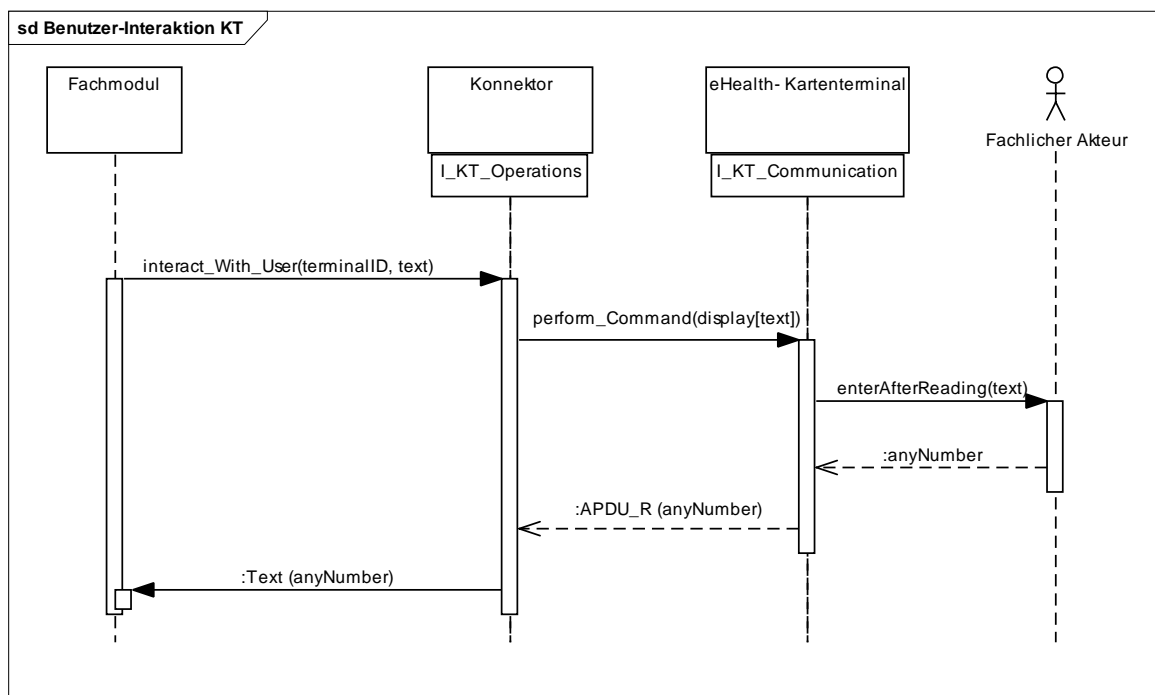


Abbildung 21: Ablauf: Benutzerinteraktion am Kartenterminal

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.

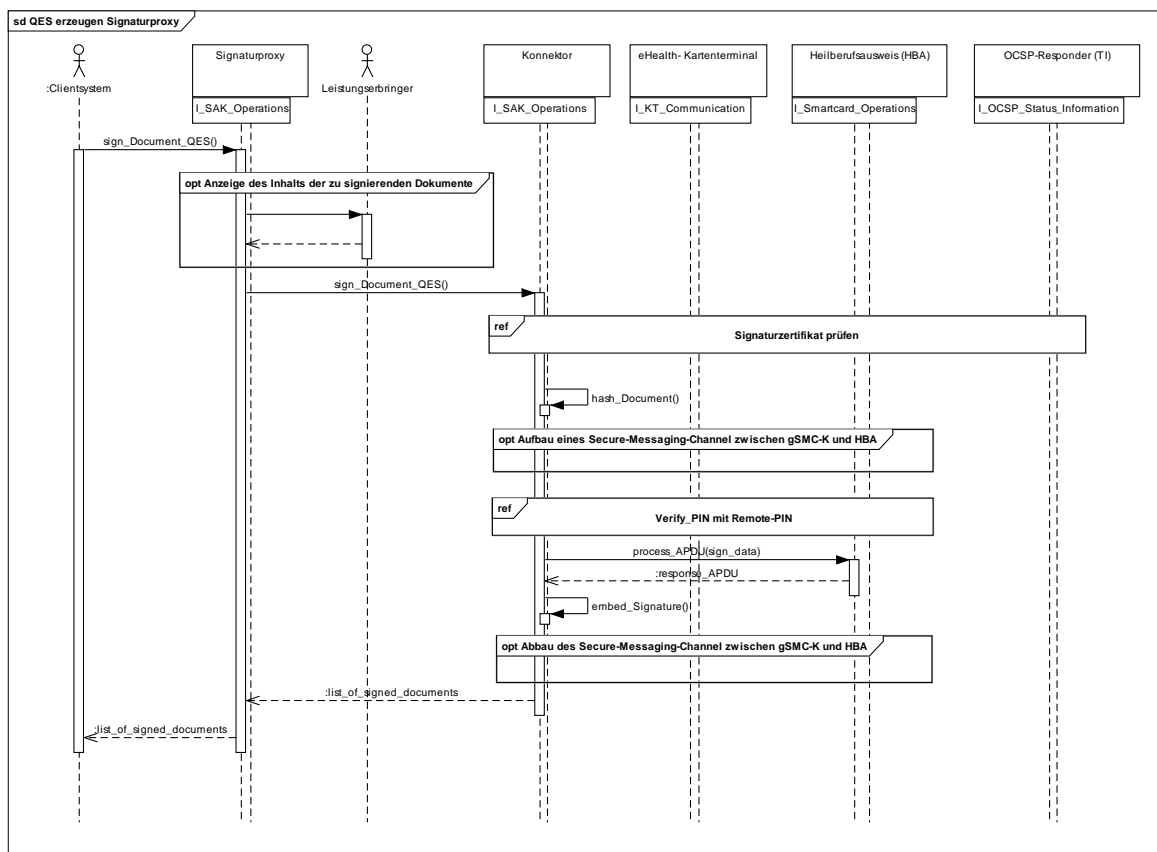


Abbildung 22: Ablauf: QES erzeugen

Abbildung 22 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 22 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.

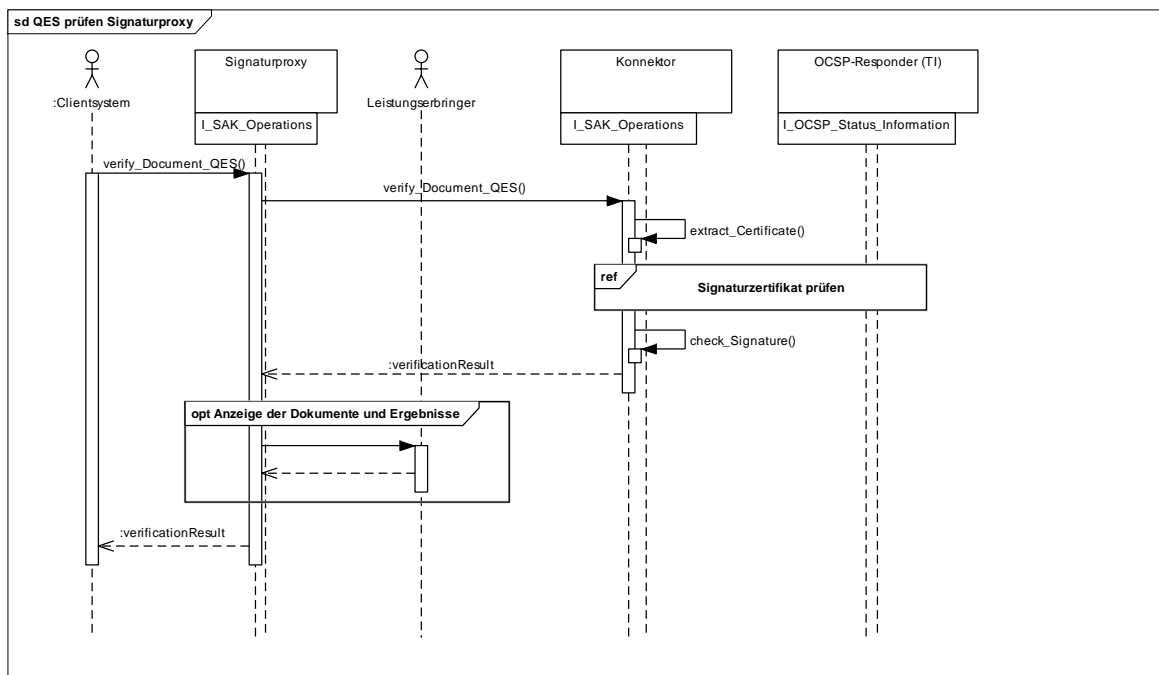


Abbildung 23: Ablauf: QES prüfen

Abbildung 23 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 23 separat dargestellt.

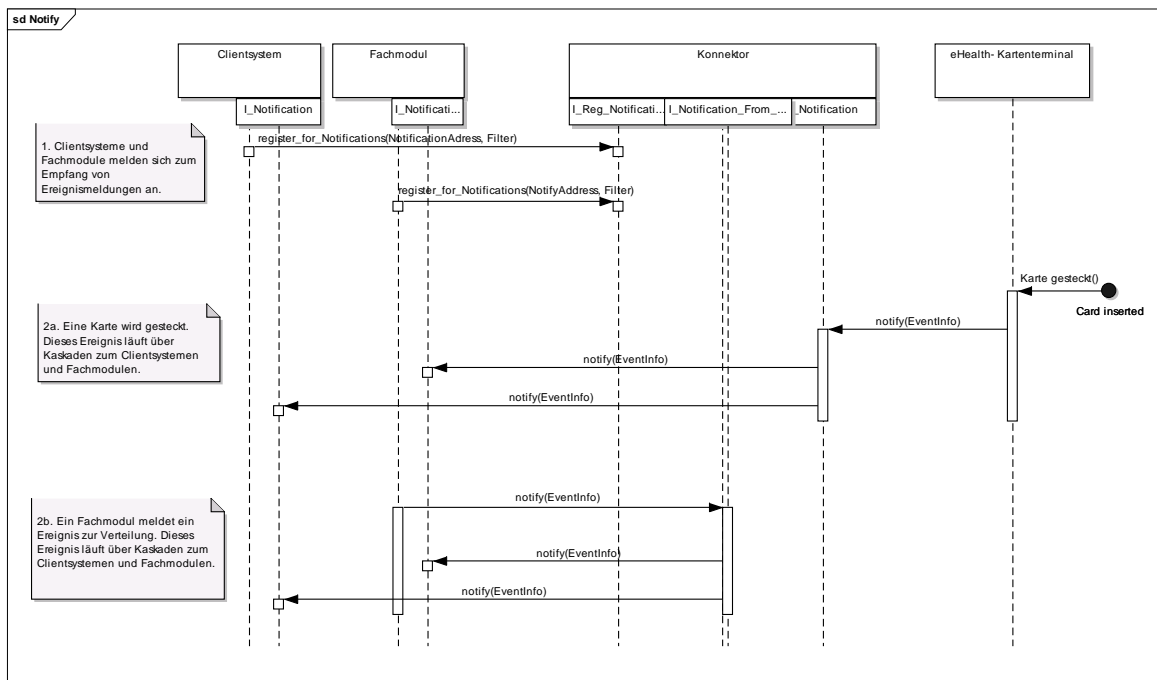
Alternativ zur Darstellung in der Abbildung kann das Clientsystem auch direkt die Operation des Konnektors aufrufen. In diesem Fall kann keine Anzeige der Inhalte und Ergebnisse erfolgen. ☒

## 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.



**Abbildung 24: 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.

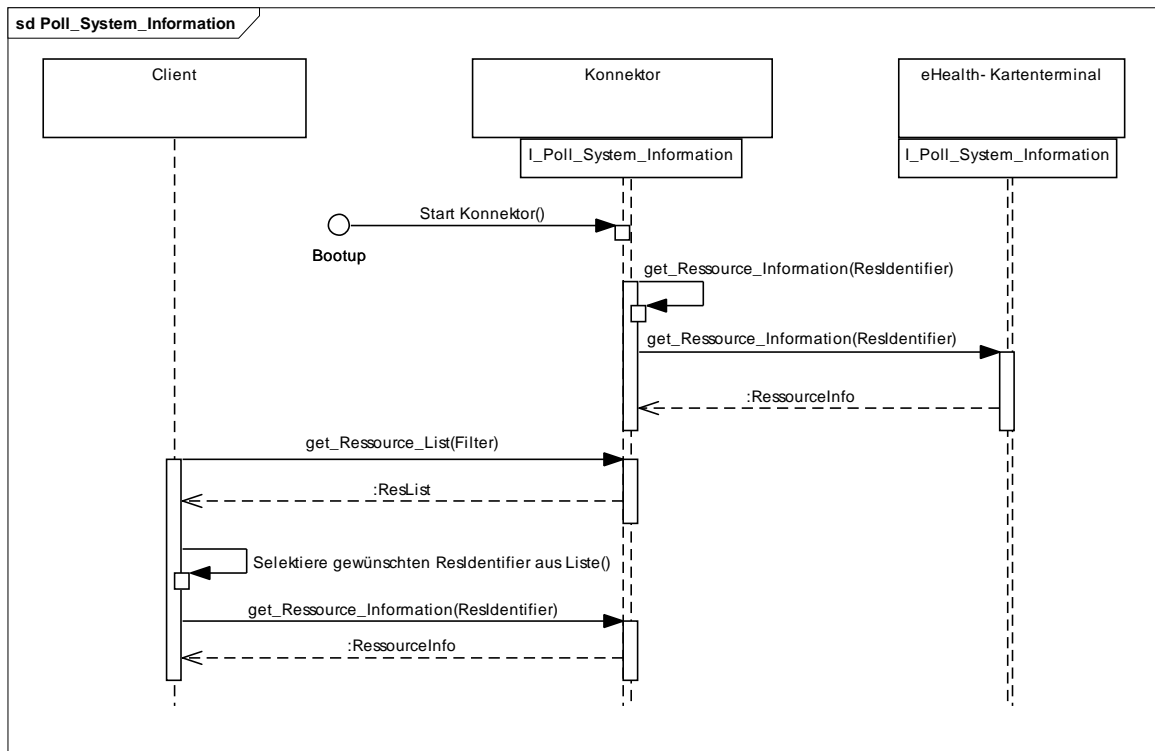
2b. Ein Fachmodul möchte ein fachspezifisches Event zur Verteilung melden. Es ruft dazu `notify` des Konnektors auf. Dieser sendet diese Eventinformation an alle registrierten Clientsysteme und Fachmodule, die sich über ihren bei der Registrierung übergebenen Filter für diese Art der Meldung abonniert 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

Alle am Ablauf „Sammeln der Umgebungsinformationen und Abfrage RessourcenInfo“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.



**Abbildung 25: 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 (Herstellernamen, 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 `Resldentifizier` wird im Folgeaufruf der Operation `get_Ressource_Information` verwendet, um alle zu dieser so eindeutig identifizierten Komponente verfügbaren Detailinformation zu erhalten. ☒

## 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.

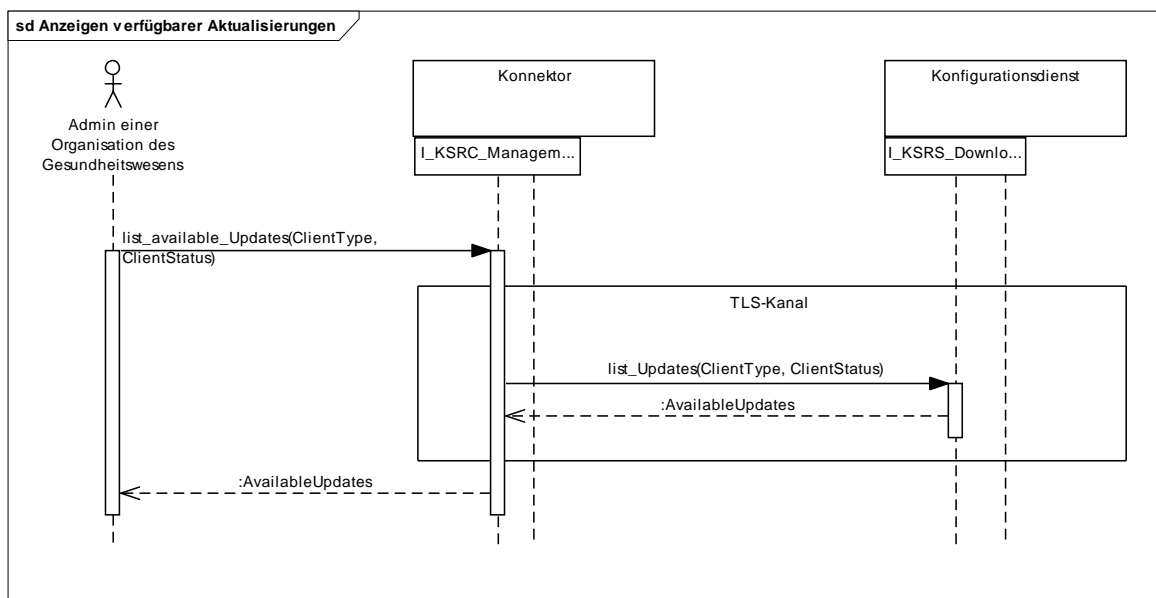


Abbildung 26: Ablauf: Anzeigen verfügbarer Aktualisierungen

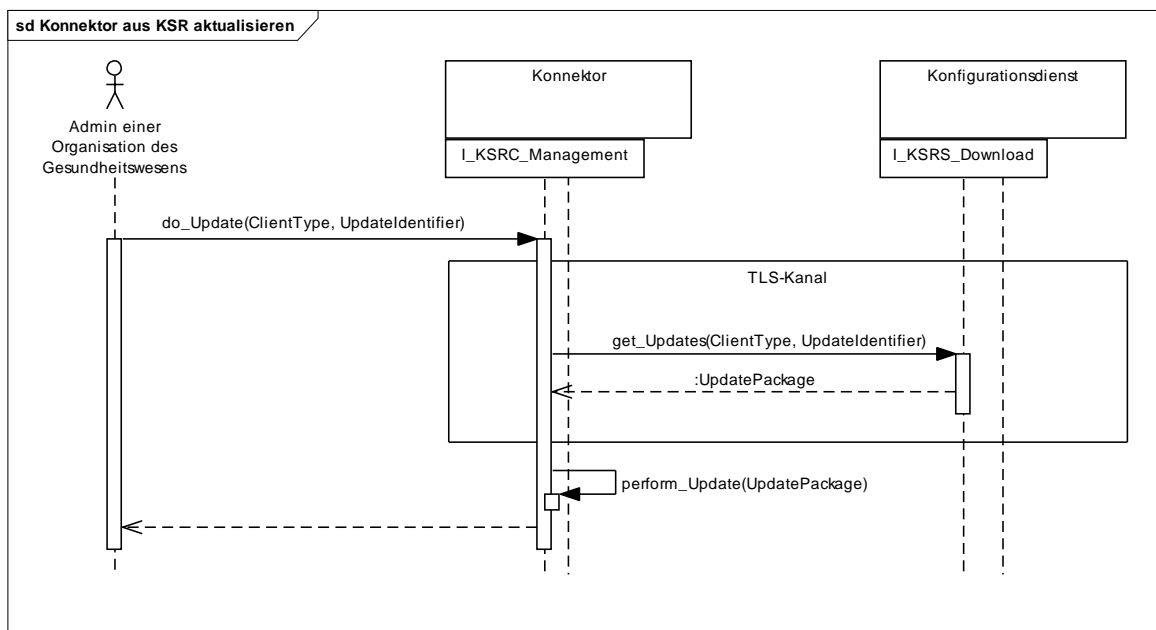
Der Administrator kann sich mit der Operation `list_Available_Updates` des Produkttyps Konnektor verfügbare Aktualisierungen anzeigen lassen.

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

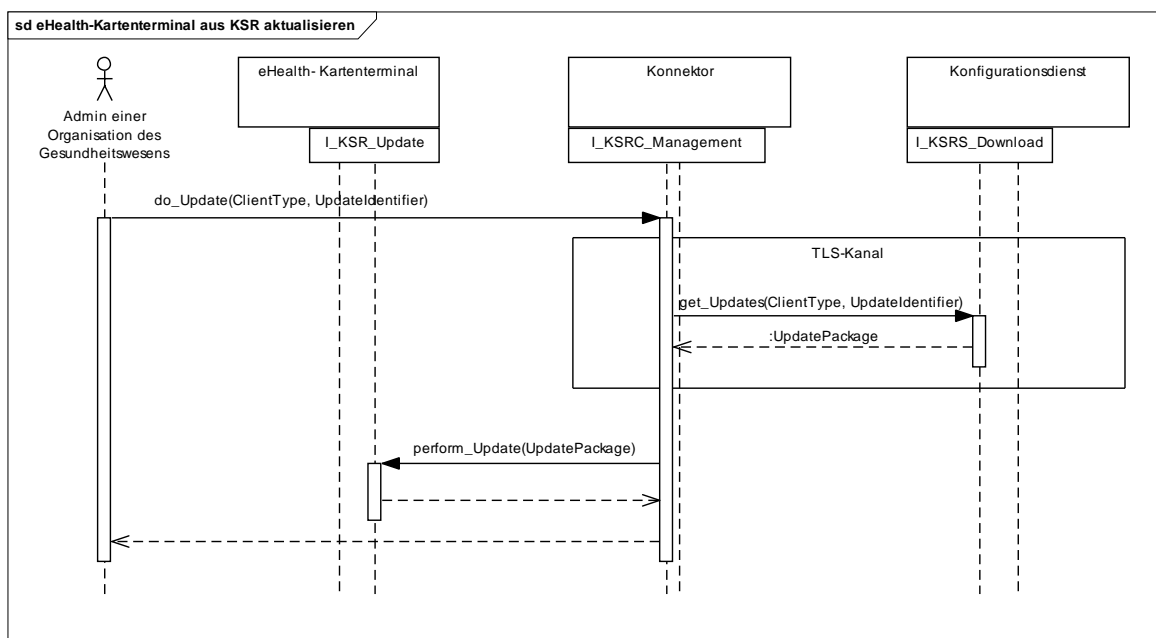
Alle am Ablauf „Software oder Konfigurationen über KSR aktualisieren“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.



**Abbildung 27: Ablauf: Konnektor aus Konfigurationsdienst aktualisieren**

Abbildung 27 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 28: Ablauf: eHealth-Kartenterminal aus Konfigurationsdienst aktualisieren**

Abbildung 28 stellt die Aktualisierung des Produkttyps eHealth-Kartenterminal aus dem Konfigurationsdienst dar.



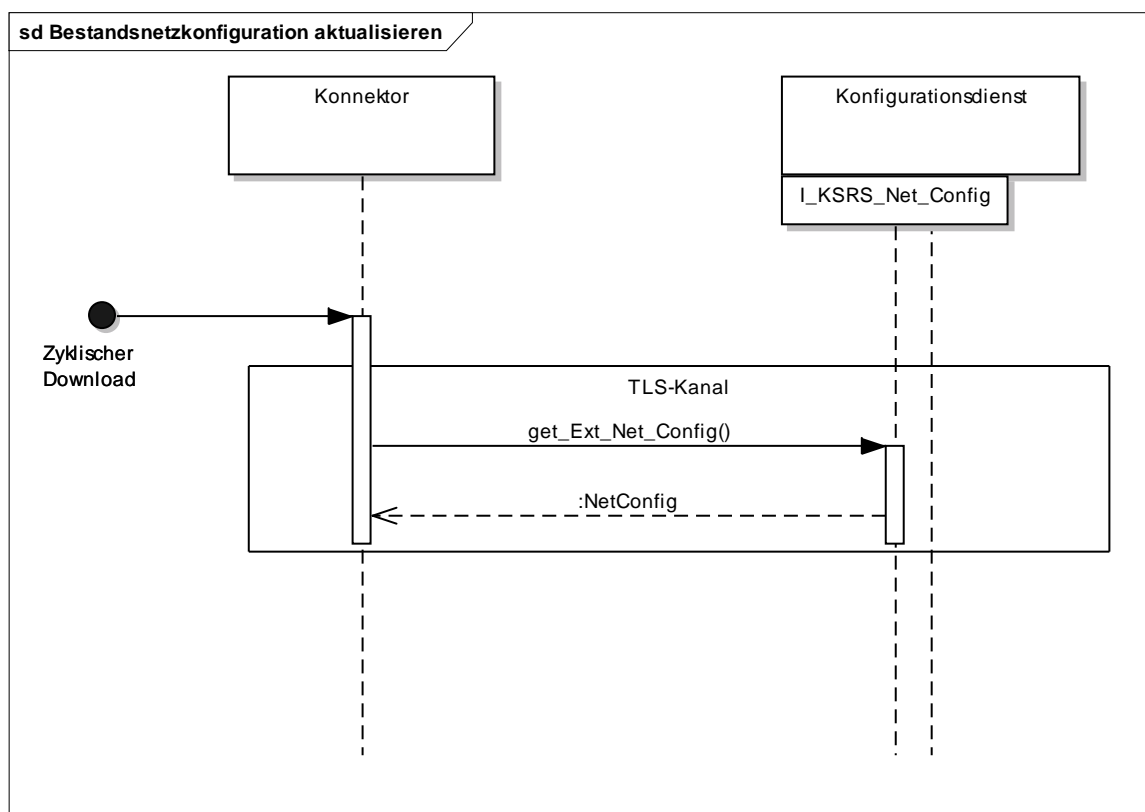
Zwischen Konnektor und Konfigurationsdienst wird eine TLS-Verbindung unter Nutzung der kryptographischen Identität ID.ZD.TLS\_S zur Serverauthentisierung aufgebaut.

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 Bestandsnetzkonfigurationen aktualisieren

##### ☒ TIP1-A\_5116 Ablauf Bestandsnetzkonfigurationen aktualisieren

Alle am Ablauf „Bestandsnetzkonfigurationen aktualisieren“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.



**Abbildung 29: Ablauf: Bestandsnetzkonfigurationen aktualisieren**

Der Konnektor lädt zyklisch die aktuelle Konfigurationsdatei mit den nötigen Bestandsnetzparametern vom Konfigurationsdienst. Im Fall einer Änderung der Parameter passt der Konnektor seine Konfigurationsmöglichkeiten dementsprechend an.

Neu angeschlossene Bestandsnetze müssen im Konnektor durch den Administrator freigeschaltet werden bevor die entsprechende Konfiguration angewendet wird und die Bestandsnetze für angeschlossenen Clientsysteme erreichbar sind.

Die Konfiguration entfallener Bestandsnetze wird im Konnektor automatisch gelöscht.

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 TLS und Vertrauensliste der BNetzA in Produkttypen

### 7.2.5.1 Ablauf Aktualisierung der TLS über die TI-Plattform

#### ☒ TIP1-A\_3683 Ablauf Aktualisierung der TLS über die TI-Plattform

Alle am Ablauf „Aktualisierung der TLS über die TI-Plattform“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

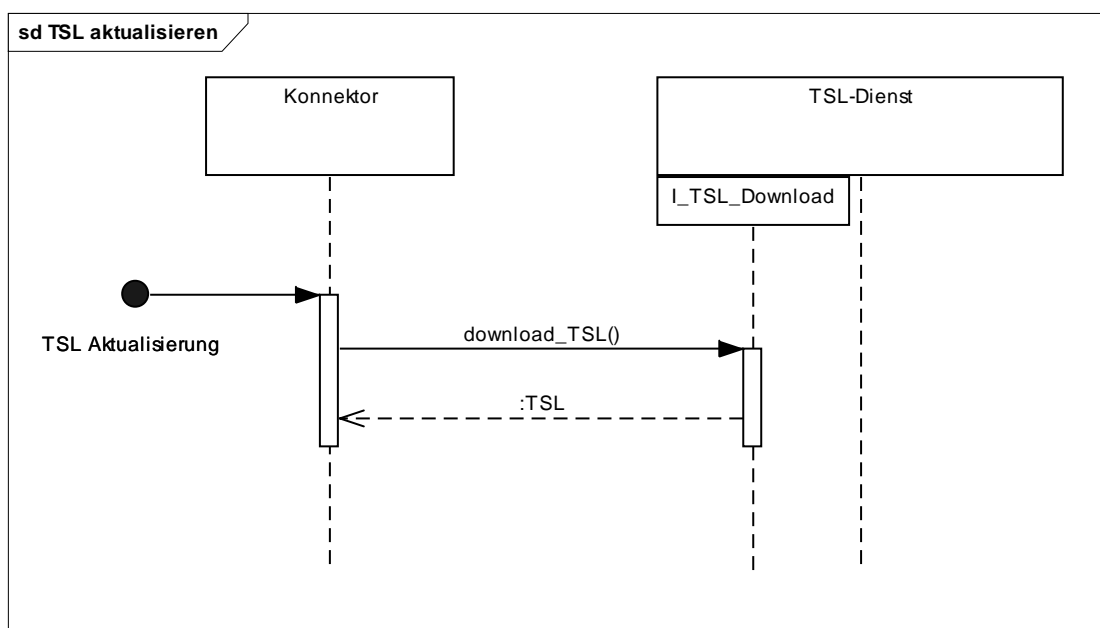


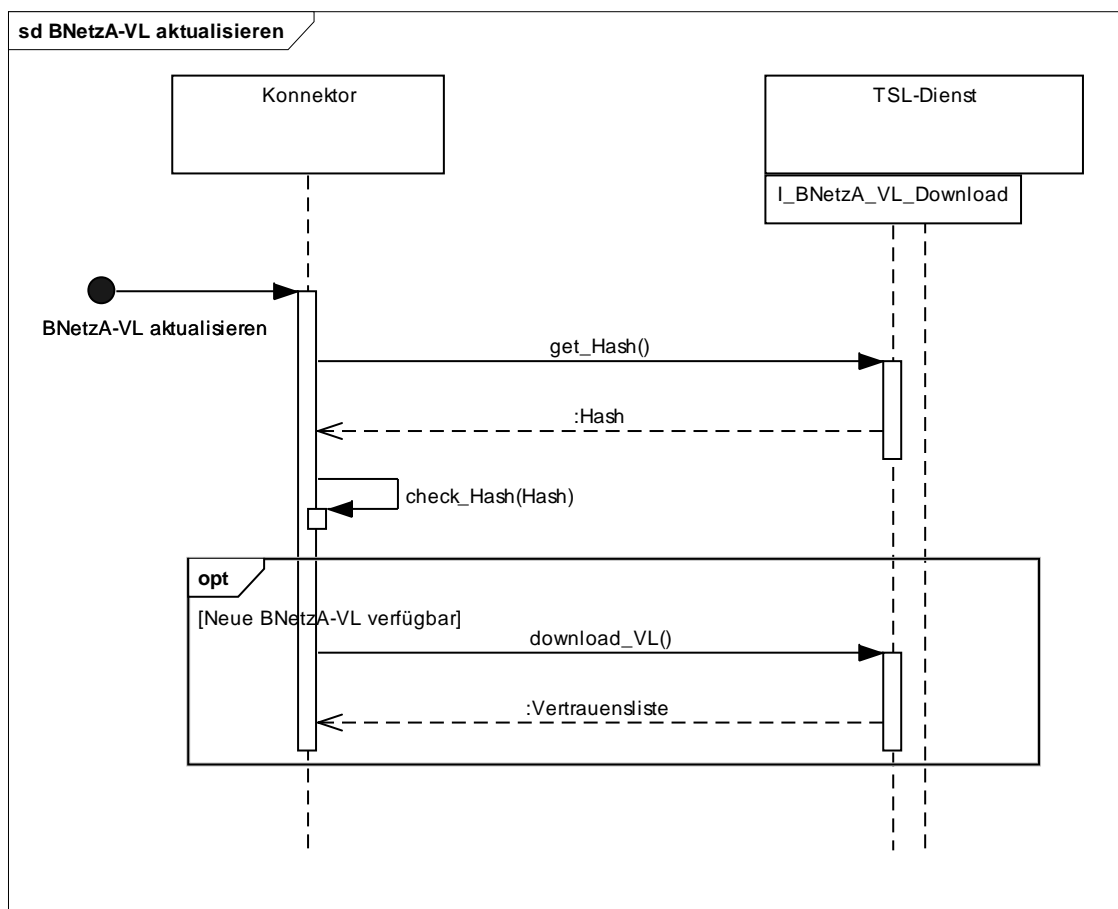
Abbildung 30: Ablauf: Aktualisierung der TLS über die TI-Plattform

Der am Beispiel Konnektor gezeigte Ablauf trifft auch für den Produkttyp VPN-Zugangsdienst 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.



**Abbildung 31: 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.

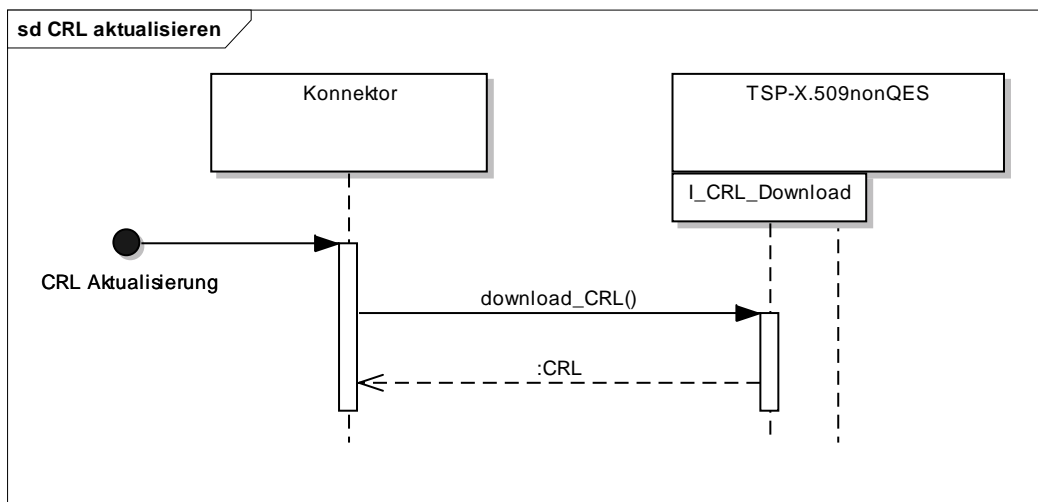


Abbildung 32: Ablauf: Aktualisierung der CRL im Konnektor

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.

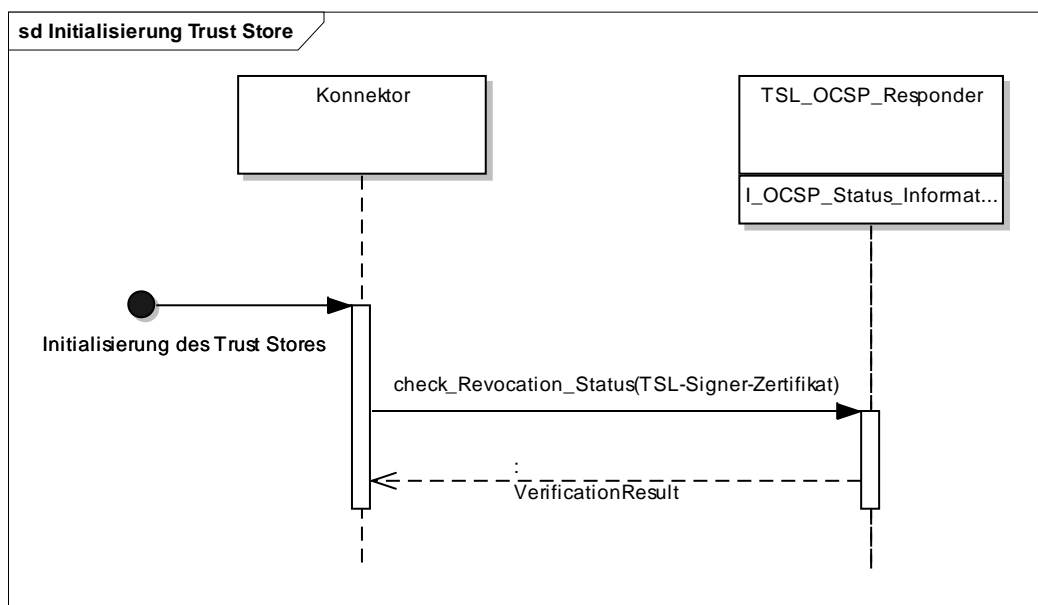


Abbildung 33: Ablauf: Initialisierung Trust Store

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. 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.

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.

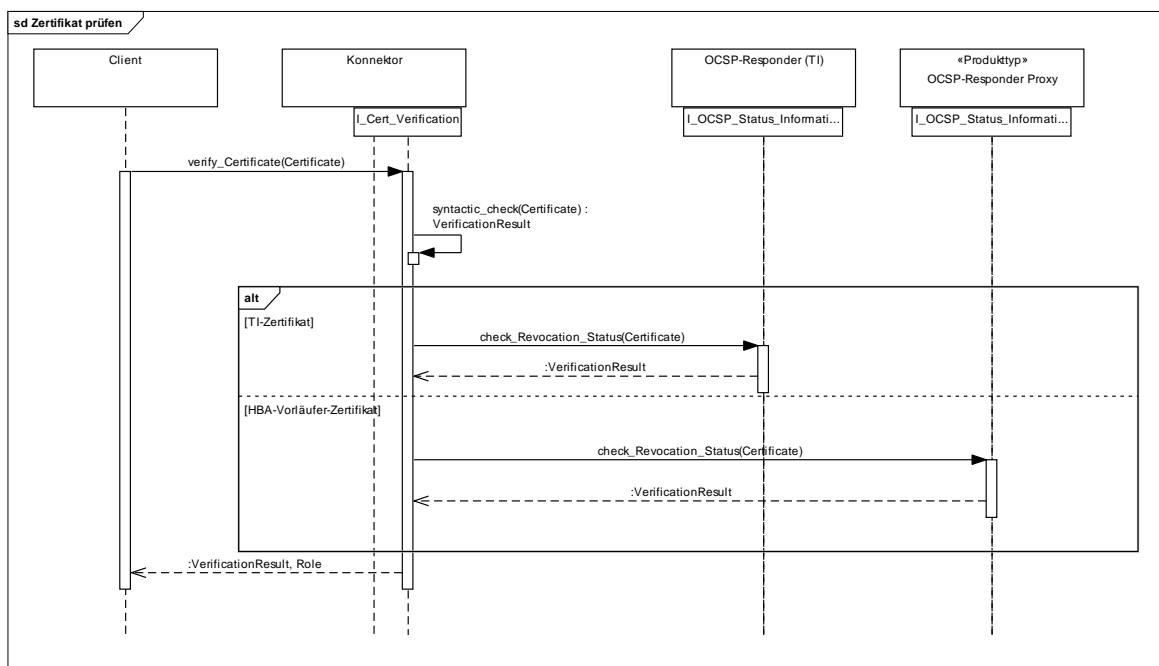


Abbildung 34: Ablauf: Zertifikat prüfen

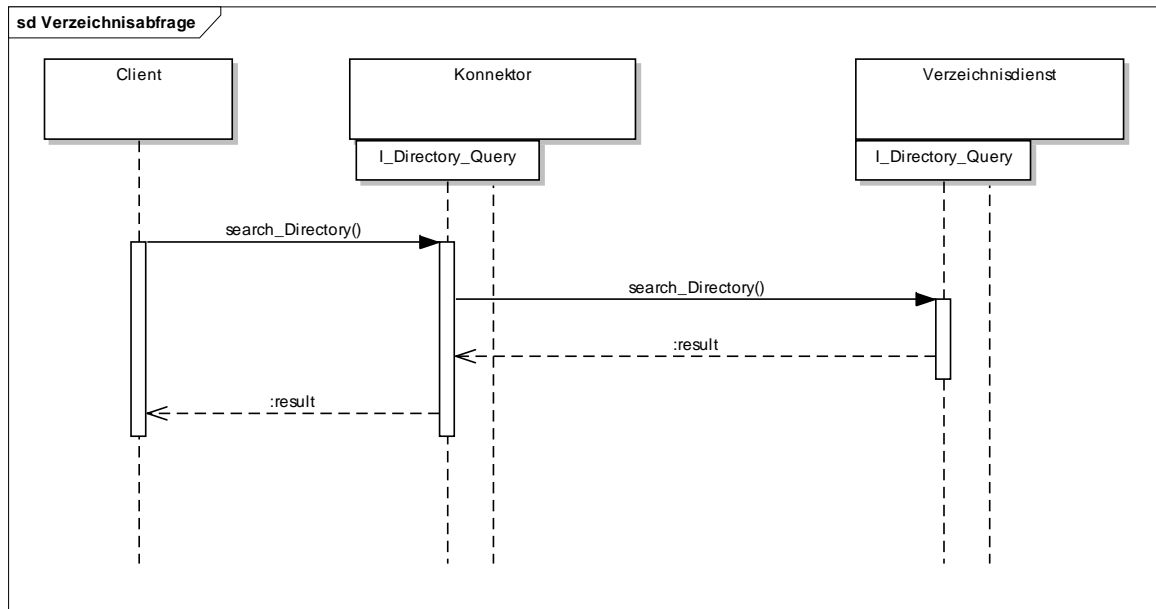
Im Rahmen der Zertifikatsprüfung muss im Online-Fall der Zertifikatsstatus des zu prüfenden Zertifikats ermittelt werden, um festzustellen ob das Zertifikat nicht bereits gesperrt wurde. Für jedes zu prüfende Zertifikat ist über die TSL die Adresse des relevanten OCSP-Responders hinterlegt. Zur Steigerung 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 den VPN-Zugangsdienst zu. ☒

## 7.2.8 Verzeichnis\_Identitäten

### 7.2.8.1 Ablauf Abfrage des Verzeichnisses

#### ☒ TIP1-A\_5821 Ablauf Abfrage des Verzeichnisses

Alle am Ablauf „Abfrage des Verzeichnisses“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.




**Abbildung 35: 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 Verzeichnisdienstabfrage 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. 

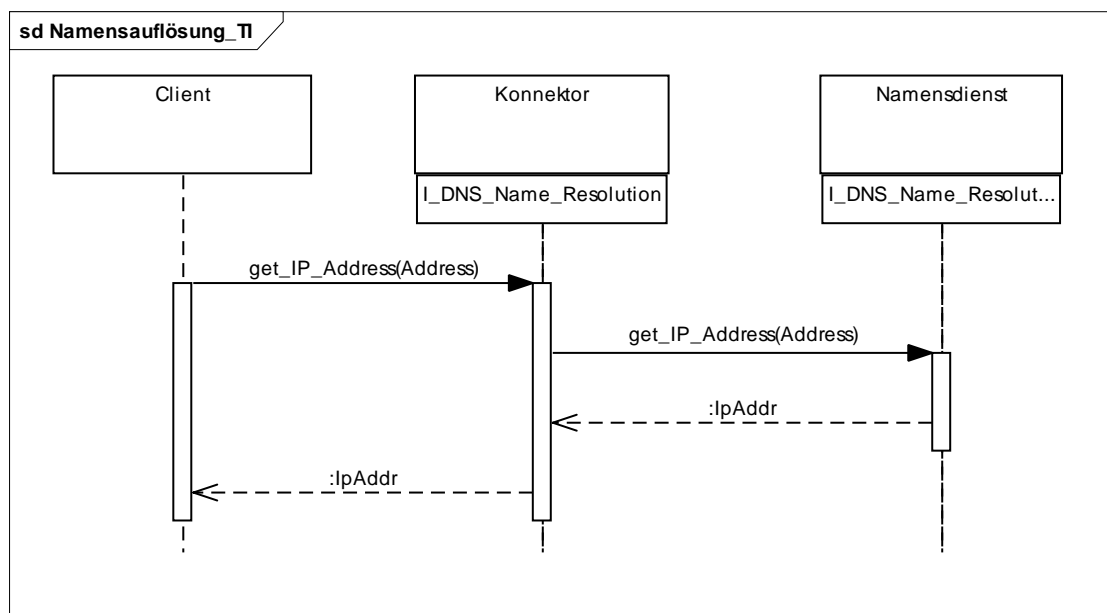
## 7.2.9 Namensauflösung

### 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:



**Abbildung 36: 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
- TSL-Dienst



- VPN-Zugangsdienst
- Zeitdienst
- Sicherheitsgateway Bestandsnetze
- Störungssampel
- Verzeichnisdienst ☒

#### 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.

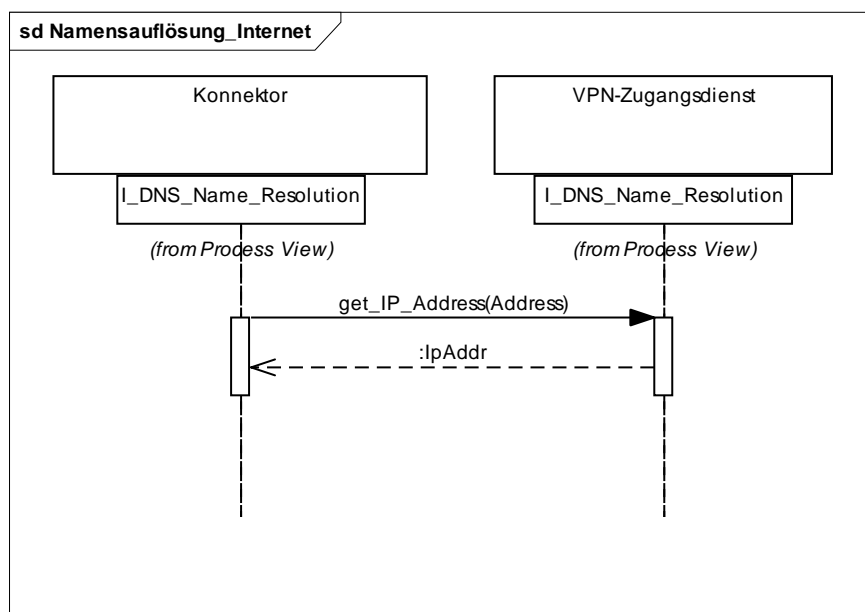


Abbildung 37: Ablauf: Namensauflösung Internet

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 Zugangsnetz) des VPN-Zugangsdienstes. Der DNS-Nameserver (Namensraum Zugangsnetz) 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 auflösen

##### ☒ TIP1-A\_2473 Ablauf FQDN aus Bestandsnetzen auflösen

Alle am Ablauf „FQDN aus Bestandsnetzen auflösen“ beteiligten Produkttypen MÜSSEN die Festlegungen zum Ablauf des Use Cases umsetzen.

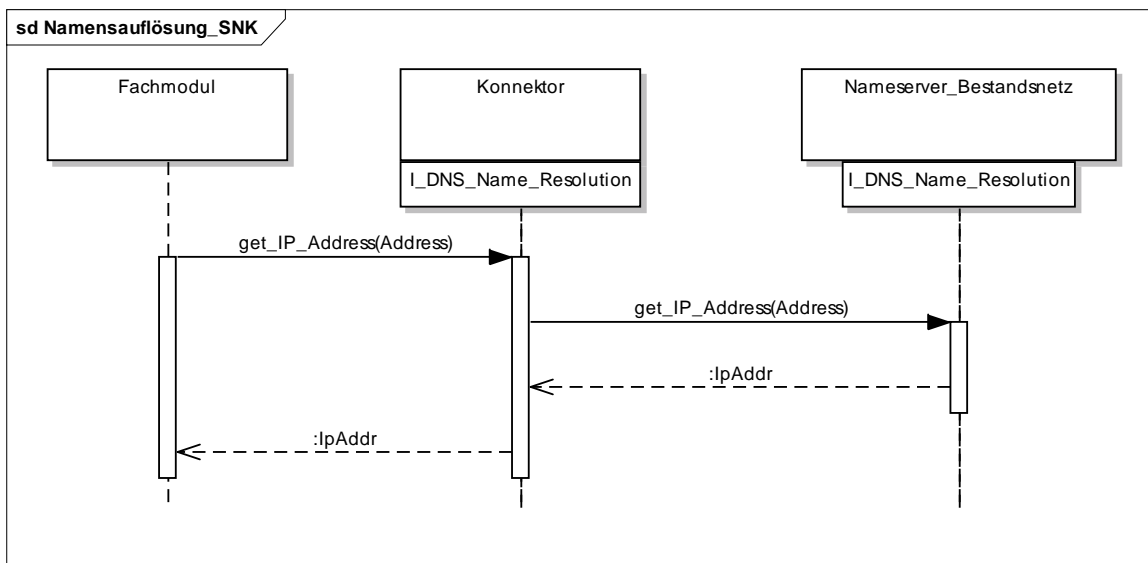


Abbildung 38: Ablauf: Namensauflösung Bestandsnetz

Um einen Dienst in einem Bestandsnetz 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) des Bestandsnetzes. 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.

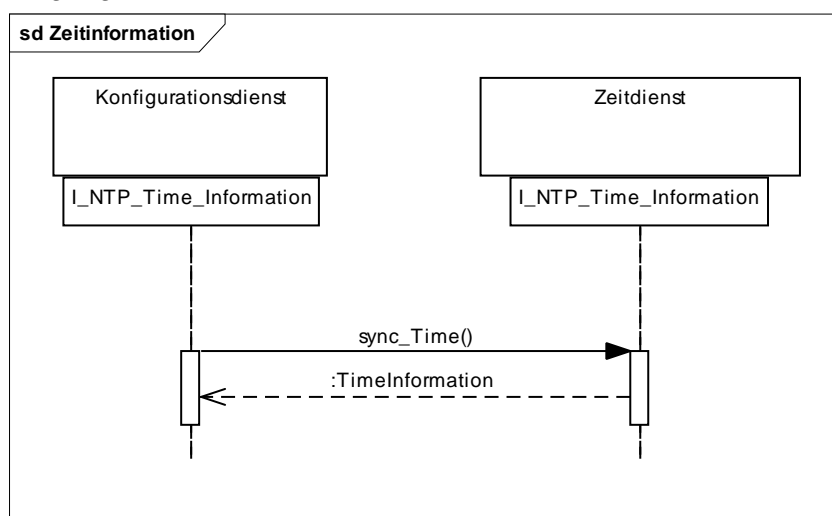


Abbildung 39: Ablauf: Zeitinformation abfragen

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
- TSL-Dienst
- VPN-Zugangsdienst
- Störungsampel
- Sicherheitgateway Bestandsnetze

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.

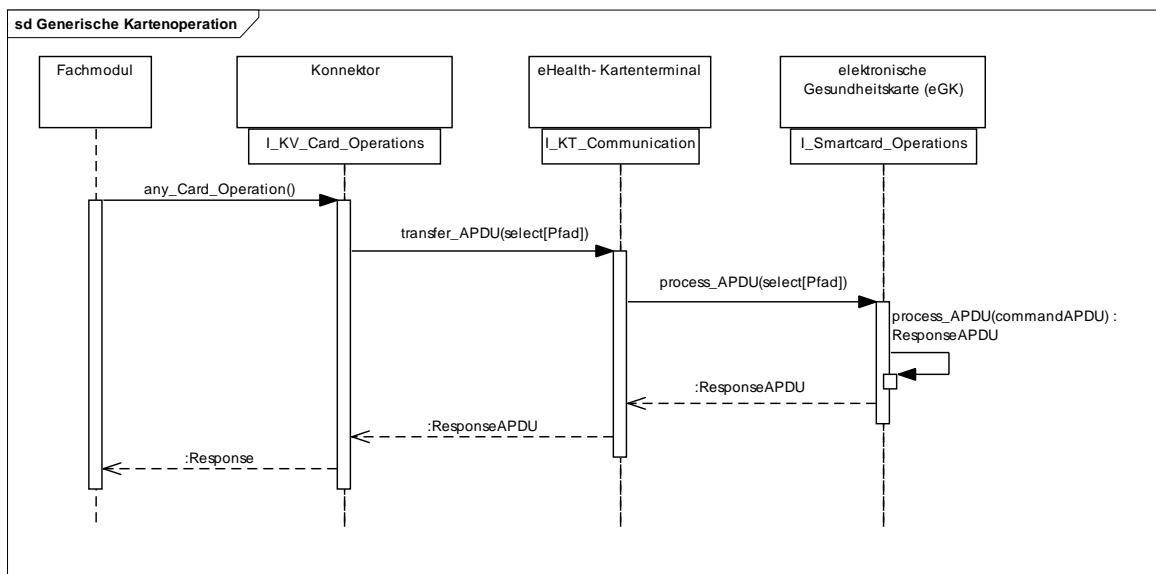
Die Synchronisation zwischen den Zeitservern von VPN-Zugangsdienst mit denen des Zeitdienstes sowie vom Konnektor mit den Zeitservern des VPN-Zugangsdienstes erfolgt ebenfalls über die Schnittstelle `I_NTP_Time_Information`. ☒

## 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.



**Abbildung 40: 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 Kommunikationsstrecke 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.

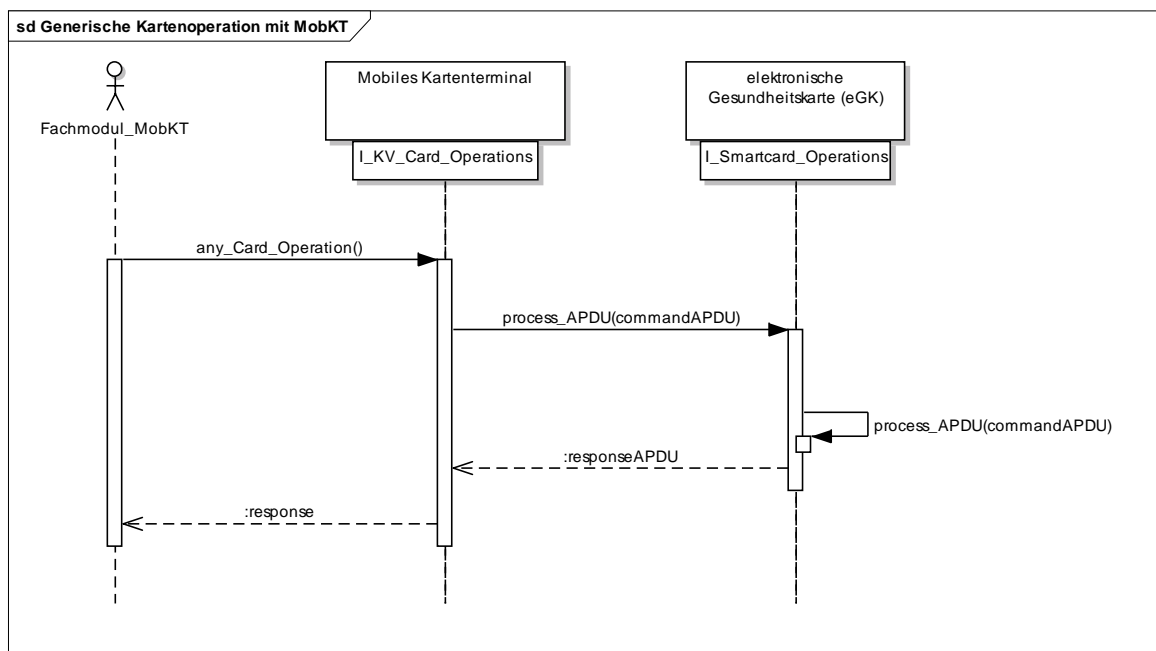
Der am Beispiel eGK gezeigte Ablauf trifft auch für die Produkttypen HBA, SMC-B und HSM-B zu.

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.



**Abbildung 41: 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.

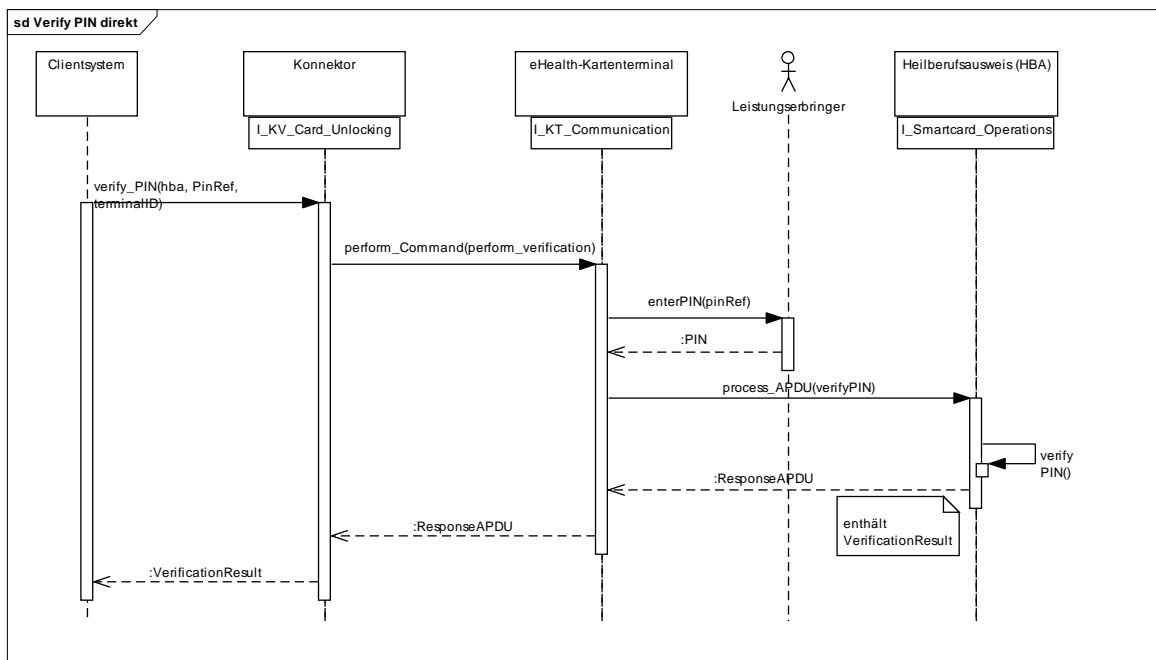


Abbildung 42: Ablauf: Verify PIN direkt

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.

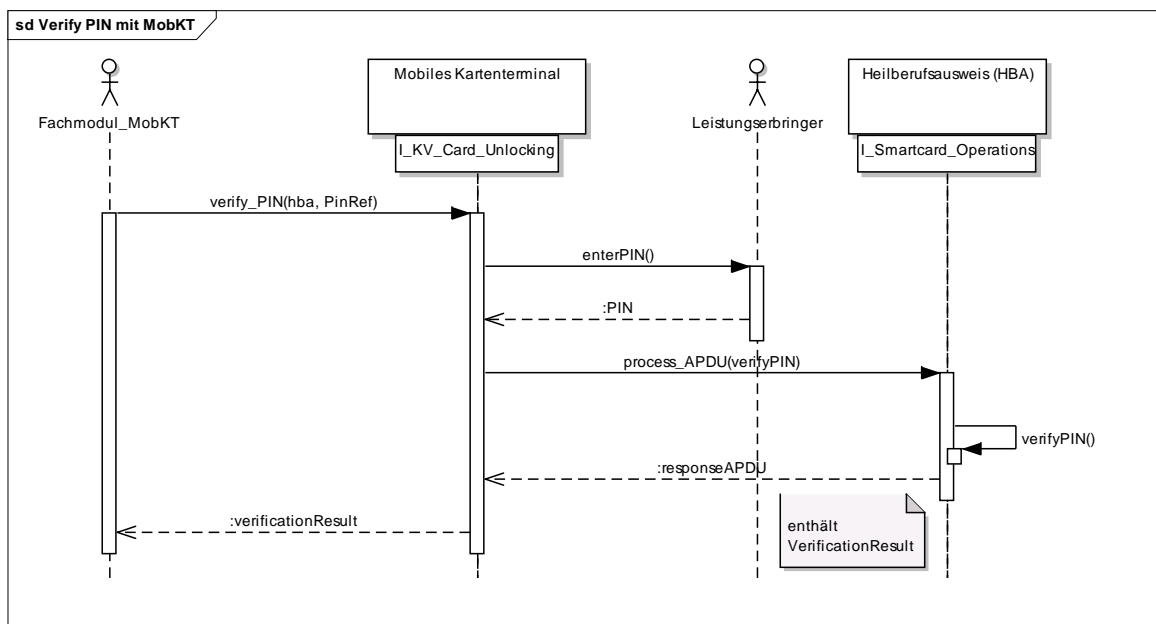
Die Kommunikation zum HSM-B erfolgt nicht über das eHealth-Kartenterminal sondern über die Schnittstelle I\_HSM\_Operations direkt zwischen Konnektor und HSM-B.

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.



**Abbildung 43: 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.

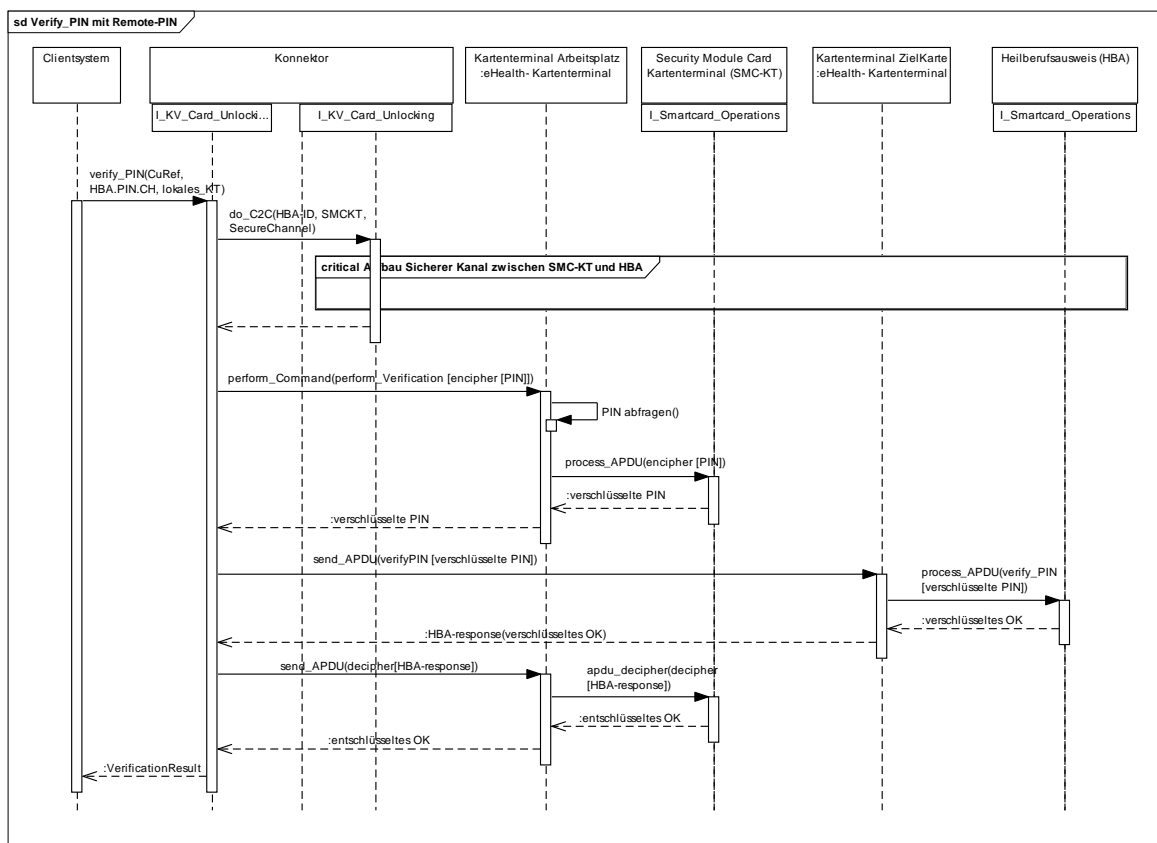
Der am Beispiel HBA gezeigte Ablauf trifft auch für den Produkttyp SMC-B zu.

*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.



**Abbildung 44: 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 Kartenterminal 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.



Die Kommunikation zum HSM-B erfolgt nicht über das eHealth-Kartenterminal, sondern direkt zwischen Konnektor und HSM-B.

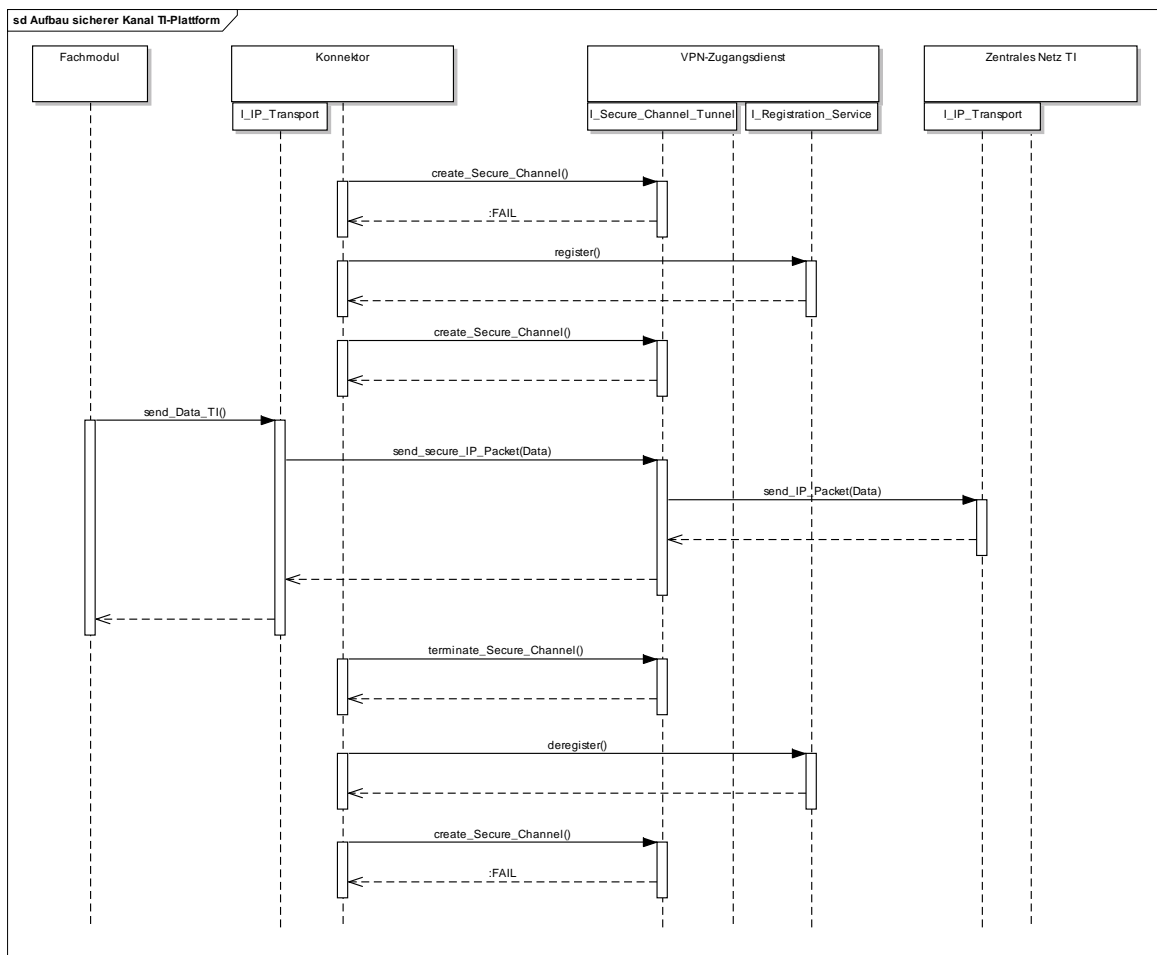
*HINWEIS: Die Übertragungsstrecke zwischen eHealth-Kartenterminals und Karten wird nicht über technische Mechanismen gesichert. ☒*

## 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 45: 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

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.

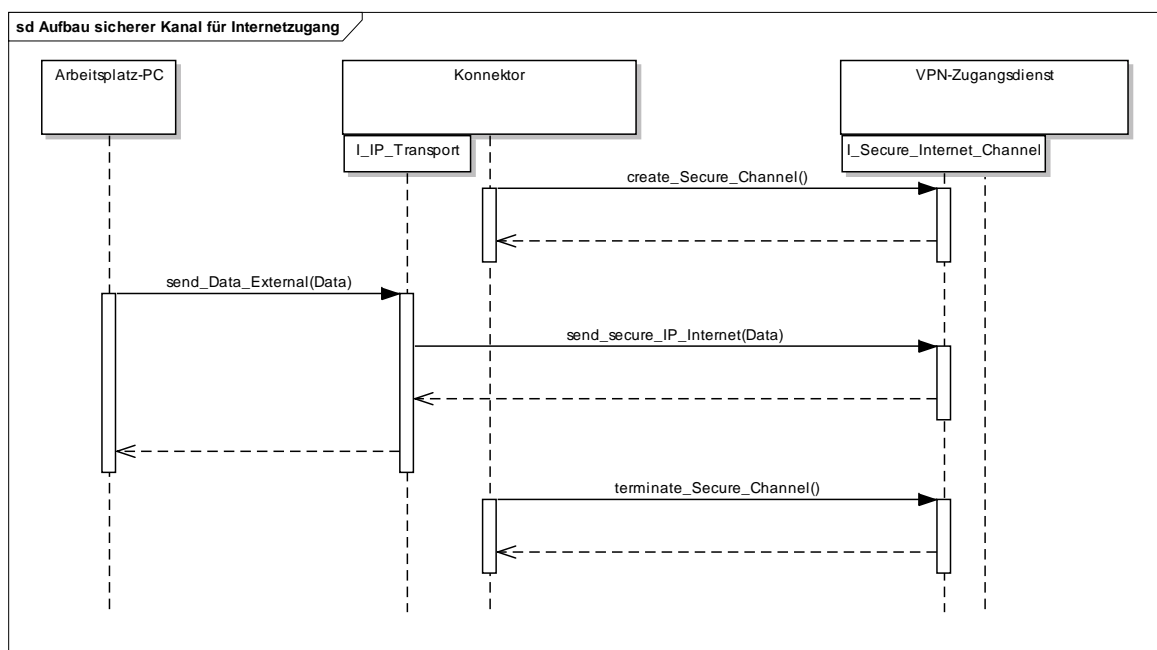


Abbildung 46: Ablauf: Aufbau eines sicheren Kanals zur Anbindung des sicheren Internetzugangs

Dieses Diagramm beschreibt den Aufbau eines sicheren Kanals (Secure Channel) zwischen Konnektor und dem VPN-Zugangsdienst.

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.  
☒

---

## Anhang A – Verzeichnisse

---

### A1 – Abkürzungen

| Kürzel | Erläuterung                             |
|--------|---|
| A      | Administrator                           |
| 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 |
| KT     | Kartenterminal                          |
| KTR    | Kostenträger                            |
| KV     | Krankenversicherung                     |
| LAN    | Local Area Network                      |
| LE     | Leistungserbringer                      |

| Kürzel | Erläuterung                          |
|--------|--------------------------------------|
| 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   |
| 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                 |
| 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: Modellierung der TI mittels Produkttypen, Produkten und Produktinstanzen .....                                    | 15  |
| Abbildung 3: Logische Architekturschichten (Zonen) und Building Blocks.....  | 16  |
| Abbildung 4: Außensicht der TI-Plattform.....  | 26  |
| Abbildung 5: CardUsageReference.....   | 28  |
| Abbildung 6: Beteiligte Komponenten beim Remote-PIN-Verfahren.....   | 31  |
| Abbildung 7: Übersicht des Gesamtsystems der TI.....   | 34  |
| Abbildung 8: Produkttypsicht.....  | 35  |
| Abbildung 9: Datenmodell Verzeichnisdienst .....   | 54  |
| Abbildung 10: Netzwerktopologie der TI .....   | 119 |
| Abbildung 11: Netzwerkverbindungen dezentral .....   | 120 |
| Abbildung 12: Netztopologie Zugangsnetz.....   | 120 |
| Abbildung 13: Netztopologie Zentrales Netz .....   | 121 |
| Abbildung 14: Netztopologie Sicherheitgateway Bestandsnetze .....  | 122 |
| Abbildung 15: Netztopologie Sicherer Internetzugang.....   | 123 |
| Abbildung 16: Messpunkte des Datenvolumens im Netzwerk der TI-Plattform.....   | 125 |
| Abbildung 17: Ablauf: Erstellung digitale Signatur.....  | 131 |
| Abbildung 18: Ablauf: Prüfung digitale Signatur .....  | 132 |
| Abbildung 19: Ablauf: TSL-Validierung .....  | 133 |
| Abbildung 20: Ablauf: Prüfung von X.509-Zertifikaten.....  | 134 |
| Abbildung 21: Ablauf: Benutzerinteraktion am Kartenterminal.....   | 135 |
| Abbildung 22: Ablauf: QES erzeugen.....  | 136 |
| Abbildung 23: Ablauf: QES prüfen .....   | 137 |
| Abbildung 24: Ablauf: Anmeldung zur Notifikation und anschließende Notifikation durch Kartenevent, bzw. Fachmodulmeldung ..... | 138 |
| Abbildung 25: Ablauf: Sammeln der Umgebungsinformationen und anschließende Abfrage RessourcenInfo durch Clientsystem .....     | 139 |
| Abbildung 26: Ablauf: Anzeigen verfügbarer Aktualisierungen .....  | 140 |
| Abbildung 27: Ablauf: Konnektor aus Konfigurationsdienst aktualisieren .....   | 141 |
| Abbildung 28: Ablauf: eHealth-Kartenterminal aus Konfigurationsdienst aktualisieren ..   | 141 |

|   |     |
|---|-----|
| Abbildung 29: Ablauf: Bestandsnetzkonfigurationen aktualisieren.....                                | 142 |
| Abbildung 30: Ablauf: Aktualisierung der TSL über die TI-Plattform.....                             | 143 |
| Abbildung 31: Ablauf: Aktualisierung der BNetzA-VL über die TI-Plattform.....                       | 144 |
| Abbildung 32: Ablauf: Aktualisierung der CRL im Konnektor.....                                      | 145 |
| Abbildung 33: Ablauf: Initialisierung Trust Store.....  | 145 |
| Abbildung 34: Ablauf: Zertifikat prüfen .....   | 146 |
| Abbildung 35: Abfrage des Verzeichnisses durch Clientsysteme und Fachmodule.....                    | 147 |
| Abbildung 36: Ablauf: Namensauflösung .....   | 148 |
| Abbildung 37: Ablauf: Namensauflösung Internet .....  | 149 |
| Abbildung 38: Ablauf: Namensauflösung Bestandsnetz .....  | 150 |
| Abbildung 39: Ablauf: Zeitinformation abfragen.....   | 150 |
| Abbildung 40: Ablauf: Generische Kartenoperation.....   | 152 |
| Abbildung 41: Ablauf: Generische Kartenoperation mit MobKT.....                                     | 153 |
| Abbildung 42: Ablauf: Verify PIN direkt .....   | 154 |
| Abbildung 43: Ablauf: Verify PIN mit MobKT.....   | 155 |
| Abbildung 44: Ablauf: PIN-Eingabe mit Remote_PIN.....   | 156 |
| Abbildung 45: Ablauf: Aufbau eines sicheren Kanals zur Anbindung an die Zentrale TI-Plattform ..... | 157 |
| Abbildung 46: Ablauf: Aufbau eines sicheren Kanals zur Anbindung des sicheren Internetzugangs.....  | 158 |
| Abbildung 47: Informationsmodell der TI-Plattform .....   | 177 |

## **A4 – Tabellenverzeichnis**

|   |    |
|---|----|
| Tabelle 1: Kommunikationsmatrix TI (Zonen).....                                     | 17 |
| Tabelle 2: Zugriffsberechtigter Personenkreis (PK) nach §291a SGB V.....            | 21 |
| Tabelle 3: Personenkreis ohne Zugriffsberechtigung nach §291a SGB V .....           | 21 |
| Tabelle 4: Fachliche Rollen.....  | 22 |
| Tabelle 5: Betriebliche Rollen .....  | 22 |
| Tabelle 6: Technische Rollen.....   | 23 |
| Tabelle 7: Schnittstellen und Prozesse des Produkttyps eGK.....                     | 38 |
| Tabelle 8: Schnittstellen und Prozesse des Produkttyps HBA.....                     | 39 |
| Tabelle 9: Schnittstellen und Prozesse des Produkttyps SMC-B.....                   | 39 |
| Tabelle 10: Schnittstellen und Prozesse des Produkttyps HSM-B.....                  | 40 |
| Tabelle 11: Schnittstellen und Prozesse des Produkttyps gSMC-KT.....                | 41 |
| Tabelle 12: Schnittstellen und Prozesse des Produkttyps gSMC-K.....                 | 41 |
| Tabelle 13: Schnittstellen und Prozesse des Produkttyps eHealth-Kartenterminal..... | 42 |

|  |    |
|--|----|
| Tabelle 14: Schnittstellen und Prozesse des Produkttyps Mobiles Kartenterminal .....                 | 43 |
| Tabelle 15: Schnittstellen und Prozesse des Produkttyps Konnektor .....                              | 47 |
| Tabelle 16: Schnittstellen und Prozesse des Produkttyps Zentrales Netz TI .....                      | 50 |
| Tabelle 17: Schnittstellen und Prozesse des Produkttyps Zeitdienst.....                              | 51 |
| Tabelle 18: Schnittstellen und Prozesse des Produkttyps Namensdienst.....                            | 52 |
| Tabelle 19: Schnittstellen und Prozesse des Produkttyps Verzeichnisdienst .....                      | 53 |
| Tabelle 20: Schnittstellen und Prozesse des Produkttyps TSL-Dienst .....                             | 55 |
| Tabelle 21: Schnittstellen und Prozesse des Produkttyps Konfigurationsdienst .....                   | 57 |
| Tabelle 22: Schnittstellen und Prozesse des Produkttyps VPN-Zugangsdienst.....                       | 57 |
| Tabelle 23: Schnittstellen und Prozesse des Produkttyps Sicherheitsgateway<br>Bestandsnetze .....    | 59 |
| Tabelle 24: Schnittstellen und Prozesse des Produkttyps Trust Service Provider X.509<br>nonQES ..... | 60 |
| Tabelle 25: Schnittstellen und Prozesse des Produkttyps Trust Service Provider X.509<br>QES .....    | 61 |
| Tabelle 26: Schnittstellen und Prozesse des Produkttyps Trust Service Provider CVC...62              |    |
| Tabelle 27: Schnittstellen und Prozesse des Produkttyps CVC-Root.....                                | 62 |
| Tabelle 28: Schnittstellen und Prozesse des Produkttyps OCSP-Responder Proxy.....                    | 62 |
| Tabelle 29: Schnittstellen und Prozesse des Produkttyps Störungssampel .....                         | 63 |
| Tabelle 30: Legende zu den Abkürzungen in den Operationstabellen.....                                | 65 |
| Tabelle 31: Operation interact_with_User .....   | 65 |
| Tabelle 32: Operation sign_Document.....   | 66 |
| Tabelle 33: Operation verify_Document.....   | 66 |
| Tabelle 34: Operation external_Authenticate .....  | 67 |
| Tabelle 35: Operation get_Certificate.....   | 67 |
| Tabelle 36: Operation sign_Document_QES .....  | 68 |
| Tabelle 37: Operation verify_Document_QES .....  | 69 |
| Tabelle 38: Operation get_Ressource_List .....   | 71 |
| Tabelle 39: Operation get_Ressource_Information .....  | 71 |
| Tabelle 40: Operation notify .....   | 72 |
| Tabelle 41: Operation notify .....   | 73 |
| Tabelle 42: Operation register_for_Notifications .....   | 73 |
| Tabelle 43: Operation list_available_Updates .....   | 74 |
| Tabelle 44: Operation do_Update .....  | 74 |
| Tabelle 45: Operation do_local_Update .....  | 75 |
| Tabelle 46: Operation perform_Update.....  | 75 |
| Tabelle 47: Operation get_Card_Usage_Reference .....   | 76 |



|  |    |
|--|----|
| Tabelle 48: Operation discard_Card_Usage_Reference ..... | 76 |
| Tabelle 49: Operation handle_Session .....               | 77 |
| Tabelle 50: Operation verify_PIN .....                   | 77 |
| Tabelle 51: Operation unblock_PIN .....                  | 78 |
| Tabelle 52: Operation initialize_PIN .....               | 78 |
| Tabelle 53: Operation change_PIN .....                   | 79 |
| Tabelle 54: Operation get_PIN_Status .....               | 79 |
| Tabelle 55: Operation do_C2C .....                       | 79 |
| Tabelle 56: Operation send_Secure .....                  | 80 |
| Tabelle 57: Operation verify_Certificate .....           | 81 |
| Tabelle 58: Operation encrypt_Document .....             | 82 |
| Tabelle 59: Operation decrypt_Document .....             | 82 |
| Tabelle 60: Operation encrypt_Document_Symmetric .....   | 83 |
| Tabelle 61: Operation decrypt_Document_Symmetric .....   | 84 |
| Tabelle 62: Operation search_Directory .....             | 84 |
| Tabelle 63: Operation read_Data .....                    | 85 |
| Tabelle 64: Operation erase_Data .....                   | 85 |
| Tabelle 65: Operation write_Data .....                   | 85 |
| Tabelle 66: Operation get_Data .....                     | 86 |
| Tabelle 67: Operation put_Data .....                     | 86 |
| Tabelle 68: Operation get_Data .....                     | 87 |
| Tabelle 69: Operation put_Data .....                     | 87 |
| Tabelle 70: Operation show_Data .....                    | 87 |
| Tabelle 71: Operation type_Data .....                    | 88 |
| Tabelle 72: Operation print_Document .....               | 88 |
| Tabelle 73: Operation configure_MobKT .....              | 89 |
| Tabelle 74: Operation get_Service_Information .....      | 89 |
| Tabelle 75: Operation get_IP_Address .....               | 90 |
| Tabelle 76: Operation get_IP_Address .....               | 90 |
| Tabelle 77: Operation sync_Time .....                    | 91 |
| Tabelle 78: Operation get_Time .....                     | 91 |
| Tabelle 79: Operation set_System_Time .....              | 91 |
| Tabelle 80: Operation extract_card_data .....            | 92 |
| Tabelle 81: Operation read_Card_Data .....               | 92 |
| Tabelle 82: Operation read_KVK .....                     | 92 |
| Tabelle 83: Operation write_Card_Data .....              | 93 |

|   |     |
|---|-----|
| Tabelle 84: Operation verify_eGK .....                      | 93  |
| Tabelle 85: Operation write_eGK_Protocol .....              | 93  |
| Tabelle 86: Operation decrypt_Data .....                    | 94  |
| Tabelle 87: Operation sign_Data .....                       | 94  |
| Tabelle 88: Operation send_APDU .....                       | 94  |
| Tabelle 89: Operation do_Reset .....                        | 95  |
| Tabelle 90: Operation configure_KTs.....                    | 95  |
| Tabelle 91: Operation perform_Command .....                 | 96  |
| Tabelle 92: Operation transfer_APDU.....                    | 96  |
| Tabelle 93: Operation send_Data_TI .....                    | 97  |
| Tabelle 94: Operation send_Data_External .....              | 97  |
| Tabelle 95: Operation set_CS_Access_Mode.....               | 98  |
| Tabelle 96: Operation add_Clientsystem .....                | 98  |
| Tabelle 97: Operation remove_Clientsystem .....             | 98  |
| Tabelle 98: Operation list_Updates .....                    | 99  |
| Tabelle 99: Operation get_Updates .....                     | 99  |
| Tabelle 100: Operation send_Secure.....                     | 100 |
| Tabelle 101: Operation register.....                        | 100 |
| Tabelle 102: Operation deregister.....                      | 101 |
| Tabelle 103: Operation get_Status.....                      | 101 |
| Tabelle 104: Operation search_Directory.....                | 102 |
| Tabelle 105: Operation add_Directory_Entry .....            | 102 |
| Tabelle 106: Operation read_Directory_Entry .....           | 103 |
| Tabelle 107: Operation modify_Directory_Entry.....          | 103 |
| Tabelle 108: Operation delete_Directory_Entry.....          | 104 |
| Tabelle 109: Operation add_Directory_FA-Attributes .....    | 104 |
| Tabelle 110: Operation delete_Directory_FA-Attributes ..... | 105 |
| Tabelle 111: Operation modify_Directory_FA-Attributes ..... | 105 |
| Tabelle 112: Operation get_Service_Location .....           | 106 |
| Tabelle 113: Operation get_IP_Address .....                 | 106 |
| Tabelle 114: Operation get_FQDN.....                        | 106 |
| Tabelle 115: Operation check_Revocation_Status.....         | 107 |
| Tabelle 116: Operation download_TSL.....                    | 107 |
| Tabelle 117: Operation download_VL .....                    | 108 |
| Tabelle 118: Operation get_Hash .....                       | 108 |
| Tabelle 119: Operation provide_Certificate .....            | 108 |

|  |     |
|--|-----|
| Tabelle 120: Operation revoke_Certificate .....                          | 109 |
| Tabelle 121: Operation download_CRL .....                                | 109 |
| Tabelle 122: Operation sync_Time .....                                   | 110 |
| Tabelle 123: Operation update_Information .....                          | 110 |
| Tabelle 124: Operation update_Information .....                          | 111 |
| Tabelle 125: Operation get_Ext_Net_Config .....                          | 111 |
| Tabelle 126: Operation send_Data .....                                   | 112 |
| Tabelle 127: Operation send_secure_IP_Packet .....                       | 112 |
| Tabelle 128: Operation send_secure_IP_Internet .....                     | 113 |
| Tabelle 129: Operation send_IP_Packet .....                              | 113 |
| Tabelle 130: Schnittstelle P_Cert_Provisioning .....                     | 114 |
| Tabelle 131: Schnittstelle P_Cert_Revocation .....                       | 114 |
| Tabelle 132: Schnittstelle P_Trust_Approval .....                        | 114 |
| Tabelle 133: Schnittstelle P_Sub_CA_Certification_CVC .....              | 115 |
| Tabelle 134: Schnittstelle P_Sub_CA_Certification_X.509 .....            | 115 |
| Tabelle 135: Schnittstelle P_CVC_Provisioning .....                      | 115 |
| Tabelle 136: Schnittstelle P_DNS_Name_Entry_Announcement .....           | 116 |
| Tabelle 137: Schnittstelle P_DNS_Zone_Delegation .....                   | 116 |
| Tabelle 138: Schnittstelle P_DNSSEC_Key_Distribution .....               | 116 |
| Tabelle 139: Schnittstelle P_DNS_Service_Entry_Announcement .....        | 116 |
| Tabelle 140: Schnittstelle P_KSRS_Maintenance .....                      | 117 |
| Tabelle 141: Schnittstelle P_Directory_Maintenance .....                 | 117 |
| Tabelle 142: Schnittstelle P_Directory_Application_Registration .....    | 117 |
| Tabelle 143: Schnittstelle P_Directory_Administration_Registration ..... | 118 |
| Tabelle 144: Festlegungen zu Adressräumen .....                          | 127 |
| Tabelle 145: Festlegungen zu Namensräumen .....                          | 128 |
| Tabelle 146: Datentypen und ihre Bedeutung .....                         | 174 |

## 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.

| [Quelle]         | Herausgeber: Titel                                |
|------------------|---|
| [gemGlossar]     | gematik: Glossar der Telematikinfrastuktur        |
| [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             |

## A5.2 – Weitere Dokumente

| [Quelle]       | Herausgeber (Erscheinungsdatum): Titel  |
|----------------|---|
| [BSI-TR-03114] | BSI TR-03114 (22.10.2007)<br>Stapelsignatur mit dem Heilberufsausweis   |
| [BSI-SiGw]     | BSI (2005): Konzeption von Sicherheitsgateways,<br>Version 1.0<br><a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Konz_SiGw_pdf.pdf">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Konz_SiGw_pdf.pdf</a> |
| [ISO/IEC27001] | ISO/IEC 27001:2005<br>Specification for an Information Security Management System,<br>ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT<br>Security techniques  |
| [RFC6598]      | RFC6598 (April 2012): IANA-Reserved IPv4 Prefix for Shared Address Space<br><a href="http://tools.ietf.org/html/rfc6598">http://tools.ietf.org/html/rfc6598</a>   |
| [RFC2119]      | RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner,<br><a href="http://tools.ietf.org/html/rfc2109">http://tools.ietf.org/html/rfc2109</a>   |
| [RFC4007]      | RFC4007 (März 2005): IPv6 Scoped Address Architecture<br><a href="http://tools.ietf.org/html/rfc4007">http://tools.ietf.org/html/rfc4007</a>  |
| [SGB V]        | BGBI. I S.2477 (20.12.1988):<br>Sozialgesetzbuch, Fünftes Buch<br>Zuletzt geändert durch Art. 4 G v. 14.4.2010 I 410<br>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<br><a href="http://www.t7ev.org/themen/entwickler/common-pki-v20-spezifikation.html">http://www.t7ev.org/themen/entwickler/common-pki-v20-spezifikation.html</a>                               |
| [RFC2560]      | RFC 2560 (Juni 1999): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP<br><a href="http://tools.ietf.org/html/rfc2560">http://tools.ietf.org/html/rfc2560</a>   |

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

| Identitätsbezeichnung  | Verwendungszweck     | Zertifikatstyp | zugeordnete Karten / Sicherheitsmodule | fachliche / technische Rolle | Architekturschicht (Zone) | Herausgeber                           | Eingesetzt in                               |
|--|----------------------|----------------|--|------------------------------|---------------------------|---------------------------------------|---|
| <b>Krypto-Identitäten zu qualifizierten Zertifikaten für eGK und HBA</b> |                      |                |  |                              |                           |                                       |   |
| 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                      |
| <b>eGK</b>   |                      |                |  |                              |                           |                                       |   |
| 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                         |
| <b>HBA</b>   |                      |                |  |                              |                           |                                       |   |

| Identitätsbezeichnung      | Verwendungszweck         | Zertifikatstyp | zugeordnete Karten / Sicherheitsmodule | fachliche / technische Rolle   | Architekturschicht (Zone) | Herausgeber | Eingesetzt in                   |
|----------------------------|--------------------------|----------------|--|--|---------------------------|-------------|---------------------------------|
| 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         | ---                             |
| <b>SMC-B, HSM-B</b>        |                          |                |  |  |                           |             |                                 |
| ID.HCI.OSIG                | Institutions-Signatur    | X.509          | SMC-B, HSM-B                           | Leistungserbringer, Mitarbeiter<br>Gesellschafterorganisation oder<br>Mitarbeiter Kostenträger | TI-Plattform dezentral    | LEO, KTR    | Erstellung_Prüfung_Signatur     |
| ID.HCI.AUT                 | Authentisierung          | X.509          | SMC-B, HSM-B                           | Leistungserbringer, Mitarbeiter<br>Gesellschafterorganisation oder<br>Mitarbeiter Kostenträger | TI-Plattform dezentral    | LEO, KTR    | Komm_Transport                  |

| Identitätsbezeichnung        | Verwendungszweck         | Zertifikatstyp | zugeordnete Karten / Sicherheitsmodule | fachliche / technische Rolle   | Architekturschicht (Zone) | Herausgeber  | Eingesetzt in                   |
|------------------------------|--------------------------|----------------|--|--|---------------------------|--------------|---------------------------------|
| ID.HCI.ENC                   | Ver-/Entschlüsselung     | X.509          | SMC-B, HSM-B                           | Leistungserbringer, Mitarbeiter<br>Gesellschafterorganisation oder Mitarbeiter<br>Kostenträger | TI-Plattform dezentral    | LEO, KTR     | Verschlüsselung_Entschlüsselung |
| ID.SMC.AUTR_CVC              | Rollenauthentisierung    | CVC            | SMC-A/B, HSM-B                         | Leistungserbringer, Mitarbeiter<br>Gesellschafterorganisation oder Mitarbeiter<br>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<br>Gesellschafterorganisation oder Mitarbeiter<br>Kostenträger | ---                       | LEO, KTR     | ---                             |
| <b>Konnektor (inkl. SAK)</b> |                          |                |  |  |                           |              |                                 |
| 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          |

| Identitätsbezeichnung                    | Verwendungszweck                     | Zertifikatstyp | zugeordnete Karten / Sicherheitsmodule | fachliche / technische Rolle      | Architekturschicht (Zone) | Herausgeber                            | Eingesetzt in  |
|--|--------------------------------------|----------------|--|-----------------------------------|---------------------------|--|--|
| 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   |
| <b>Kartenterminal</b>                    |                                      |                |  |                                   |                           |  |  |
| ID.SMKT.AUT                              | Authentisierung                      | X.509          | gSMC-KT                                | TI-Plattform                      | TI-Plattform dezentral    | TI-Plattform                           | Kartentreischaftung<br>Kartennutzung<br>Kartenterminalverwaltung |
| ID.SMC.AUTD_RPS_C VC                     | Geräteauthentisierung                | CVC            | gSMC-KT                                | TI-Plattform                      | TI-Plattform dezentral    | TI-Plattform                           | Remote-PIN   |
| <b>Vertrauensraum der TI</b>             |                                      |                |  |                                   |                           |  |  |
| ID.TSL.SIG                               | Signatur                             | X.509          | HSM                                    | TI-Plattform                      | TI-Plattform zentral      | TI-Plattform                           | PKI  |
| <b>Fachanwendungsspezifische Dienste</b> |                                      |                |  |                                   |                           |  |  |
| ID.FD. TLS-C                             | Client-Authentisierung (Fachdienste) | X.509          | Keystore / Software-Token              | Fachanwendungsspezifischer Dienst | Provider                  | von gematik beauftragter Dienstleister | Dienst-zu-Dienst-Kommunikation                                   |



| Identitätsbezeichnung   | Verwendungszweck                            | Zertifikatstyp | zugeordnete Karten / Sicherheitsmodule | fachliche / technische Rolle      | Architekturschicht (Zone) | Herausgeber                            | Eingesetzt in   |
|-------------------------|---|----------------|--|-----------------------------------|---------------------------|--|---|
| 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 |
| <b>Zentrale Dienste</b> |   |                |  |                                   |                           |  |   |
| 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   |

## Anhang C – Datentypen der TI-Plattform

**Tabelle 146: 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 Ressourceldentifizier 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:<br>- SecuredOnly<br>- 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.  |

| Datentyp             | Bedeutung  |
|----------------------|--|
| DirectoryQuery       | Filter für eine Suchanfrage an den Verzeichnisdienst.  |
| DirectoryQueryResult | Antwort auf eine Suchanfrage an den Verzeichnisdienst.   |
| DocumentType         | Format des Documents<br>- PDF/A<br>- TEXT<br>- TIFF<br>- XML<br>- MIME<br>- Binär  |
| EncBinary            | Verschlüsselte Version von binären Anwendungsdaten   |
| EncDocumentType      | Verschlüsselte Version eines Dokuments vom Typ:<br>- PDF/A<br>- XML<br>- MIME<br>- 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   |
| MFMTType             | 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:<br>- 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,   |

| Datentyp               | Bedeutung   |
|------------------------|---|
|                        | <p>MobKT.<br/>         Enthält unter anderem:</p> <ul style="list-style-type: none"> <li>- Ressourceldentifizier</li> <li>- CardInfo</li> <li>- Status Online/Offline</li> <li>- Betriebszustand der Komponente (OK=Normal, Warnung=Admin-Interaktion sinnvoll, Kritisch=Fachlich eingeschränkt, Admin-Interaktion erforderlich)</li> <li>- verfügbaren technischen Zertifikate (zur Ermittlung der verbleibenden Gültigkeitsdauer)</li> <li>- Versionsinformationen</li> </ul> |
| Ressourceldentifizier  | Identifikator für ein Gerät oder einer Identität einer bestimmten Smartcard bestehend aus einer eindeutigen ID und einer Typkennung.  |
| RessourceList          | <p>Eine Liste von Elementen, je bestehend aus:</p> <ul style="list-style-type: none"> <li>- Ressourceldentifizier</li> <li>- RessourceName</li> <li>- RessourceType</li> </ul>  |
| 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     | <p>Signierte Version eines Dokuments vom Typ:</p> <ul style="list-style-type: none"> <li>- PDF/A</li> <li>- TEXT</li> <li>- TIFF</li> <li>- XML</li> <li>- MIME</li> <li>- Binär</li> </ul>   |
| SymmetricKey           | Symmetrischer Schlüssel   |
| Text                   | alphanumerische Zeichenkette  |
| Telematik_ID           | Identifikation eines Leistungserbringers oder einer Organisation des Gesundheitswesens  |
| TimeInformation        | aktuelle Zeitinformation vom NTP-Server (zentral).  |
| UpdateIdentifizier     | 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  |

## Anhang D – Informationsmodell der TI-Plattform

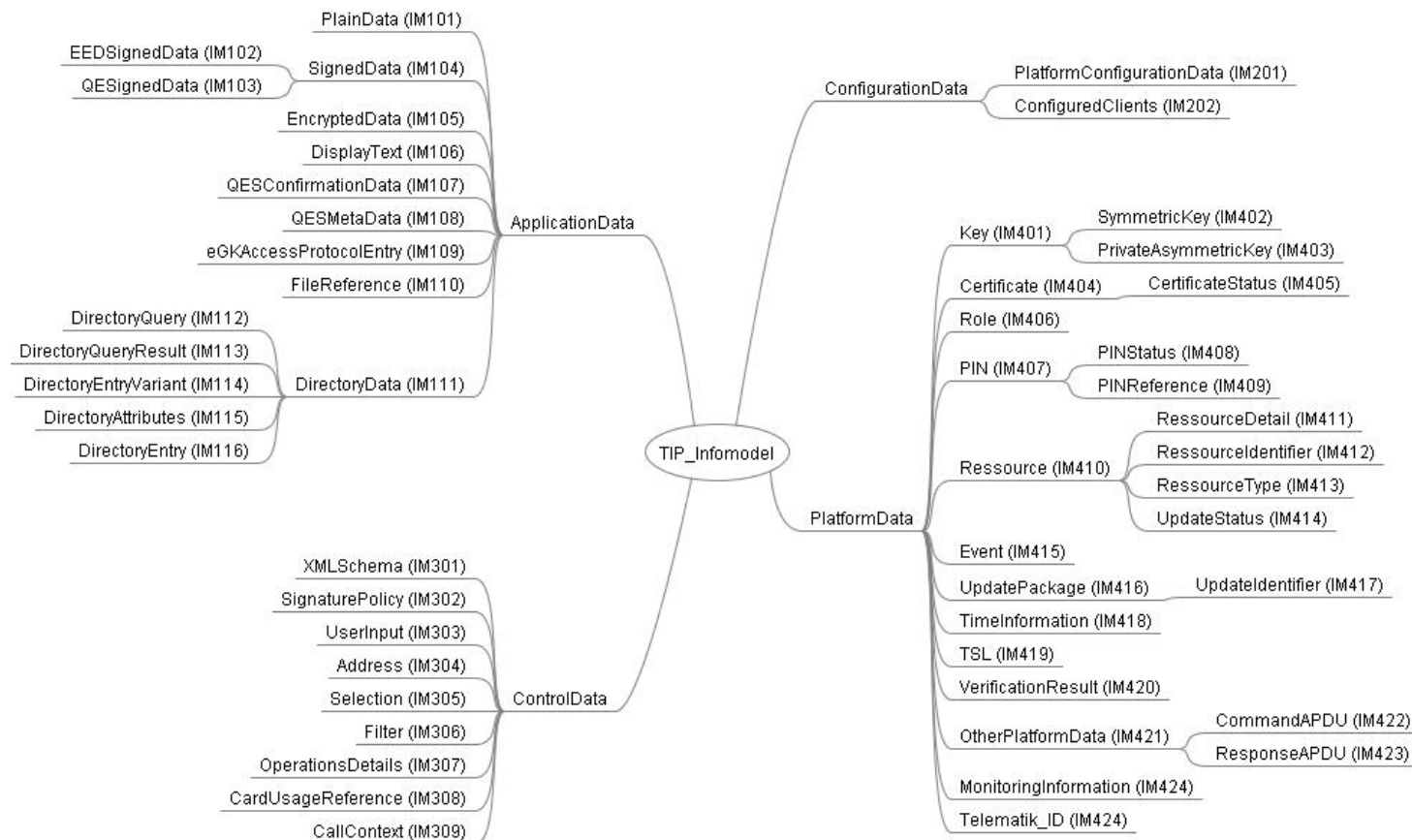


Abbildung 47: Informationsmodell der TI-Plattform