GESUNDHEITS· FOREN

Transplantationsregister

Technische Spezifikation - Neudatenübermittlung

Autor

Geschäftsstelle der Transplantationsregisterstelle

Datum

19. Oktober 2023

Version

1.12

Impressum

Gesundheitsforen Leipzig
Hainstraße 16 | 04109 Leipzig

vertreten durch die Geschäftsführung: Roland Nagel, Susanne Pollak und Axel Schmidt

Ansprechpartner
Martin Grohmann
+49 341 98988 350
office@transplantations-register.de
https://transplantations-register.de

Gesundheitsforen Leipzig GmbH

Hainstraße 16 | 04109 Leipzig
+49 341 98988 300
kontakt@gesundheitsforen.net
www.gesundheitsforen.net

Geschäftsführung:
Dipl.-Inf. (FH) Roland Nagel, Executive MBA (HSG)
M.A. Susanne Pollak
Dipl.-Wirtsch.-Inf. Axel Schmidt

Amtsgericht Leipzig HRB 25802 | USt-IdNr.: DE268809429 |
Bankverbindung: Sparkasse Leipzig | BIC: WELADE8L | IBAN: DE27 8605 5592 1100 9841 58

Dokumentenhistorie

Version	Datum	Änderungen
1.0	31.01.2019	Initiale Version
1.1	28.06.2019	Überarbeitungen der initialen Version
1.2	03.06.2020	Anpassung der Beschreibungen an neue BED-Struktur und Einführung XML-Verschlüsselung
1.3	26.06.2020	Anpassung an aktuellen Prozess Neudatenübermittlung
1.4	15.02.2021	Rückmeldung TPG-Auftraggeber vom 22.01.2021
1.5	01.06.2021	Neustrukturierung und Aktualisierung
1.6	30.06.2021	Versionsnummer referenzierte Dokumente aktualisiert, Layout Tabellen
1.7	14.07.2021	Anpassung XSD-Schema: Zusammenführung von Datenlieferungen, Bedingungen für IQTIG Datenexport; Anpassungen anhand Rückmeldung Auftraggeber
1.8	29.07.2021	Rückmeldung TPG-Auftraggeber vom 28.07.2021
1.9	08.09.2021	Rückmeldung TPG-Auftraggeber vom 07.09.2021
1.10	05.10.2021	Fehler- und Statuscodes der TxVST hinzugefügt
1.11	04.10.2022	Anpassung an neues Corporate Design
1.12	19.10.2023	Anpassung des Prozesses zur Überprüfung der Patienteneinwilligung

Referenzversionen

Dieses Dokument referiert auf folgende Dokumente und Versionen:

Dokument	Version	vom
Technische Spezifikation - Registerdatenbank	1.7	04.10.2022
Technische Spezifikation - Datenübermittlung durch das Tx-Register	1.8	04.10.2022
Verfahrensordnung	2.0	12.03.2021
Protokollierungskonzept	1.1	14.07.2021
Datenvalidierungskonzept	1.3	01.07.2020
Löschkonzept	1.2	27.07.2021

GESUNDHEITS· FOREN

Inhaltsverzeichnis

1 Abkürzungsverzeichnis

Abkürzung	Bezeichnung
BED	bundesweit einheitliche Datensatz
BED-DB	bundesweit einheitliche Datensatz-Datenbank
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
DIMDI	Deutsches Institut für Medizinische Dokumentation und Information
DSO	Deutsche Stiftung Organtransplantation
ET	Eurotransplant
GKV-Spitzenverband	Spitzenverband Bund der Krankenkassen
HTTP	Hypertext Transfer Protocol
ICD	International Classification of Diseases
IQTIG	Institut für Qualitätssicherung und Transparenz im Gesundheitswesen
OPS	Operationen- und Prozedurenschlüssel
PKI	Public-Key-Infrastruktur
REST-Schnittstelle	Representational State Transfer-Schnittstelle
TPG	Transplantationsgesetz
Tx-Register	Transplantationsregister
Tx-Registerstelle	Transplantationsregisterstelle
TxRegG	Transplantationsregistergesetz
TxVST	Vertrauensstelle des Transplantationsregisters
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
XML	Extensible Markup Language
XSD	XML-Schema-Definition

2 Einleitung

2.1 Einführung

Derzeit gibt es in Deutschland - im Gegensatz zu anderen Ländern wie beispielsweise den USA - keine zentrale Stelle, die Daten über Organspenden, Transplantationen, Spender und Empfänger bündelt. Bisher werden die Daten dezentral erhoben, organisiert und gespeichert. Mit dem Transplantationsregister (Tx-Register) werden erstmals medizinisch relevante Daten von verstorbenen Organspendern, Organempfängern und Lebendspendern zentral zusammengefasst und miteinander verknüpft.

Die Bundesregierung will mit der Änderung des Transplantationsgesetzs (TPGs), die am 01.11.2016 in Kraft trat, für mehr Patientensicherheit, Transparenz und Qualität in der Transplantationsmedizin sorgen. Das Tx-Register soll dazu beitragen, die erzielten Ergebnisse zu verbessern. Um möglichst rasch erste Erkenntnisse zu gewinnen, werden in der Aufbauphase auch Altdaten rückwirkend bis zum 1. Januar 2006 in das Register aufgenommen.

Zielsetzung des Projektes ist die Herstellung eines zentralen bundesweiten Tx-Registers, in dem transplantationsmedizinische Daten gespeichert werden. Diese Daten sollen nachfolgend genutzt werden, um wesentliche Erkenntnisse zu gewinnen, die zu einer Verbesserung und Weiterentwicklung der transplantationsmedizinischen Versorgung und zur Erhöhung der Transparenz führen. Die TPG-Auftraggeber sind der Spitzenverband Bund der Krankenkassen (GKV-Spitzenverband), die Bundesärztekammer und die Deutsche Krankenhausgesellschaft. Sie legen gemeinsam im Einvernehmen mit dem Verband der Privaten Krankenversicherung die im TPG vorgeschriebenen Verfahren für die Datenübermittlung fest.

Die Gesundheitsforen Leipzig GmbH ist von den TPG-Auftraggebern mit dem Führen des Tx-Registers beauftragt. Dieses Projekt beinhaltet den Aufbau und Betrieb des Tx-Registers und einer Geschäftsstelle sowie die Durchführung von Auswertungen und ein Berichtswesen. Für das Tx-Register wurden die zwei Stellen Vertrauensstelle des Transplantationsregisters (TxVST) (geführt durch die Firma Nortal AG sowie die Tx-Registerstelle (geführt durch die Gesundheitsforen Leipzig GmbH) eingerichtet.

Für die zentrale Speicherung und Zusammenführung der transplantationsmedizinischen Daten wird ein bundesweit einheitliche Datensatz (BED) entwickelt, welcher alle zur Verfügung stehenden Daten kombiniert. Die erste Version dieses Datensatzes (Altdaten) wird die Originaldaten unverändert aufnehmen, d.h. die Daten der Datenlieferanten werden nicht übersetzt oder vereinheitlicht. Eine Konsolidierung der Daten soll erst in den späteren Versionen erfolgen.

Das Projekt ist untergliedert in vier Stufen:

Stufe I

Zusammenführung der Altdaten der Datenlieferanten Deutsche Stiftung Organtransplantation (DSO), Eurotransplant (ET), Institut für Qualitätssicherung und Transparenz im Gesundheitswesen (IQTIG) aus den Jahren 2006 bis 2016

Stufe II
Initialisierung mit Neudaten der Datenlieferanten DSO, ET und IQTIG

Stufe III
Regelbetrieb mit Neudaten

Stufe IV
Weiterentwicklung des Regelbetriebs mit Neudaten

Im Tx-Register werden nur anonymisierte (Altdaten) bzw. pseudonymisierte Daten (Neudaten) abgespeichert. Die Anonymisierung und Pseudonymisierung wird durch die TxVST durchgeführt. Mittels geeigneter zweifacher Verschlüsselung erhält die TxVST keinen Einblick in die transplantationsmedizinischen Daten und die Tx-Registerstelle keinen Einblick in die unmittelbar personenbeziehbaren Daten.

2.2 Beteiligte Akteure

TPG-Auftraggeber
Die TPG-Auftraggeber sind die nach dem TPG beauftragten Organisationen der Selbstverwaltung zur konkreten Umsetzung von Aufgaben das Tx-Register betreffend. Die TPG-Auftraggeber sind die Selbstverwaltungspartner GKV-Spitzenverband, Deutsche Krankenhausgesellschaft und Bundesärztekammer.

Gesundheitsforen Leipzig GmbH
Die *Gesundheitsforen Leipzig GmbH* ist die von den TPG-Auftraggebern beauftragte Firma sowohl zum Aufbau und Betrieb der Tx-Registerstelle als auch der Geschäftsstelle. Zudem obliegen ihr die Durchführung von Datenvalidierungen und das Berichtswesen.

Nortal AG
Die *Nortal* AG ist die von den TPG-Auftraggebern beauftragte Firma zur Erstellung und zum Betrieb der TxVST. Ab Stufe II pseudonymisiert die TxVST unmittelbar personenbeziehbare Daten (im Weiteren als "patientenidentifizierende Daten" bezeichnet). Alle Daten werden von den Datenlieferanten verschlüsselt an die TxVST geliefert. Nach der Pseudonymisierung werden die Daten an die Tx-Registerstelle weitergeleitet, um dort gespeichert zu werden.

Deutsche Stiftung Organtransplantation
Die Koordinierungsstelle nach § 11 TPG *Deutsche Stiftung Organtransplantation* (DSO) „hat die Zusammenarbeit zur Organentnahme bei verstorbenen Spendern und die Durchführung aller bis zur Übertragung erforderlichen Maßnahmen [...] zu organisieren". Dadurch verfügt die DSO insbesondere über die wesentlichen Informationen zu postmortalen Spendern, deren gespendeten Organen sowie zur Organentnahme und zu deren Transport. Durch die DSO wird die sogenannte DSO-Kennnummer generiert, welche zur eindeutigen Identifikation von postmortalen Spendern genutzt wird. Die DSO liefert ab Stufe I Daten an das Tx-Register.

Eurotransplant
Die Vermittlungsstelle nach § 12 TPG *Eurotransplant (ET)* vermittelt zur Verfügung

stehende Organe an auf der Warteliste für ein Spenderorgan stehende Patienten. Dabei sind Organe nach den „Regeln, die dem Stand der Erkenntnisse der medizinischen Wissenschaft entsprechen, insbesondere nach Erfolgsaussicht und Dringlichkeit für geeignete Patienten“ zu vermitteln. ET generiert sowohl für Spender als auch Empfänger ET-Nummern zur eindeutigen Identifizierung. ET liefert ab Stufe I Daten an das Tx-Register.

G-BA und IQTIG

Das Institut für Qualitätssicherung und Transparenz im Gesundheitswesen (IQTIG) erarbeitet im Auftrag des Gemeinsamen Bundesausschusses (G-BA) Maßnahmen zur Qualitätssicherung und zur Darstellung der Versorgungsqualität im Gesundheitswesen und wirkt an deren Umsetzung mit. Im Rahmen dieses Auftrages erhält das IQTIG transplantationsmedizinische Daten von leistungserbringenden Krankenhäusern. Das IQTIG liefert ab Stufe I im Auftrag des G-BA Daten an das Tx-Register.

Transplantationszentren

In den *Transplantationszentren* (Tx-Zentren) werden die Organtransplantationen durchgeführt. Dafür werden in den Tx-Zentren die wesentlichen Daten zum Organempfänger, zum lebenden Organspender, zur Transplantation selbst und zu wesentlichen Teilen der Nachsorge erhoben. Diese Daten fließen primär zur Vermittlungsstelle ET sowie zum IQTIG und von dort zur Tx-Registerstelle. In späteren Stufen des Projektes können, wie im Gesetz vorgesehen, die Tx-Zentren auch selbständig Daten an das Tx-Register liefern.

Mit der Nachsorge betraute Einrichtungen und Ärzte

Damit sind alle ambulanten Leistungserbringer gemeint, die im Nachgang zu einer Transplantation die Organempfänger und lebenden Organspender parallel oder ergänzend zu den Tx-Zentren ambulant betreuen. In späteren Stufen des Projektes können, wie im Gesetz vorgesehen, diese Leistungserbringer selbständig Daten an das Tx-Register liefern.

Fachbeirat

Der *Fachbeirat* angesiedelt bei der Tx-Registerstelle und bestehend aus Vertretern der Datenlieferanten, der Deutschen Transplantationsgesellschaft (DTG), der Prüfungskommission und Überwachungskommission (PÜK) als auch maßgeblicher Patientenorganisationen wurde von den TPG-Auftraggebern vor Aufnahme der Tätigkeiten der Tx-Registerstelle eingerichtet. Der Fachbeirat ist an der Festlegung der Verfahrensordnungen beteiligt und verantwortet den Vorschlag des bundesweit einheitlichen Datensatzes (BED) inkl. dessen Fortschreibung. Ferner verfügt er über das Anhörungsrecht bei Anträgen auf Übermittlung pseudonymisierter Daten zu Forschungszwecken.

3 Struktur des Dokuments

3.1 Struktur der Teilspezifikation Neudatenübermittlung

Die Teilspezifikation behandelt folgende Kapitel:

- Gesamtprozess Datenlieferung
- Datenaktualisierung
- Datenlöschung
- Datensatz
- Lieferdateien
- Public-Key-Infrastruktur
- Tx-Registerstelle Schnittstellenbeschreibung
- Tx-Vertrauensstelle Schnittstellenbeschreibung
- Tx-Vertrauensstelle REST-Client

Das Dokument dient der adressatengerechten Beschreibung der Neudatenübermittlung an die Tx-Registerstelle. Damit sollen die am Datenfluss beteiligten Stellen bestmöglich unterstützt werden.

Die technischen Teilspezifikationen sind jeweils als lebendige Dokumente zu verstehen. Auf Basis der initialen Fassungen werden im Rahmen der Entwicklungs- und Verbesserungsarbeiten fortlaufend Inhalte ergänzt und erweitert. Anmerkungen von am Prozess beteiligten Akteuren werden ebenfalls in die Spezifikationen aufgenommen. Alle Versionen der technischen Teilspezifikationen werden chronologisch auf der Webseite `http://transplantations-register.de/` unter Servicedateien aufgelistet und zum Download zur Verfügung gestellt.

Inhaltlich wird maßgeblich auf die technische Umsetzung eingegangen. Von den kompakten Modellen werden mittels Top-Down-Darstellung die Erläuterungen detailliert beschrieben. Durch diese Top-Down-Herangehensweise erhält der Leser alle nötigen Informationen in aufeinander aufbauender Reihenfolge.

3.2 Leseanleitung

Diese technische Spezifikation folgt in ihrem Aufbau der Reihenfolge der zugrundeliegenden Prozesse. Zur Vereinfachung der Lesbarkeit sowie Zuordnung der Prozessverantwortlichkeiten sind für die folgenden Abschnitte die addressierten Zielgruppen angegeben. Dies ist in folgendem Beispiel zu erkennen.

Datenempfänger, Datenlieferanten, TxVST, Tx-Registerstelle

4 Gesamtprozess Datenlieferung

Datenlieferanten, TxVST, Tx-Registerstelle

Seit Änderung des § 15e TPG am 01.11.2016 ist die Einwilligung von in die Warteliste aufgenommenen Patienten, Organempfängern und Lebendspendern Voraussetzung, um Daten in das Tx-Register aufzunehmen. Daten, die gemäß § 15e (6) TPG zu neu erfassten und bereits bestehenden Fällen erhoben werden, werden als Neudaten bezeichnet. Eine zu Lebzeiten getroffene Entscheidung gegen die Erteilung der Einwilligung ist dabei auch über den Tod hinaus im Rahmen des postmortalen Persönlichkeitsrechts zu berücksichtigen. Die Einwilligung, die für einen Minderjährigen durch dessen Vertreter erteilt wurde, gilt auch beim Erreichen der Volljährigkeit bis zum Widerruf fort.

Dieses Kapitel beschreibt unter Angabe der technischen sowie formalen Beschränkungen die Prozesse und Unterprozesse, die bei der Neudatenübermittlung an die Tx-Registerstelle durchlaufen werden. Abbildung 4.1 zeigt den genannten Prozess und nennt die verantwortlichen Personen für die einzelnen Prozessschritte.

In Stufe II erfolgt die Initialisierung des Tx-Register mit den Neudaten des Erhebungszeitraumes vom 01.01.2017 bis 31.12.2020. Der Regelbetrieb (Stufe III) wird voraussichtlich im Jahr 2021 aufgenommen. Ab Stufe III erfolgen Lieferungen an die Tx-Registerstelle gemäß Verfahrensordnung einmal jährlich mit den erfassten Daten eines Erhebungsjahres. Die Übermittlung der Datensätze durch die Datenlieferanten muss dabei für ein Erhebungsjahr bis zum 31.03. des dem Erhebungsjahr folgenden Jahres an die Tx-Registerstelle erfolgen. Innerhalb der genannten Fristen können die Datenlieferanten auch beliebig oft Korrekturlieferungen bzw. Aktualisierungen vornehmen, die die jeweils zuvor getätigte Lieferung ersetzen. Von Seiten der Tx-Registerstelle wird keine Ablehnung von unterjährig gelieferten Daten vorgenommen. Die Tx-Registerstelle führt nach Datenannahme für jede Datenlieferung, wie in Abschnitt 5.2 beschrieben, eine Vollständigkeitsprüfung (Abgleich mit Extensible Markup Language (XML)-Schema) und eine Vollzähligkeitsprüfung (Abgleich mit Sollstatistik) durch. Für jede Datenlieferung wird ein strukturiertes Ergebnis- bzw. Fehlerprotokoll bereit gestellt (siehe Abschnitt B.3.4.5). Darüber hinaus stellt die Tx-Registerstelle, wie ebenfalls in Abschnitt 5.2 beschrieben, spätestens vier Wochen nach Ende des jeweiligen Übermittlungszeitraums ein Datenvalidierungsprotokoll zur Verfügung, das Ergebnisse der Prüfungen auf Vollzähligkeit, Vollständigkeit und der Plausibilisierung des gesamten Datenbestandes enthält. Das Datenvalidierungsprotokoll kann ggf. eine Forderung nach einer Korrekturlieferung durch die Datenlieferanten, die gemäß dem Prozess der Datenaktualisierung (siehe Kapitel 6) erfolgt, enthalten. Die Frist für Korrekturlieferungen (Berichtigungen und Ergänzungen) durch den entsprechenden Datenlieferanten beträgt zwei Kalendermonaten nach Verfügbarkeit des Datenvalidierungsprotokolls.

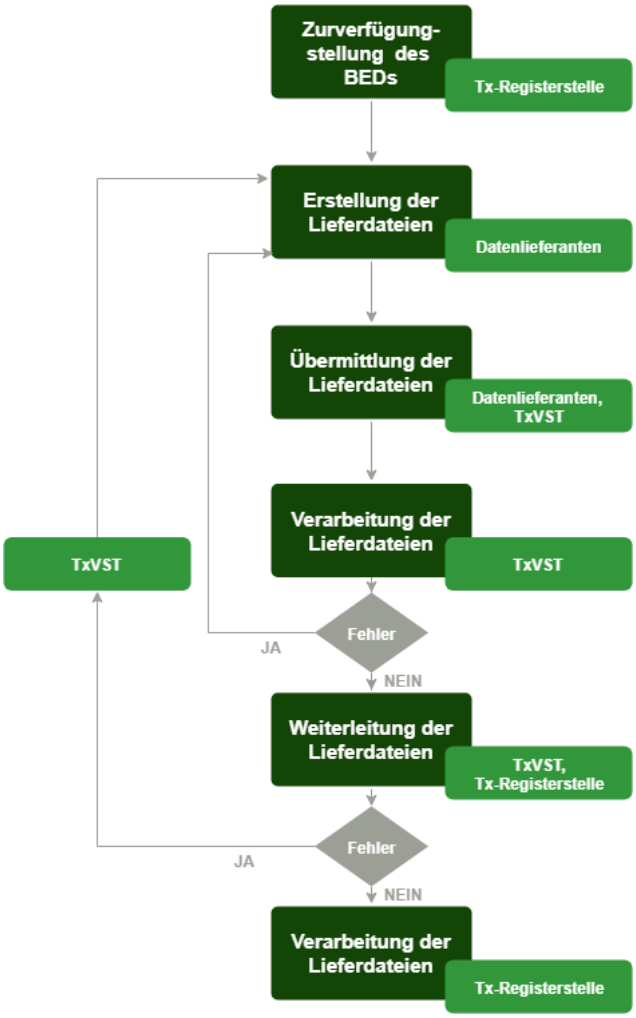


Abbildung 4.1: Prozessschritte der Neudatenübermittlung an die Tx-Registerstelle mit Angabe der verantwortlichen Institutionen.

4.1 Zurverfügungstellung des BEDs

Gemäß §15d (2) TPG wird der zu liefernde Datensatz an das Tx-Register vom Fachbeirat erstellt und von den TPG-Auftraggebern einvernehmlich mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) als fachliche Vorgabe festgelegt. Die jeweils aktuell gültige Version des BED wird im Bundesanzeiger veröffentlicht.

Die Tx-Registerstelle stellt den Datenlieferanten und der TxVST die technische Darstellung des Datensatzes anhand dreier Repräsentationsformen zur Verfügung:

- Datensatz-Portal der Gesundheitsforen Leipzig GmbH
- Datensatzbeschreibung im PDF-Format
- XML-Schema-Definition (XSD)

Eine genauere Beschreibung der technischen Darstellungsformen des Datensatzes folgt in Abschnitt 8.2. Mittels dieser Technologien und Dateien können die Datenlieferanten eine schemakonforme und fachlich korrekte Erstellung der Lieferdateien umsetzen.

4.2 Erstellung der Lieferdateien durch die Datenlieferanten

Lieferdateien werden von den Datenlieferanten (aktuell IQTIG, DSO, ET) erzeugt und mittels eines seriellen Verfahrens innerhalb der in der Verfahrensordnung festgelegten und oben genannten Lieferfrist über die TxVST an die Tx-Registerstelle weitergeleitet. Die Datenlieferungen für die Initialisierung des Tx-Registers mit Neudaten beziehen sich auf den Zeitraum 01.01.2017 bis 31.12.2020. Der Export und die Übermittlung der Lieferdateien erfolgt im XML-Format und auf Basis des BEDs. Den Datenlieferanten obliegt dabei die korrekte technische Umsetzung der XML-Dateien sowie der zu übermittelnden Datenzeiträume. Datenlieferung ab Berichtsjahr 2021 erfolgen Jahresweise bzw. bei Bedarf auch unterjährig.

4.2.1 Export der Lieferdateien und Mapping auf den BED

Die Daten für die Neudatenübermittlung sind von den Datenlieferanten aus den eigenen Datenbeständen (z. B. Datenbank) zu exportieren. Welche Daten von den jeweiligen Datenlieferanten zu extrahieren und zu übermitteln sind, ist durch die Definition von Teildatensätzen im BED geregelt.

Gemäß § 15e (6) TPG fallen unter die Neudaten alle Daten, die ab dem 01.01.2017 zu postmortalen Spendern sowie in die Warteliste aufgenommenen Patienten, Organempfängern und Lebendspendern, deren eindeutige Einwilligung vorliegt, erhoben wurden. Folglich sind die Neudaten von den Altdaten über das Datum (01.01.2017) und das verpflichtende Einwilligungskennzeichen für Patienten, Organempfänger und lebende Organspender abzugrenzen. Für die Erstellung der Lieferdatei werden die Daten anhand dieser Kriterien gefiltert. Für die Datumsangabe verwenden die jeweiligen Datenlieferanten folgende Datenfelder:

IQTIG

- **AUFNDATUM** bzw. **FUERHEBDATUM** nicht vor 01.01.2017

ET

- **Date of Transplant** nicht vor 01.01.2017 oder
- **Date put on waiting list** nicht vor 01.01.2017

DSO

- **Entnahme am** nicht vor 01.01.2017

Des Weiteren ist von den Datenlieferanten in ihren Filtern zu berücksichtigen, dass bei einer EU-Vermittlung mindestens eine der unten genannten Bedingungen erfüllt sein muss, damit Daten mit den Lieferdateien exportiert werden:

- Postmortemspender aus Deutschland und/oder
- Lebendspender aus Deutschland (inkl. Follow Up) und/oder
- Transplantation in Deutschland und/oder

- Empfänger aus Deutschland (inkl. Follow Up)

Die Exportdaten sind von den Datenlieferanten auf den BED abzubilden. Von der Tx-Registerstelle wird hierfür eine XSD zur Verfügung gestellt, die das technisch verpflichtende Mapping enthält. Mit der XSD kann strukturiert durch Implementation eines Algorithmus ein automatisiertes Mapping seitens der Datenlieferanten durchgeführt und die Einhaltung der XML-Struktur sowie der Datentypen geprüft werden. Die Prüfung der Wohlgeformtheit der XML-Dateien unterliegt der Verantwortung der Datenlieferanten und wird nicht von der Tx-Registerstelle durch Hilfsmittel unterstützt.

Anhand eines Auszugs aus der Datensatzbeschreibung im PDF-Format, die aus der XSD generiert wird, soll das Mapping der Datenfelder der Datenlieferanten auf die Felder des BED veranschaulicht werden. Abbildung 4.2 zeigt einen Ausschnitt der Datensatzbeschreibung in Tabellenform. Die Spalte `Quellvariablenname` gibt den (falls vorhanden) Tabellennamen bzw. das Modul und den Variablennamen in der Form an, wie diese bei den Datenlieferanten vorliegen. Die Spalte `Elementname` gibt den Namen des Datenfeldes im BED an. Die Daten aus dem Element der Spalte `Quellvariablenname` sind von den Datenlieferanten auf das Element der Spalte `Elementname` des BEDs zu mappen.

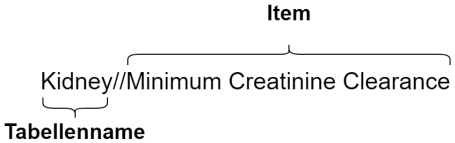
Elementname	Beschreibung	Häufigkeit	Inhalt/Form	Quellvariablenname	Hinweis
E_Basisdaten_Blutgruppe_IQTIG	Blutgruppe	1	Auswahlliste: "A", "B", "0", "AB"	HTXM:B//BLUTGRUPPE , LUTX:B//BLUTGRUPPETX , PNTX:B//BLUTGRUPPETX	

Abbildung 4.2: Spaltenangaben der Datensatzbeschreibung

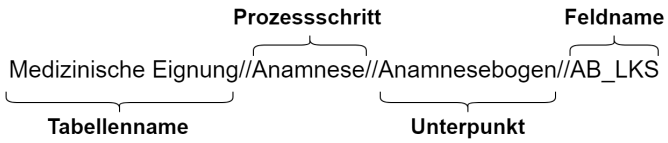
Im Folgenden wird für die jeweiligen Datenlieferanten die Zusammensetzung des Quellvariablennamens dargestellt. Anhand eines Beispiels wird gekennzeichnet, aus welchen Modulen bzw. Tabellennamen und Feldern der Datenlieferanten die Daten stammen. Der Quellvariablenname setzt sich für die jeweiligen Datenlieferanten wie folgt zusammen:

IQTIG

ET



DSO



Der folgende Codeausschnitt zeigt, wie das technisch verpflichtende Mapping in der XSD, die von den Datenlieferanten zum Mapping der Datenfelder auf die des BEDs zu verwenden ist, umgesetzt wird. Unter dem Attribut „`variable_name`“ ist der Quellvariablenname zu der entsprechenden Variable hinterlegt. Des Weiteren sind zu jedem Element des BEDs der Datentyp unter `type` und die Beschreibung der Variable unter „`variable_description`“ hinterlegt.

```
...
<xs:element name="Patientenidentifizierende_Daten">
  <xs:complexType>
    <xs:sequence>
      <xs:element minOccurs="0" name="P_EmpfaengerNummerET_ET" type="
          ↪ et_nummer_type">
        <xs:annotation>
          <xs:documentation>Empfänger ET-Nummer. Identifikationsnummer des
              ↪ Empfängers durch ET vergeben.</xs:documentation>
          <xs:documentation source="variable_name">General//Recipient Number</
              ↪ xs:documentation>
          <xs:documentation source="variable_description">Recipient Number</
              ↪ xs:documentation>
          <xs:appinfo source="isUniqueKey">true</xs:appinfo>
          <xs:appinfo source="shortName">PIdEmpfaengerNrETET</xs:appinfo>
        </xs:annotation>
      </xs:element>
      <xs:element minOccurs="0" name="P_SpenderNummerET_IQTIG" type="
          ↪ et_nummer_type">
        <xs:annotation>
          <xs:documentation>Spender ET-Nummer. Identifikationsnummer des Spenders
              ↪  durch ET vergeben</xs:documentation>
          <xs:documentation source="variable_name">LLSFU:B//IDSPENDER , NLSFU:B//
              ↪ IDSPENDER , LLS:B//IDSPENDER , LUTX:T//IDSPENDER , LLS:B//
              ↪ IDSPENDER , NLS:B//IDSPENDER , HTXM:T//IDSPENDER , PNTX:T//
              ↪ IDSPENDER</xs:documentation>
          <xs:documentation source="variable_description">Spender ID</
              ↪ xs:documentation>
          <xs:appinfo source="isUniqueKey">true</xs:appinfo>
          <xs:appinfo source="shortName">PIdSpenderNrETIQTIG</xs:appinfo>
        </xs:annotation>
      </xs:element>
      <xs:element minOccurs="0" name="P_DSOKennnummer_DSO" type="dso_nummer_type"
          ↪ >
        <xs:annotation>
```

```
            <xs:documentation>DSO Spender Kennnummer</xs:documentation>
            <xs:documentation source="variable_name">Basisdaten//Identifikation//
                ↪ DSO-KennNummer</xs:documentation>
            <xs:documentation source="variable_description">DSO Spender Kennnummer<
                ↪ /xs:documentation>
            <xs:appinfo source="isUniqueKey">true</xs:appinfo>
            <xs:appinfo source="shortName">PIdDSOKennnummerDSO</xs:appinfo>
              </xs:annotation>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
</xs:element>
...
```

4.2.2 Erstellung der Sollstatistik

Neben der XML-Lieferdatei sind die Datenlieferanten damit beauftragt, quantitative Angaben über die übermittelten Datensätze je Elementliste mitzuliefern. Diese sind in einer Sollstatistik (siehe Abschnitt 9.4) als Teil der Lieferdatei zu erfassen. Die Vorlage zur Erzeugung der Statistik ist in der XSD-Datei unter dem Element `<xs:element name="Sollstatistik">` enthalten.

4.2.3 Verschlüsselung der Lieferdatei

Vor der Weiterleitung der erfolgreich erstellten Lieferdatei an die TxVST ist eine XML-Verschlüsselung durch die Datenlieferanten vorzunehmen. Die Übermittlung selbst erfolgt ebenfalls verschlüsselt. Siehe dazu Anhang B.5 und Anhang B.4.

Für die XML-Verschlüsselung betreibt die Tx-Registerstelle eine Public-Key-Infrastruktur (PKI), die in Kapitel 10 beschrieben ist. Über eine PKI-Webanwendung sind die Public-Key-Zertifikate der Kommunikationspartner, die den öffentlichen Schlüssel beinhalten, herunterzuladen. Die Datenlieferanten müssen vor jeder Verschlüsselung prüfen, ob mit einem gültigen Zertifikat gearbeitet wird und ggf. ein aktuelles Zertifikat herunterladen.

Es ist eine getrennte Verschlüsselung der transplantationsmedizinischen und der patientenidentifizierenden Datenbereiche mit dem jeweiligen öffentlichen Schlüssel der autorisierten Datenempfänger vorzunehmen. Hierzu benötigen die Datenlieferanten die Public-Key-Zertifikate der TxVST und der Tx-Registerstelle.

Im Rahmen der Neudatenübermittlung darf der TxVST zu keiner Zeit Einblick in die transplantationsmedizinischen Daten möglich sein und der Tx-Registerstelle dürfen nur transplantationsmedizinische Daten sowie durch die TxVST pseudonymisierte patientenidentifizierende Daten vorliegen. Daher müssen die transplantationsmedizinischen Daten mit dem öffentlichen Schlüssel der Tx-Registerstelle und die patientenidentifizierenden Daten mit dem öffentlichen Schlüssel der TxVST verschlüsselt werden.

Die Verantwortung zur korrekten Verschlüsselung der Datenblöcke liegt bei den Datenlieferanten.

4.3 Übermittlung der Lieferdateien an die Tx-Vertrauensstelle

Für die Übermittlung der XML-Lieferdateien stehen von Seiten der TxVST zwei Optionen zur Verfügung. Zum einen direkt über die Representational State Transfer-Schnittstelle (REST-Schnittstelle) (siehe Anhang B.4), über die XML-Daten serialisiert per HTTPS übertragen werden können. Darüberhinaus biete die TxVST einen REST-Client (siehe Anhang B.5) an, mittels dem verschlüsselte XML-Lieferdateien von den Datenlieferanten an die TxVST übertragen werden können.

4.4 Verarbeitung der Lieferdateien durch die Tx-Vertrauensstelle

Die TxVST ist nur temporär im Besitz der über die REST-Schnittstelle entgegengenommenen Lieferdateien. Nach Abschluss der Verarbeitungs- und Prüfschritte sind die übermittelten Dateien zu löschen.

4.4.1 Überprüfung Patienteneinwilligung

Der TxVST obliegt unter anderem eine Prüfung der Einwilligungskennzeichen und der formalen Korrektheit der unmittelbar personenbeziehbaren Datenfelder. Die Überprüfung der Einwilligungskennzeichen wird nach der Entschlüsselung der Datenfelder mit dem privaten Schlüssel der TxVST durchgeführt. Fehlt ein Einwilligungskennzeichen nach § 15e (6) TPG oder schlägt die Entschlüsselung fehl, wird der patientenidentifizierende sowie der medizinische Datenbereich aus der Lieferdatei entfernt und stattdessen das XML-Datenfeld `Datenschutz` eingefügt. Die Datenlieferanten erhalten anschließend eine entsprechende Fehlermeldung. Treten keine Fehler auf, erfolgt die formale Validierung der DSO- Kennnummern, der ET -Empfängernummern und der ET- Spendernummern (beispielsweise eine Überprüfung der Feldlänge und gültiger Zeichen).

4.4.2 Pseudonymisierung

Um eine datenschutzkonforme Verarbeitung der Lieferdateien im Tx-Register zu gewährleisten, ist die TxVST für die Pseudonymisierung der unmittelbar personenbeziehbaren Daten zuständig. Dabei sind die ET- Spendernummern, die ET- Empfängernummern, die ET- Transplantationsnummern sowie die DSO- Kennnummern zu pseudonymisieren. Die Pseudonyme werden deterministisch erzeugt und liefern somit ein konstantes Ergebnis, d. h. gleiche Nummern führen zum selben Pseudonym.

4.4.3 XML-Verschlüsselung

Vor der Weiterleitung der Lieferdatei an die Tx-Registerstelle ist eine XML-Verschlüsselung der personenbeziehbaren Felder vorzunehmen. Hierzu benötigt die TxVST das Public-

Key-Zertifikat der Tx-Registerstelle. Das Zertifikat kann über die PKI-Webanwendung unter der Ansicht *Schlüsselverwaltung* heruntergeladen werden (siehe Kapitel 10).

Die Zertifizierung der öffentlichen Schlüssel der Kommunikationspartner über die PKI ist Voraussetzung für eine sichere Kommunikation. Die TxVST unterliegt der Verantwortung vor jeder XML-Verschlüsselung zu prüfen, ob das gültige Public-Key-Zertifikat verwendet wird.

4.5 Weiterleitung der Lieferdateien an die Tx-Registerstelle

Die verschlüsselten Pseudonyme sind mit den ungelesenen transplantationsmedizinischen Daten an die Tx-Registerstelle über eine REST-Schnittstelle weiterzuleiten. Die REST-Schnittstelle ist nur für den IP-Adressbereich der TxVST und die zugewiesenen Authentifizierungsdaten freigeschaltet.

Die XML-Lieferdatei inklusive der von den Datenlieferanten erzeugten Sollstatistik werden im Body des Hypertext Transfer Protocol (HTTP) POST Requests übermittelt. Eine genauere Beschreibung befindet sich in der Schnittstellenspezifikation in Anhang B.3. Die Verarbeitung der Lieferdatei bei der Tx-Registerstelle wird im folgenden Kapitel 5 beschrieben.

5 Datenannahme

Datenlieferanten, TxVST

Die Annahme der Lieferdateien erfolgt über eine REST-Schnittstelle, die ausschließlich für den IP-Adressbereich der TxVST freigeschalten und authentifizierte Kommunikationspartner zugänglich ist. Mit Upload der Lieferdateien per HTTP POST Request durch die TxVST werden die in Abbildung 5.1 dargestellten Verarbeitungs- und Validierungsschritte initiiert. Jede ausgeführte Operation wird in der Log-Datenbank gemäß Protokollierungskonzept erfasst und Fehler- bzw. Erfolgsmeldungen in Form von Ergebnisprotokollen zum Abruf über die REST-Schnittstelle bereit erstellt. Die einzelnen Prozessschritte werden im Folgenden beschrieben.

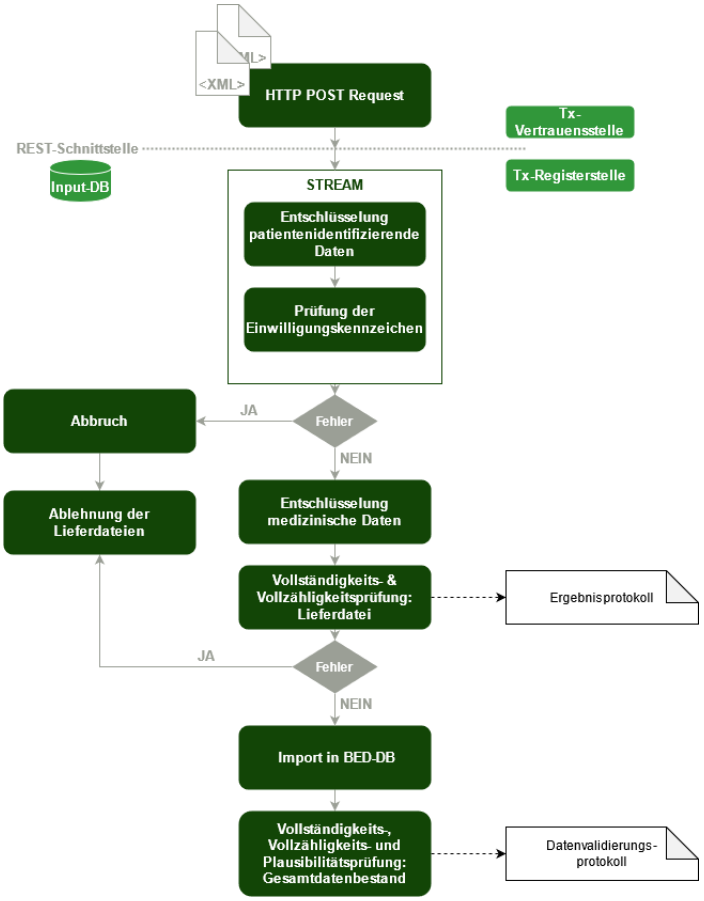


Abbildung 5.1: Verarbeitungsschritte, die von der Tx-Registerstelle nach der Datenübermittlung durch die TxVST durchgeführt werden.

5.1 Überprüfung Patienteneinwilligung

Die übermittelte Lieferdatei wird vor dem Datenimport auf das Vorhandensein des Einwilligungskennzeichens geprüft. Hierfür wird der von der TxVST pseudonymisierte und verschlüsselte patientenidentifizierende Datenblock mit dem privaten Schlüssel der Tx-Registerstelle entschlüsselt und die gemäß § 15e (6) TPG geforderte Einwilligung der in die Warteliste aufgenommenen Patienten, Organempfänger und Lebendspender überprüft. Die Prüfung betrifft die Elemente `Empfaenger` und `Lebendspender`. Die Einwilligung ist in der XSD über das Attribut `einwilligung` gekennzeichnet.

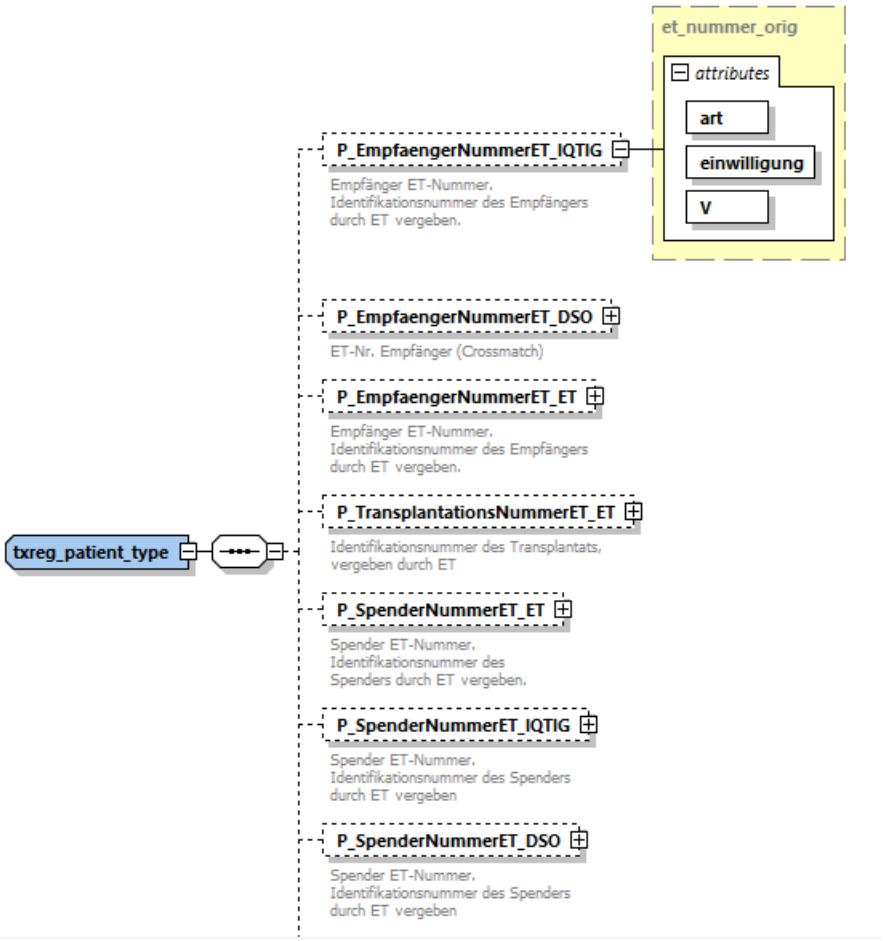


Abbildung 5.2: XSD: Patientenidentifizierende Daten und Attribut Einwilligung

Das Attribut `einwilligung` kann dabei drei Zustände einnehmen: `J, N, X`.

```
<xs:simpleType name="enum_et_einwilligung_type">
<xs:restriction base="xs:string">
<xs:enumeration value="J">
<xs:annotation>
<xs:documentation>Einwilligung vorliegend</xs:documentation>
</xs:annotation>
</xs:enumeration>
<xs:enumeration value="N">
<xs:annotation>
```

```
<xs:documentation>Einwilligung nicht vorliegend</xs:documentation>
</xs:annotation>
</xs:enumeration>
<xs:enumeration value="X">
<xs:annotation>
<xs:documentation>Einwilligung nicht erforderlich</xs:documentation>
</xs:annotation>
</xs:enumeration>
</xs:restriction>
</xs:simpleType>
```

Im Falle der Abwesenheit eines Kennzeichens oder eines negativen Eintrags (*Einwilligung nicht vorliegend*), wird der Vorgang abgebrochen und die Datenlieferung abgelehnt. Dies gilt auch, wenn die Entschlüsselung des patientenidentifizierenden Datenblocks fehlschlägt. Bei einer fehlerfreien Prüfung werden die vollständig abgearbeiteten Fragmente der XML-Lieferdatei in die Input-Datenbank (Input-DB) übertragen. Mit dem letzten Schritt gilt die Datenlieferung als angenommen. Informationen zu Erfolg und Misserfolg werden als HTTP-Status zurückgegeben.

Im Zuge der Datenannahme wird automatisch ein eindeutiger Universally Unique Identifier (UUID), der in diesem Kontext als Transaktions-ID bezeichnet wird, generiert. UUIDs sind 16-Byte-Zahlen der Form □□□□□□□□–□□□□–□□□□–□□□□–□□□□□□□□□□□□, die im Hexadezimalsystem dargestellt werden und folglich mit Zahlen von 0-9 oder Buchstaben von a-f gefüllt sind.

Beispiel: 10c2c9e7-8d8c-4446-b955-643e59e707b0

Die Transaktions-ID dient der Kommunikation mit der TxVST. Mit dieser ist die Referenzierung auf spezifische Datenlieferungen möglich. Die TxVST erhält die Transaktions-ID inklusive des Zeitstempels des Liefereingangs im Header der HTTP Response über die REST-Schnittstelle. Mit der Transaktions-ID kann der Verarbeitungsstatus sowie das Ergebnisprotokoll der Datenlieferung als HTTP Request über die REST-Schnittstelle abgefragt werden (siehe Anhang B.3).

5.2 Validitätsprüfung und Datenübertragung in die BED-Datenbank

Nach der initialen Kontrolle der Einwilligungskennzeichen bei der Datenannahme wird der medizinische Datenblock mit dem privaten Schlüssel der Tx-Registerstelle entschlüsselt. Die Daten liegen zu diesem Zeitpunkt in Rohform als Bytearray in der Input-Datenbank (Input-DB) des Tx-Registers vor. Jeder Eintrag in der Datenbank ist eine Datenlieferung bestehend aus der Datei selbst, der Transaktions-ID und dem Zeitstempel des Liefereingangs.

Gemäß Datenvalidierungskonzept der Tx-Registerstelle führt die Tx-Registerstelle für jede individuelle Datenlieferung, wie in den folgenden Abschnitten dargestellt, Validitätsprüfungen durch. Dies umfasst eine Vollständigkeitsprüfung (Abgleich mit XML-Schema)

und eine Vollzähligkeitsprüfung (Abgleich übermittelter Datenfelder mit Sollstatistik), die erneut zur Ablehnung der Lieferdatei führen können. Abgelehnte Lieferungen werden aus der Input-Datenbank (Input-DB) gelöscht. Alle Erfolgs- und Fehlermeldungen, die während der Prüfungen generiert werden, werden unter dem Eintrag der spezifischen Datenlieferung (Transaktions-ID) in der Input-Datenbank (Input-DB) abgelegt. Wie oben beschrieben, können diese in Form eines Ergebnisprotokolls für jede Datenlieferung von der TxVST über die REST-Schnittstelle abgefragt werden (siehe Anhang B.3).

Die angenommenen Daten werden in die Struktur des BED transformiert und in der bundesweit einheitliche Datensatz-Datenbank (BED-DB) gespeichert. Um bei Fehlern während des Beladeprozesses die Integrität der BED-Datenbank nicht zu gefährden, wird vorher ein Abbild der BED-DB erstellt und auf dieser Kopie gearbeitet. Das Abbild, das als Spiegel-Datenbank bezeichnet wird, läuft in einer eigenen Docker-Umgebung und ist dadurch von den anderen Systemen getrennt. Die BED-DB ist als MySQL-Datenbank aufgebaut. Die Länge von Objektnamen in MySQL ist begrenzt. Daher werden beim Import der Lieferdaten in die BED-DB über eine Anzahl von Regeln aus den teilweise relativ langen Variablennamen shortnames erzeugt (siehe Anhang B.2). Die Umwandlung verläuft automatisiert. Bei den Regeln für die Erzeugung wurde darauf geachtet, dass der Variablenname zwar verkürzt wird, aber trotzdem lesbar bleibt. Damit die Datenempfänger ohne Mehraufwand die Exportdatei in eine eigene MySQL-Datenbank übertragen können, bleiben die shortnames in den Exportdaten erhalten. Zusätzlich wird eine .csv-Datei zur Verfügung gestellt, die die entsprechenden langen Variablennamen auflistet.

Nach Ende jedes Übermittlungszeitraums führt die Tx-Registerstelle auf dem gesamten Datenbestand weitere Validitätsprüfungen durch. Diese umfassen weitere Vollständigkeits-, Vollzähligkeits- und Plausibilitätsprüfungen, die in den folgenden Abschnitten genannt werden und im Datenvalidierungskonzept der Tx-Registerstelle detailliert beschrieben sind. Die Ergebnisse der Validitätsprüfungen werden in Form eines Datenvalidierungsprotokolls bis spätestens vier Wochen nach Ende des Übermittlungszeitraums durch die Tx-Registerstelle zur Verfügung gestellt.

Alle Operationen innerhalb der Registerdatenbank werden detailliert protokolliert. Dafür werden Statusmeldungen der Prozessschritte ohne Angabe personenidentifizierbarer Daten in der Log-DB gespeichert.

5.2.1 Vollständigkeitsprüfung

Jede Lieferdatei wird gegen das XML-Schema geprüft. Das Ergebnis der Schemaprüfung wird zusammen mit der Referenz zur Transaktions-ID in der Input-Datenbank abgelegt. Fehlerhafte Schemata werden von der Tx-Registerstelle abgelehnt und initiieren eine erneute Iteration des Gesamtprozesses. Informationen zu Schemafehlern, wie auch Erfolgsmeldungen, sind Teil des Ergebnisprotokolls. Darüber hinaus werden im Rahmen der Validitätsprüfungen auf dem gesamten Datenbestand am Ende jeden Übermittlungszeitraums Befüllungsgrade für die einzelnen Datenfelder berechnet und im Datenvalidierungsprotokoll bereitgestellt.

5.2.2 Vollzähligkeitsprüfung

Nicht vollzählige Datenlieferungen sollen durch den Abgleich mit der Sollstatistik, die von jedem Datenlieferanten mitzuliefern ist, vermieden werden. Hierfür bestimmt die Tx-Registerstelle die Anzahl der Elemente jeder Lieferdatei, die anschließend mit der in der Sollstatistik ausgewiesenen Anzahl abgeglichen wird. Informationen zu nicht vollzähligen Lieferdateien, wie auch Erfolgsmeldungen, werden für jede Transaktions-ID in der Input-Datenbank (Input-DB) festgehalten und sind Teil des Ergebnisprotokolls.

Darüber hinaus werden am Ende jedes Übermittlungszeitraums im Rahmen der Validitätsprüfungen für den gesamten Datenbestand Quervergleiche zwischen Datenlieferanten und Abgleiche mit externen Datenquellen ermittelt und im Datenvalidierungsprotokoll protokolliert.

5.2.3 Plausibilitätsprüfungen

Die Plausibilitätsprüfungen werden ausschließlich auf dem gesamten Datenbestand durchgeführt. Dies geschieht am Ende jedes Übermittlungszeitraums, ausschließlich nachdem die Daten auf den BED transformiert und in die BED-DB transferiert wurden. Die Plausibilitätsprüfungen sind im Datenvalidierungskonzept der Tx-Registerstelle im Detail beschrieben. Die Ergebnisse werden als Teil des Datenvalidierungsprotokolls zur Verfügung gestellt.

6 Datenaktualisierung

Datenlieferanten, TxVST

Datenlieferanten können innerhalb des in der Verfahrensordnung festgelegten Zeitraums Datenlieferungen aktualisieren. Eine Lieferdatei kann beliebige Datensätze enthalten, d. h. es können nur Aktualisierungen zu einzelnen Pseudonymen erfolgen, aber auch neue Daten zu erhobenen Fällen angelegt werden. Die Prozesse und Unterprozesse der Datenaktualisierung entsprechen dem seriellen Verfahren, wie in Kapitel 5 beschrieben. Eine Differenzierung bei der Datenannahme durch die Tx-Registerstelle ist nicht nötig, da die Datenlieferungen sequentiell nach dem Lieferdatum abgearbeitet werden. Eine Löschung von Daten aus der Tx-Registerdatenbank kann im Zuge einer Datenaktualisierung nicht vorgenommen werden. Diese ist gesondert zu betrachten und als eigenständiger Prozess definiert, der in Kapitel 7 beschrieben ist.

Eine Korrekturlieferung muss erfolgen, wenn die Datenannahme fehlschlägt oder die Validitätsprüfung auf dem gesamten Datenbestand am Ende des Erfassungszeitraums eine Korrekturlieferung durch den Datenlieferanten erforderlich macht. Im Falle einer fehlgeschlagenen Datenlieferung ist eine erneute Übermittlung der gesamten Lieferdatei notwendig. Details können über das Ergebnisprotokoll (siehe Anhang B.3) abgerufen werden. Die Korrekturlieferungen müssen laut Verfahrensordnung innerhalb von zwei Kalendermonaten nach Verfügbarkeit des Ergebnisprotokolls oder der Datenvalidierungshinweise erfolgen.

Sollte eine Korrekturlieferung seitens der Datenlieferanten nicht möglich sein, muss eine Rückmeldung mit enthaltenen Gründen an die Tx-Registerstelle (office@transplantationsregister.de) kommuniziert werden. Jede korrigierte bzw. aktualisierte Lieferdatei muss den technischen Vorgaben entsprechen und über die TxVST an die Tx-Registerstelle weitergeleitet werden. In der Tx-Registerdatenbank erfolgt die Abhandlung der Datenlieferung gemäß den Verarbeitungs- und Validierungsschritten.

Mit der Neulieferung werden in der Tx-Registerdatenbank nicht vorhandene Datenfelder neu angelegt und gelieferte Datensätze zu bereits bestehenden Datenfeldern überschrieben. Gültig ist jeweils die aktuellste Datenlieferung.

Hinweis: Bereits gelieferte Werte werden durch eine Aktualisierung mit NULL überschrieben, sollte in der Aktualisierungs-Lieferung das entsprechende Element fehlen.

7 Datenlöschung

Datenlieferanten, TxVST

Innerhalb des durch die Verfahrensordnung festgelegten Lieferzeitraumes oder in Datensätzen der Vorjahre können Datenlieferanten bereits übermittelte Daten mit fehlender Einwilligung der oder des Betroffenen löschen lassen. Dazu muss aktiv eine Löschaufforderung an die TxVST gestellt werden, welche diese an die Tx-Registerstelle weiterleitet. Dies erfolgt auf Seiten der Tx-Registerstelle über die identische REST-Schnittstelle wie für Datenlieferungen (siehe Anhang B.3). Details zu Löschen von Daten sind dem Löschkonzept zu entnehmen.

Um eine Löschung der Daten innerhalb des Tx-Registers vorzunehmen, muss eine sog. NULL-Lieferung vorgenommen werden. Dazu muss der Block `Patientenidentifizierende_Daten` mit den zuvor gelieferten patientenidentifizierenden Daten geliefert werden, wobei das Attribut Einwilligung die Ausprägung „L“ haben muss. Der Block `Medizinische_Daten` bleibt dabei, bis auf die Auswahl des Datenlieferanten, leer. Die zuvor gelieferten Werte werden damit mit NULL überschrieben.

Die unzulässig übermittelten Daten werden durch die Tx-Registerstelle nach Löschaufforderung unverzüglich gelöscht und der Status des Vorgangs über das Ergebnisprotokoll der REST-Schnittstelle kommuniziert.

Beispielsweise:

```
<?xml version="1.0" encoding="UTF-8"?>
<TxDatensatz xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    ↪ xsi:noNamespaceSchemaLocation="Tx_BED.xsd">
  <version>BED 2020.1</version>
  <Faelle>
    <Fall_Nr Nr="1">
      <Patientenidentifizierende_Daten>
        <P_EmpfaengerNummerET_ET art="ETE" einwilligung="L" xsi:type="
            ↪ et_nummer_orig" V="123456"/>
      </Patientenidentifizierende_Daten>
      <Medizinische_Daten>
        </ET>
      </Medizinische_Daten>
    </Fall_Nr>
  </Faelle>
</TxDatensatz>
```

8 Datensatz

Datenlieferanten, TxVST

8.1 Datensatzstruktur

Der BED zur Transplantation wird vom Fachbeirat gemäß § 15d (2) TPG vorgeschlagen und fortgeschrieben. Er führt alle Variablen, die bei den drei Datenlieferanten abgebildet werden, zusammen.

Insgesamt besteht der BED aus sieben Entitäten, die getrennt voneinander behandelt werden, um redundante Datenübermittlungen zu vermeiden. Zentrales Bindeglied ist die Entität Transplantation mit der Transplantationsnummer, die organübergreifend das Transplantationsgeschehen abbildet. Jede Transplantationsnummer ist dabei eindeutig einer Transplantation zugeordnet. Über die Transplantation sind die Empfänger- und Spenderdaten miteinander verbunden. Dem Empfänger lassen sich drei Entitäten zuordnen: allgemeine Empfängerdaten, Wartelisteneinträge sowie Follow Up Daten des Empfängers. Analog dazu enthält das Datenmodell für den Spender weitere drei Entitäten: allgemeine Spenderdaten (jeweils unterteilt nach postmortalem Spender und Lebendspender), die Organentnahme sowie Follow Up Daten des Spenders, falls die entnommenen Organe zur Transplantation von einem lebenden Spender stammen. Jede Entität besteht aus einer oder mehreren Tabellen, die sich jeweils aus patientenidentifizierenden Variablen, beschreibenden Variablen und gegebenenfalls einem Untersuchungsdatum zusammensetzen. Patientenidentifizierende Variablen werden dabei von der TxVST verschlüsselt (pseudonymisiert) übermittelt. Weiterhin werden wiederholt auftretende Daten, wie z. B. Untersuchungsdaten oder Follow Up Daten, in dafür vorgesehenen Entitäten abgebildet. So können Entitäten mit wiederholt auftretenden Daten mehrfach angelegt werden. Entitäten welche Basisdaten enthalten, werden nur einmal angelegt.

Datenmodell und Datensatzstruktur des BEDs sind so konzipiert, dass sie flexibel erweiter- und änderbar sind. So ist jede Entität separiert, wodurch diese Flexibilität gewährleistet ist.

8.2 Repräsentation des BEDs

Die technischen Repräsentationsformen des Datensatzes, der gemäß § 15d (2) TPG vom Fachbeirat vorgeschlagen wird, werden im Folgenden erläutert.

8.3 Datensatz-Portal

Das Datensatz-Portal ist eine Web-Applikation, die unter der Uniform Resource Locator (URL) `https://datensatz.transplantations-register.de` erreichbar ist. Um den Zugriff nicht autorisierter Nutzer auf die Funktionalitäten der Anwendung zu verhindern, ist der Zugang durch eine Nutzerauthentifizierung gesichert.

Die Zugangsdaten werden den autorisierten Stellen durch die Tx-Registerstelle zur Verfügung gestellt. Bei Bedarf können weitere Zugangsdaten unter `helpdesk-tx-register@gesundheitsforen.net` angefragt werden. Es erfolgt eine stichprobenhafte Überprüfung der Authentizität.

Im Datensatz-Portal wird eine stets aktuelle Version des Datensatzes visuell repräsentiert. Zusätzlich besteht die Möglichkeit, diese mit älteren Datensatzversionen zu vergleichen. Die Tabellenstruktur der Datensatzbeschreibung ist den Anforderungen des Datensatz-Portals angepasst und in Abbildung 8.1 dargestellt. Nachfolgend sind die Tabellenspalten beschrieben.

Elementname: In dieser Spalte befindet sich der Name des XML-Elements, wie er im BED spezifiziert ist. Die Groß- und Kleinschreibung ist zu beachten.

Beschreibung: Sie gibt die inhaltliche Bedeutung des Elements an. Die Beschreibung entspricht den Vorgaben der Datenlieferanten (Beschreibungstexte von ET sind ins Deutsche übersetzt).

Inhalt/Form: Welcher Inhalt in dem XML-Element zulässig ist, wird in dieser Spalte beschrieben. Handelt es sich bei dem beschriebenen XML-Element um ein Containerelement, so befindet sich in der Inhaltszelle zu diesem Element ein Verweis auf den Abschnitt in der Datensatzbeschreibung, in dem der Inhalt dieses Containerelements beschrieben wird (z. B. „siehe 2.1“).

Quellvariablenname: Hier werden die Variablen- und evtl. Tabellennamen aus den Quellsystemen der Datenlieferanten angezeigt. Somit ist eine einfachere Zuordnung für die Datenlieferanten möglich.

Elementname	Beschreibung	Inhalt/Form	Quellvariablenname
E_Identifikation_EmpfaengerNummerET_ET	Recipient ET registration number. Identification number of the recipient as known outside Eurotransplant.	et_nummer_type	General//Recipient Number
E_Identifikation_EmpfaengerNummerET_IQTIG	Empfänger ID	et_nummer_type	HTXM:B//IDEMPFAENGER , LTX:B//IDEMPFAENGER , LUTX:B//IDEMPFAENGER , PNTX:B//IDEMPFAENGER

Abbildung 8.1: Tabellenstruktur des Datensatz-Portals

Die Darstellung ist an die Struktur der abzugebenden XML-Lieferdateien angelehnt, eine konkrete Angabe aller technischen Feinheiten der XML-Dateien erfolgt nicht. Zwischenversionen während der Arbeiten am Datensatz lassen sich im Datensatz-Portal durch am Prozess der Entwicklung beteiligte Personen herunterladen. Releaseversionen werden auf `https://transplantations-register.de` unter Servicedateien veröffentlicht.

8.4 Datensatzbeschreibung

Die Datensatzbeschreibung ist eine visuelle und menschenlesbare Repräsentation der abzugebenden Lieferdateien. Diese umfasst die Struktur und Formatvorgaben aller enthaltenen Felder. Jede technische Beschränkung des Inhalts der Lieferdateien wird in der Datensatzbeschreibung erläutert.

Die druckbare Version des Datensatzes wird in Form eines PDF-Dokuments als Datensatzbeschreibung bereitgestellt. Dabei werden alle XML-Elemente des BEDs gelistet. Die Detailbeschreibung der XML-Elemente erfolgt in tabellarischer Form. Die Spalten der Tabelle sind nachfolgend beschrieben.

Elementname: In dieser Spalte befindet sich der Name des XML-Elements, wie er im BED spezifiziert ist. Die Groß- und Kleinschreibung ist zu beachten.

Beschreibung: Sie gibt die inhaltliche Bedeutung des Elements an. Die Beschreibung entspricht den Vorgaben der Datenlieferanten (Beschreibungstexte von ET sind ins Deutsche übersetzt).

Häufigkeit: In dieser Spalte wird die Häufigkeit des XML-Elements angegeben. Sie gibt an, wie häufig das XML-Element an dieser Position innerhalb der XML-Struktur, die durch die Tabellenzeile dargestellt wird, vorkommen darf.

- **1**: genau einmal
- **0 .. 1**: gar nicht oder genau einmal
- **1 .. n**: mindestens einmal bis beliebig häufig
- **0 .. n**: gar nicht oder beliebig häufig

Inhalt/Form: Welcher Inhalt in dem XML-Element zulässig ist, wird in dieser Spalte beschrieben. Handelt es sich bei dem beschriebenen XML-Element um ein Containerelement, so befindet sich in der Inhaltszelle zu diesem Element ein Verweis auf den Abschnitt in der Datensatzbeschreibung, in dem der Inhalt dieses Containerelements beschrieben wird (z. B. „siehe 2.1“).

Quellvariablenname: Hier werden die Variablen- und evtl. Tabellennamen aus den Quellsystemen der Datenlieferanten angezeigt. Somit ist eine einfachere Zuordnung für die Datenlieferanten möglich.

Hinweis: Hier werden weitere Angaben zu dem Element gemacht.

Die Datensatzbeschreibung ist versioniert, da durch fachliche Fortschreibungen das Datenmodell geändert werden kann. Die Tabellenversionen unterscheiden sich aufgrund unterschiedlicher Zielgruppen in ihrem Umfang. Für die Veröffentlichung des Datensatzes im Bundesanzeiger wird eine gekürzte Tabellenversion verwendet, in welcher die Spalten Häufigkeit und Hinweis nicht enthalten sind. Die Dateinamen werden mit Angabe der Zielgruppe und Tabellenversion eindeutig gekennzeichnet. Zum Beispiel:

- JJJJMMTT_Tx-BED-Bundesanzeiger_v2020.0.5.pdf,
- JJJJMMTT_Tx-BED-Datensatzbeschreibung_v2020.0.5.pdf und
- JJJJMMTT_Tx-BED-Schema_v2020.0.5.xsd

Aktuelle und im Bundesanzeiger veröffentlichte Versionen werden zusätzlich auf `https://transplantations-register.de` unter Servicedateien veröffentlicht.

Für die Altdaten trägt der BED eine inkrementierte Versionsnummer. Die finale und im Bundesanzeiger veröffentlichte Version trägt die Versionsnummer 1.2.3.

Beginnend mit den Neudaten beinhaltet die Versionsnummer das jeweils gültige Datenjahr (z. B. 2020), die Iteration der im Bundesanzeiger veröffentlichten Version (0 bedeutet noch nicht veröffentlicht; 1 entspricht der ersten veröffentlichten Version) und eine interne Versionsnummer als Inkrement.

8.5 XSD-Datei

Bei der XSD handelt es sich um eine maschinenlesbare Datei, die alle technischen Vorgaben für Lieferdateien umfasst. Diese beinhaltet Vorgaben zur Struktur der XML-Dateien, der enthaltenen Felder sowie deren Datentyp bzw. deren festgelegter Ausprägung. Auf Basis dieser ist eine computergestützte Überprüfung einer XML-Datei durch alle Stellen möglich. Eine Überprüfung der inhaltlichen Korrektheit der Werte kann nicht durchgeführt werden.

Hinweis: Die Überprüfung der Schemakorrektheit setzt eine erfolgreich durchgeführte Prüfung auf XML-Wohlgeformtheit voraus. Im Sprachgebrauch wird dies häufig unter „Überprüfung auf Schemakorrektheit“ verstanden. Technisch betrachtet sind dies jedoch zwei unabhängige Prozeduren. Öffentlich bereitgestellte bzw. proprietäre Software sowie Softwareplugins führen in der Regel beide Prozeduren sequentiell durch. Sollte eine Eigenentwicklung zur Überprüfung der Schemakorrektheit eingesetzt werden, muss sichergestellt werden, dass vor der Prüfung auf Schemakorrektheit eine erfolgreiche Prüfung der XML-Wohlgeformtheit durchgeführt wurde.

Die Struktur der XSD-Schemadatei (und daraus resultierend der zu liefernden XML-Dateien) ist in B.1 beschrieben.

8.6 Externe Listen

Die Datenlieferanten liefern u. a. Datenfelder mit Angaben zu International Classification of Diseases (ICD)- und Operationen- und Prozedurenschlüssel (OPS)-Codes. Die Abbildung der Codes im Datensatz erfolgt als Freitextfeld. Eine Überprüfung der Korrektheit und Plausibilität der gelieferten Codes wird nicht vorgenommen, da keine Informationen über den Zeitpunkt der Erfassung vorliegen und somit kein Vergleich mit den Listen des Deutsches Institut für Medizinische Dokumentation und Information (DIMDI) möglich ist.

9 Lieferdateien

Datenlieferanten, TxVST

Die Lieferdatei bezeichnet eine durch die Datenlieferanten zu erstellende Datei, die den Schemavorgaben des BED folgt.

Die Erstellung der Dateien erfolgt durch Datenexport aus der Datenbank der Datenlieferanten sowie einer Konvertierung bzw. Formatanpassung der Daten an die im XML-Schema festgelegten Vorgaben.

Seitens der Tx-Registerstelle werden zusätzlich technische Rahmenbedingungen vorgegeben, um einen reibungslosen Datenfluss vom Datenlieferanten zur Tx-Registerstelle gewährleisten zu können.

9.1 Dateiformat

Die Lieferdateien sind als gültige XML-Dateien zu erstellen, die entsprechend des vorgegebenen XML-Schemas formuliert werden.

Die XML-Datei hat die in Abbildung 9.1 gezeigte Struktur:

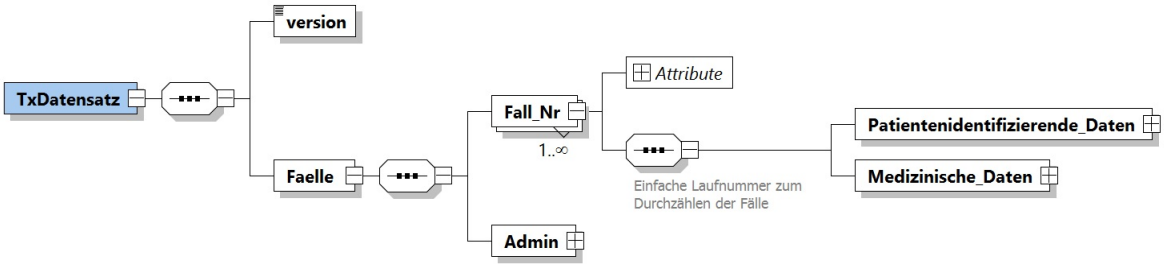


Abbildung 9.1: Struktur der zu übermittelnden XML-Datei

Das Element `version` beinhaltet den String zur Version des BED:

```
<xs:element name="version" type="xs:normalizedString" fixed="BED-Datensatz 2020.1
    ↪ "/>
```

Die Fälle gruppieren die medizinischen Daten zu einer Person bzw. einem Transplantationsvorgang. So ist sichergestellt, dass die verschlüsselten patientenidentifizierenden Daten zu den korrekten medizinischen Daten gruppiert sind.

9.2 Dateinamensbeschränkung

Generierte Exportdateien müssen einer vorgegebenen Namenskonvention zur Dateibenennung folgen. Dies ist notwendig, sodass

- weder bei der TxVST noch bei der Tx-Registerstelle Daten überschrieben werden und Daten verloren gehen.
- TxVST und Tx-Registerstelle konkrete Rückmeldungen zu den Lieferdateien geben können. Wenn nötig, kann konkret zu spezifischen Lieferdateien Rückmeldungen zur Verbesserung der Datenqualität gegeben werden.

Die Dateien müssen nach folgender Vorschrift benannt werden:

```
<Datenlieferant>_<Zeitstempel-des-Exports>_<ID-Lieferung>.xml
```

Unter `Datenlieferant` stehen folgende Auswahlelemente zur Verfügung:

- ET
- DSO
- IQTIG

Der `Zeitstempel-des-Exports` bezeichnet einen sekundengenauen Zeitstempel, der den Zeitpunkt des Exports angibt. Dies erfolgt im folgenden Format:

```
YYYY_MM_DD_hh_mm_ss
```

Beispielhaft demzufolge:

```
2019_02_15_23_59_59
```

Die `ID-Lieferung` gibt eine ID der Lieferung an, die durch den Datenlieferanten vergeben wird. Es handelt sich um eine zweistellige Ganzzahl, die bei 0001 beginnt und hochgezählt wird (führende Nullen müssen angegeben werden).

Bei der Verarbeitung der Lieferdateien in der Tx-Registerstelle erfolgt **keine** sequenzielle Abarbeitung der Dateien auf Basis der ID. Diese dient ausschließlich der Kennzeichnung und Differenzierung von Lieferdateien, z. B. aufgrund der Aufspaltung einer Lieferdatei in mehrere Dateien (siehe dazu Abschnitt 9.3). In diesem Fall ist zu beachten, dass auch die Dateien der Teillieferungen den Anforderungen an Wohlgeformtheit und Schemakorrektheit genügen müssen. Beispielhaft sind im Folgenden Dateinamen für die unterschiedlichen Datenlieferanten angegeben:

```
ET_2019_04_05_14_05_23_0001.xml
ET_2019_04_05_14_05_23_0002.xml
DSO_2019_05_02_09_58_46_0001.xml
IQTIG_2019_06_15_08_01_0001.xml
```

9.3 Dateigrößen und Anzahl der Lieferdateien

Für die TxVST sowie die Tx-Registerstelle ist es notwendig, eine Beschränkung der maximalen Dateigröße der Lieferdateien festzulegen. Die maximale Dateigröße beträgt pro Datei 5 Gigabyte. Dies ist erforderlich, damit alle beteiligten Serversysteme entsprechend den Anforderungen

- korrekt skaliert werden können.
- auf korrekte Funktionsweise bei maximaler Last vor der produktiven Nutzung getestet werden können.

Um dennoch die Vollständigkeit des zu liefernden Datenbestandes nicht einzuschränken, kann eine Aufteilung der Lieferdateien durch die Datenlieferanten vorgenommen werden. Jede dieser Lieferdateien muss entsprechend der zur Verfügung gestellten XML-Schemadatei formuliert werden. Sollte für Einzeldateien die Prüfung auf XML-Wohlgeformtheit sowie XML-Schema Dateien nicht fehlerfrei abgeschlossen werden, werden ausschließlich betroffene Einzeldateien bei der TxVST abgelehnt. Eine Nachlieferung einzelner Dateien ist nicht vorgesehen. Aus diesem Grund empfiehlt die Tx-Registerstelle den Datenlieferanten selbstständig die notwendigen XML-Prüfungen durchzuführen.

Eine fallorientierte Aufteilung muss nicht vorgenommen werden. Das heißt, es müssen nicht alle zu einem Spender/Empfänger vorliegenden Daten innerhalb einer Lieferdatei zu finden sein. Eine Aufteilung der Daten eines Spenders/Empfängers von bspw. Wartelisten-Daten in einer Datei sowie Untersuchungsdaten in einer anderen Datei ist ohne Probleme durch TxVST und Tx-Registerstelle verarbeitbar.

9.4 Sollstatistik

Gemäß der XSD-Vorgaben muss eine Aufstellung der Anzahl der erfassten und in der Lieferdatei übermittelten Daten je Elementliste durch die Datenlieferanten erfolgen.

```
<xs:element name="Sollstatistik">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="Anzahl_uebermittelte_Datensaetze_Empfaenger" minOccurs="1
          ↪ " maxOccurs="1" type="xs:integer">
        <xs:annotation>
          <xs:documentation>Soll-Anzahl der uebermittelten Datensaetze aus
              ↪ Elementliste Empfaenger</xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="
          ↪ Anzahl_uebermittelte_Datensaetze_Empfaenger_Dringlichkeit"
          ↪ minOccurs="1" maxOccurs="1" type="xs:integer">
        <xs:annotation>
          <xs:documentation>Soll-Anzahl der uebermittelten Datensaetze aus
              ↪ Elementliste Empfaenger_Dringlichkeit</xs:documentation>
        </xs:annotation>
```

```
        </xs:element>
        ...
```

Anhand des Ausschnitts aus der XML-Schemadatei wird ersichtlich, dass für jede der Elementlisten (Empfaenger, Empfaenger_Dringlichkeit, Organ_Entnahme_Darm, etc.) die Angabe der Soll-Anzahl der übermittelten Datensätze erfolgen muss.

Zweck der Sollstatistik ist es, die angegebenen Werte mit der tatsächlichen Anzahl an gelieferten Datensätzen zu vergleichen, um somit eventuelle Unstimmigkeiten aufzudecken.

Sie dient daher zur absichernden Überprüfung, ob alle zu liefernden Datensätze auch tatsächlich geliefert werden. Die Überprüfung ist technisch nicht mittels der XML-Schemadatei durchführbar, sondern muss gesondert vorgenommen werden.

10 Public-Key-Infrastruktur

Die PKI dient zur Bereitstellung und Zertifizierung der Zertifikate, welche sowohl zur Verschlüsselung der unmittelbar personenbeziehbaren bzw. der transplantationsmedizinischen Datenfelder und zur Transportverschlüsselung verwendet werden. Dadurch können die Datenlieferanten gemäß § 15e (1) TPG, die TxVST sowie die Tx-Registerstelle sicherstellen, dass nur korrekte Schlüssel im Kontext des Tx-Registers verwendet werden.

Hierfür wird von der Tx-Registerstelle eine PKI-Webanwendung zur Verfügung gestellt, die die Bereitstellung und Verwaltung von öffentlichen Schlüsseln und den zugehörigen Zertifikaten unterstützt.

Die PKI für die im Produktiv-Einsatz zu nutzenden Zertifikate und Schlüssel ist unter der folgenden Adresse erreichbar:

https://pki.transplantations-register.de

Die PKI für den Test-Einsatz unter folgender Adresse:

https://pki.test.transplantations-register.de

10.1 Benutzerkonten zur Nutzung der PKI-Webanwendung

Um die in der PKI-Webanwendung bereitgestellten Funktionalitäten zu verwenden, müssen sich die Datenlieferanten gemäß § 15e (1) TPG sowie die TxVST zunächst registrieren und von der Tx-Registerstelle freigeschaltet werden. Nachfolgend werden der Registrierungsprozess und die benutzerspezifischen Komponenten dargestellt.

10.1.1 Registrierung

Initial ist eine Registrierung bei der PKI-Webanwendung notwendig. Hierfür muss das Registrierungsformular (siehe Abbildung 10.1) ausgefüllt werden.

Nach Absenden der Registrierung wird eine E-Mail mit einem Bestätigungslink an den Registrierenden des Benutzerkontos geschickt. Das Benutzerkonto besitzt zu diesem Zeitpunkt den Status `ungeprüft`. Der neue Nutzer kann sich erst nach Verifikation und Freischaltung durch die Tx-Registerstelle anmelden.

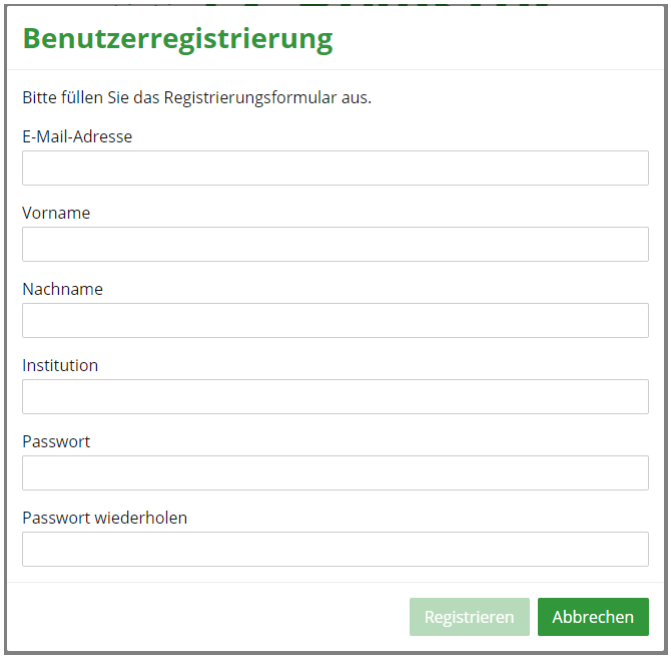


Abbildung 10.1: Registrierungsformular der PKI-Webanwendung

10.1.2 Verifizierung durch die Tx-Registerstelle

Nach der Registrierung eines neuen Benutzers prüft die Tx-Registerstelle, ob die Institution zur Nutzung berechtigt ist.

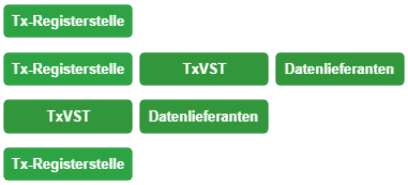
Bei erfolgreicher Prüfung schaltet die Tx-Registerstelle das Benutzerkonto über die *Benutzerverwaltung* frei. Der Status des Benutzerkontos wird in diesem Fall von `ungeprüft` auf `verifiziert` gesetzt und der neue Benutzer erhält Zugriff auf die benutzerspezifischen Ansichten (Kapitel 10.1.3).

Führt die Prüfung zu einer Ablehnung der neu registrierten Institution und damit einhergehend einer Verweigerung zur Nutzung der Funktionalitäten, erhält das Benutzerkonto den Status `gesperrt`.

10.1.3 Ansichten und Funktionalitäten der Benutzerkonten

Nach erfolgreichem Abschluss der Registrierung und der Verifizierung durch die Tx-Registerstelle, können die autorisierten Benutzer auf die Komponenten der PKI-Webanwendung mit ihren Anmeldedaten zugreifen. Der Zugriff ist nur möglich, solange der Status des Kontos `verifiziert` ist. Sollte aufgrund von Kompromittierungen des Benutzerkontos eine Sperrung erfolgen (Status `gesperrt`), verliert der jeweilige Benutzer die Autorisierung zur Nutzung der Funktionalitäten.

Nachfolgend sind die verfügbaren Ansichten für die jeweiligen Benutzer, d. h. die Datenlieferanten gemäß § 15e (1) TPG, die TxVST sowie die Tx-Registerstelle, dargestellt.



Benutzerverwaltung

In der *Benutzerverwaltung* werden alle registrierten Benutzer aufgelistet und deren Profildaten angezeigt. Das Sperren oder Verifizieren eines Nutzerkontos ist von der Tx-Registerstelle in der Benutzerverwaltung auszuführen.

Kompromittierte Benutzerkonten müssen umgehend über die *Benutzerverwaltung* gesperrt werden. Mit dem Sperren eines Kontos geht das Sperren der zugehörigen Public-Key-Zertifikate einher.

Dashboard

Im *Dashboard* sind die Benutzerdaten und offene Aktionen aufgeführt. Die Benutzerdaten umfassen E-Mail-Adresse, Name, Rolle (TxVST, Tx-Registerstelle oder Datenlieferant), den Status des Benutzerkontos (`ungeprüft`, `verifiziert`, `gesperrt`) und den letzten Login. Unter Aktionen werden Nutzer beispielsweise darauf hingewiesen, dass noch kein Schlüssel eingereicht wurde.

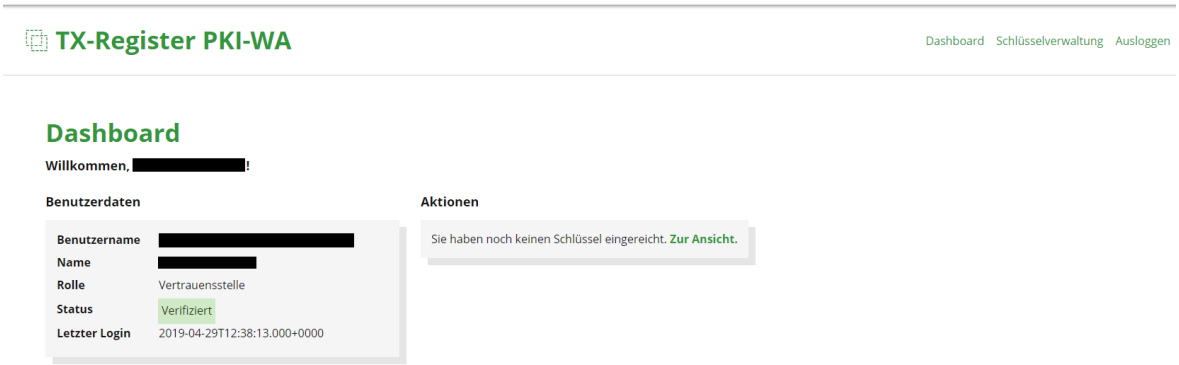


Abbildung 10.2: Dashboard Ansicht der PKI-Webanwendung für einen verifizierten Nutzer der Rolle TxVST.

Schlüsselverwaltung

In der *Schlüsselverwaltung* erhalten die Benutzer eine Übersicht über die eigenen eingereichten öffentlichen Schlüssel. Das Einreichen von neuen Schlüsseln, um diese zertifizieren zu lassen, wird ebenfalls in der Schlüsselverwaltung vorgenommen. Sobald ein neuer Schlüssel eingereicht wird, wird der letzte aktive Schlüssel auf `gesperrt` gesetzt, um zu verhindern, dass mehrere Zertifikate verwendet werden. Initial ist der Schlüssel `ungeprüft`, sobald die Tx-Registerstelle den Schlüssel freigibt, ändert sich der Status auf `freigegeben` und das Zertifikat kann heruntergeladen werden.

Neben den eigenen Schlüsseln bzw. Zertifikaten können die Public-Key-Zertifikate der anderen Benutzerkonten eingesehen und zur Verschlüsselung der XML-Dateien bzw. des Transports heruntergeladen werden. Hier sind jedoch nur die aktuellen Zertifikate mit Status `freigegeben` aufgelistet. Ein Zertifikat mit Status `gesperrt` oder `ungeprüft` kann nur vom Ersteller selbst oder der Tx-Registerstelle eingesehen werden.

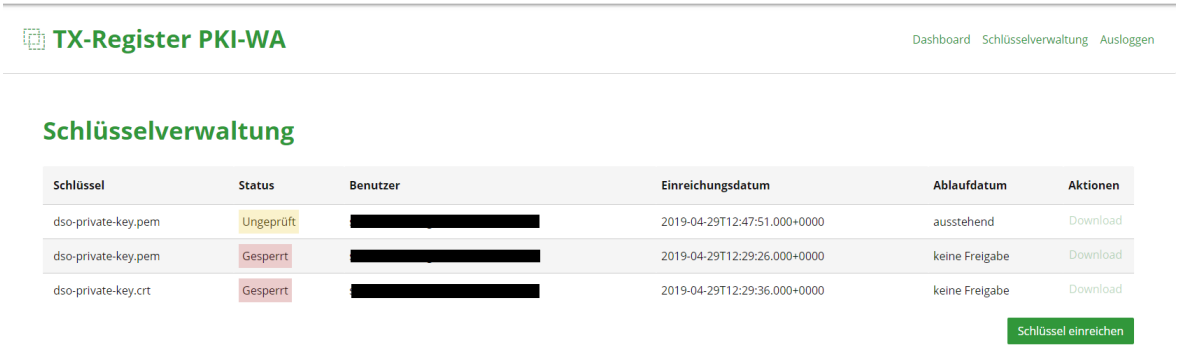


Abbildung 10.3: Schlüsselverwaltungsansicht

10.2 Zertifikatsinformationen

Der Signierungsprozess der Tx-Registerstelle geschieht durch zwei verschiedene Zertifikate. Das Stammzertifikat hat eine Gültigkeit von 30 Jahren. Mit diesem werden Signierungszertifikate, welche in der PKI hinterlegt werden, mit einer Gültigkeit von fünf Jahren erstellt.

Beide Zertifikate tragen die folgenden Informationen im Zertifikats-Feld `Aussteller`:

```
E  = office@transplantations-register.de
CN = Tx-Registerstelle CA [Prod/Test]
OU = Tx-Registerstelle Geschaeftsstelle
O  = Gesundheitsforen Leipzig GmbH
L  = Leipzig
S  = Sachsen
C  = DE
```

Durch diese Zertifizierungshierarchie wird sichergestellt, dass Daten von der Tx-Registerstelle auch mit einem zukünftigen Zertifikat retrospektiv entschlüsselt werden können.

Die von der TxVST in der PKI hinterlegten Zertifikate tragen die folgenden Informationen im Feld `Antragsteller`:

```
E  = txvst@nortal.com
CN = TxVST [Prod/Test]
OU = Vertrauensstelle Transplantationsregister [Prod/Test]
O  = Nortal AG
L  = Berlin
S  = Berlin
```

`C = DE`

Das Feld `Aussteller` ist nach der Signierung durch die PKI mit den o. g. Daten der Tx-Registerstelle gefüllt.

Sowohl von der TxVST als auch der Tx-Registerstelle wird genau ein Zertifikat im Format `.crt` in der PKI hinterlegt. Dieses wird sowohl für die XML-Verschlüsselung der transplantationsmedizinischen und patientenidentifizierenden Daten als auch die Transportverschlüsselung und Authentifizierung genutzt.

10.3 Signierung und Verifikation von öffentlichen Schlüsseln

Nachfolgend ist der Prozess zur Signierung und Verifikation von öffentlichen Schlüsseln dargestellt.

1. Initial erzeugt der Benutzer (TxVST, Tx-Registerstelle) ein Schlüsselpaar, bestehend aus privatem und öffentlichem Schlüssel. Die Wahl der Software zur Schlüsselerstellung ist dabei dem Benutzer überlassen.
2. Zur Signierung des Zertifikats meldet sich der registrierte und verifizierte Benutzer mit seinen Zugangsdaten bei der PKI-Webanwendung an. In der Komponente *Schlüsselverwaltung* wird der zuvor generierte öffentliche Schlüssel als .csr (Certificate Signing Request) Datei eingereicht.
3. Die Webanwendung erzeugt automatisiert ein durch die Tx-Registerstelle signiertes Public-Key-Zertifikat, das maximal auf fünf Jahre limitiert ist. Das generierte Zertifikat wird in Zuge dessen mit dem Status `ungeprüft` in die *Schlüsselverwaltung* eingetragen.
4. Die Tx-Registerstelle gleicht den Fingerprint des eingereichten öffentlichen Schlüssels telefonisch mit dem Benutzer ab. Stimmen die Fingerprints überein, weist die Tx-Registerstelle dem Zertifikat den Status `freigegeben` zu, andernfalls wird es auf `gesperrt` gesetzt. Gesperrte Zertifikate werden nicht benutzerübergreifend angezeigt und stehen somit anderen nicht zum Download zur Verfügung.
5. Das freigegebene Public-Key-Zertifikat, das den öffentlichen Schlüssel enthält, steht anschließend den potentiellen Verschlüsselungspartnern zum Download in der Ansicht *Schlüsselverwaltung* zur Verfügung.

Schlüsselinhaber	Zieladressaten		
	Datenlieferanten	TxVST	Tx-Registerstelle
	XML-Verschlüsselung		
TxVST	X		
Tx-Registerstelle	X		X
	Transport-Verschlüsselung		
TxVST	X		
Tx-Registerstelle			X

Tabelle 10.1: Darstellung wessen öffentliche Schlüssel (rechts) die Datenlieferanten, die TxVST bzw. die Tx-Registerstelle im Rahmen der Neudatenübermittlung herunterladen müssen.

10.4 Zertifizierungshierarchie

Die Public-Key-Zertifikate für die gesicherte Kommunikation werden mittels eines Signierungszertifikats erstellt. Hierfür erzeugt die Tx-Registerstelle ein Stammzertifikat, aus dem anschließend ein Signierungszertifikat generiert wird. Die Zertifikate bestehen jeweils aus einem öffentlichen und einem privaten Schlüssel.

Der private Schlüssel des Stammzertifikats wird offline gespeichert und physisch geschützt. Durch die Speicherung des Zertifikats auf einer nicht wiederbeschreibbaren CD wird die Langlebigkeit garantiert. Die Gültigkeit des Stammzertifikats ist auf 30 Jahre limitiert.

Auf Basis des Stammzertifikats wird ein weiteres Schlüsselpaar, das Signierungszertifikat, generiert. Das erzeugte Zertifikat ist für die Signierung der öffentlichen Schlüssel der Benutzer im laufenden Betrieb und besitzt eine Gültigkeit von fünf Jahren. Sollte es innerhalb der fünf Jahre zur Kompromittierung kommen, wird das Signierungszertifikat deaktiviert und auf Basis des Stammzertifikates ein neues erstellt.

Die Tx-Registerstelle führt die Schlüsselerzeugung beider Zertifikate mittels OpenSSL durch und es werden folgende Verfahren und Algorithmen genutzt. Diese werden auch den Datenlieferanten und der TxVST für die Schlüsselerzeugung empfohlen.

- RSA mit einer Schlüssellänge von 4096 bit
- AES-256 zur Verschlüsselung des Keys
- Signatur Algorithmus: ECDSA mit SHA-256
- Elliptic Curve secp521r1

Zusätzliche OpenSSL Konfiguration, welche eine hohe Sicherheit der Zertifikate sicherstellt:

```
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always, issuer
basicConstraints        = critical, CA:true
keyUsage                = critical, digitalSignature, cRLSign, keyCertSign
```

A Glossar

Begriff	Beschreibung
Deutsche Stiftung Organtransplantation	Die Koordinierungsstelle nach § 11 TPG *Deutsche Stiftung Organtransplantation* (DSO) „hat die Zusammenarbeit zur Organentnahme bei verstorbenen Spendern und die Durchführung aller bis zur Übertragung erforderlichen Maßnahmen […] zu organisieren“. Dadurch verfügt die DSO insbesondere über die wesentlichen Informationen zu postmortalen Spendern, deren gespendeten Organen sowie zur Organentnahme und zu deren Transport. Durch die DSO wird die sogenannte DSO-Kennnummer generiert, welche zur eindeutigen Identifikation von postmortalen Spendern genutzt wird. Die DSO liefert ab Stufe I Daten an das Tx-Register.
Eurotransplant	Die Vermittlungsstelle nach § 12 TPG *Eurotransplant (ET)* vermittelt zur Verfügung stehende Organe an auf der Warteliste für ein Spenderorgan stehende Patienten. Dabei sind Organe nach den „Regeln, die dem Stand der Erkenntnisse der medizinischen Wissenschaft entsprechen, insbesondere nach Erfolgsaussicht und Dringlichkeit für geeignete Patienten“ zu vermitteln. ET generiert sowohl für Spender als auch Empfänger ET-Nummern zur eindeutigen Identifizierung. ET liefert ab Stufe I Daten an das Tx-Register.
Fachbeirat	Der *Fachbeirat* angesiedelt bei der Tx-Registerstelle und bestehend aus Vertretern der Datenlieferanten, der Deutschen Transplantationsgesellschaft (DTG), der Prüfungskommission und Überwachungskommission (PÜK) als auch maßgeblicher Patientenorganisationen wurde von den TPG-Auftraggebern vor Aufnahme der Tätigkeiten der Tx-Registerstelle eingerichtet. Der Fachbeirat ist an der Festlegung der Verfahrensordnungen beteiligt und verantwortet den Vorschlag des bundesweit einheitlichen Datensatzes (BED) inkl. dessen Fortschreibung. Ferner verfügt er über das Anhörungsrecht bei Anträgen auf Übermittlung pseudonymisierter Daten zu Forschungszwecken.

Begriff	Beschreibung
G-BA und IQTIG	Das Institut für Qualitätssicherung und Transparenz im Gesundheitswesen (IQTIG) erarbeitet im Auftrag des Gemeinsamen Bundesausschusses (G-BA) Maßnahmen zur Qualitätssicherung und zur Darstellung der Versorgungsqualität im Gesundheitswesen und wirkt an deren Umsetzung mit. Im Rahmen dieses Auftrages erhält das IQTIG transplantationsmedizinische Daten von leistungserbringenden Krankenhäusern. Das IQTIG liefert ab Stufe I im Auftrag des G-BA Daten an das Tx-Register.
Gesundheitsforen Leipzig GmbH	Die *Gesundheitsforen Leipzig GmbH* ist die von den TPG-Auftraggebern beauftragte Firma sowohl zum Aufbau und Betrieb der Tx-Registerstelle als auch der Geschäftsstelle. Zudem obliegen ihr die Durchführung von Datenvalidierungen und das Berichtswesen.
Input-Datenbank (Input-DB)	Teil des Transplantationsregisters in Form einer relationalen Datenbank zur Speicherung der angenommenen, originären Lieferdateien sowie von Ergebnissen der Validitätsprüfung. Die Datenbank besitzt eine REST-Schnittstelle zur Übermittlung der Lieferdateien durch die TxVST.
Mit der Nachsorge betraute Einrichtungen und Ärzte	Damit sind alle ambulanten Leistungserbringer gemeint, die im Nachgang zu einer Transplantation die Organempfänger und lebenden Organspender parallel oder ergänzend zu den Tx-Zentren ambulant betreuen. In späteren Stufen des Projektes können, wie im Gesetz vorgesehen, diese Leistungserbringer selbständig Daten an das Tx-Register liefern.
Nortal AG	Die *Nortal* AG ist die von den TPG-Auftraggebern beauftragte Firma zur Erstellung und zum Betrieb der TxVST. Ab Stufe II pseudonymisiert die TxVST unmittelbar personenbeziehbare Daten (im Weiteren als ”patientenidentifizierende Daten” bezeichnet). Alle Daten werden von den Datenlieferanten verschlüsselt an die TxVST geliefert. Nach der Pseudonymisierung werden die Daten an die Tx-Registerstelle weitergeleitet, um dort gespeichert zu werden.

Begriff	Beschreibung
TPG-Auftraggeber	Die TPG-Auftraggeber sind die nach dem TPG beauftragten Organisationen der Selbstverwaltung zur konkreten Umsetzung von Aufgaben das Tx-Register betreffend. Die TPG-Auftraggeber sind die Selbstverwaltungspartner GKV-Spitzenverband, Deutsche Krankenhausgesellschaft und Bundesärztekammer.
Transplantationszen	In den *Transplantationszentren* (Tx-Zentren) werden die Organtransplantationen durchgeführt. Dafür werden in den Tx-Zentren die wesentlichen Daten zum Organempfänger, zum lebenden Organspender, zur Transplantation selbst und zu wesentlichen Teilen der Nachsorge erhoben. Diese Daten fließen primär zur Vermittlungsstelle ET sowie zum IQTIG und von dort zur Tx-Registerstelle. In späteren Stufen des Projektes können, wie im Gesetz vorgesehen, die Tx-Zentren auch selbständig Daten an das Tx-Register liefern.

B Anhang

B.1 XSD-Schema

Um das XML-Schema zur Erstellung der Lieferdateien zu beschreiben werden nachfolgend unter anderem Diagramme verwendet. In der Tabelle B.1 werden die Symbole dieser XSD-Diagramme kurz erläutert:

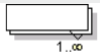
Symbol	Beschreibung
	**Obligatorisches Element**: Kardinalität 1
	**Optionales Element**: Kardinalität 0..1
	**Mehrfach wiederholbares Element**: Die Kardinalität ist unter dem Symbol festgelegt.
	**Auswahl von Elementen**: Die Auswahl ist auf ein einziges Element aus der Liste limitiert.
	**Folge von Elementen**: Die Reihenfolge der Elemente muss der Reihenfolge im Schemadiagramm entsprechen.
	Element ohne Kind-Elemente
	Element mit Kind-Elementen (Eltern-Element)

Tabelle B.1: Symbole der XSD-Diagramme.

B.1.1 Grundstruktur

Die Grundstruktur des Schemas der XML-Lieferdateien ist in Abbildung B.1 abgebildet.

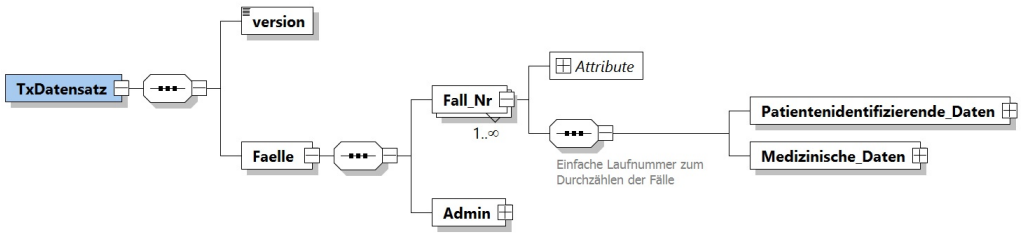


Abbildung B.1: Grundstruktur der XSD-Datei

Das globale Element `TxDatensatz` bildet das root-Element, welches die Kind-Elemente `version`, und `Faelle` besitzt. Das Element `Faelle` wiederum enthält sämtliche in das Register zu übertragende Fälle (`Fall_Nr`) sowie das Element `Admin`. Jeder einzelne Fall enthält die Elemente `Patientenidentifizierende_Daten` und `Medizinische_Daten`.

Die Kind-Elemente des root-Elements `TxDatensatz` sind wie folgt definiert. Die Kind-Elemente `<Patientenidentifizierende_Daten>` und `<Medizinische_Daten>` werden in den Abschnitten B.1.2 und B.1.3 detaillierter beschrieben.

Kind-Elemente	Beschreibung
`<version>`	Enthält einen vorgegebenen Wert vom Typ `xs:normalizedString`, der die Versionsnummer des aktuellen BED angibt. Das Präfix `xs` verweist darauf, dass es ein vordefinierter Datentyp des W3C XML Schema ist. Mit Änderung des BED wird dieser Wert entsprechend angepasst.
`<Faelle>`	Enthält alle in der Lieferdatei übermittelten Fälle (`<Fall_Nr>`) und das Element `<Admin>`.
`<Fall_Nr>`	Enthält für jeden übermittelten Fall die Elemente `<Patientenidentifizierende_Daten>` und `<Medizinische_Daten>`.
`<Admin>`	Enthält Angaben zur Sollstatistik.
`<Patientenidentifizierende_Daten>`	Enthält eine Liste aller möglichen patientenidentifizierenden Elemente, welche für einen Fall ausgefüllt werden können.
`<Medizinische_Daten>`	Enthält die Auswahl-Elemente DSO, ET und IQTIG, die die jeweiligen Teildatensätze der Datenlieferanten umfassen. Für die Datenlieferanten ist jeweils das gleichnamige Kind-Element relevant.

Tabelle B.2: Kind-Elemente des root-Elements `TxDatensatz`

Die folgenden Tabellen listet mögliche Definitionen und Attribute der Kind-Elemente.

Definition	Beschreibung
`xs:schema`	Schema-Dokumentelement, das dem Namensraum xmlns:xs="http://www.w3.org/2001/XMLSchema"(W3C XML Schema) angehört.
`xs:element`	Definition eines Elements.
`xs:complexType`	Definiert, dass ein Element Attribute tragen darf oder Kind-Elemente enthalten darf.
`xs:sequence`	Definiert, dass die Kind-Elemente in einer bestimmten Folge auftreten müssen.
`xs:choice`	Definiert, dass eines der umschlossenen Elemente ausgewählt werden muss.

Tabelle B.3: Definitionen der Elemente der Grundstruktur. Das Präfix `xs` wird zur Verknüpfung mit dem W3C XML-Schema verwendet.

Attribut	Beschreibung
`name`	Name des Elements.
`type`	Datentyp des Elements.
`fixed`	Festgesetzter Wert des Elements.

Tabelle B.4: Attribute der Elemente der Grundstruktur. Das Präfix `xs` wird zur Verknüpfung mit dem W3C XML-Schema verwendet.

Der Container <xs:annotation> enthält ergänzende Informationen, die wiederum in einem der zwei Container <xs:documentation> und <xs:appinfo> enthalten sind.

Container	Beschreibung
<xs:documentation>	Informationen zu Datenexport und -beschreibung.
<xs:appinfo>	Informationen zu Datenimport und -zusammenführung.

Tabelle B.5: Container innerhalb des Containers <xs:annotation>

Die oben genannten Container können ein Attribut source enthalten, das Informationen für den Datenexport beim Datenlieferanten (Datenquellen, Exportbedingungen) angibt oder für den Aufbau der BED-DB relevante Informationen enthält (Primärschlüssel, Bezeichnung von Variablen).

Attribut	Beschreibung
variable_description	Beschreibung der BED Variable beim Datenlieferanten.
variable_name	Quellvariablenname beim Datenlieferanten für die BED Variable.
variable_choices	Auswahlliste gültiger Optionen für die angegebene Quellvariable.
condition_X_field	Bedingung für den Export des Datums beim Datenlieferanten. Export ausschließlich, wenn angegebene Quellvariable beim Datenlieferanten für übermittelten Fall vorhanden ist oder den in condition_X_value angegebenen Wert hat. Mehrere Bedingungen X werden per ODER verknüpft.
condition_X_value	Bedingung für den Export des Datums beim Datenlieferanten. Export ausschließlich, wenn in condition_X_value angegebene Quellvariable den angegebenen Wert hat.
condition_year	Bedingung für den Export des Datums beim Datenlieferanten. Export ausschließlich für das angegebene Erfassungsjahr. Mehrere Bedingungen werden per ODER verknüpft.
isUniqueKey	Angabe, ob Variable als Primärschlüssel in der BED-DB genutzt wird. Wenn true, dann ist der Wert verpflichtend.
identifier	Patientenidentifizieren Daten, mit denen die entsprechenden medizinischen Daten verknüpft sind.
identifier_key	Patientenidentifizieren Daten, mit denen die entsprechenden medizinischen Daten verknüpft sind und die auch als Primärschlüssel in der BED-DB genutzt werden.
shortName	Abgekürzter Elementname für den Aufbau der BED-DB.

Tabelle B.6: Werte des Attributs source der Container <xs:appinfo> und <xs:documentation>

B.1.2 Patientenidentifizierende Daten

In dem Element `<Patientenidentifizierende_Daten>` werden, wie in Abbildung B.2 gezeigt, die unmittelbar patientenidentifzierenden Daten (bspw. DSO-Kennnummer oder ET-Nummer) gesammelt. Für jedes enthaltene Element ist mit dem Attribut `type` der Datentyp festgelegt.

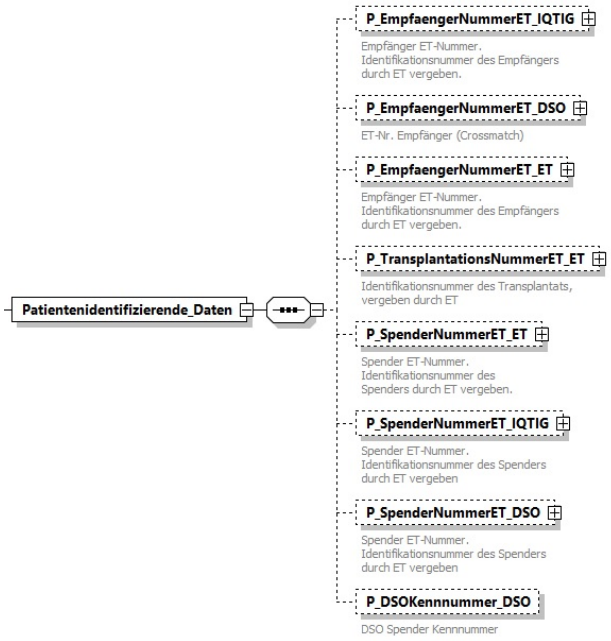


Abbildung B.2: Grundstruktur der XSD-Datei

```
<xs:element minOccurs="0" name="P_EmpfaengerNummerET_ET" type="et_nummer_type">
        <xs:annotation>
                <xs:documentation>Empfänger ET-Nummer. Identifikationsnummer des
                    ↪ Empfängers durch ET vergeben.</xs:documentation>
                <xs:documentation source="variable_name">General//Recipient
                    ↪ Number</xs:documentation>
                <xs:documentation source="variable_description">Recipient Number<
                    ↪ /xs:documentation>
                <xs:appinfo source="isUniqueKey">true</xs:appinfo>
                <xs:appinfo source="shortName">PEmpfaengerNrETET</xs:appinfo>
        </xs:annotation>
</xs:element>
```

Die patientenidentifizierenden Elemente tragen neben der ET- bzw. DSO-Nummer zwei Attribute:

```
<!-- Abstrakte ET-Nummern-Klasse -->
<xs:complexType abstract="true" name="et_nummer_type">
        <xs:attribute name="art" type="enum_et_nummer_type" use="required"/>
        <xs:attribute name="einwilligung" type="enum_et_einwilligung_type" use="
            ↪ required"/>
</xs:complexType>
```

Das Attribut `einwilligung` kann eine der drei Ausprägungen annehmen:

J Einwilligung vorliegend

N Einwilligung nicht vorliegend

X Einwilligung nicht erforderlich (z. B. postmortale Spender)

Das Attribut `art` kann eine der vier Ausprägungen annehmen:

ETE Eurotransplantnummer des Empfängers

ETL Eurotransplantnummer des Lebend-Spenders

ETP Eurotransplantnummer des Postmortem-Spenders

ETT Eurotransplantnummer des Transplantats

B.1.3 Medizinische Daten

In dem Elemen <Medizinische_Daten> werden alle medizinischen Angaben gebündelt.

```
...
<xs:element name="Elemente_Spender_Postmortem" minOccurs="0">
  <xs:annotation>
    <xs:appinfo source="identifier">P_SpenderNummerET_IQTIG</xs:appinfo>
    <xs:appinfo source="identifier_key">P_SpenderNummerET_IQTIG</xs:appinfo>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:element maxOccurs="unbounded" name="Element_Spender_Postmortem">
        <xs:complexType>
          <xs:sequence>
            <xs:element maxOccurs="1" minOccurs="0" name="
                ↪ S_Postmortem_Basisdaten_Alter_IQTIG" type="xs:integer">
...
            </xs:element>
            <xs:element maxOccurs="1" minOccurs="0" name="
                ↪ S_Postmortem_Basisdaten_Blutgruppe_IQTIG">
              <xs:annotation>
                <xs:documentation>Blutgruppe, Blutgruppe des Spenders, Blutgruppe
                    ↪ </xs:documentation>
                <xs:documentation source="variable_name">LUTX:T//BLUTGRUPPESPEN,
                    ↪ PNTX:T//BLUTGRUPPESPEN, HTXM:T//BLUTGRUPPESPEN</
                    ↪ xs:documentation>
                <xs:documentation source="variable_choices">1_A# 2_B# 3_0# 4_AB</
                    ↪ xs:documentation>
                <xs:appinfo source="shortName">SPostmBasisBlutgrIQTIG</xs:appinfo
                    ↪ >
              </xs:annotation>
              <xs:simpleType>
                    <xs:restriction base="xs:normalizedString">
                        <xs:enumeration value="A"/>
                        <xs:enumeration value="B"/>
                        <xs:enumeration value="0"/>
                        <xs:enumeration value="AB"/>
                    </xs:restriction>
              </xs:simpleType>
            </xs:element>
...
```

Der obige Ausschnitt zeigt exemplarisch die Entität `Elemente_Spender_Postmotem` und das Element `S_Postmortem_Basisdaten_Blutgruppe_IQTIG`.

B.1.4 Auswahl-Elemente DSO, ET, IQTIG

Innerhalb des Elements <Medizinische_Daten> findet sich das Auswahl-Elemente (<choice>) mit den Optionen <DSO>, <ET> und <IQTIG>. Jedes besitzt weitere Kind-Elemente, die die

medizinischen Daten gruppieren.

Eine Detailansicht für das Element
<Element_Empfaenger> ist in Abbildung B.3 zu sehen. Die abgebildete Struktur ist für alle Kind-Elemente der drei Datenlieferanten äquivalent definiert. Eine verallgemeinerte Beschreibung der Elemente ist in Tabelle B.7 gegeben.

Kind-Elemente	Beschreibung
<Elemente_X>	Kind-Element von einem der Auswahl-Elemente <IQTIG>, <DSO>, <ET>, das wiederum ein mehrfach wiederholbares Element <Element_X> enthält.
<Element_X>	Mehrfach wiederholbares Element in <Elemente_X>.

Tabelle B.7: Elemente der Auswahl-Elemente <IQTIG>, <DSO>, <ET>

Die Darstellung in der XSD-Datei sieht dabei wie folgt aus:

```
...
<xs:element name="Elemente_Empfaenger" minOccurs="0">
  <xs:annotation>
    <xs:appinfo source="identifier">P_EmpfaengerNummerET_IQTIG</xs:appinfo>
    <xs:appinfo source="identifier_key">P_EmpfaengerNummerET_IQTIG</xs:appinfo>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
          <xs:element maxOccurs="unbounded" name="Element_Empfaenger">
            <xs:complexType>
              <xs:sequence>
                <xs:element maxOccurs="1" minOccurs="0" name="
                    ↪ E_Basisdaten_Blutgruppe_IQTIG">>
...
                <\xs:element>
              <\xs:sequence>
            <\xs:complexType>
          <\xs:element>
        <\xs:sequence>
  <\xs:complexType>
<\xs:element>
...
```

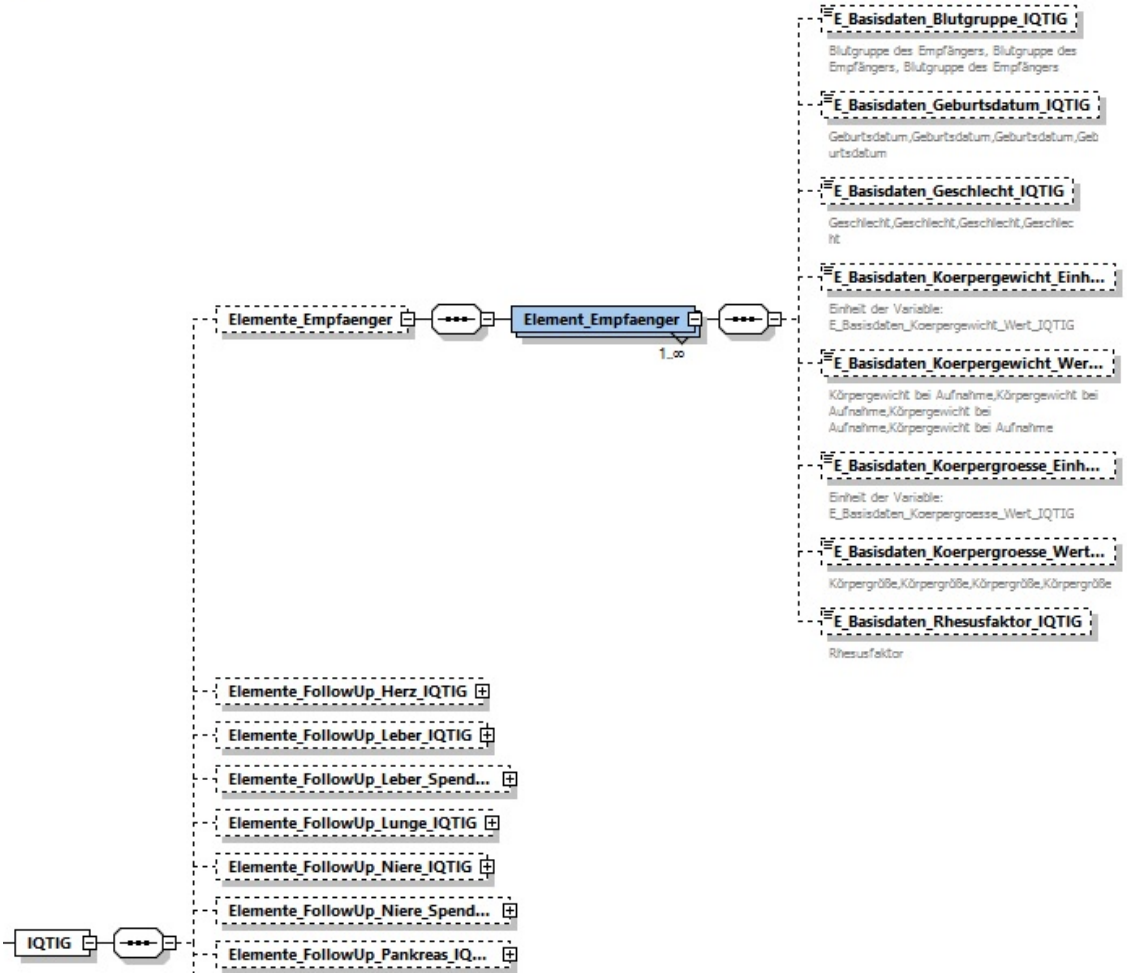


Abbildung B.3: Detailansicht des Elements <Element_Empfaenger>

B.2 Erzeugung Shortnames

Die Länge von Spaltenbezeichnungen ist in der der BED-DB zugrunde liegende SQL-Datenbank aus technischen Gründen begrenzt. Die BED-Variablennamen werden in der BED-DB daher durch sogenannte *Shortnames* ersetzt. Diese *Shortnames* bleiben auch beim Datenexport die Bezeichnungen der Spalten der exportierten Tabellen. Die Erzeugung der *Shortnames* aus den BED-Variablennamen erfolgt durch Ersetzung der Bezeichner entsprechend Tabelle B.8 (Altdaten) und B.9 (Neudaten).

BED	Shortname
_ (Unterstrich)	(wird entfernt)
Anamnese	Anamn
Basisdaten	Basis
Blutgruppe	Blutgr
Crossmatch	Crossm
Dringlichkeit	Dringl
Herz	H
Identifikation	Id
Immunologie	Imm
Lebend	Leb
Leber	Le
Lunge	Lu
Medikation	Medi
Monitoring	Monit
Niere	N
Pankreas	P
Postmortem	Postm
Virologie	Vir

Tabelle B.8: Ersetzungsliste für die Umwandlung der BED-Variablennamen in Shortnames (Altdaten).

BED	Shortname
_ (Unterstrich)	(wird entfernt)
Anamnese	Anamn
Basisdaten	Basis
Blutgruppe	Blutgr
Clavien	Cla
Crossmatch	Crossm
Dindo	Din
Dringlichkeit	Dringl
Herz	He
Identifikation	Id
Immunologie	Imm
Kreislaufunterstuetzungssystem	KLUS
Lebend	Leb
Leber	Le
Lunge	Lu
Mechanisch	Mech
Medikation	Medi
Mikrobiologie	Mikrob
Monitoring	Monit
Niere	Ni
Nummer	Nr
Pankreas	Pa
Pathologie	Path
Postmortem	Postm
Toxikologie	Toxik
Untersuchung	Untersuch
Virologie	Vir

Tabelle B.9: Ersetzungsliste für die Umwandlung der BED-Variablennamen in Shortnames (Neudaten).

B.3 Tx-Registerstelle Schnittstellenbeschreibung

B.3.1 Allgemein

Der vorliegende Anhang beschreibt die REST-Schnittstelle, die die Tx-Registerstelle der TxVST zur Datenübermittlung bereit stellt. Es werden, neben der technischen Spezifikation der Schnittstelle, Informationen zur Authentifizierung sowie Verschlüsselung des Datentransports und der XML-Dateien zur Verfügung gestellt. Weiterhin ist das Ergebnisprotokoll, das für jede Datenlieferung erstellt wird und über die REST-Schnittstelle abrufbar ist, beschrieben.

B.3.2 Authentifizierung

Die Authentifizierung der Datenübertragung erfolgt mittels Server- und Client-Zertifikaten, welche über die PKI (siehe Kapitel 10) bereitgestellt werden.

B.3.3 Einsatz von Verschlüsselung

Transportverschlüsselung

Alle Datenverbindungen zwischen der TxVST, der Tx-Registerstelle und zwischen den Servern der Tx-Registerstelle erfolgt transportverschlüsselt. Zusätzlich sind bei der Tx-Registerstelle eingehende Datenverbindungen nur für den IP-Adressbereich der TxVST freigeschalten. Dies dient der zusätzlichen Sicherheit, damit keine andere Instanz mit kompromittierten Zertifikaten im Namen der TxVST Daten senden kann.

Datenverbindungen, die nicht auf ssh basieren, z. B. die Verbindung per REST-Schnittstelle oder der Abruf der Webseiten, nutzen Secure Socket Layer (SSL) und Transport Layer Security (TLS) 1.2 oder 1.3 mit Forward Secrecy. Außerdem wird HSTS (HTTP Strict Transport Security) eingesetzt, damit alle Verbindungen nach dem initialen Verbindungsaufbau verschlüsselt sind. Dies ist ein zusätzlicher Schutz gegen Man-in-the-Middle-Angriffe. Es werden nur die folgenden Cipher zugelassen. Die Reihenfolge der Kompatibilitätsprüfung ist maßgebend. Andere als die aufgeführten Cipher sind nicht zugelassen, um eine Nutzung potentiell unsicherer Cipher zu verhindern.

- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA

Software, welche sich mit den Schnittstellen verbindet (z. B. Webbrowser oder Software zur Kommunikation mit der REST-Schnittstelle), muss diese Einstellungen zwingend unterstützen. Dies schließt u. a. die Nutzung von Internet Explorer kleiner Version 11 und Java kleiner Version 8 aus.

Verschlüsselung der XML-Dateien

Die Datenblöcke `<Patientenidentifizierende_Daten>` und `<Medizinische_Daten>` sind mit

einer XML-Verschlüsselung anhand des öffentlichen Schlüssels des jeweiligen Zieladressaten zu versehen (siehe Abschnitt 10.2). Die Verschlüsselung erfolgt asymmetrisch mit einem öffentlichen Schlüssel.

Die Patientenidentifizierenden-Daten sind immer mit dem öffentlichen Schlüssel der TxVST zu verschlüsseln. Die Medizinischen-Daten sind immer mit dem öffentlichen Schlüssel der Tx-Registerstelle zu verschlüsseln. Diese Verschlüsselung baut auf dem W3C-XML-Encryption-Standard auf.

Folgende spezielle Elemente sind bei der XML-Verschlüsselung zu beachten:

`EncryptedData` ist das einschließende Element für die XML-Verschlüsselung. Der gesamte Inhalt des übergeordneten Elements einschließlich der Attribute ist verschlüsselt

`CipherData` ist das verschlüsselte Element

`CipherValue` enthält die verschlüsselten Daten

`KeyInfo` erhält Informationen zum verwendeten Schlüssel

`id` enthält den Namen des Public Keys

Im Header der zu übertragenden XML-Datei ist der genutzte Schlüssel zu benennen:

```
<header>
  <encryption>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="pub.patient_tx
        ↪ -1.0.0">
          <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="
              ↪ patient_tx">
          <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
              ↪ oaep-mgf1p" />
            <xenc:CipherData>
              <xenc:CipherValue>lHnSrTuFccg801m3Y02/vsp33J+pN6nkKJe+
                  ↪ bKDbbf8azEWpKCAyrFmccuUMflwH7AKE3yuydFRo</xenc:CipherValue>
            </xenc:CipherData>
          </xenc:EncryptedKey>
    </ds:KeyInfo>
        ...
```

Die XML-Datei mit den verschlüsselten Datenblöcken hat folgendes Format:

```
<Faelle>
  <Fall Fall_Nr="1">
    <Patientenidentifizierende_Daten>
          <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Type
              ↪ ="http://www.w3.org/2001/04/xmlenc#Content">
          <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#
              ↪ aes128-cbc" />
            <xenc:CipherData>
```

```
            <xenc:CipherValue>lHnSrTuFccg801m3Y02/vsp33J+pN6nkKJe+
                ↪ bKDbbf8azEWpKCAyrFmccuUMflwH7AKE3yuydFRo</xenc:CipherValue>
            </xenc:CipherData>
          </xenc:EncryptedData>
    </Patientenidentifizierende_Daten>

        <Medizinische_Daten>
          <xenc:EncryptedData  Type="http://www.w3.org/2001/04/xmlenc#Content">
            <xenc:EncryptionMethod  Algorithm="http://www.w3.org/2001/04/xmlenc#
                ↪ aes128-cbc"  />
            <xenc:CipherData>
              <xenc:CipherValue>lHnSrTuFccg801m3Y02/vsp33J+pN6nkKJe+
                  ↪ bKDbbf8azEWpKCAyrFmccuUMflwH7AKE3yuydFRo</xenc:CipherValue>
            </xenc:CipherData>
          </xenc:EncryptedData>
        </Medizinische_Daten>
  </Fall>
</Faelle>
```

B.3.4 Technische Schnittstellenbeschreibung

Die Tx-Registerstelle stellt eine REST-Schnittstelle bereit, die im Rahmen der Neudatenübermittlung an das Tx-Register die Datenübermittlung/ Datenaktualisierung sowie eine automatisierte Abfrage des Bearbeitungsstatus der Datenlieferungen durch die TxVST ermöglicht. Diese Schnittstelle ist unter der URL

https://in.transplantations-register.de

erreichbar.

Die äquivalente Testinstanz (nur für Testzwecke und nicht für Produktivdaten zu nutzen) ist unter folgender URL erreichbar:

https://in.test.transplantations-register.de

Die Schnittstelle ist nur für den IP-Adressbereich der TxVST zugänglich. Die Übermittlung der XML-Dateien erfolgt im Body des Requests.

B.3.4.1 Datenlieferung über die Tx-Vertrauensstelle

Request

	Beschreibung
Request URL	/api/upload
Request Method	HTTP POST
Request Header	Accept: application/json
	Authorization: <Zugangsdaten (Basic-Authentifizierung)>
Request Body	File (String-Format)

Tabelle B.10: Request zur Datenlieferung durch die TxVST

Wurde der Datensatz erfolgreich per HTTP Request an die Tx-Registerstelle übermittelt, erhält die TxVST als Response den HTTP-Statuscode 201 sowie im Header einen zum Datensatz eindeutig bestimmten Location-Link, der die Transaktions-ID (UUID) enthält, und unter welchem das Ergebnisprotokoll heruntergeladen werden kann.
Im Fehlerfall wird der HTTP-Status 400 mit einem im Header angegebenen Location-Link, über welchen das Fehlerprotokoll heruntergeladen werden kann, zurückgegeben.
Der HTTP-Statuscode 500 wird zurückgegeben, falls ein technischer Fehler aufgetreten ist, der nicht mit der Lieferdatei im Zusammenhang steht. In diesem Fall muss eine erneute Lieferung vorgenommen werden.

Response

	Erfolg	Fehler
HTTP Statuscode	201	400/500
Header	Location-Link mit Transaktions-ID (UUID)	Location-Link mit Transaktions-ID (UUID)

Tabelle B.11: Response zur Datenlieferung durch die TxVST

B.3.4.2 Statusabfrage von Lieferdateien durch die Tx-Vertrauensstelle

Die Tx-Registerstelle stellt für jede Datenlieferung einen Request-URL zur Verfügung, der die Transaktions-ID (UUID) enthält und über den mittels eines GET-Requests die Ergebnisse der Verarbeitung einer Lieferdatei abgefragt werden können. Als Response sind die Statuscodes 200 sowie 400 und 500 möglich.

Der Statuscode 200 steht für eine erfolgreiche Annahme und Übertragung der Lieferdatei in die BED-DB. Der Statuscode 400 steht für eine nicht erfolgreiche Transformation der Lieferdatei in die BED-DB. Die genaue Information für eine nicht erfolgreiche Transformation können dem Fehlerprotokoll (Location-Link) entnommen werden. Der Statuscode 500 steht für einen technischen Fehler innerhalb der Tx-Registerstelle.

Die Response enthält das Ergebnisprotokoll, dessen Inhalt im Abschnitt B.3.4.5 beschrieben ist.

Request

	Beschreibung
Request URL	/api/upload/status/<Transaktions-ID>
Request Parameter (Verpflichtend)	Enthält die eineindeutige Transaktions-ID zur Identifizierung einer Lieferdatei
Request Method	HTTP GET
Request Header	Authorization: <Zugangsdaten (Basic-Authentifizierung)>

Tabelle B.12: Request zur Statusabfrage durch die TxVST

Response

	Erfolg	Fehler
HTTP Statuscode	200/204	404
Response Body	Transaktions-ID, Zeitstempel und Importlog	Die angegebene Transaktions-ID konnte nicht gefunden werden

Tabelle B.13: Response zur Statusabfrage durch die TxVST

B.3.4.3 Datenaktualisierung über die Tx-Vertrauensstelle

Die REST-Schnittstelle zur Datenaktualisierung ist identisch zur Schnittstelle der Datenlieferung (Abschnitt B.3.4.1), da Datenlieferungen chronologisch nach Lieferdatum abgearbeitet werden und somit eine Differenzierung nicht nötig ist.

B.3.4.4 Datenlöschung über die Tx-Vertrauensstelle

Die REST-Schnittstelle zur Datenlöschung ist identisch zur Schnittstelle der Datenlieferung (Abschnitt B.3.4.1).

B.3.4.5 Ergebnisprotokoll

Strukturierte Ergebnisprotokolle bilden die Basis für eine unkomplizierte und zielgerichtete Korrektur fehlerhafter Datenlieferungen seitens der Datenlieferanten. Das Ergebnisprotokoll enthält sowohl die Resultate der Vollzähligkeitsprüfung (Abgleich mit Sollstatistik) als auch der Vollständigkeitsprüfung (Abgleich mit XML-Schema).

Feldname	Erläuterung
id	Transaktions-ID der Lieferung (UUID)
name	Dateiname der Lieferdatei
createdAt	Zeitstempel zum Erhalt der Lieferung
fileDetails	Internes Objekt zur Verarbeitung von Lieferdateien
downloadQueueStatus	Listenobjekt zur Dokumentation der Dateiverarbeitung
message	Logmeldung des Prozessschrittes bei Gesamtverarbeitung
queueType	Geplanter Prozessschritt bei Gesamtverarbeitung
statusType	Ergebnisstatus des Prozessschrittes bei Gesamtverarbeitung
createdAt	Zeitstempel (Beginn) des Prozessschrittes bei Gesamtverarbeitung
updatedAt	Zeitstempel (Ende) des Prozessschrittes bei Gesamtverarbeitung
uploadStatus	Listenobjekt zur Dokumentation des Upload-Status
message	Logmeldung des Verarbeitungsschrittes beim Upload
statusType	Status des Verarbeitungsschrittes beim Upload
createdAt	Zeitstempel des Verarbeitungsschrittes beim Upload
downloadStatus	Listenobjekt zur Dokumentation des Importprozesses in BED-DB
message	Logmeldung des Importprozesses in BED-DB
statusType	Status des Importprozesses in BED-DB
deleteStatus	Listenobjekt zur Dokumentation des Löschen-Status
message	Logmeldung des Löschprozesses
statusType	Status des Löschprozesses

Tabelle B.14: Ergebnisprotokoll

Status	Erläuterung
IMPORT	Lieferdatei wird importiert
REIMPORT	Lieferdatei wird erneut importiert
DELETE	Lieferdatei wird gelöscht
DELETE_-REQUEST	Lieferdatei ist eine Löschanfrage [1]

Tabelle B.15: Ausprägungen von queueType für downloadQueueStatus

Status	Erläuterung
READY	Lieferdatei bereit für Import
RUNNING	Import der Lieferdatei wird verarbeitet
FINISHED	Import der Lieferdatei abgeschlossen
ERROR	Fehler beim Import der Lieferdatei

Tabelle B.16: Ausprägungen von statusType für downloadQueueStatus

[1] Löschen einzelner Daten oder Widerspruchslöschung, nicht Löschen von gesamter Lieferdatei

Status	Erläuterung
AGREED	Einverständniserklärung wurde erfolgreich geprüft
DECRYPTED	Lieferdatei wurde erfolgreich entschlüsselt
VALIDATED	Lieferdatei wurde erfolgreich auf XML-Wohlgeformtheit und XML-Schema geprüft
STORED	Lieferdatei wurde erfolgreich im Dateisystem abgespeichert
ERROR	Bei der Verarbeitung der Lieferdatei ist ein Fehler aufgetreten

Tabelle B.17: Ausprägungen von statusType für uploadStatus

Status	Erläuterung
INFO	Logmeldung während Import in die BED-DB
ERROR	Fehlermeldung während Import in die BED-DB

Tabelle B.18: Ausprägungen von statusType für downloadStatus

Status	Erläuterung
RECEIVED	Löschanfrage erkannt/erhalten
START_DELETING_PROCESS	Löschprozess gestartet
START_DELETING_FILE_INPUT_DB	Löschen von Lieferdatei in Input-DB
FINISHED_DELETING_FILE_INPUT_DB	Löschen von Lieferdatei in Input-DB abgeschlossen
START_DELETING_FILE_BED_DB	Löschen von gecachter Lieferdatei in BED-DB
FINISHED_DELETING_FILE_BED_DB	Löschen von gecachter Lieferdatei in BED-DB abgeschlossen
START_DELETING_DATA_BED_DB	Löschvorgang (Lieferdatei) in BED-DB gestartet
FINISHED_DELETING_DATA_BED_DB	Löschvorgang (Lieferdatei) in BED-DB abgeschlossen
START_REIMPORT_DATA_BED_DB	Reimport in BED-DB gestartet
FINISHED_REIMPORT_DATA_BED_DB	Reimport in BED-DB abgeschlossen
FINISHED_DELETING_PROCESS	Löschvorgang (Lieferdatei) in BED-DB abgeschlossen
ERROR	Fehler beim Löschvorgang

Tabelle B.19: Ausprägungen von statusType für deleteStatus

B.4 Tx-Vertrauensstelle Schnittstellenbeschreibung

Der folgende Anhang beschreibt die von der TxVST zur Verfügung gestellte REST-Schnittstelle, über die Datenlieferanten XML-Lieferdateien serialisiert per HTTPS übertragen können.

Nortal

TXVST

Transplantionsregister Vertrauensstelle

SCHNITTSTELLENBESCHREIBUNG

DATUM:

17.11.2020

VERANTWORTLICH FÜR DIESES DOKUMENT:

Dirk Buchhorn

Financial Solutions

dirk.buchhorn@nortal.com

Inhaltsverzeichnis

1 Allgemein

Die Schnittstellenbeschreibung beschreibt die Schnittstellen, die die Vertrauensstelle des Transplantationsregisters für andere Systeme bereit stellt. Es werden neben den Schnittstellenmethoden und -datenformaten die Wertebereiche einzelner Parameter sowie mögliche Fehler beim Schnittstellenaufruf, Einschränkungen hinsichtlich Berechtigungen beschrieben.

Ergänzend zu diesem Dokument ist die technische Spezifikation der Datenstrukturen der Vertrauensstelle innerhalb des Pakets TxVST-XML-Strukturen zu sehen. Darin werden die Regeln der Datenstrukturen innerhalb von Schema-Dateien beschrieben und durch Beispiel-XML-Dateien veranschaulicht.

Alle Schnittstellen nutzen die REST-Paradigmen. Sie sind über HTTPS aufrufbar. Alle Daten können in XML serialisiert übertragen werden. Dies gilt für Anfragedaten ebenso wie für Antwortdaten.

2 Authentifizierung

Der Zugriff auf die Vertrauensstelle kann nur durch autorisierte Aufrufer erfolgen. Aus diesem Grund müssen sich Aufrufer am System authentifizieren.

2.1 HTTPs-Client-Zertifikate

Die Authentifizierung an der Schnittstelle der Vertrauensstelle Transplantationsregister erfolgt durch die Verwendung von HTTPs-Client-Zertifikaten.

HTTPS-Client-Zertifikate werden jeweils beim Verbindungsaufbau für die Authentifizierung eines Requests genutzt. Ohne bzw. mit einem ungültigen Zertifikat wird der Zugriff auf das System bereits auf der TLS-Ebene unterbunden. Prinzipbedingt wird das Zertifikat selbst nicht bei der Authentifizierung übertragen sondern nur zur Signierung der Anfrage genutzt. Der Server ordnet das Client-Zertifikat des Aufrufers einem Benutzerkonto zu und teilt diese Information mit der Verarbeitungslogik der Vertrauensstelle, die in der Folge die Autorisierung des Benutzerkontos für die aufgerufene Aktion prüfen kann.

Das Zertifikat wird von den Schnittstellennutzer als Private- / Public-Key-Paar erzeugt und von der zentralen PKI der Transplantationsregisters signiert. Es besitzt eine begrenzte Gültigkeit von typischerweise zwei bis vier Jahren und muss daher regelmäßig erneuert werden.

3 Einsatz von Verschlüsselung

3.1 Verschlüsselung der Datenübertragung

Die Übertragung der Daten erfolgt durch eine mit Server- und Client-Zertifikaten abgesicherte HTTPs-Verbindung mittels TLS-Verschlüsselung, die sich jeweils am aktuellen Stand der Technik orientiert.

3.2 Verschlüsselung der Inhalte in XML

Der W3C bietet einen hybriden Verschlüsselungsstandard XML-ENC, womit Elemente in einer XML-Datei verschlüsselt werden können. Dieses wird für die XML-Daten im Rahmen der Vertrauensstelle Transplantationsregister eingesetzt.

Alle Patientendaten in einer XML-Lieferung werden mit einem für jede Lieferung neu generiertem symmetrischen Schlüssel verschlüsselt. Dieser symmetrische Schlüssel wird mit dem öffentlichen Schlüssel der Vertrauensstelle asymmetrisch verschlüsselt. So kann nur die Vertrauensstelle den symmetrischen Schlüssel wiederherstellen, um die Patientendaten lesen zu können.

Die medizinischen Daten sind ebenfalls mit dem öffentlichen Schlüssel des TxRegisters zu verschlüsseln. Wird der RestClient für die Übertragung der Daten eingesetzt, dann übernimmt dieser auch die Datenverschlüsselung, wenn die Daten noch nicht verschlüsselt vorliegen.

4 Technische Schnittstellenbeschreibung

4.1 Schnittstellenoperationen

Die folgende Tabelle listet eine Übersicht aller Schnittstellenoperationen auf, die von der Vertrauensstelle Transplantationsregister zur Verfügung gestellt werden. Die konkrete Beschreibung der einzelnen Operation erfolgt in den folgenden Unterabschnitten.

Operation	HTTP Methode + URL	Beschreibung	Parameter
Dateneingang			
data delivery	`POST <Basis-URL>/txvst/v1/delivery/txvst-process/CORRECTION`	registriert einen neuen Vertrag für den Gutschein mit der übergebenen Nummer	*Siehe Abschnitt data delivery* Alle Werte werden in der Anfrage übergeben (Request-Body).
Datenprotokoll			
Status	`GET <Basis-URL>/txvst-status/v1/status/<trackingNumber>`	lädt die Details für eine Lieferung	Trackingnummer

4.2 Basis-URLs

Test-System: https://test.tx-vertrauensstelle.de

Produktiv-System: https://tx-vertrauensstelle.de

4.3 Standard Antwort

Folgendes Standard-Antwort-Format wird auf Seiten der Vertrauensstelle verwendet.

```
<response>
    <status>SUCCESS</status>
    <trackingNumber>de1-2020111208350264-0</trackingNumber>
    <errors>
        <error>
            <id>String</id>
            <module>String</module>
            <message>String</message>
        </error>
    </errors>
    <warnings>
        <warning>
            <id>String</id>
            <module>String</module>
            <message>String</message>
        </warning>
    </warnings>
    <-- Schnittstellen spezifische Daten -->
</response>
```

Response

Attribut	Beschreibung
status	Der Status der Anfrage. Mögliche Werte sind: SUCCESS, WARNING, ERROR
trackingNumber	Eindeutige Nummer für den Request. Jeder Protokolleintrag enthält diese Nummer. Eine Analyse ist anhand der Trackingnummer einfach möglich.
errors	Enthält Fehlermeldungen
warnings	Enthält Warnungen

Error und Warning

Attribut	Beschreibung
id	Id der Nachricht (z.B. COMMONS-1)
module	Name des Moduls in dem die Nachricht erstellt wurde
message	Nachricht

4.4 Fehler IDs

Id	Beschreibung
COMMONS-1	Allgemeiner Fehler
COMMONS-2	Interner Server Fehler
COMMONS-3	Der Medientyp wird nicht unterstützt
COMMONS-4	Daten können nicht verarbeitet werden
COMMONS-5	Header Parameter fehlen
COMMONS-6	Request Body fehlt
COMMONS-7	Autorisierungsfehler
COMMONS-8	Der angegebene Parameter wird nicht unterstützt
COMMONS-9	Nicht gefunden
COMMONS-10	Authentifizierungsfehler

4.5 Allgemeine Fehler

Folgende Fehlermeldungen sind über alle Schnittstellen hinweg möglich:

Antwort für Fehler	Status Code: 401 UNAUTHORIZED Beschreibung: Der Aufrufer konnte nicht authentifiziert werden. Status Code: 403 FORBIDDEN Beschreibung: Der Benutzer darf die Aktion benutzen oder auf die Ressource nicht zugreifen. Status Code: 415 UNSUPPORTED MEDIA TYPE Beschreibung: Die übermittelte Nachricht ist nicht vom Typ application/xml. Status Code: 50x Beschreibung: Bei der Verarbeitung ist es zu einem unvorhergesehenen Problem gekommen. Die Verarbeitung der Nachricht hat nicht stattgefunden.

4.6 data delivery

Beschreibung	• Übertragung von Daten durch Datenlieferanten, die pseudonymisiert und an einen Datenempfänger weitergeleitet werden sollen. • Die Daten werden nach dem Eingang gegen ein entsprechende XSD-Schema validiert. • Für fachliche und technische Fehler, die nicht von der Infrastruktur erzeugt werden, wird eine Fehlernachricht an den Client übergeben.
URL	`/txvst/v1/delivery/txvst-process/CORRECTION`
Methode	POST
URL Parameter	Nein
HTTP-Header Attribute	VST-Organization: txvst_org
Typ der Nachricht	application/xml
Request-Body	XML gültig nach dem TxReg Schema interface_DL_VST.xsd
Typ der Antwort	application/xml oder application/json abhängig vom Accept Header
Erfolgreiche Antwort	Status Code: 200 OK Beschreibung: Die Daten sind valide. Content:

```
<response>
    <status>SUCCESS</status>
    <trackingNumber>de1-2020111208350264-0</trackingNumber>
    <delivery>
        <deliveryTrackingNumber>de1-2020111208350264-
0</deliveryTrackingNumber>
        <certSerialId>1234567890</certSerialId>
        <workflowStatus>ACTIVE</workflowStatus>
        <workflowStartTs>2020-11-
12T07:35:03.749+0000</workflowStartTs>
        <workflowEndTs/>
        <durationInMillis/>
        <workflowHasIncidents>false</workflowHasIncidents>
        <workflowCompleted>false</workflowCompleted>
    </delivery>
</response>
```

4.6.1 Beschreibung des Antwortformats

Response

Attribut	Beschreibung
status	Der Status der Anfrage. Mögliche Werte sind: SUCCESS, WARNING, ERROR
trackingNumber	Eindeutige Nummer für den Request. Jeder Protokolleintrag enthält diese Nummer. Eine Analyse ist anhand der Trackingnummer einfach möglich.
delivery	Details zur Lieferung

Delivery

Attribut	Beschreibung
deliveryTrackingNumber	Enthält die Tracking Nummer, die bei der Lieferung generiert wurde
certSerialId	Die Serial des Client Zertifikates
workflowStatus	Der Status des internen Workflows. Mögliche Werte: ACTIVE, COMPLETED, ERROR, EXTERNALLY_TERMINATED Diese Werte sind abhängig von der eingesetzten Workflow Engine. Um zu prüfen ob der Workflow beendet ist sollte das Attribut "workflowCompleted" verwendet werden. Ob ein Workflow Fehler enthält kann mit dem Attribut "workflowHasIncidents" geprüft werden.
workflowStartTs	Zeitpunkt wenn der interne Workflow gestartet wurde
workflowEndTs	Zeitpunkt als der interne Workflow beendet wurde
durationInMillis	Dauer der Verarbeitung
workflowHasIncidents	Gibt an, ob der Workflow Fehler enthält
workflowCompleted	Gibt an, ob der Workflow beendet ist

4.7 status

Beschreibung	Abruf des Status von Datenlieferungen anhand der Tracking Nummer einer Lieferung.
URL	`/txvst-status/v1/status/[trackingNumber]`

Methode	GET
URL Parameter	trackingNumber - Die Tracking Nummer, die bei Übermittlung der Daten zurückgemeldet wurde.
Header Attribute	keine
Typ der Antwort	application/xml oder application/json abhängig vom Accept Header
Erfolgreiche Antwort	Status Code: 200 OK Beschreibung: Die Daten sind valide. Content: <response> <status>SUCCESS</status> <trackingNumber>txvst-status-2020111314464767-0</trackingNumber> <workflowStatus> <deliveryTrackingNumber>de1-2020101211543238-0</deliveryTrackingNumber> <workflowStatus>COMPLETED</workflowStatus> <workflowStartTs>2020-10-12T09:54:33.851+0000</workflowStartTs> <workflowEndTs>2020-10-12T09:55:12.336+0000</workflowEndTs> <durationInMillis>38485</durationInMillis> <workflowHasIncidents>false</workflowHasIncidents> <workflowCompleted>true</workflowCompleted> </workflowStatus> <txRegisterStatus> <status>COMPLETED</status> <statusMessage>Processing completed</statusMessage> <statusTs>2020-10-01T14:51:57.148+0200</statusTs> </txRegisterStatus> </response>
Antwort für Fehler	Status Code: 404 NOT FOUND Beschreibung: Anmeldung und Request sind gültig, aber diese Trackingnr. ist nicht für den aktuellen Abfragenden freigeschaltet. Content:

```
<response>
    <status>ERROR</status>
    <trackingNumber>txvst-status-2020111314503103-0</trackingNumber>
    <errors>
        <error>
            <id>COMMONS-9</id>
            <module>txvst-status</module>
            <message>Kein Status für remoteCertSerial 123456789 und
Trackingnummer de1-2020101211543238-0 gefunden. </message>
        </error>
    </errors>
</response>
```

workflowStatus

Attribut	Beschreibung
deliveryTrackingNumber	Enthält die Tracking Nummer, die bei der Lieferung generiert wurde
certSerialId	Die Serial des Client Zertifikates
workflowStatus	Der Status des internen Workflows. Mögliche Werte: ACTIVE, COMPLETED, ERROR, EXTERNALLY_TERMINATED Diese Werte sind abhängig von der eingesetzten Workflow Engine. Um zu prüfen ob der Workflow beendet ist sollte das Attribut "workflowCompleted" verwendet werden. Ob ein Workflow Fehler enthält kann mit dem Attribut "workflowHasIncidents" geprüft werden.
workflowStartTs	Zeitpunkt wenn der interne Workflow gestartet wurde
workflowEndTs	Zeitpunkt als der interne Workflow beendet wurde
durationInMillis	Dauer der Verarbeitung
workflowHasIncidents	Gibt an, ob der Workflow Fehler enthält
workflowCompleted	Gibt an, ob der Workflow beendet ist

txRegisterStatus

Attribut	Beschreibung
status	Status der Verarbeitung beim TxRegister. Mögliche Werte: COMPLETED, ERROR, IN_PROGRESS

Attribut	Beschreibung
statusMessage	Status Nachricht
statusTs	Zeitpunkt an dem der Status gesetzt wurde

B.5 Tx-Vertrauensstelle REST-Client

Der folgende Anhang beschreibt den von der TxVST zur Verfügung gestellten REST-Schnittstelle-Client, mittels dem verschlüsselte XML-Lieferdateien von den Datenlieferanten an die TxVST übertragen werden können.

TxVST

Brief instruction REST-Client

Version 1.01

16.10.2020

Table of Content

Liste of figures

List of tables

1 Introduction

The REST-Client is an application which enables data providers to operate the interfaces provided by the trusted third party (Vertrauensstelle) in order to transmit encrypted data to the transplant register (Tx-Reg). The REST-Client checks the encryption of the data before transmission to the transplant register and encrypts it if necessary.

2 Configuration

The REST-Client is provided as a zip-file. Unzip the file to a folder to be able to configurate the REST-Client before the inital start.

folder	description
config	contains the application properties that need to be configurated
data	all program files are stored here, a reset of the REST-Client is done by deleting the content of this folder
jdk11	contains java runtime
keys	contains Trusted Third Party Public Key and TxReg Public Key
lib	contains REST-Client application
log	contains logfile
schema-zip	XML schema.zip needs to be stored here
tmp	The temp directory shows all files that have been transmitted, encrypted and / or transformed. The files are not deleted automatically.

table 1 folder structure

In order to be able to communicate with the server interface of the trusted third party, the adress of the interface, the client certificate with the relating password and public keys must be integrated. The REST-Client is configured by opening the "application.properties" file, which is within the "config" folder. The editor can be used to specify the path to the user interface, the path to the client certificate and the path to public keys used.

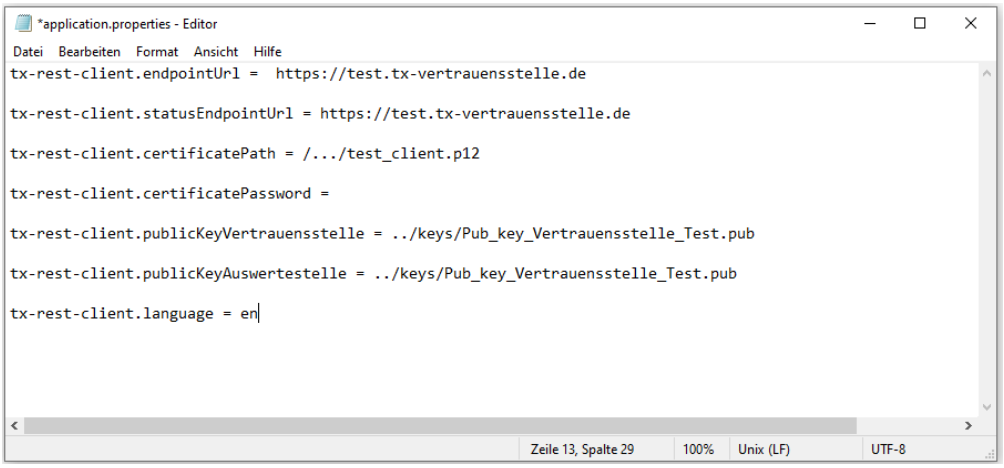


figure 1 configuration of the REST-Client

application properties	description
tx-rest-client.endpointUrl	adress to status interface
tx-rest-client.statusEndpointUrl	adress to status interface
tx-rest-client.certificatePath	insert the path to p.12 client certificate
tx-rest-client.certificatePassword	insert the password for the client certificate
tx-rest-client.publicKeyVertrauens-stelle	path to public keys for encryption, which are stored within the file "keys"
tx-rest-client.publicKeyAuswerte-stelle	path to public keys for encryption, which are stored within the file "keys"
tx-rest-client.language	choose language "en" or "de"

table 2 application properties

2.1 Procedure for the p12 file

1. Each data provider has to create its own private key and a certifcate signing request (csr).
2. The certificate signing request (csr) has to be uploaded to the PKI of the TxReg.
3. TxReg will sign the csr.
4. The signed file (crt) can be downloaded from the PKI.
5. The data provider is generating a p12 file from their own private key and the signed crt file.
6. The p12 file has to be implemented in the application properties.

note: A data delivery is only possible, if the Trusted Third Party is informed about the certificate serial of the client certificate, a user name and a emailadress.

2.2 XML schema-zip file

The REST-Client ist delivered with a XML schema.zip file. This zip file has to be inserted in the schema_zip folder.

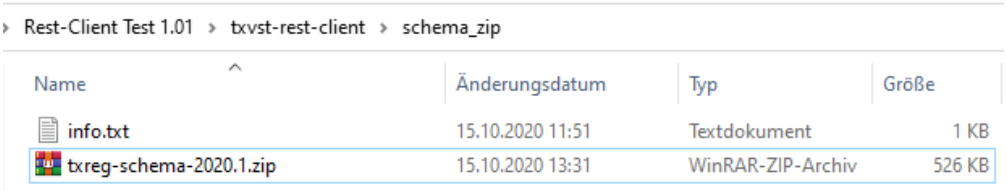


figure 2 Insert schema-zip file

The REST-Client unpacks the XML schema-zip file at the first start. The XML schema-zip file is unpacked into the "data/schema" folder and contains the used XML filestrutures.

One XML schema-zip file is required at least to use the REST-Client. If an updated version of the XML schema-zip file is inserted, the REST-Client chooses the most up to date file and unpacks it while starting.

3 Starting the REST-Client

To start the REST-Client use the supplied batch file (txvst-rest-client.bat) in the file folder. An installation is not necessary.

If there is any finding about missing configuration the REST-Client will show a message.

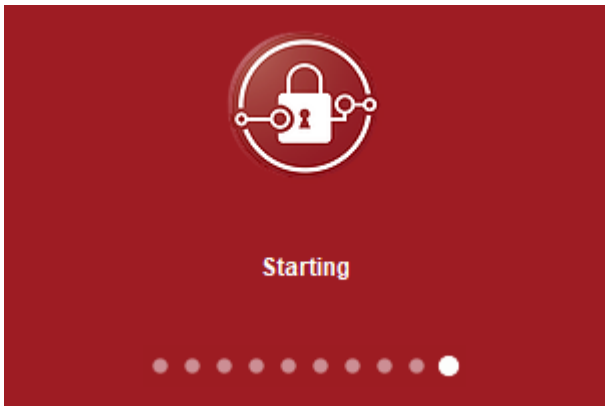


figure 3 starting the REST-Client

4 Upload of data

TxVST REST-Client starts with the user view "upload" that is structured in three different parts.

Configuration:

- adress to interface
- path to the used certificate
- Trusted Third Party public key
- TxRegister public key

File:

- file selection for upload

Upload:

- confirmation of upload process

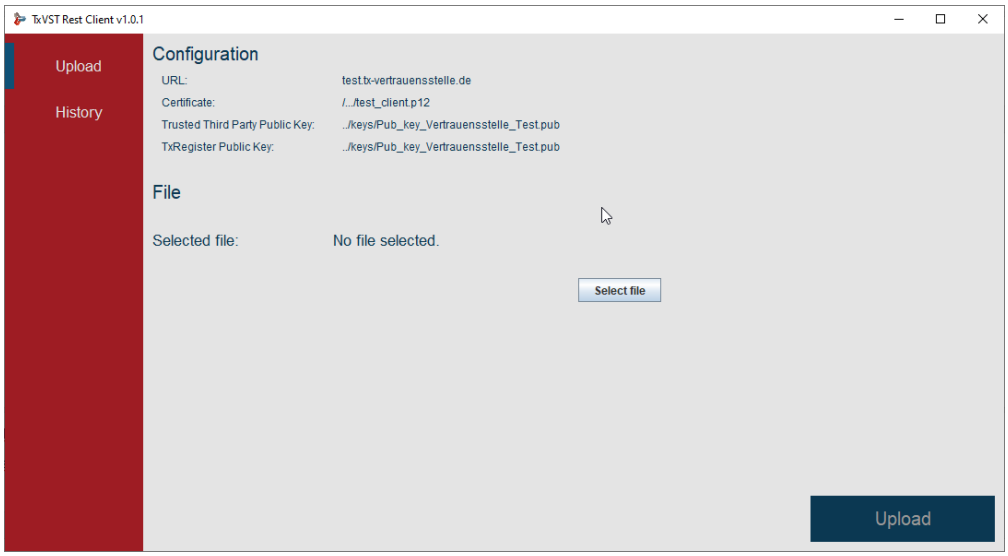


figure 4 user view REST-client "upload"

By pressing "select file" the file selection dialog will open. The requested format is xml. Pressing the "open" button will close the file selection dialog and the file can be uploaded.
butto

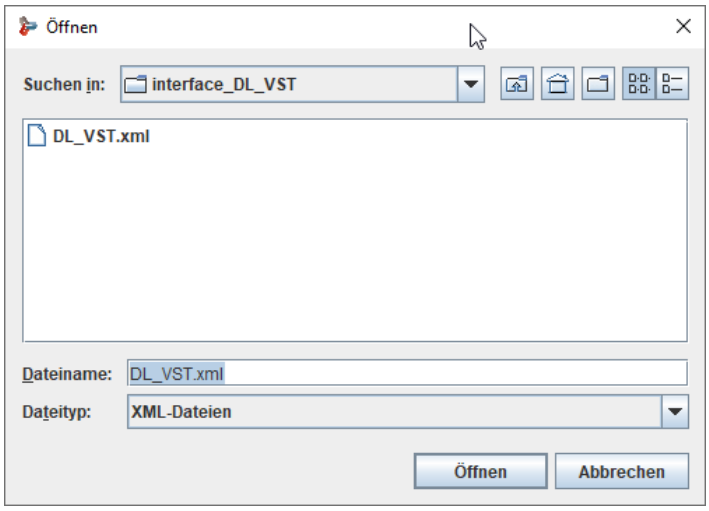


figure 5 file selection

The REST-Client checks the selected file for encryption of patient data and medical data. In case of the encryption of the selected file with the public keys (Transplant Register, Trusted Third Party) the REST-Client transmits the data to the transplant register.

A upload status will show the status relating the selected xml file. A green text will occure if the upload was successful. A red text will show that the upload was not successful.

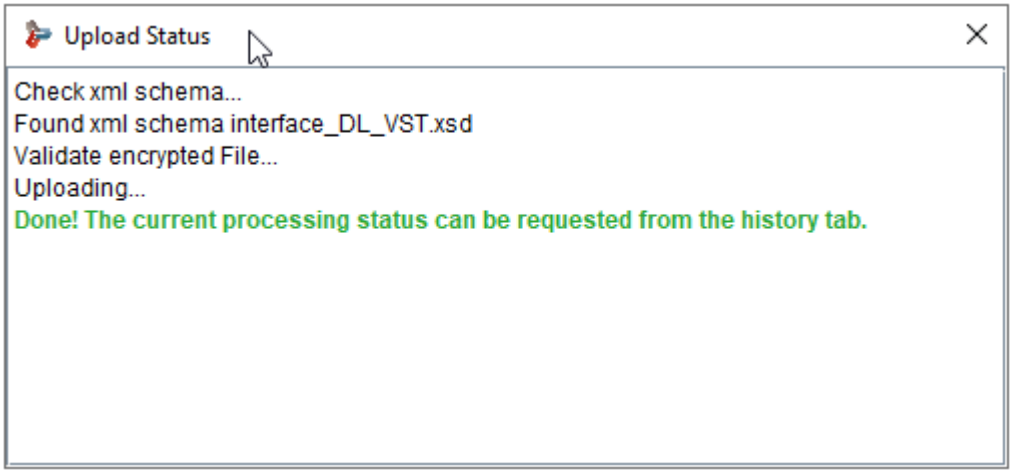


figure 6 check XML schema

If there is no encrpytion found, the REST-Client will encrypt the selected file and start the transmission to the transplant register. A status about the encryption, the location of the encrypted file and the transmittal to the transplant register is given.

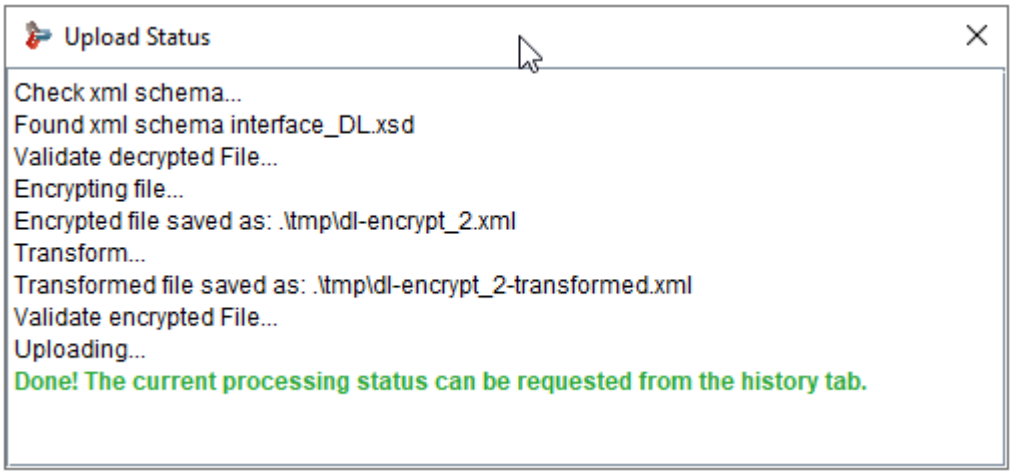


figure 7 status of encryption

5 Upload error

A failed encryption is shown in the upload status. A transmission to the transplant register is not done.

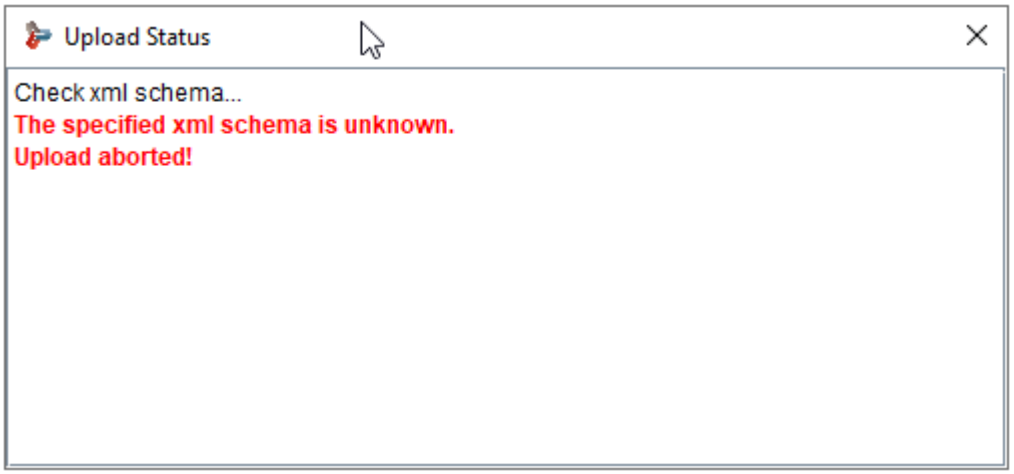


figure 8 error message "invalid xml scheme"

6 View of history

The view "history" shows the uploaded files in a chronological order.

Each uploaded file has a specific tracking number, an upload date, a status of the workflow of the Trusted Third Party and a status of the Tx-Reg. Each upload information can be refreshed to receive an update on the status. The upload information can also be removed from the history.

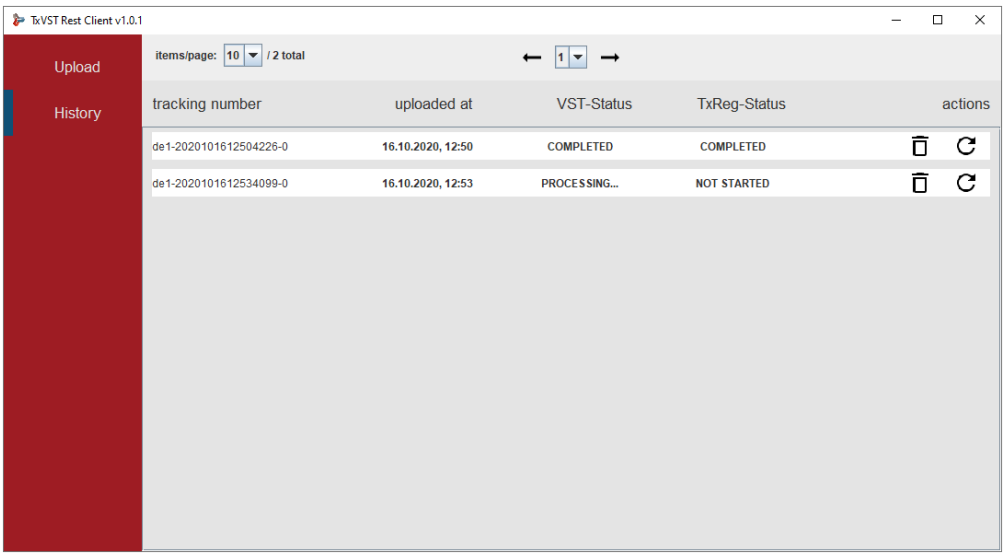


figure 9 user view REST-client "history"

property	description
tracking-number	identification number of the transmitted files
uploaded at	showing time and date of each upload
VST-Status	
UPLOADED	file has been uploaded to the Trusted Third Party
PROCESSING	file is within the workflow of the Trusted Third Party
COMPLETED	file has completed the workflow of the Trusted Third Party
TxReg-Status	
NOT STARTED	file has not been send to TxReg
IN PROGRESS	file is in progess at TxReg
COMPLETED	file has completed the workflow at TxReg
ERROR	file can not be send to TxReg

table 3 user view REST-Client "history"

7 Update

If necessary a new file of the REST-Client, the schema-zip file or the public keys will be made available.