Koordinierungsstelle
für IT-Standards

IT-Planungsrat

XTA - Rahmenbedingungen (Version 0.1)

1. Dezember 2023 / Draft

Inhaltsverzeichnis

Vorwort

Der Standard OSCI–Transport ist entwickelt worden, um sichere und zuverlässige Nachrichtenübermittlungen über das grundsätzlich unsichere Internet zu gewährleisten. Die Nutzung dieses Standards generiert auch in sicheren Netzen Mehrwerte, wie zum Beispiel Ende-zu-Ende Sicherheit und Adressierung, oder auch Nachweise zur Integrität der Nachrichten, die durch die Netzebene allein nicht abgedeckt werden.

Im Rahmen der Umsetzung des Standards OSCI-Transport auf allen Verwaltungsebenen und in verschiedenen fachlichen Bereichen ist eine OSCI–Infrastruktur entstanden, der auch Komponenten wie das DVDV zuzurechnen sind. Durch die Vielzahl der Einsatzgebiete und durch wechselnde rechtliche Rahmenbedingungen sind die Anforderungen an die Schnittstellen zwischen den Fachverfahren und der Transportinfrastruktur der öffentlichen Verwaltung stark gestiegen.

Es hat sich gezeigt, dass in den meisten E–Government-Anwendungen eine Aufteilung zwischen Fach- und spezialisierten Transportverfahren sinnvoll sein kann. In solchen Fällen wird eine standardkonforme Kommunikation zumeist nur zwischen den Transportverfahren der beauftragten Rechenzentren der öffentlichen Verwaltung gewährleistet, während die Kommunikation zwischen den Transportverfahren und den Fachanwendungen über proprietäre Schnittstellen erfolgt. Dies führt zu erhöhten Aufwendungen bei den Beteiligten und bei den Herstellern überregionaler Fachanwendungen, da diese unterschiedliche Schnittstellen unterstützen müssen. Auch kann eine datenschutzgerechte Umsetzung der Kommunikation zwischen den Fachverfahren aufgrund dieser individuellen Schnittstellen nicht einheitlich umgesetzt werden. Die in diesem Kontext entstehenden Fragestellungen und Lücken sind fachunabhängig oder zumindest fachübergreifend und daher im Zuständigkeitsbereich des IT–Planungsrats zu behandeln.

Diese Lücken werden im Auftrag des IT-Planungsrats durch den Standard XTA geschlossen.

Dieses Dokument wurde vom Expertengremium Sicherer Transport erstellt.

1 Einleitung

Das Dokument XTA Rahmenbedingungen wendet sich an Prozessverantwortliche, Verfahrenshersteller, IT- und Projektleiter. Es erläutert die grundlegenden Konzepte von XTA und beschreibt die Anforderungen an einen rechtskonformen und sicheren Einsatz. Außerdem werden Aussagen zur Infrastruktur und Grundprinzipien getroffen. Entwickler können es vor der Implementierung von Anwendungen für den Einstieg in den Bereich Sicherer Transport nutzen und später als Grundlage für die Kommunikation mit den Projektleitenden bzw. Verantwortlichen verschiedener Bereiche verwenden. Die Spezifikation des Standards XTA, insbesondere die Beschreibung des Moduls XTA Webservice, richtet sich primär an die Entwickler. Die Pflege und Herausgabe der XTA Rahmenbedingungen ist von den Release-Zyklen der Spezifikation von XTA entkoppelt.

Das Dokument ist wie folgt aufgebaut:

- Kapitel 1, *Einleitung* – Aufbau und Zielgruppe dieses Dokuments sowie Abgrenzung zu den anderen Dokumenten des Standards XTA (dieses Kapitel).
- Kapitel 2, *Einführung* – Überblick über die XTA Module, deren Ziele und Einordnung in das Ebenenmodell und das Zusammenwirken der Infrastrukturen.
- Kapitel 3, *Einsatzumfeld und Rollen* – Herleitung und ausführliche Beschreibung des XTA Rollenmodells
- Kapitel 4, *Abläufe und Verfahren* – Grundlegende Beschreibung der Abläufe beim Steuern durch XTA Service Profile und Versand und Empfang durch XTA Webservice.
- Kapitel 5, *Normen, Standards und Regeln* – Beschreibung von Normen, Standards und Regeln, die bei der Entwicklung des Standards XTA beachtet / verwendet werden.
- Stichwortverzeichnis

2 Einführung

2.1 XTA Module

Der Standard XTA besteht aus zwei Modulen:

XTA Service Profile (XTA-SP)
Das Modul XTA Service Profile ist das Instrument zur einheitlichen Definition und Konfiguration der regelgeleiteten Anforderungen an den Transport. Mit diesem Werkzeug können die Anforderungen an Datenschutz und Datensicherheit – z. B. bzgl. der Sicherung der Vertraulichkeit und Zweckbindung – für einen Transport definiert und damit einheitlich konfigurierbar gemacht werden.

Die öffentliche Verwaltung erhält mit den Serviceprofilen die Möglichkeit der *normativen* und *regelgeleiteten* Steuerung.

XTA Webservice (XTA-WS)
Das Modul XTA Webservice vereinheitlicht die funktionalen Schnittstellen zwischen Fach- und Transportverfahren (auch innerhalb eines Landes oder Rechenzentrums), um die Übermittlung von Nachrichten – also den Transport – zu standardisieren. Zum Auslieferungsgegenstand der Spezifikation gehört neben dem vorliegenden Dokument mit dem Spezifikationstext eine WSDL-Datei, die alle benötigten XTA Schemata einbindet.

Die öffentliche Verwaltung erhält mit dem XTA Webservice die Möglichkeit der *funktionalen* Steuerung.

XTA Webservice und XTA Service Profile stehen konzeptionell in starkem Bezug zueinander, beide Module können unabhängig voneinander eingesetzt werden.

Die formale Definition der Module befindet sich im Dokument *Spezifikation XTA*. Die Verwendung dieser Module wird im Kapitel 4, *Abläufe und Verfahren* erläutert.

2.2 Interoperabilität im E–Government

Erfolgreiches E–Government in föderalen Strukturen zeichnet sich durch den konsequenten Einsatz und die Durchsetzung offener Standards aus. Diese gewährleisten die für den reibungslosen Nachrichtentransport notwendige Interoperabilität bei allen betroffenen IT-Verfahren.

Beim Nachrichtentransport werden Ebenen unterschieden, auf denen die jeweiligen Aufgaben mit spezifischen Mechanismen gelöst werden. Manche Ebenenmodelle sind sehr differenziert (siehe z. B. das Open Systems Interconnection Model der ISO), für die Diskussion im Rahmen dieses Dokuments ist eine Betrachtung von drei Ebenen ausreichend[1]:

Anwendungsebene
Die Akteure der Anwendungsbene sind die untereinander kommunizierenden Fachverfahren. Ihre Aufgabe ist die Abwicklung fachlicher Prozesse. Standards sorgen für eine einheitliche Interpretation der fachlichen Daten und eine einheitliche Anbindung an die Transportinfrastruktur. Beispielswei-

[1] Vereinfachte Darstellung, orientiert am TCP/IP-Referenzmodell, siehe RFC 1122 – Requirements for Internet Hosts – Communication Layers. – Oktober 1989 (Internet Engineering Task Force, englisch).

se wird durch den Fachstandard OSCI–XMeld gleichsam eine gemeinsame Sprache (Syntax und Semantik) für Sachverhalte des Meldewesens vereinbart, die jedes IT-Verfahren im Meldewesen beherrschen muss.

Transportebene

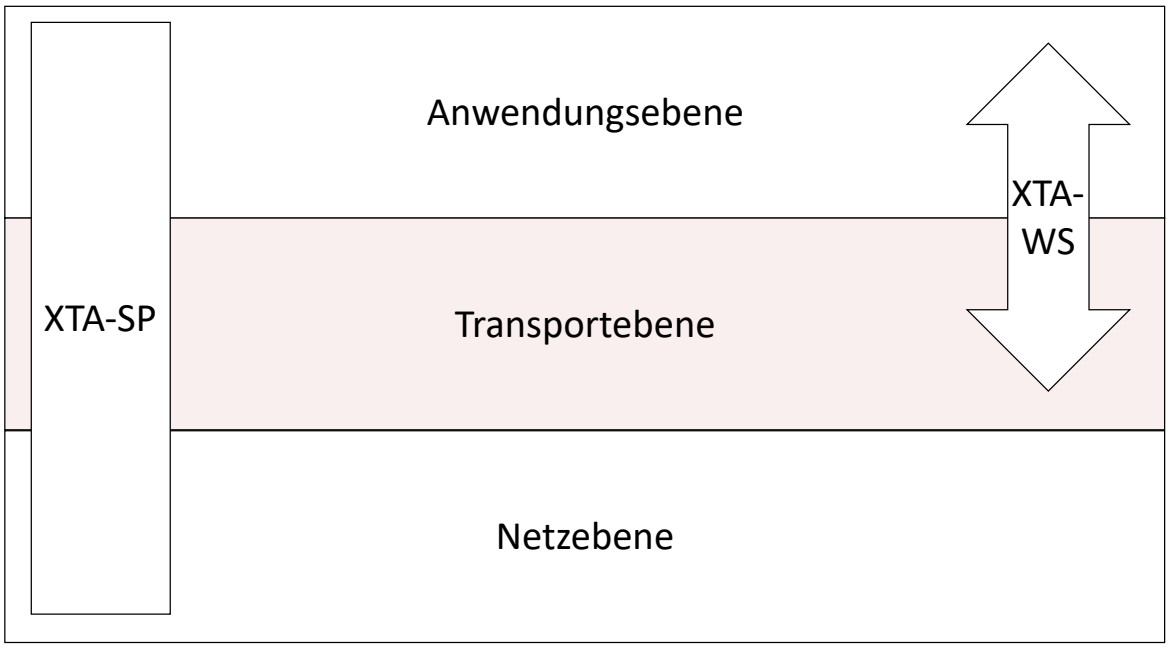
Die Akteure der Transportebene sind die untereinander kommunizierenden Transportverfahren. Ihre Aufgabe ist die Realisierung von Kommunikation der Anwendungsebene. Standards sorgen für eine einheitliche Interpretation der technischen Daten und eine einheitliche Anbindung an die Netzwerkinfrastruktur. Beispielsweise betrifft dies die Adressierung auf Basis verwaltungseigener Verzeichnisdienste, die zuverlässige Zustellung, die Sicherstellung von Anforderungen des Datenschutzes und der Informationssicherheit sowie die Behandlung von Fehlern.

Netzebene

Die Akteure der Netzebene stellen Direktverbindungen zwischen Netzwerkkomponenten her. Ihre Aufgabe ist die Weiterleitung von empfangenen Datenpaketen an das ermittelte nächste Zwischenziel. Im Kontext des E–Government können verwaltungseigene Netze (z.B. Verbindungsnetz gemäß IT-NetzG) oder das Internet genutzt werden. Die Interoperabilität auf der Netzebene wird durch Industriestandards gewährleistet.

Der Standard XTA bietet mit seinen Modulen XTA Webservice (XTA-WS) eine funktionale und XTA Service Profile (XTA-SP) eine modale Steuerung des *Transports*, siehe Abbildung 2.1.

Abbildung 2.1. Das XTA Ebenenmodell



2.3 Sicherer und zuverlässiger Nachrichtentransport

Die Organisation eines zuverlässigen und sicheren Nachrichtentransports ist eine komplexe Aufgabe:

- Elektronische Adressen müssen aus Verzeichnisdiensten ermittelt, Sicherheitsmechanismen konfiguriert und der Versand nachverfolgt werden.

- Störungen, wie der Verlust einer Nachricht, müssen erkannt und nachhaltig behoben werden.
- Fristen sind zu überwachen und Eskalationsmechanismen zu bestimmen.
- Die rechtlichen Rahmenbedingungen sind einzuhalten.

Für die Bewältigung dieser Aufgaben reicht die reine Verwendung von Übertragungstechnologien nicht aus. Relevant ist ihre korrekte Verwendung gemäß den funktionalen und normativen Anforderungen. Diese Anforderungen sind formal zu spezifizieren (XTA-SP), ebenso wie ihre Umsetzung in ihre spezifische Parametrisierung der Übertragungstechnologie. Nur so kann die Sicherheit und Rechtskonformität des Nachrichtentransports flächendeckend, einheitlich und in einer hohen Qualität gewährleistet werden. Damit zwischen der Anwendungs- und Transportebene die Anforderungen und Aufgaben klar voneinander getrennt werden können, erfordert es einer formalen und einheitlichen Beschreibung der Schnittstellen zwischen den genannten Ebenen (XTA-WS).

Aus den genannten Anforderungen ist der Standard XTA im Bereich der Innenverwaltung entstanden. Aufgrund seiner Qualität, Flexibilität und vielfachen Anwendbarkeit kommt er in immer mehr Bereichen zum Einsatz. In den Bereichen, für die XTA relevant ist, werden jährlich mehrere hundert Millionen von Nachrichten zwischen insgesamt über 100.000 Kommunikationspartnern ausgetauscht.[2]:

- Im elektronischen Rechtsverkehr (Justiz) wird OSCI–Transport in besonders starkem Maße auch für die Nachrichtenübermittlung mit Kommunikationspartnern außerhalb der öffentlichen Verwaltung genutzt.
- Die OSCI-Infrastruktur deckt die Anforderungen der Innenverwaltung (z.B. Melde-, Ausländer- und Personenstandswesen) ab.
- Für die OZG-Antragsübermittlung an Fachverfahren sollen die Standards OSCI-Transport & XTA flächendeckend zum Einsatz kommen und sind bereits in mehreren Bereichen etabliert.
- OSCI wird auch in vielen weiteren Bereichen eingesetzt: beispielsweise ZKS Abfall, Emissionshandel, Marken- und Patentanmeldung

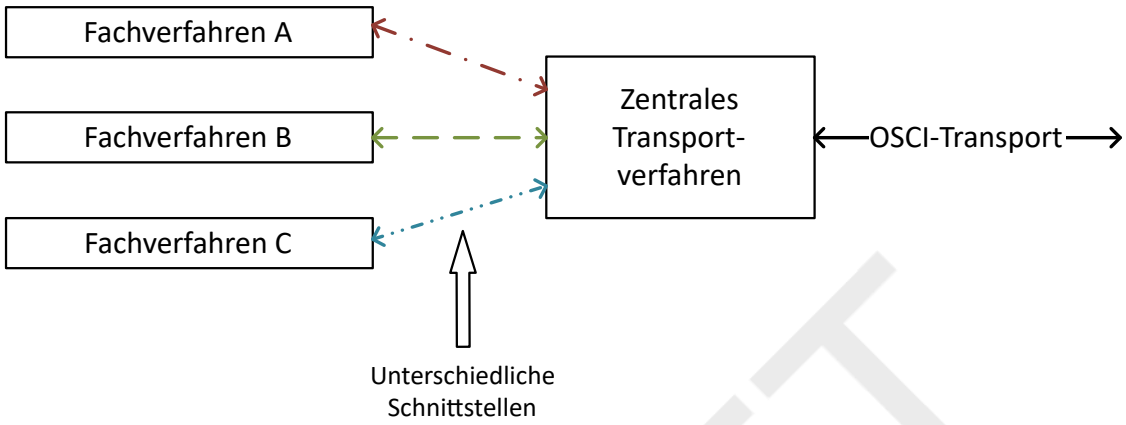
Die in vielen Bundesländern eingerichteten Clearing- oder Vermittlungsstellen (Betreiber von Transportverfahren) gehören der Transportebene an. Auf der Anwendungsebene sind zum Beispiel die Kommunen (Betreiber von Fachverfahren) mit unterschiedlichen, betriebenen XÖV-Standards anzusiedeln. In den folgenden Abschnitten wird gezeigt, wie nicht standardisierte Schnittstellen zwischen Fach- und Transportverfahren auf beiden Seiten zu erheblichen Unsicherheiten und Mehraufwänden führen.

2.3.1 Aufwand auf Seiten zentral betriebener Transportverfahren

Insbesondere die Betreiber zentraler Transportverfahren (z. B. Clearingstellen) sehen sich mit vielen unterschiedlichen Schnittstellen von Fachverfahren (z.B. von Kommunen) konfrontiert, wie in Abbildung 2.2 auf Seite 6 dargestellt. Dies führt zu hohen Aufwänden und Kosten auf Seiten der Transportverfahren.

[2] Es gibt keine übergreifende statistische Auswertung des Nachrichtenaufkommens, weil OSCI-Transport und XTA offene Standards sind, die in vielen unterschiedlichen Fachszenarien eingesetzt werden.

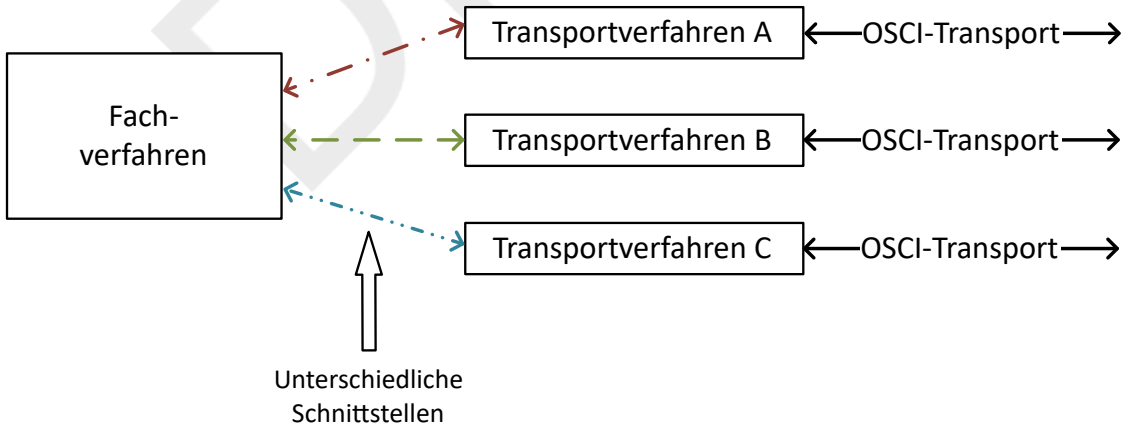
Abbildung 2.2. Zentrale Transportverfahren: Heterogene Anbindung von kommunalen Fachverfahren



2.3.2 Aufwand auf Seiten überregional eingesetzter Fachverfahren

Eine ähnliche Situation ergibt sich für Hersteller überregional eingesetzter Fachverfahren. Diese müssen an die Transportverfahren der Länder angebunden werden, siehe Abbildung 2.3 auf Seite 6. Sofern diese Schnittstelle nicht vereinheitlicht ist, muss das Fachverfahren jeweils eine eigene Anbindung implementieren. Dies führt zu hohen Aufwänden und Kosten auf Seiten der überregional eingesetzten Fachverfahren.

Abbildung 2.3. Überregional eingesetzte Fachverfahren: Heterogene Anbindung von Transportverfahren in den Ländern



2.4 Ziele von XTA

XTA vereinheitlicht die Schnittstellen zwischen Fach- und Transportverfahren und reduziert damit Aufwände und Kosten bei der wechselseitigen Anbindung. Damit erhalten Verfahren, Verfahrenshersteller und -betreiber Planungs- und Entwicklungssicherheit. XTA trifft dazu nachfolgende Regelungen:

- Einheitliche technische Schnittstellen zwischen Fach- und Transportverfahren
  - Transportnachrichten (Transportauftrag + Fachnachricht)
  - Methoden zum Versand und Empfang von Transportnachrichten
  - Überprüfung des Transports (Berichte inklusive Ereignisprotokolle und gesonderte Quittungen)
  - Bedarfsspezifische Erweiterungen für einen einheitlichen, bereichsübergreifenden Einsatz
  - Prozesse für die Abwicklung des Transports
- Festlegung von Aufgaben und Zuständigkeiten (XTA Rollenmodell)
- Einheitliche Definition und Vorgabe von zu erreichenden Servicequalitäten
  - Anforderungen an die Transportinfrastruktur

Zusammenfassend lässt sich sagen: „**Der Standard XTA schafft die Voraussetzungen dafür, dass auf der gesamten Strecke des Nachrichtentransports die Anforderungen der Fachverfahren durch die Verwaltung definiert und nachweislich wirksam durchgesetzt werden können.**“

Dies gilt für alle Kontexte, in denen Fachverfahren im Dienste der Verwaltung kommunizieren: länderübergreifend, landesintern und auch zwischen Land und Bund. Die Anforderungen betreffen nicht nur die Umsetzung der entsprechenden Prozesse, sondern auch deren Leistungsfähigkeit sowie die Aspekte Datensicherheit und Datenschutz. Die verbindliche Definition der Anforderungen schließt explizit auch die Überprüfbarkeit der Einhaltung dieser Vorgaben mit ein. XTA bedient sich für den Nachrichtentransport bestehender offener Standards und ergänzt diese um den übergeordneten Transportprozess und die notwendigen qualitätssichernden Maßnahmen.

3 Einsatzumfeld und Rollen

3.1 Einsatzumfeld

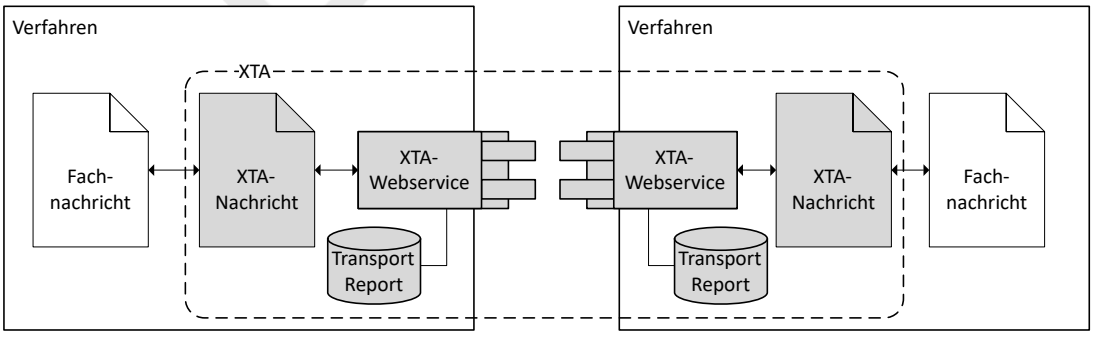
Im Austausch von Fachnachrichten sind der Versand und der Empfang von Nachrichten zentrale Abläufe, die von allen Anwendungen unabhängig von ihrem fachlichen Kontext abgebildet werden müssen. Für den standardisierten, fachunabhängigen Austausch von Fachnachrichten stellt XTA mit seinen Modulen XTA Webservice und XTA Service Profile folgende Lösungen zur Verfügung:

- einheitliche Transportnachrichten (XTA-Nachrichten), in die Fachnachrichten eingebettet werden
- einheitliche Transportaufträge für den Austausch von Fachnachrichten
- einheitliche Schnittstellen zum Austausch von XTA-Nachrichten zwischen Verfahren und Abruf von Berichten
- einheitliche Datenstrukturen zur Beschreibung und Vorgabe von Servicequalitäten an den Nachrichtentransport

In einer Kommunikation mit dem XTA-Webservice verschickt und empfängt das Verfahren generische Transportnachrichten (sogenannte XTA-Nachrichten). Somit kann ein Verfahren Fachnachrichten in stets der gleichen Art und Weise abgeben oder empfangen. Der XTA-Webservice wird somit zu einem Transportadapter, der in beliebigen Fachkontexten wiederverwendet werden kann. Darüber hinaus sind Verfahren, die XTA im selben Umfang unterstützten, zu einander kompatibel und können ohne weiteren Aufwand mittels XTA untereinander Nachrichten austauschen.

Die nachfolgende Abbildung zeigt, dass der Einflussbereich des Standards XTA mit der XTA-Nachricht beginnt und endet. Die Verfahren müssen in der Lage sein, Fachnachrichten in XTA-Nachrichten und XTA-Nachrichten in Fachnachrichten umzuwandeln. Diese Transformationen sind nicht Teil von XTA. Einheitliche Schnittstellen und standardisierte Protokollierung stehen für den fachunabhängigen Transport zur Verfügung.

Abbildung 3.1. Grenzen des Standards XTA



In gleichem Maße, wie die standardisierten Schnittstellen den Austausch zwischen XTA-Anwendern erleichtert, können mit Serviceprofilen in einheitlicher Weise Anforderungen an den Transport von Fach-

nachrichten formuliert und ausgetauscht werden. Deren Einhaltung kann anhand der standardisierten Berichte nachvollzogen werden. Für den Nachrichtentransport ist die Verwendung von Serviceprofilen und die Erstellung der Berichte im Rahmen der normativen Vorgaben zwingend erforderlich.

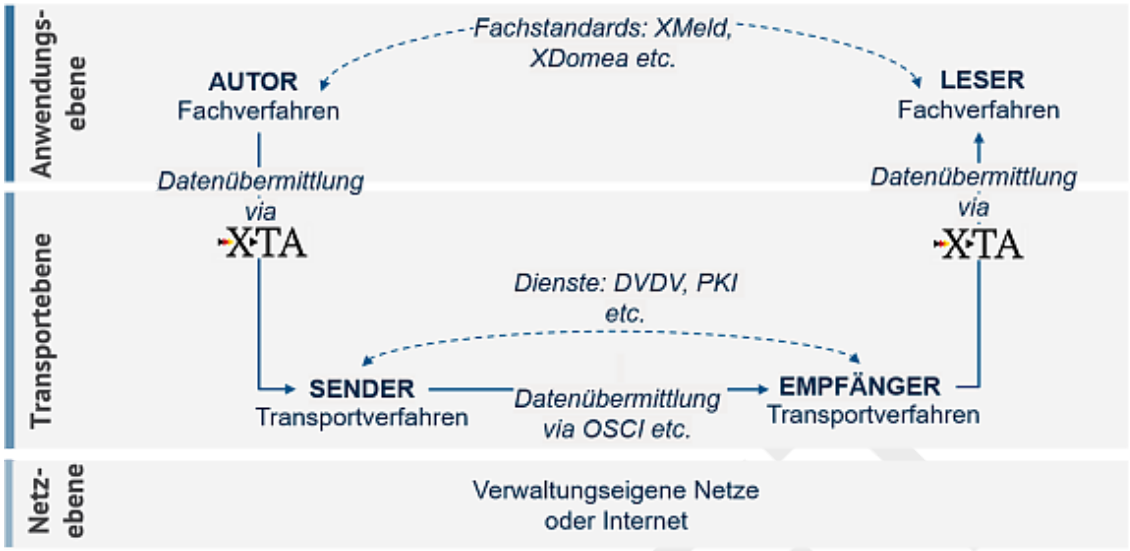
3.2 XTA Rollenmodell

Das konstruktive und zielgerichtete Zusammenspiel unterschiedlicher Akteure bedarf immer einer Steuerung. Die normative Verantwortung wird von den Prozessverantwortlichen für die Fachlichkeit (Fachverantwortlicher, z.B. BMI) und den Transport (Transportverantwortlicher, z.B. IT-Planungsrat) wahrgenommen. Sie erlassen die notwendigen Vorgaben. Die Verantwortung der operativen Anwendung dieser Vorgaben liegt bei den von ihnen benannten Akteuren (z.B. Behörden). Diese Akteure haben die notwendigen Prüfungen durchzuführen, um die Einhaltung der Anforderungen nachweisen oder ggf. Korrekturmaßnahmen auslösen zu können.

Im Rahmen des Nachrichtentransports werden zumeist personenbezogene Daten verarbeitet, die für betroffene Personen Risiken erzeugen. Hierfür sind datenschutzrechtliche Anforderungen (insbes. DSGVO) die normativen Vorgaben, aus der sich Aufgaben für die Akteure ergeben. Für das Erteilen dieser Aufgaben und die Überprüfung der Ergebnisse ist der Fachverantwortliche verantwortlich. Der Transportzuständige (z.B. ein öffentlich rechtlicher Dienstleiter) muss den Nachrichtentransport gemäß den Vorgaben gewährleisten. Für die Erfüllung der Aufgaben ist eine Zusammenarbeit und eine Abstimmung unter den Akteuren notwendig. Die gesetzlichen Vorgaben und die untereinander festgelegten Verträge werden in Form von Profilen (z.B. schriftlich oder XTA-SP) festgeschrieben und in funktionale Vorgaben transformiert.

Beim Nachrichtentransport sind die Vorgaben der Anwendungsebene und der Transportebene umzusetzen. Bedingt durch eine fachliche Anforderung initiiert ein Autor den Nachrichtentransport mit einem Leser. Für die Kommunikation bedienen sich die Rollen Autor und Leser technischer Dienstleister: Sender und Empfänger. Diese Rollen übernehmen den eingentlichen Transport der Daten, ohne dafür auf die Daten der Fachlichkeit zugreifen zu müssen oder zu dürfen. Abgegrenzte Aufgabenpakete in einer Rolle werden für eine bessere Modularisierung technisch gekapselt. Zum Beispiel werden in den Rollen Sender und Empfänger für die Datenübertragung per OSCI dedizierte Clients und Server als Komponenten benötigt. Diese Komponenten sind nicht Teil des XTA Rollenmodells. Folglich kommt ein 4-Corner-Modell zum Einsatz, wie es zum Beispiel bei Peppol und eDelivery genutzt wird. Anhand eines XTA Rollenmodells werden die operativen Rollen, deren Aufgaben sowie die Schnittstellen festgelegt und beschrieben:

Abbildung 3.2. Das XTA Rollenmodell



Aus der Sicht der Fachverfahren überträgt der Autor eine Nachricht an den Leser. Für die technische Abwicklung bedienen sie sich der Dienstleitung von Transportverfahren. Die Kommunikation zwischen Fachverfahren und Transportverfahren findet über die XTA-Schnittstelle (XTA-WS) statt. Zur Datenübertragung zwischen Sender und Empfänger werden weitere Infrastrukturdienste und Technologien genutzt, wie Identitäts- und Adressverzeichnisse, XRepository, PKI-Dienste, Standards und Transportkanäle. In den nachfolgenden Unterkapiteln werden die Aufgaben bzw. Verantwortlichkeiten der Rollen zusammengefasst.

3.2.1 Fachverfahren

Auf der Anwendungsebene werden die Rollen Autor und Leser durch Fachverfahren realisiert. Die Vorgaben stammen vom Prozessverantwortlichen für die Fachlichkeit. Bei der Kommunikation mit den Transportverfahren kommen die Vorgaben des Prozessverantwortlichen für den Transport zum Tragen.

3.2.1.1 Autor

Der Autor ist zuständig für die operative Abwicklung des Nachrichtenversands. Er ist verantwortlich für die Inhalte der Fachnachricht, des Transportauftrags und deren Konsistenz zueinander. Zu den Aufgaben gehören:

- Erstellung der Fachnachricht
  - Einhaltung des Fachstandards
  - Umsetzung der Vorgaben des Schutzprofils, z.B. Signatur und Verschlüsselung
  - Bestätigung des Abschlusses des Versands
- Erstellung des Transportauftrags
  - Festlegung des fachlich zuständigen Lesers inkl. des Identitätsverzeichnisses
  - Bestimmung der gesetzlich festgelegten und vertraglich vereinbarten Servicequalitäten
  - Verwendung eines eindeutigen Identifikators für den Transport
- Durchführung des Transports
  - Beauftragung des Senders für den Transport

- Überwachung des Transports (Berichte inklusive Ereignisprotokolle und gesonderte Quittungen)

3.2.1.2 Leser

Der Leser ist zuständig für die operative Abwicklung des Nachrichtenempfangs. Er ist verantwortlich für die Auswertung der Inhalte der Fachnachricht, des Transportauftrags und deren Konsistenz zueinander. Zu den Aufgaben gehören:

- Durchführung des Transports
  - Abholung beim Empfänger
  - Überprüfung des Transports (Berichte inklusive Ereignisprotokolle und gesonderte Quittungen)
  - Bestätigung des Abschlusses des Empfangs
- Prüfung der Fachnachricht
  - Einhaltung des Fachstandards
  - Umsetzung der Vorgaben des Schutzprofils, z.B. Signatur und Verschlüsselung
- Prüfung des Transportauftrags
  - fachliche Zuständigkeit des Autors inkl. des Identitätsverzeichnisses
  - Einhaltung der gesetzlich festgelegten und vertraglich vereinbarten Servicequalitäten

3.2.2 Transportverfahren

Auf der Transportebene werden die Rollen Sender und Empfänger durch Transportverfahren realisiert. Die Vorgaben stammen vom Prozessverantwortlichen für den Transport. In ihrer Arbeit werden sie durch den Transportauftrag der Fachverfahren gesteuert.

3.2.2.1 Sender

Der Sender ist für den Nachrichtenversand im Auftrag des Autors zuständig. Er transportiert die Nachricht an den vom Leser beauftragten Empfänger. Zu den Aufgaben gehören:

- Kommunikation mit dem Autor
  - Authentifizierung des Autors
  - Erzeugung eines eindeutigen Identifikators für den Transport
- Prüfung des Transportauftrags
  - Autorisierung des Autors und des Lesers für den Transport (Fachkontext + Behördenkategorie)
  - Prüfung der Erreichbarkeit des Lesers inkl. des Identitätsverzeichnisses
- Durchführung des Transports
  - Erzeugung der Transportnachricht
  - Umsetzung der Vorgaben des Schutzprofils, z.B. Signatur und Verschlüsselung der Transportnachricht
  - Einhaltung der gesetzlich festgelegten und vertraglich vereinbarten Servicequalitäten
  - Übertragung der Transportnachricht an den Empfänger
  - Erzeugung der Transportnachweise (Berichte inklusive Ereignisprotokolle und gesonderte Quittungen)

3.2.2.2 Empfänger

Der Empfänger ist für den Nachrichtenempfang im Auftrag des Lesers zuständig. Er nimmt die an einen seiner Leser adressierte Nachricht von einem Sender entgegen und stellt diese dem Leser zur Verfügung. Zu den Aufgaben gehören:

- Durchführung des Transports
  - Annahme einer Transportnachricht
  - Überprüfung der Akkreditierung des Senders[1]
  - Autorisierung des Autors und des Lesers für den Transport (Fachkontext + Behördenkategorie)
  - Einhaltung der gesetzlich festgelegten und vertraglich vereinbarten Servicequalitäten
- Prüfung des Transportauftrags
  - Prüfung der Umsetzung des Schutzprofils, z.B. Signatur und Verschlüsselung der Transportnachricht
  - Erzeugung der Transportnachweise (Berichte inklusive Ereignisprotokolle und gesonderte Quittungen)
- Kommunikation mit dem Leser
  - Authentifizierung des Lesers
  - Bereitstellung der Nachricht

[1] In einigen Bereichen ist eine vollständige Überprüfung der Akkreditierung des Senders aktuell nur eingeschränkt möglich. Da oft nur technische Parameter des Senders vorliegen, kann eine indirekte Identitätsprüfung und somit die Rechtmäßigkeit des Nachrichtentransports sichergestellt werden.

4 Abläufe und Verfahren

4.1 Steuern durch XTA Service Profile

Dieses Kapitel führt das Konzept der Profilierung des Nachrichtentransports ein und gibt einen Überblick in die Thematik. Es werden in Abschnitt 4.1.1 auf Seite 14 zunächst die wichtigsten Leistungsmerkmale des Profilkonzepts erklärt. In Abschnitt 4.1.2 auf Seite 15 wird erläutert, wie Serviceprofile eines Fachstandards bereitgestellt werden. Anschließend wird in Abschnitt 4.1.3 auf Seite 16 die Anwendung der Profile durch die verschiedenen Rollen zur Laufzeit erläutert.

Die Prozessverantwortlichen müssen stets gewährleisten, dass die von ihr beauftragte IT-Infrastruktur für den Nachrichtentransport ordnungsgemäß eingesetzt wird. Sie müssen in der Lage sein den Nachtrichtentransport zu steuern und eine effektive Governance auszuüben.

Durch die Profile werden folgende Kernthemen adressiert:

- **Kommunikationsszenario**: Es wird vorgegeben, wie die Interaktion der Akteuere beim Nachrichtentransport aussehen soll. Handelt es sich um einen synchrone oder asynchrone Interaktion, welche Fachnachrichten und welche Reaktion werden erwartet?
- **Infrastruktur**: Es wird vorgegeben, welche Komponenten der verfügbaren Infrastruktur in welcher Konstellation für den Geschäftsprozess zu verwenden sind.
- **Erforderliches Leistungsniveau**: Die Festlegung von Verfügbarkeit der Dienste, der Zustellfristen, der Löschfristen, etc.
- **Technische Transformationen**: Die Transformationen spezifizieren den Aufbau der Transportnachrichten, die Anwendung der technischen Schutzmaßnahmen und deren Nachweisbarkeit.
- **Datensicherheit**: Die transportierten Nachrichten müssen gegen unbefugte Einsichtnahme und Verfälschung abgesichert werden. Die Echtheit der elektronischen Identitäten muss sichergestellt und ihre Berechtigungen müssen geprüft werden.
- **Datenschutz**: Der Nachrichtentransport muss auf allen Teilstrecken vom Autor bis zum Leser gemäß des Schutzbedarfs der Daten ausgeführt werden. Auf die personen- und organisationsbezogenen Daten und dem Risiko für betroffene Personen darf nur konform auf Basis der rechtlichen Grundlagen, wie sie konzentriert als *Grundsätze* im Artikel 5 der DSGVO aufgelistet sind, zugegriffen werden.

Alle Aspekte, von denen hier die Rede ist, werden als *Service Qualitäten* des Nachrichtentransports bezeichnet. Während die Prozessverantwortlichen die Service Qualitäten vorgeben, wird deren Einhaltung durch die Rollen (Autor, Sender, Empfänger und Leser) sichergestellt und geprüft. Im Rahmen von Audits überwachen die Prozessverantwortlichen die Einhaltung der Vorgaben durch diese Rollen.

Klare Vorgaben in Bezug auf Service Qualitäten zu machen ist in der aktuellen Praxis nur eingeschränkt möglich, verschiedene Missstände lassen dies deutlich werden:

- Es ist eine große Vielfalt an Vorgaben anzutreffen, auf deren Basis IT-Dienstleister die Nachrichtenübermittlung zu steuern versuchen.
- Vorgaben sind selten explizit und nachvollziehbar formuliert. Vielmehr sind sie auf unterschiedliche Weise implizit in die Transportverfahren eingebaut.
- Fachlich-rechtliche und technische Vorgaben werden in der Kooperation von Fachstandard und IT-Infrastruktur vermischt, also die jeweils zuständigen Rollen und Kompetenzen nicht differenziert und zugewiesen.

- Viele der Service Qualitäten werden mittels handgeschriebener OSCI-Transport-Profile innerhalb der Fachstandards dokumentiert.

XTA Serviceprofile sind XML-Dokumente, die auf einer in XTA 2 standardisierten XML Schema-Definition basieren. Sie werden genutzt, um die benötigten Service Qualitäten eindeutig, einheitlich und maschinenverarbeitbar zu definieren.

4.1.1 Ziele des XTA Profilkonzepts

Um die Prozessverantwortlichen in die Lage zu versetzen, den Einsatz ihrer IT-Infrastruktur zu steuern, stellt der Standard XTA 2 das Modul **XTA Service Profile** bereit. Dieser kann grundsätzlich in allen Bereichen angewendet werden. Hier wird er im Kontext der Anwendung des Moduls XTA-WS dargestellt (siehe Abschnitt 4.2 auf Seite 19).

Drei Ziele sollen damit erreicht werden:

1. **Einheitlichkeit und Eindeutigkeit**: Die Bestimmung der Service Qualitäten soll auf der Basis eines Standards vorgenommen werden können.
2. **Steuerbarkeit und Überprüfbarkeit**: Die Einhaltung von rechtlichen Anforderungen soll nachvollziehbar gesteuert und überprüft werden können.
3. **Abtrennung von der Technik**: Die Service Qualitäten werden für die Fachlichkeit und die Technik getrennt definiert. Die Transformationen übersetzen bei Bedarf zwischen diesen Begriffswelten. Dadurch muss die Fachlichkeit nur ein Minimum von der Technik verstehen und andersherum.

(1) Standard für die Festlegung von Service Qualitäten

Das Konzept der XTA Service Profile definiert, wie geforderte Service Qualitäten eindeutig zu formulieren sind. Es stellt hierfür eine standardisierte begriffliche Struktur bereit, d.h. definierte Begriffe für Service Qualitäten mit definierten Ausprägungen. Außerdem gibt das Konzept vor, durch wen die Profile zu erstellen sind und wie diese Informationen verfügbar gemacht werden. Im Ergebnis sind die Voraussetzungen geschaffen, dass Anforderungen in Bezug auf die Service Qualitäten einheitlich formuliert und gebündelt abgelegt werden können.

Die aktuelle Praxis ist durch die nachfolgenden Merkmale gekennzeichnet und muss verbessert werden:

1. Die Anforderungen an den Nachrichtentransport im E-Government werden im jeweiligen rechtlichen Rahmen festgelegt: Der Gesetz- oder Verordnungsgeber legt fest, unter welchen Umständen eine Datenübertragung zulässig ist und welche Qualität bzgl. Leistungsfähigkeit, Datensicherheit und Datenschutz und anderen Modalitäten erwartet wird.

   Die zu berücksichtigenden Aspekte werden innerhalb juristischer Texte formuliert, zur Umsetzung müssen sie interpretiert und aus der juristischen in eine technische Sprache übersetzt werden. Diese Herleitungen und Übersetzungen können bei gleichen oder sehr ähnlichen Ausgangssituationen stark voneinander abweichen.
2. Die Erwartung der Prozessverantwortlichen, dass die Umsetzung und Einhaltung dieser Anforderungen leicht nachvollziehbar und überprüfbar sind, kann nicht erfüllt werden. Das hat die Konsequenz, dass es keine einfache Überprüfung der Qualität des Nachrichtentransports geben kann.

Hier schaffen die standardisierten Profilierungen Abhilfe, indem sie eine einheitliche Sprache zur Formulierung der geforderten Service Qualitäten an die Hand geben. Die Prozessverantwortlichen können nun die durch den jeweiligen rechtlichen Rahmen vorgegebenen Anforderungen nachvollziehbar formulieren. Für die technische Umsetzung liegen erstmals unmissverständliche Vorgaben vor.

Ein gewünschter Effekt dieser Einheitlichkeit ist, dass sie zu größerer Einfachheit führt:

- Die Definition der Serviceprofile geht mit einer Standardisierung der durch den rechtlichen Rahmen vorgebbaren Attribute einher, so dass die Anzahl der Serviceprofile gering und damit der Aufwand

der Pflege der Profile überschaubar bleibt. Die Idee ist, dass der Gesetz- oder Verordnungsgeber für ein konkretes Kommunikationsszenario das passende Serviceprofil aus den bereits Bestehenden auswählt.

- Es wird erwartet, dass sich durch die Serviceprofile die heute bestehende Vielfalt von Anforderungen stark reduzieren lässt. Das gilt einerseits für die Festlegung von Anforderungen an einen zu beauftragenden Nachrichtentransport. Andererseits trifft das für die Konfiguration der technischen Umsetzung dieser Anforderungen zu. Auch hier sind wiederkehrende Standardkonfigurationen zu erwarten, deren Abruf durch die Transportverfahren ein großes Potential an Reduzierung von Komplexität bedeutet.

(2) Steuerung des Nachrichtentransports und Überprüfung der Einhaltung von rechtlichen Anforderungen

XTA Serviceprofile machen es möglich, die Tranformation rechtlicher Anforderungen in definierte Servicequalitäten transparent zu gestalten. Bei der Festlegung eines Serviceprofils für einen Fachstandard wird eine begründete und zu dokumentierende Auswahl zwischen den angebotenen Alternativen getroffen.

Die Steuerung des Nachrichtentransports bedeutet die Vorgabe der geforderten Servicequalitäten. Die Überprüfung der Einhaltung der Servicequalitäten bedeutet dann gleichzeitig die Überprüfung der Einhaltung der entsprechenden rechtlichen Anforderungen.

(3) Entkopplung der Transporttechnik von der Fachlichkeit

Bisher werden die technischen Parameter, die für den Transport benötigt werden, vielfach durch den Fachstandard, wie z. B. im OSCI-Transport-Profil für XMeld[1], vorgegeben. Dies widerspricht der Entkopplung der Transporttechnik von der Fachlichkeit und bürdet der Fachlichkeit die Notwendigkeit auf, die Transporttechnik genau zu kennen.

XTA Service Profile ermöglichen eine saubere Trennung der technischen Transportimplementierung von der Fachlichkeit. Aus Sicht der Fachlichkeit werden die Anforderungen, also die erforderlichen Servicequalitäten, voerst nur technikneutral formuliert. Hier wird noch nicht die konkrete technische Konfiguration der Transportinfrastruktur adressiert. Die Erstellung dieser Konfiguration ist ein separater Folgeschritt, der explizit kenntlich macht, wie gemäß eines bestimmten Standes der Technik die jeweilige Servicequalität realisiert wird.

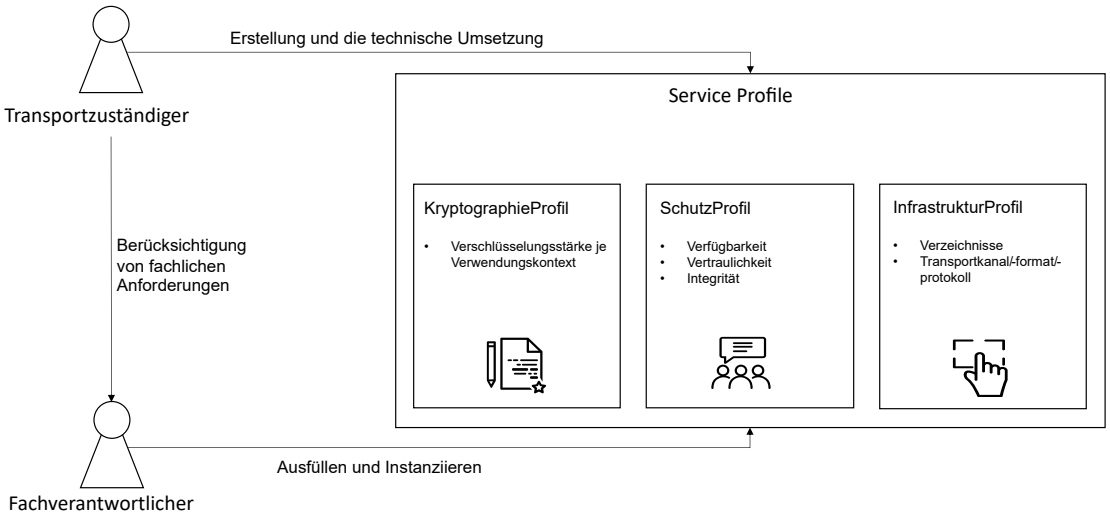
4.1.2 Umsetzung und Zusammenwirken mit den Fachstandards

Die Struktur der Serviceprofile wird vom Standard XTA 2 vorgegeben. Die Syntax und Semantik bilden die einheitliche Sprache, mit der die geforderten Servicequalitäten aus den Anforderungen der Fachlichkeit abgeleitet werden. Der Umfang der Servicequalitäten deckt alle Schutzziele des Datenschutzes und der Datensicherheit ab (siehe Abschnitt 5.1 auf Seite 28). Zum Ziel Verfügbarkeit kann zum Beispiel die Verfügbarkeitstufe des Dienstes festgelegt werden (z.B. *99,9% 24/7*). Hinter allen diesen Zielen stecken konkrete Maßnahmen, die technisch gewährleistet werden müssen. Die unterschiedlichen Anforderungen werden in Profiltypen gruppiert. Die Serviceprofile beinhalten diese Profiltypen als Unterprofile (*Schutz-, Infrastruktur- und Kryptographieprofil*). Die Profiltypen bilden die Gesamtheit der konkreten Anforderungen an den Nachrichtentransport. Die Unterprofile können in anderen Fachbereichen wiederverwendet werden.

Der Transportzuständige unterstützt bei der Erstellung des Serviceprofils. Er prüft die Anforderungen und gibt die dafür notwendigen technischen Maßnahmen an. Bei der Erstellung dieser Profile muss der Transportzuständige die fachlichen Anforderungen der Fachverantwortlichen berücksichtigen und mit ihnen gemeinsam gesetzeskonform ausarbeiten. Der Fachverantwortliche ist zuständig für das Instanziieren der vollständig ausgefüllten Serviceprofile. Als Ergebnis liegt ein Serviceprofil (XML-Instanz) mit eindeutigen Identifikationsmerkmalen vor und kann bei der Beauftragung des Nachrichtentransports referenziert / vorgegeben werden.

[1] Vgl. OSCI-XMeld 3.4 vom 31.07.2023, Anhang C.

Abbildung 4.1. Zusammenwirken von Transport- und Fachverantwortlichem

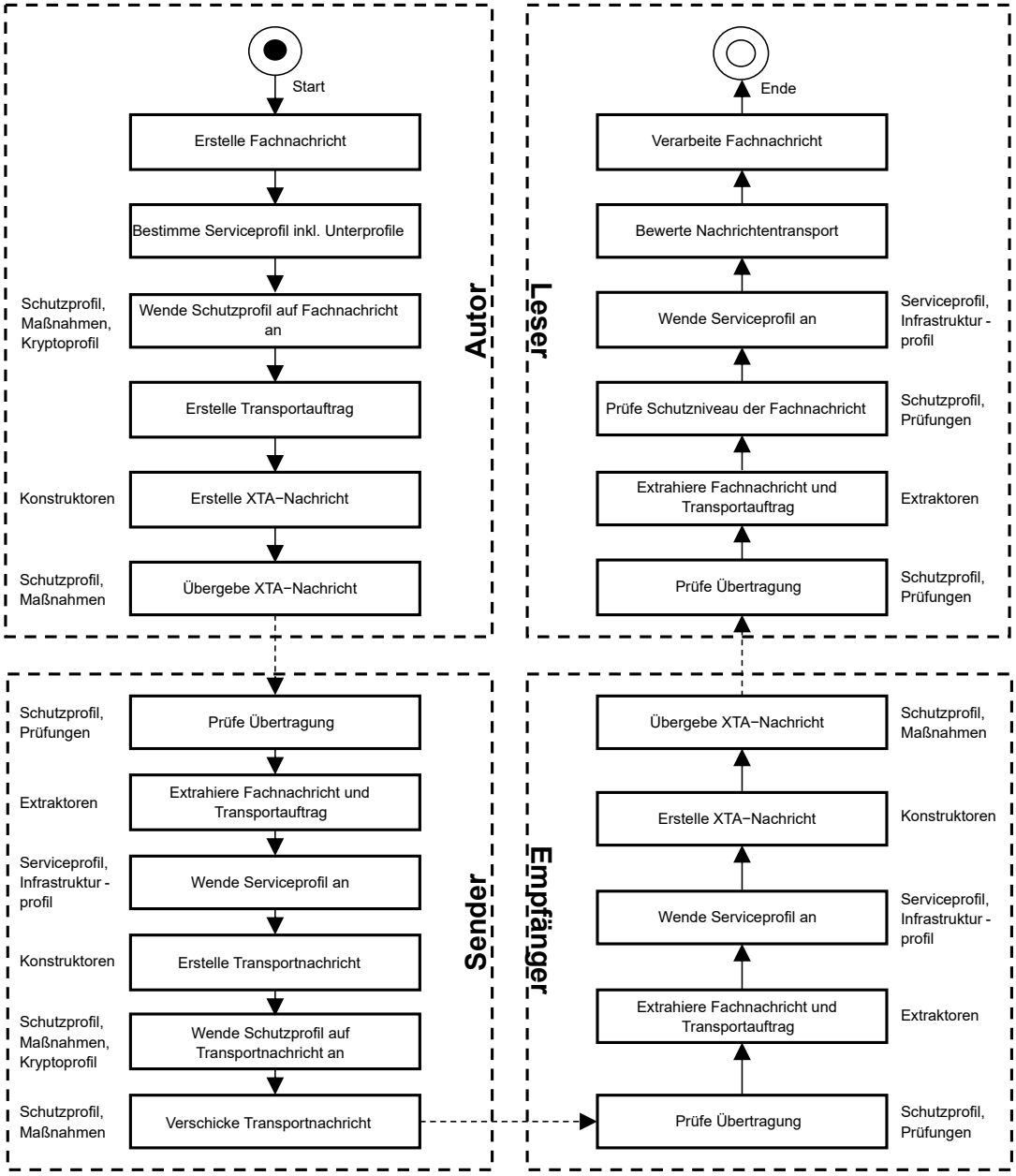


4.1.3 Anwendung der Serviceprofile

Die Profilinstanzen stellen Handlungs- und Konstruktionsvorschriften dar, die von den Rollen auf der Ebene der Technik anzuwenden sind, um einen Transportauftrag auszuführen. Durch seine generelle Anwendbarkeit ist das Konzept der Serviceprofile sehr flexibel. Um sein Wirken und seine Möglichkeiten konkreter darzustellen und damit handhabbar zu machen, wird es hier im Kontext von XTA-WS dargestellt.

Die Anwendung einer Serviceprofilinstanz erfolgt im Rahmen eines konkreten Prozesses. Im Folgenden wird der Prozess des Nachrichtentransports mittels XTA 2 (Module XTA-SP + XTA-WS) dargestellt. An dem Prozess sind alle Rollen beteiligt und jede Rolle muss bestimmte Prozessschritte vollziehen. In den unterschiedlichen Prozessschritten kommen unterschiedliche Profiltypen zum Einsatz und entfalten dort ihre Wirkung zum Ziel einer Steuerung durch die Fachverantwortlichen.

Abbildung 4.2. Anwendung der Serviceprofile durch die Rollen beim Nachrichtentransport



In Abbildung 4.2, „Anwendung der Serviceprofile durch die Rollen beim Nachrichtentransport“ sind die grundlegenen Schritte dargestellt, die die Rollen durchlaufen müssen. Dabei wird angegeben, welche Profilarten in den jeweiligen Prozessschritten zur Anwendung kommen.

Autor

1. **Erstelle Fachnachricht**: Der Autor erstellt für den aktuellen Geschäftsprozess die vorgegebene Fachnachricht.

2. **Bestimme Serviceprofil inkl. Unterprofile**: Der Autor ermittelt aus dem Geschäftsprozess die Serviceprofilinstanz mit ihren Unterprofilinstanzen.
3. **Wende Schutzprofil auf Fachnachricht an**: Der Autor bringt eine Signatur an und/oder verschlüsselt die Fachnachricht für den Leser gemäß Schutzprofilinstanz.
4. **Erstelle Transportauftrag**: Der Autor erstellt einen zur Fachnachricht konsistenten Transportauftrag, der das verwendete Serviceprofilinstanz referenziert.
5. **Erstelle XTA-Nachricht**: Der Autor bereitet die Fachnachricht und den Transportauftrag für die Übergabe an den Sender vor.
6. **Initiiere Versand**: Der Autor beauftragt den Sender, indem er die XTA-Nachricht mittels XTA-Webservice übergibt.

Sender

1. **Prüfe Übertragung**: Der Sender nimmt die XTA-Nachricht entgegen und prüft, ob die Datenübertragung gemäß der XTA-Webservice-Spezifikation erfolgte.
2. **Extrahiere Fachnachricht und Transportauftrag**: Der Sender entnimmt aus der XTA-Nachricht den Transportauftrag und die Fachnachricht. Der Transportauftrag enthält die Anweisungen für die weitere Übertragung der Fachnachricht.
3. **Wende Serviceprofil an**: Der Sender entnimmt aus dem Serviceprofilinstanz die Vorgaben, welche Inftrastruktur zu verwenden und wie die Transportnachricht zu erstellen ist.
4. **Erstelle Transportnachricht**: Der Sender bereitet die Transportauftragsdaten und die Fachnachricht für die Übertragung an den Empfänger.
5. **Wende Schutzprofil auf Transportnachricht an**: Der Sender bringt eine Signatur an und/oder verschlüsselt die Transportnachricht für den Empfänger gemäß Schutzprofilinstanz und Transportspezifikation.
6. **Verschicke Transportnachricht**: Der Sender überträgt die vorbereitete Transportnachricht an den Empfänger über die vorgegebene Infrastruktur.

Empfänger

1. **Prüfe Übertragung**: Der Empfänger nimmt die Transportnachricht entgegen und führt eine Sicherheitsprüfung der erfolgten Datenübertragung durch.
2. **Extrahiere Fachnachricht und Transportauftrag**: Der Empfänger entnimmt aus der Transportnachricht den Transportauftrag und die Fachnachricht. Dabei wird die Transportnachricht entschlüsselt und/oder die Signatur geprüft.
3. **Wende Serviceprofil an**: Der Empfänger wertet anhand des Transportauftrags und der Serviceprofilinstanz aus, ob der Nachrichtentransport gemäß der Schutzprofilinstanz und Transportspezifikation erfolgte.
4. **Erstelle XTA-Nachricht**: Der Empfänger bereitet die Fachnachricht und den Transportauftrag für die Übergabe an den Leser vor.
5. **Übergebe XTA-Nachricht**: Der Empfänger übergibt die XTA-Nachricht an den adressierten Leser gemäß dem Serviceprofilinstanz.

Leser

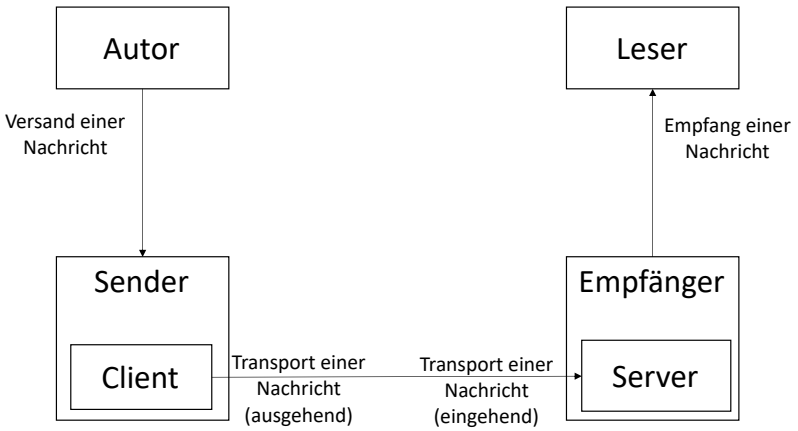
1. **Prüfe Übertragung**: Der Leser nimmt die XTA-Nachricht entgegen und führt eine Sicherheitsprüfung der erfolgten Datenübertragung durch.
2. **Extrahiere Fachnachricht und Transportnachricht**: Der Leser entnimmt aus der XTA-Nachricht den Transportauftrag und die Fachnachricht.
3. **Prüfe Schutzniveau der Fachnachricht**: Der Leser prüft, ob der Nachrichtentransport gemäß dem Schutzprofilinstanz erfolgte.

4. **Wende Serviceprofil an**: Der Leser prüft ob das Geschätsszenario seinerseits unterstützt wird. Folglich entschlüsselt er die Fachnachricht und/oder prüft die Signatur von dem Autor gemäß Schutzprofil.
5. **Bewerte Nachrichtentransport**: Der Leser prüft, ob die Protokollierung gemäß den Vorgaben erfolgte.
6. **Verarbeite Fachnachricht**: Der Leser liest die Fachnachricht leitet die interne Verarbeitung der Daten ein (z.B. Schema-Validierung und konkrete Geschäftsprozesse).

4.2 Versand und Empfang durch XTA Webservice

Ein Ziel von XTA ist die Abstraktion des Transportprozesses von genutzten Übertragungstechnologien. Dazu ist es notwendig, einheitliche Schnittstellen, klare Verantwortlichkeiten und Abläufe der beteiligten Rollen festzulegen. Die Schnittstellen werden im XTA Modul "Webservice" definiert, die Verantwortlichkeiten im Rollenmodell und die Abläufe in diesem Kapitel nochmal konkretisiert.

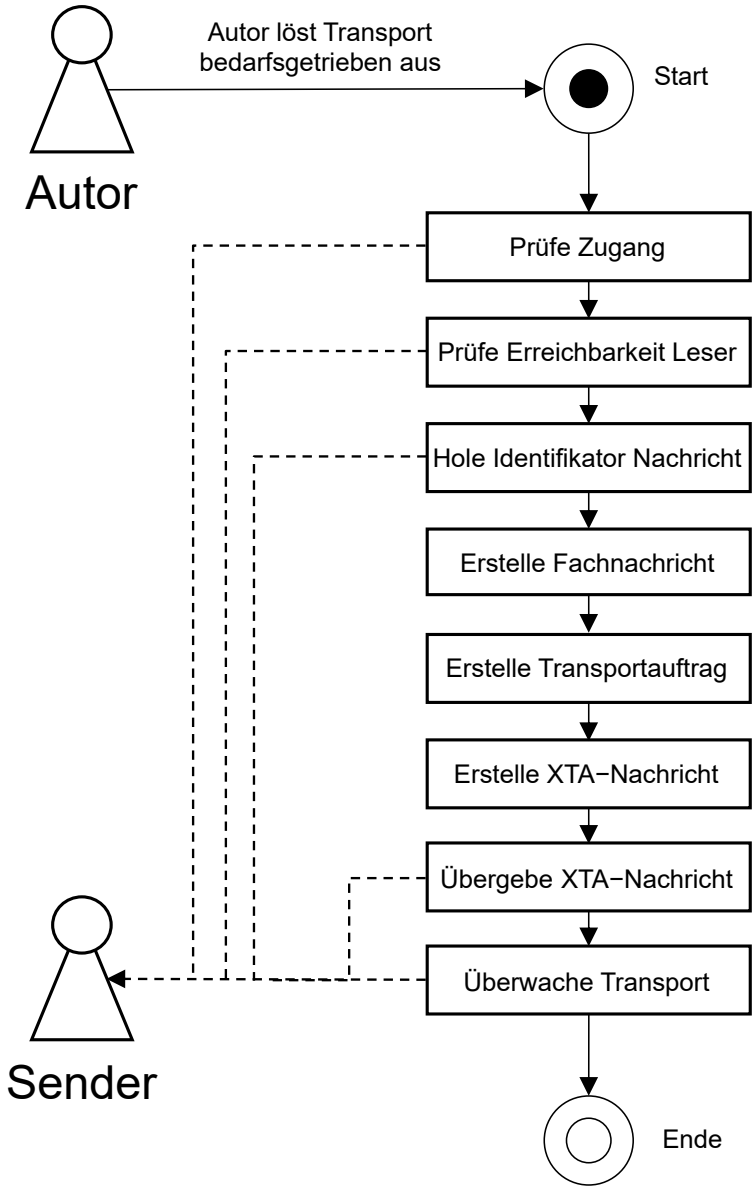
Abbildung 4.3. Übergreifendes Prozessbild



Die Übertragungstechnologien sind bei dem Sender und dem Empfänger in technischen Komponenten gekapselt. Dabei werden der Client, ein Bestandteil des Senders, als Ausgehende-Instanz und der Server, ein Bestandteil des Empfängers, als Eingehende-Instanz verwendet. Die einzelnen Abläufe sind in den nachfolgenden Abschnitten beschrieben.

4.2.1 Autor: Versand einer Nachricht

Abbildung 4.4. Autor: Versand einer Nachricht



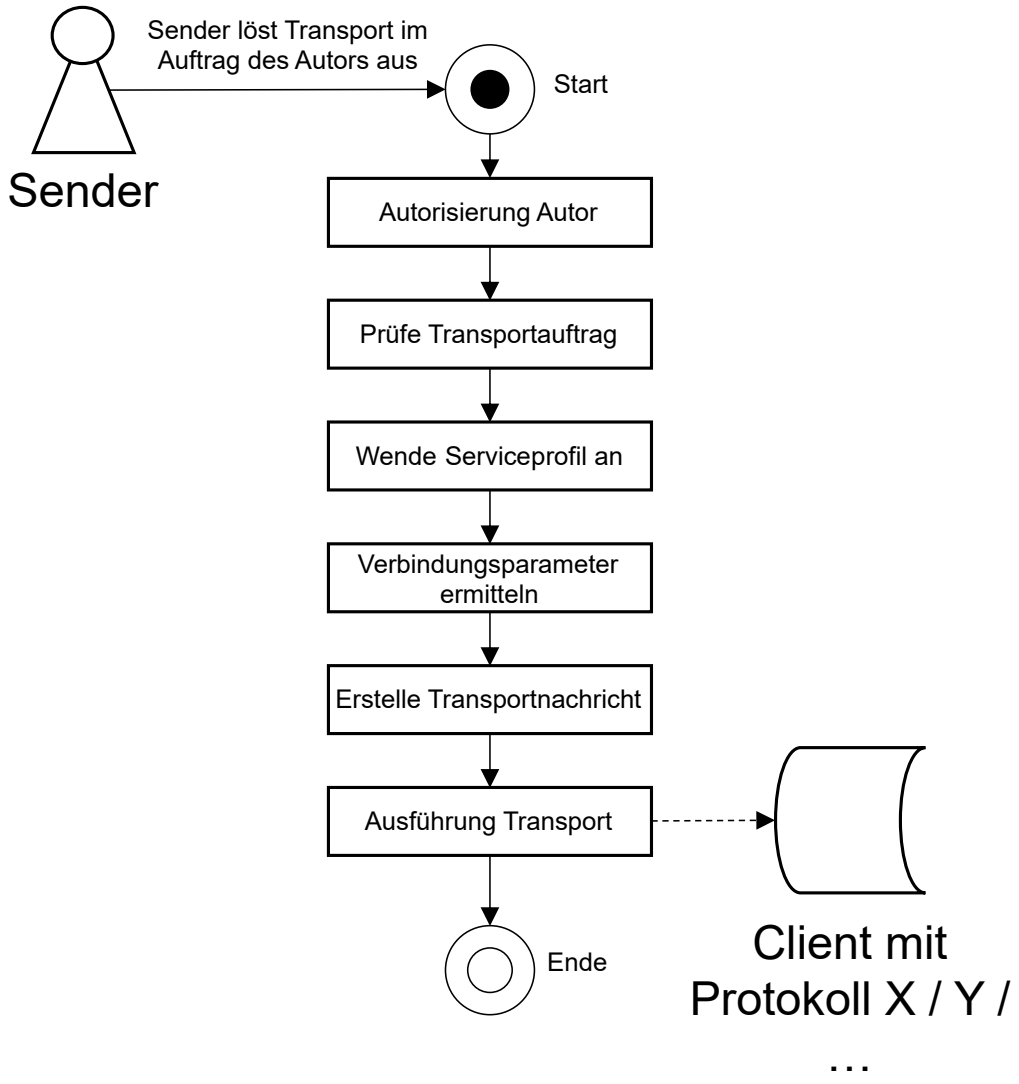
Der Versand einer Nachricht wird seitens Autor bedarfsgetrieben ausgelöst. Die einzelnen Prozessschritte beinhalten:

- **Prüfe Zugang:** Der Autor überprüft, ob sein Zugang zu dem Sender gültig und die Transportinfrastruktur (z.B. Firewall) verfügbar ist. Je nach Bedarf reicht es auch aus, den Zugang z.B. ein Mal am Tag zu prüfen.

- **Prüfe Erreichbarkeit Leser:** Vor dem Transportauftrag prüft der Autor, ob der Leser den fachlichen Dienst anbietet und den digitalen Zugang eröffnet hat. Zusätzlich wird aus dem Identitätsverzeichnis der Schlüssel für die Verschlüsselung der Fachnachricht geholt.
- **Hole Identifikator Nachricht:** Für die eindeutige Kennzeichnung des Transportsauftrags, lässt der Autor den Sender einen Identifikator erzeugen.
- **Erstelle Fachnachricht:** Der Autor erstellt eine an den Leser fachlich adressierte und in einem Fachstandard definierte Fachnachricht. Die vorgegebenen technischen Maßnahmen für Durchsetzung der Schutzziele werden angewendet (z.B. eine Anbringung einer Signatur und/oder Verschlüsselung für den Leser).
- **Erstelle Transportauftrag:** Der Autor hinterlegt alle notwendigen Metadaten im Transportauftrag. Er füllt alle Pflichtfelder aus und gibt ein Serviceprofil vor.
- **Erstelle XTA-Nachricht:** Der Autor führt die Fachnachricht und den Transportauftrag zu einer XTA-Nachricht für die Übergabe an den Sender zusammen.
- **Übergebe XTA-Nachricht:** Der Autor ruft den Sender auf und übergibt die XTA-Nachricht zur Ausführung des Transports.
- **Überwache Transport:** Der Autor ruft zu einem gegebenen Zeitpunkt die Berichte inklusive Ereignisprotokolle und gesonderte Quittungen ab und überprüft die Korrektheit des Transports.

4.2.2 Sender: Transport einer Nachricht (ausgehend)

Abbildung 4.5. Sender: Transport einer Nachricht (ausgehend)



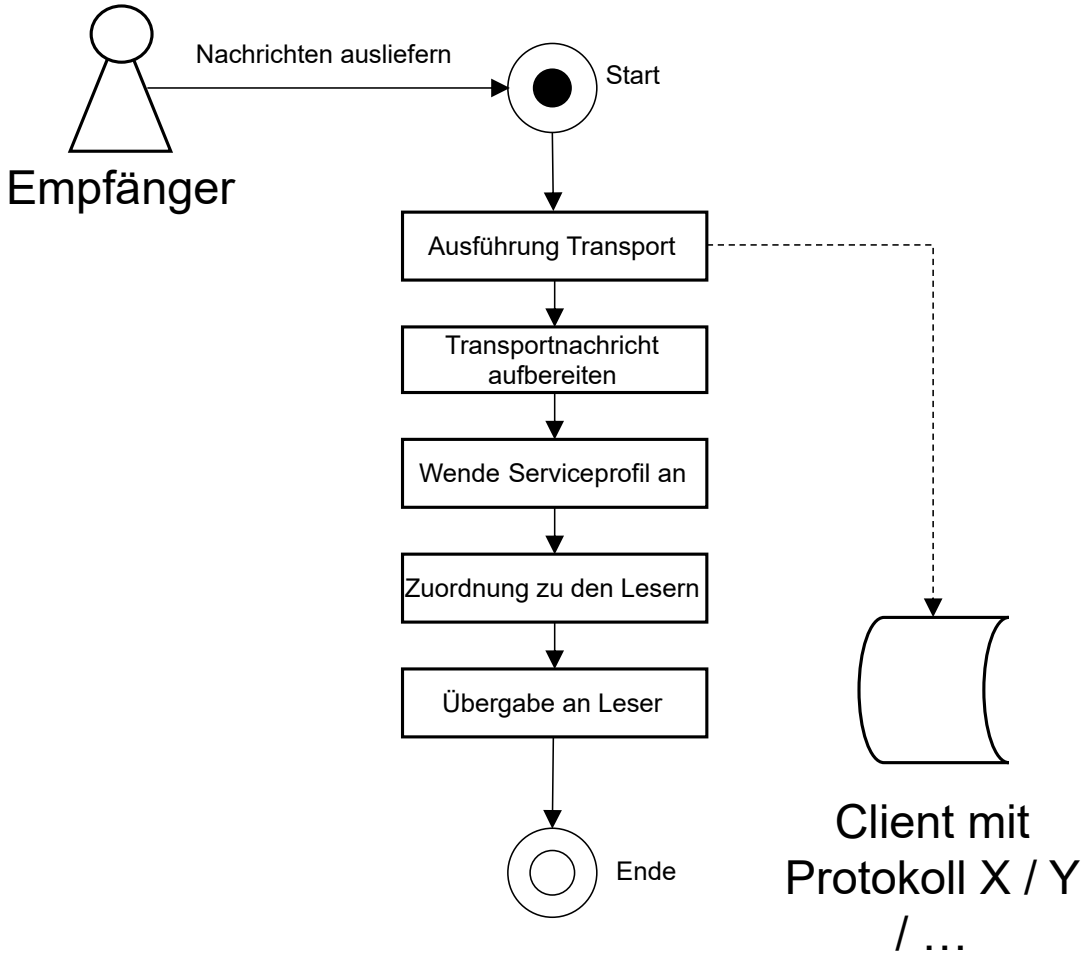
Der Transport einer Nachricht wird im Auftrag des Autors vom Sender ausgeführt. Die einzelnen Prozessschritte beinhalten:

- **Autorisierung Autor:** Der Sender überprüft, ob der Zugang des Autors gültig ist und er für diesen Autor für den Versand einer Nachricht zuständig ist.

- **Prüfe Transportauftrag:** Die Transportauftragsdaten werden hinsichtlich der fachlichen Vorgaben geprüft.
- **Wende Serviceprofil an:** Die Vorgaben aus den Serviceprofilen werden für die weitere Verarbeitung ermittelt, z.B. Vorgaben bzgl. der Inftrastruktur und Kryptoverfahren.
- **Verbindungsparameter ermitteln:** Die Verbindungsparameter werden gemäß dem Infrastrukturprofil aus dem Adressverzeichnis abgefragt z.B. die notwendig anzusprechenden Infrastrukturkomponenten wie ein OSCI-Intermediär.
- **Erstelle Transportnachricht:** Der Sender erstellt eine Transportnachricht gemäß dem Transportnachrichtenformat aus dem Infrastrukturprofil. Hierbei werden die Fachnachrichten und der Transportauftrag des Autors in die neue Transportnachricht, z.B. eine OSCI-Nachricht, eingebettet. Die vorgegebenen technischen Maßnahmen werden zur Durchsetzung der Schutzziele angewendet (z.B. eine Anbringung einer Signatur und/oder Verschlüsselung für den Empfänger).
- **Ausführung Transport:** Der Sender nutzt seinen spezifischen Client für das im Infrastrukturprofil vorgegebenen Transportprotokoll. Er verwendet diesen, um die Transportnachricht zum Empfänger zu übertragen. Die bereitzustellenden Transportberichte an den Autor werden stets aktualisiert.

4.2.3 Empfänger: Transport einer Nachricht (eingehend)

Abbildung 4.6. Empfänger: Transport einer Nachricht (eingehend)



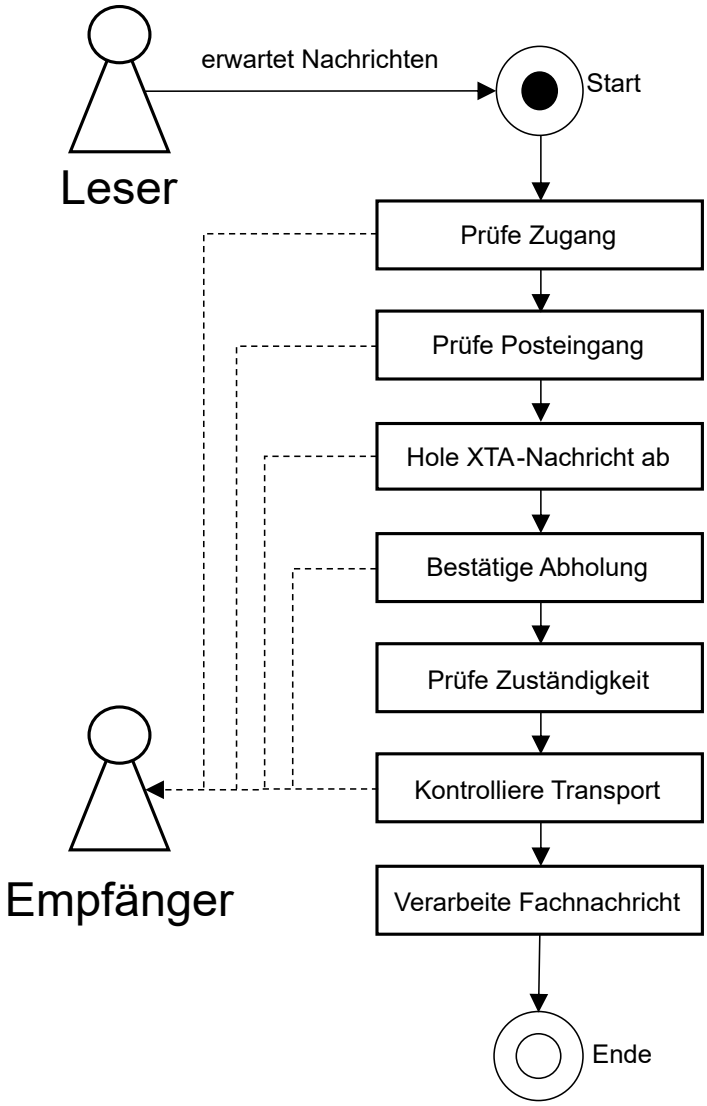
Die Auslieferung einer Nachricht wird im Auftrags des Lesers durch den Empfänger durchgeführt. Die einzelnen Prozessschritte beinhalten:

- **Ausführung Transport:** Der Empfänger nutzt einen spezifischen Server für jedes vom Autor beauftragte Transportprotokoll. Er verwendet diesen, um die Transportnachrichten abzuholen. Die bereitzustellenden Transportberichte an den Leser werden stets aktualisiert.

- **Transportnachricht aufbereiten:** Der Empfänger verarbeitet eine Transportnachricht gemäß dem Transportnachrichtenformat aus dem Infrastrukturprofil. Hierbei werden die Fachnachrichten und der Transportauftrag des Autors aus der Transportnachricht, z.B. eine OSCI-Nachricht, extrahiert. Die vorgegebenen technischen Maßnahmen für Durchsetzung der Schutzziele werden angewendet (z.B. eine Prüfung/Auflösung einer Signatur und/oder Verschlüsselung des Senders).
- **Wende Serviceprofil an:** Die Einhaltung der Vorgaben aus den Serviceprofilen werden geprüft und in der weiteren Verarbeitung berücksichtigt, z.B. Vorgaben bzgl. der Infrastruktur und Kryptoverfahren.
- **Zuordnung zu den Lesern:** Die Transportauftragsdaten werden hinsichtlich der fachlichen Vorgaben geprüft. Der Empfänger prüft, ob die Nachricht an einen seiner Leser adressiert ist.
- **Übergabe an Leser:** Der Empfänger stellt die Nachricht dem Leser gemäß dem Kommunikationsszenario zur Verfügung.

4.2.4 Leser: Empfang einer Nachricht

Abbildung 4.7. Leser: Empfang einer Nachricht



Die Entgegennahme einer Nachricht wird seitens Leser durch den Eingang einer Nachricht ausgelöst. Die einzelnen Prozessschritte beinhalten:

- **Prüfe Zugang:** Der Leser überprüft, ob sein Zugang zu dem Empfänger gültig ist und die Transportinfrastruktur (z.B. Firewall) verfügbar ist. Je nach Bedarf reicht es aus, den Zugang z.B. ein Mal am Tag zu prüfen.

- **Prüfe Posteingang:** Im asynchronen Kommunikationsszenario prüft der Leser beim Empfänger, ob neue Nachrichten gemäß den Selektionskriterien für ihn vorliegen.
- **Hole XTA-Nachricht ab:** Der Leser holt eine XTA-Nachricht inkl. Transportauftrag und Fachnachricht von dem Empfänger ab.
- **Bestätige Abholung:** Der Leser bestätigt dem Empfänger, dass die Nachricht abgeholt werden konnte.
- **Prüfe Zuständigkeit:** Der Leser prüft anhand des Transportauftrags seine Zuständigkeit und die des Autors.
- **Kontrolliere Transport:** Anhand des Transportberichts, bereitgestellt vom Empfänger, prüft der Autor die Einhaltung des Serviceprofils.
- **Verarbeite Fachnachricht:** Der Leser überprüft und verarbeitet die Inhalte der Fachnachricht. Im Zuge dessen werden die vorgegebenen technischen Maßnahmen für Durchsetzung der Schutzziele angewendet (z.B. eine Überprüfung/Auflösung einer Signatur und/oder Verschlüsselung des Autors).

5 Normen, Standards und Regeln

In diesem Kapitel werden Normen, Standards und Regeln beschrieben, die bei der Entwicklung des Standards XTA beachtet / verwendet werden.

5.1 Datenschutz und Datensicherheit

Die allgemein gültigen datenschutzrechtlichen Anforderungen (DSGVO, BDSG, LDSG, Justizrichtlinie) werden berücksichtigt und das Standard-Datenschutzmodell (SDM)[1] [2] zu deren praktischen Umsetzung genutzt.

5.1.1 Integrität

Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. *Integrität* meint, dass die Daten vollständig und unverändert sind.

Die Informationstechnik fasst den Begriff in der Regel aber weiter und wendet ihn auf „Informationen“ an. Der Begriff „Information“ wird dabei für „Daten“ verwendet, denen je nach Zusammenhang eine bestimmte Semantik wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden kann. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

Integritätssicherung auf der Transportstrecke meint nicht die nachweisbare Abgabe einer Willenserklärung, sondern die mathematische Nachprüfbarkeit der Unverfälschtheit der Nachricht.

5.1.2 Intervenierbarkeit

Intervenierbarkeit stellt sicher, dass Betroffene bzw. Akteure mit legitimierten Eingriffsbefugnissen auf ein Verfahren mit Personenbezug wirksam eingreifen und bestehende Verfahren ändern können.

Weil es sich bei XTA um eine Infrastruktur handelt, die nur mittelbar in einer Beziehung zum betroffenen Bürger steht, stehen Maßnahmen zur Steuerung der Infrastruktur und Maßnahmen zur Steuerung des unmittelbaren Workflows des Kommunikationsvollzugs im Vordergrund.

5.1.3 Nichtverkettbarkeit

Nichtverkettbarkeit stellt sicher, dass die Datenverarbeitung bzw. der Transport von Nachrichten der Zweckbestimmung des Verfahrens insgesamt folgt. Damit soll eine vorsätzliche, fahrlässige oder funktional-fehlerhafte Datenverarbeitung, die ein Risiko für die Einhaltung der Zweckbindung darstellt, wesentlich erschwert werden.

Die Nichtverkettbarkeit im Kontext von IT-Infrastrukturen wird insbesondere durch organisatorische – und nicht technische – Maßnahmen erreicht.

5.1.4 Transparenz

Mit *Transparenz* soll im Sinne der Herstellung von Prüfbarkeit erreicht werden, dass alle Beteiligten nachweisen können, dass sie den rechtlichen Anforderungen (gemäß des anzuwendenden Schutzpro-

[1] Beschluss des IT-Planungsrats vom 25.03.2020, Az,; GS IT-PLR-22001/#31.
[2] SDM-Repository: www.datenschutz-mv.de/datenschutz/datenschutzmodell.

fils) genügt haben. Transparenz soll die Prüffähigkeit des gesamten Verfahrens sowie einzelner Komponenten sicherstellen.

Der Nachweis der Rechtskonformität bzw. die Prüfbarkeit ist für folgende Bereiche relevant:

- im Binnenverhältnis Autor–Sender und Leser–Empfänger
- für die funktionale Aufsicht bzgl. der deutschlandweiten (europaweiten) Sicherstellung von Interoperabilität und Effizienz durch den IT–Planungsrat
- für die Prüfbarkeit von Informationssicherheit und Datenschutz durch die Aufsichtsbehörden.

Die Sicherung der Transparenz ist Voraussetzung für ein Qualitätsmanagement durch den Auftraggeber (IT–Planungsrat), zu der auch eine externe Auditierung des Verfahrens zählen kann.

5.1.5 Verfügbarkeit

Die *Verfügbarkeit* von Dienstleistungen und Funktionen eines IT-Systems, von IT-Anwendungen oder von IT-Netzen oder auch die Verfügbarkeit von Informationen ist gegeben, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

5.1.6 Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

5.2 Technische Standards

XTA nutzt verschiedene Standards zur Definition von Datenstrukturen und der Kommunikationsschnittstellen. Für die Beschreibung der Datenstrukturen wird die W3C XML Schema Definition Language (XSD), und der Kommunikationsschnittstellen die Web Services Description Language (WSDL) genutzt. Folglich werden als Basis Artefakte für die Implementierenden herausgegeben, die einen SOAP-Webservice mit definierten XML-Datenstrukturen beschreiben. Somit kann die Validierung der Funktionsaufrufe und der Daten standardisiert und zum großen Teil automatisiert durchgeführt werden. Die normativen Vorgaben der Spezfikation werden nicht auf diese beschriebene technische Ausprägung begrenzt, sondern können unter Einsatz anderer Technologien/Architekturen zukünftig oder in eigens definierten Szenarien zusätzlich umgesetzt werden.

5.3 Verzeichnisse

Für den Nachrichtentransport werden sämtliche fachliche und technische Daten benötigt. Hierfür müssen geeignete Verzeichnisse vorgehalten werden. Unabhängig davon, ob es sich um interne oder öffentliche Verzeichnisse handelt, muss die Qualität der Daten mindestens dem Schutzbedarf der Prozesse entsprechen. Das stellt entsprechende Anforderungen an die Prozesse zur Akkreditierung der Identitäten und Eintragung der Daten.

5.3.1 Identitätsverzeichnis

Eine Identität besteht mindestens aus:

- **Rolle**: Zu einer Rolle gehören Rechte, die an anderer Stelle beschrieben werden. Beim Nachrichtentransport wäre es z. B. das Recht, eine bestimmte Nachricht an eine andere Behörde mit einer bestimmten Rolle schicken zu dürfen.

- **Fachliche Kennung**: Die fachliche Kennung muss eineindeutig sein und einen Präfix enthalten, der eindeutig für die Rolle ist.
- **Öffentlicher Verschlüsselungsschlüssel**: Der Autor einer Nachricht verschlüsselt diese mit dem öffentlichen Schlüssel des Lesers. Das gewährt die Vertraulichkeit und durch die Fähigkeit der Entschlüsselung weist der Leser seine Identität nach, da nur der Leser im Besitz des privaten Schlüssels sein darf.
- **Öffentlicher Signaturschlüssel**: Der Autor einer Nachricht signiert diese mit seinem privaten Schlüssel. Durch die Signaturprüfung mit dem öffentlichen Signaturschlüssel prüft der Leser die Integrität der Nachricht und die Identität des Autors.

Die Identitäten der an einem Nachrichtentransport beteiligten Akteure müssen überprüfbar sein. Dazu werden alle Identitäten in einem Identitätsverzeichnis veröffentlicht. Das Vertrauensniveau dieses Verzeichnisses muss angemessen sein für den Schutzbedarf der transportierten Nachrichten. Entsprechend sicher ist z. B. der Akkreditierungsprozess zu gestalten.

5.3.2 Adressierungsverzeichnis

In einem Adressierungsverzeichnis werden die technischen Parameter für die adressierbaren Einheiten je Transportprotokoll veröffentlicht. Die fachliche Sicht auf die adressierbare Einheit wird durch ein Serviceprofil beschrieben und umfasst insbesondere eine Reihe von unterstützten Nachrichtentypen.

5.3.3 Metadatenverzeichnis

In einem Metadatenverzeichnis werden die fachlichen und technische Vorgaben maschinenlesbar vorgehalten. Für einen sicheren und zuverlässigen Nachrichtentransport müssen alle Vorgaben aller beteiligten Akteure bekannt sein.

5.4 Technische Vorgaben

Für die einwandfreie Nachverfolgbarkeit und gezielte Steuerung des Nachrichtentransports müssen alle Zeitstempel in einem UTC Format inkl. Zeitzone gesetzt werden.

Ein Beispiel des W3-Konsortiums für eine in UTC definierte Zeitangabe ist *1994-11-05T13:15:30Z*.

5.5 Transformationen

Transformationen wandeln Daten bzw. Nachrichten in andere Daten bzw. Nachrichten um. Zum Beispiel werden eine Fachnachricht und ein Transportauftrag in eine Transportnachricht transformiert. Um welche Daten oder Nachrichten es sich genau handelt, spielt für die abstrakte Betrachtung keine Rolle. Die Nennung konkreter Daten und Nachrichten dient ausschließlich der Verdeutlichung. Die Transformationen können für unterschiedliche Zwecke genutzt werden:

- **Konstruktoren**: Ein Konstruktor erzeugt aus gegebenen Daten eine neue Nachricht, die die Daten enthält. Dazu werden die Daten an festgelegten Stellen eingefügt.
- **Extraktoren**: Ein Extraktor liest aus einer Nachricht die enthaltenen Daten aus und stellt sie zur Verfügung.
- **Maßnahmen**: Zur Erreichung eines angemessenen Schutzniveaus (gemäß SDM) sind die Daten und Nachricht mit geeigneten kryptographischen Verfahren zu behandeln. Hierbei kann es sich z. B. um die Anbringung einer Signatur oder einer Verschlüsselung handeln.
- **Prüfungen**: Mit einer Prüfung wird die korrekte Anwendung einer Maßnahme überprüft und zugleich werden die Maßnahmen zurückgenommen, z. B. durch eine Entschlüsselung. In den kryptografischen Schlüsseln verwendete Identitätsinformationen werden zur Verfügung gestellt.

5.6 Kommunikationsarten

5.6.1 Synchrone Kommunikation

Unter *synchroner Kommunikation* versteht man einen Modus der Kommunikation, bei dem der Autor einer Nachricht (Prozess) auf die Antwort des Kommunikationspartners wartet. Erst nach Erhalt der Antwort kann der sendende Prozess fortgesetzt werden. Der Vorteil für den Autor ist, dass er die Ergebnisse seiner Anfrage direkt erhält.

5.6.2 Asynchrone Kommunikation

Unter *asynchroner Kommunikation* versteht man einen Modus der Kommunikation, bei dem das Senden und Empfangen von Daten zeitlich versetzt und ohne Blockieren des Prozesses durch Warten auf die Antwort des Lesers stattfindet. Der Vorteil für den antwortenden Prozess ist, dass er die Möglichkeit hat zeitversetzt zu antworten.

Stichwortverzeichnis