

Vorwort zur Veröffentlichung

Die Beauftragung der vorliegenden Studie wurde vom IT-Planungsrat als eine vergleichende Analyse verschiedener Kommunikationstechnologien der nationalen Business-to-Government- (B2G) und Government-to-Government-Kommunikation (G2G) angestoßen. Die Studie diene der Vorbereitung verbindlicher Entscheidungen des IT-Planungsrats für die zukünftige Ausrichtung der B2G- und G2G-Kommunikation in Deutschland. Sie wurde bis zu dieser Veröffentlichung intern in föderalen Gremien zur Beratung verwendet und kritisch diskutiert.

Dieses Vorwort zur Veröffentlichung im Oktober 2026 dient dazu, einige der kontroversen Themen zum besseren Verständnis durch den Leser zu adressieren. Ansonsten ist diese veröffentlichte Studie identisch zur Version 1.0, die im August 2026 an den Auftraggeber übergeben wurde.

Zur inhaltlichen Diskussion:

Alle betrachteten Technologien werden derzeit aktiv weiterentwickelt. Die Studie beruht auf den Analysen der offiziell verfügbaren Dokumente, die im Zeitraum zwischen Februar und Juli abgerufen oder bereitgestellt wurden, sowie den Aussagen aus Experteninterviews, die zwischen April und Juli 2026 durchgeführt wurden. Insbesondere bei Technologien in frühen Entwicklungsphasen wie ZapuK oder NOOTS lagen in diesem Zeitraum Lücken in finalisierten, offiziell verfügbaren Konzepten vor. Gleichzeitig existieren für diese Technologien derzeit auch noch keine beobachtbaren, produktiv genutzten Infrastrukturen im zielnahen Ausbau. Diesbezügliche Technologierisiken oder potenzielle Schwächen, die in der Analyse aus lückenhaft dokumentierten Konzepten oder mangelnden Beobachtungsmöglichkeit resultieren, werden in der Studie benannt. Heute könnten manche dieser Schlussfolgerungen oder Bewertungen im Licht aktualisierter Informationen anders ausfallen. Die Ergebnisse der vorliegenden Studie sind also als Momentaufnahme des offiziellen Konzeptions- und Entwicklungsstands aus der ersten Jahreshälfte 2026 zu interpretieren.

Auch an der vergleichenden, kondensierten Bewertung über die vier grundlegenden Kommunikationsszenarien aus Abschnitt 5.4 haben sich kontroverse Diskussionen entzündet. Es wurde die Befürchtung geäußert, dass eine Technologie, die in der kondensierten Vergleichsmatrix eine breite funktionale Unterstützung aufweist, als generell besser oder geeigneter erscheine als derzeit noch spezialisiertere Technologien oder solche in frühen Entwicklungsphasen. Diesen Schluss haben die Autoren der Studie jedoch bewusst nicht gezogen. In der Studie wird ausdrücklich erklärt, dass spezifischere Anwendungsfälle als die der

Basisszenarien oft Anforderungen stellen, die durch funktional vielseitige „Alleskönner“-Technologien nicht umgesetzt werden können. Die Studie legt jedoch auftragsgemäß den Fokus auf die funktional breiten, generischen Szenarien von B2G/G2G-Kommunikation. Der besondere Wert des szenariobasierten Vergleichs besteht aus Sicht der Autoren darin, Entwicklungsbedarfe von möglicherweise heute noch spezialisierten Technologien in Richtung allgemeiner Einsatzmöglichkeiten aufzuzeigen. Sie bietet keine Anhaltspunkte, ob eine Technologie „gut“ oder „schlecht“ ist.

Von Vertretern bestimmter, noch nicht voll entwickelter Technologien wurde schließlich Kritik daran geäußert, dass das funktionale Potenzial ihrer Technologie in der Studie zu restriktiv beurteilt und nicht entsprechend gewürdigt wurde. Diese Kritik vernachlässigt aus Sicht der Autoren, dass die akkumulierten Defizite älterer Technologien ebenfalls ein Behebungspotenzial besitzen und dass umgekehrt mit der funktionalen Erweiterung einer Technologie oft neue Probleme einhergehen, die in der Folge zu adressieren sind. Man kann daher nicht der einen Technologie das Entwicklungspotenzial zu- und der anderen das Verbesserungspotenzial absprechen. Da in der Studie auch Technologien berücksichtigt werden sollten, die sich derzeit noch in Entwicklung befinden, haben die Autoren für die Analyse und Bewertung mindestens das Vorliegen von aussagekräftigen Konzepten vorausgesetzt. Reines Entwicklungspotenzial ohne klare Darlegung, wie die Ziele erreicht werden sollen, wurde von der Bewertung ausgeschlossen. Auch dies ist in der Studie ausdrücklich erklärt.

Die Autoren

Kaiserslautern im Oktober 2026

Studie zur Analyse der B2G- und G2G-Kommunikation mit Fokus auf Nachrichten-, Transport- und Verschlüsselungsprotokollen

Autoren:

Patrick Dzubba
Matthias Gerbershagen
Fabienne Hammer
Eva Jansohn
Natalie Meides
Christoph Müller
Dr. Reinhard Schwarz
Prof. Dr.-Ing. Nikolay Tcholtchev
Dr. Joachim Weber
Balthasar Weitzel
Dr. Armin Wolf

IESE-Report Nr. 011.26/D
Version 1.0
21. August 2026

Impressum

Das Fraunhofer IESE ist ein Institut der Fraunhofer-Gesellschaft.

Das Institut transferiert innovative Software-Entwicklungstechniken, -Methoden und -Werkzeuge in die industrielle Praxis. Es hilft Unternehmen, bedarfsgerechte Software-Kompetenzen aufzubauen und eine wettbewerbsfähige Marktposition zu erlangen.

Das Fraunhofer IESE steht unter der Leitung von

Prof. Dr.-Ing. Peter Liggesmeyer
Prof. Dr.-Ing. Jörg Dörr

Fraunhofer-Platz 1
67663 Kaiserslautern

Hinweis zur sprachlichen Gleichbehandlung

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Kurzfassung

Die Technologielandschaft der nationalen *Business-to-Government*- (B2G) und *Government-to-Government*- (G2G) Kommunikation zeichnet sich durch große Heterogenität aus. Der IT-Planungsrat hat die Durchführung der vorliegenden Studie initiiert, um die zukünftige Ausrichtung der Nachrichten- und Datenaustauschtechnologien in diesen Bereichen verbindlich zu klären.

Ziel der Studie ist eine umfassende Analyse und Bewertung der technischen Grundlagen und Sicherheitsaspekte der digitalen B2G- und G2G-Kommunikation mit dem Fokus auf Nachrichten- und Transportprotokollen, Kommunikationsinfrastrukturen sowie Verschlüsselungs- und Sicherheitsprotokollen. Die Studie soll die Grundlage für Entscheidungen bezüglich der Auswahl, Implementierung und Weiterentwicklung sicherer und interoperabler Kommunikationslösungen im öffentlichen Sektor liefern.

Zu diesem Zweck wurde im Rahmen der vorliegenden Studie anhand von Desktop-Recherchen und Experteninterviews ein Bewertungsmodell erstellt und grundlegende Kommunikationsszenarien der B2G- und G2G-Kommunikation identifiziert. Die in Frage kommenden Technologien wurden anhand des Bewertungsmodells sowie der Anforderungen der separaten Kommunikationsszenarien einzeln analysiert und in vergleichbarer Weise bewertet.

Die Ergebnisse dieser Analysen und Bewertungen zeichnen ein differenziertes Bild der Reifegrade und der Eignung unterschiedlicher Technologien für verschiedene Kommunikationsszenarien. Diese Erkenntnisse ermöglichen Entscheidungsgremien die Steuerung des Einsatzes und der Weiterentwicklung geeigneter Technologien. Zusätzlich gibt die Studie technische und Governance-bezogene Handlungsempfehlungen und benennt entsprechende Best Practices.

Schlagworte: GovTech, Verwaltungsdigitalisierung, Registermodernisierung, Nachrichtentransporttechnologien

Inhaltsverzeichnis

Kurzfassung	v
Abbildungsverzeichnis	ix
Tabellenverzeichnis	x
Abkürzungsverzeichnis	xi
Management Summary	xv
1 Untersuchungsgegenstand.....	1
1.1 Zielsetzung der Studie	1
1.2 Methodisches Vorgehen.....	2
1.3 Scope und Betrachtungsgegenstände	2
2 Kommunikationsmodelle im B2G- und G2G-Kontext.....	5
2.1 4-Corner-Modell	6
2.2 3-Corner-Modell	7
2.3 2-Corner-Modell	8
2.4 Überlegungen zur Ende-zu-Ende-Verschlüsselung (E2EE)	8
2.5 Implikationen eines 3- oder 4-Corner-Modells.....	10
2.6 Szenarien in der B2G- und G2G-Kommunikation	13
2.7 Deutschland-Stack	19
3 Technische Grundlagen des Nachrichtenaustauschs	21
3.1 Datenformate	21
3.2 Schnittstellenstandards.....	23
3.3 SOAP versus REST	25
3.4 Transport- und Nachrichtenprotokolle	27
3.5 Verschlüsselungs- und Sicherheitsprotokolle	31
4 Transportarchitekturen und -standards.....	35
4.1 Analysierte Technologien	35
4.2 OSCI.....	38
4.3 XTA.....	48
4.4 FIT-Connect	65
4.5 NOOTS	74
4.6 ZaPuK.....	85
4.7 X-Road	92
4.8 eDelivery AS4	99

5	Technologiebewertung.....	107
5.1	Bewertungsmodell	107
5.2	Allgemeine Technologiebewertung mittels SWOT-Analyse.....	110
5.3	Szenarienbasierte Technologiebewertung	150
5.4	Zusammenfassende Bewertung für Kommunikationsszenarien	163
6	Handlungsempfehlungen	169
6.1	Technische Handlungsempfehlungen.....	169
6.2	Handlungsempfehlungen zur Governance	172
	Liste der Interviews	183
	Literaturverzeichnis	185

Abbildungsverzeichnis

Abbildung 1	4-Corner-Modell (Quelle: Fraunhofer IESE).....	7
Abbildung 2	3-Corner-Modell (Quelle: Fraunhofer IESE).....	8
Abbildung 3	Darstellung der Kommunikationsebenen durch die OSCI-Spezifikation [24]	39
Abbildung 4	Heterogene Anbindung von kommunalen Fachverfahren an einen Betreiber von Transportverfahren ohne vereinheitlichte XTA-Schnittstelle [20]	50
Abbildung 5	Heterogene Anbindung eines Fachverfahrens zu den zentralen Transportverfahren in unterschiedlichen Bundesländern [20]	50
Abbildung 6	Datenübertragung mittels XTA zwischen Sender und Empfänger [43]	52
Abbildung 7	Datenübertragung zwischen Autor und Leser über das XTA-Protokoll [48]	53
Abbildung 8	Szenario einer testweisen Übertragung von Daten eines Portals über XTA an die OSCI- Infrastruktur zu entweder XTA- oder OSCI-Abnehmern [49]	54
Abbildung 9	Unterteilung der Service-Profile [43]	56
Abbildung 10	Netzübergänge bei XTA [53]	62
Abbildung 11	Nachrichtenmuster Request-Response/Sync für fachlich synchronen Nachweisabruf [81] ..	76
Abbildung 12	Nachrichtenmuster Request-Response mit erneutem Abruf [81]	76
Abbildung 13	Übersicht über die X-Road-Architektur [109]	94
Abbildung 14	Kommunikationsmodell des eDelivery-AS4 in Anlehnung an die Darstellung in [18]	101
Abbildung 15	XTA-Kooperationsmodell für die Definition von Service-Profilen [48]	118
Abbildung 16	Spezifikationsdarstellung »One-Way-Message« [24, S. 26]	152

Tabellenverzeichnis

Tabelle 1	Grundlegende Kommunikationsszenarien für die B2G- und G2G-Kommunikation	15
Tabelle 2	Unterstützte Signaturalgorithmen der OSCI-Spezifikation	42
Tabelle 3	In OSCI-Spezifikation erlaubte Verschlüsselungsalgorithmen	44
Tabelle 4	Bewertungsdimensionen und Bewertungskriterien	108
Tabelle 5	Eignung der Technologien für Szenario »Asynchron, mit oder ohne Antwort über separaten Kanal«	164
Tabelle 6	Eignung der Technologien für Szenario »Asynchron, mit asynchroner Nachricht über denselben Kanal«	164
Tabelle 7	Eignung der Technologien für Szenario »Synchron, Abruf«	165
Tabelle 8	Eignung der Technologien für Szenario »Synchron, Nachrichtenversand mit synchroner Rückmeldung«	166
Tabelle 9	Gesamtüberblick über alle Kommunikationsszenarien	167

Abkürzungsverzeichnis

ADR	Architecture Decision Record
AES	Advanced Encryption Standard
API	Application Programming Interface (Anwendungsprogrammierschnittstelle)
AS	Applicability Statement
B2B	Business-to-Business (Unternehmen zu Unternehmen)
B2G	Business-to-Government (Unternehmen zu Behörde)
beWiNr	bundeseinheitlichen Wirtschaftsnummer
BKN	Basiskomponente Nachweisabruf
BLK	Bund-Länder-Kommission
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BPSS	Baseline Personnel Security Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVA	Bundesverwaltungsamt
BVN	Bundesverwaltungsnetz
BW	Bundeswehr
CPU	Central Processing Unit
CSV	Comma-Separated Values
DAMAS	Datenmanagementsystem
DC	Data Consumer
DDoS	Distributed Denial of Service
DIN	Deutsches Institut für Normung
DMZ	Demilitarisierte Zone (Zwischenbereich zwischen Internet und internem Netz)
DP	Data Provider
DSC	Datenschutzcockpit
DÜ	Datenübermittlung
DVC	Deutsche Verwaltungscloud
DVDV	Deutsches Verwaltungsdienstverzeichnis
E2E	Ende-zu-Ende
E2EE	End-to-End Encryption (Ende-zu-Ende-Verschlüsselung)
ebMS	electronic business Messaging Service
ECDH-ES	Elliptic Curve Diffie-Hellman Ephemeral Static
EdDSA	Edwards-curve Digital Signature Algorithm
EDI	Electronic Data Interchange
EfA	»Einer für Alle«-Prinzip

Abkürzungsverzeichnis

EGVP	Elektronisches Gerichts- und Verwaltungspostfach
eID	[European] electronic Identification
ELSTER	Elektronische Steuererklärung
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
EUDI	European Digital Identity
EU-OOTS	European Once-Only Technical System
EU-TDD	EU-Technical Design Documents
FIM	Föderales Informationsmanagement
FIT-AB	Föderales IT-Architekturboard
FIT-SB	Föderales IT-Standardisierungsboard
FITKO	Föderale IT-Kooperation
FTP[S]	File Transfer Protocol [Secure]
G2B	Government-to-Business (Behörde zu Unternehmen)
G2G	Government to Government (Behörde zu Behörde)
G2X	Government to anyone
HTTP[S]	Hypertext Transport Protocol [Secure]
IAM	Identity- und Accessmanagement
IAM-B	Identity- und Accessmanagement für Behörden
IDA	Identitätsdaten-Abrufverfahren
IDM-P	Identity-Management für Personen
IDM-U	Identity-Management für Unternehmen
IDNr	Identitätsnummer
IDNrG	ID-Nummerngesetz
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IoT	Internet of Things (Internet der Dinge)
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Informationstechnik
IT-PLR	IT-Planungsrat
IVBB	Informationsverbund Berlin-Bonn
IVÖV	Informationsverbund der öffentlichen Verwaltung
JSON	JavaScript Object Notation
JWE	JSON Web Encryption
JWT	JSON Web Token
KoSIT	Koordinierungsstelle für IT-Standards
KPI	Key Performance Indicator (Leistungskennzahl)

MDN	Message Disposition Notification
Megolm	Matrix Extension Group Olm
MGF	Mask Generation Function
MIME	Multipurpose Internet Mail Extensions
MLS	Message Layer Security
mTLS	mutual Transport Layer Security
NdB	Netze des Bundes
NIIS	Nordic Institute for Interoperability Solutions
NOOTS	Nationales Once-Only Technical System
NRW	Nordrhein-Westfalen
OAEP	Optimal Asymmetric Encryption Padding
OASIS	Organization for the Advancement of Structured Information Standards
OCI	Oracle Cloud Infrastructure
OCSP	Online Certificate Status Protocol
OMEMO	OMEMO Multi-End Message and Object Encryption
OOT	Once-Only Technical System
OSCI	Online Services Computer Interface
OSCP	Online Certificate Status Protocol
OSI	Open Systems Interconnection
OSS	Open Source Software
OZG	Onlinezugangsgesetz
PDF	Portable Document Format
Peppol	Pan-European Public Procurement OnLine
PGP	Pretty Good Privacy
PKI	Private-Key Infrastructure
RAM	Random-access memory
RDN	Registerdatennavigation
REST	Representational State Transfer
RFC	Request for Comments
RSA	Rivest–Shamir–Adleman Kryptosystem
SAFE	Secure Access to Federated E-Justice/E-Government
SAK	Sicherer Anschlussknoten
SDG-VO	Single Digital Gateway-Verordnung
SDK	Software Development Kit
SHA	Secure Hash Algorithm
SID	Sächsische Informatik-Dienste
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTPS	Simple Mail Transfer Protocol Secure
SOAP	(ursprünglich) Simple Object Access Protocol

Abkürzungsverzeichnis

SSL	Secure Socket Layer
SVN	Sächsische Verwaltungsnetz
SWOT	Strengths, Weaknesses, Opportunities, and Risks
TCP	Transmission Control Protocol
TI	Telematik-Infrastruktur
TLS	Transport Layer Security
UMH	User Message Handler
UI	User Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF	Unicode Transformation Format
V-PKI	Verwaltungs-PKI
VS	Vermittlungsstelle
W3C	World Wide Web Consortium
WebRTC	Web Real-Time Communication
WS	Web Service
WSDL	Web Services Description Language
WSS	Web Services Security
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol
XÖV	XML in der öffentlichen Verwaltung
XSD	XML Schema Definition
XTA	XML in der öffentlichen Verwaltung Transport Adapter
XTA-SP	XTA-Service-Profil
XTA-WS	XTA-Webservice
ZaPuK	Zielarchitektur für Postfach- und Kommunikationslösungen
ZBDS	Zentraler Basisdienst Zahlungsabwicklung
ZBP	Zentrales Bürgerpostfach

Management Summary

In seiner 46. Sitzung hat der IT-Planungsrat mit dem Beschluss 2025/18 entschieden, eine Studie zur verbindlichen Klärung der zukünftigen Ausrichtung des Nachrichtenaustauschs von Business-to-Government- (B2G) und Government-to-Government-Kommunikation (G2G) zu veranlassen. Die Studie erfolgte in Abstimmung mit dem Strategischen Schwerpunktthema Digitale Anwendungen, dem föderalen IT-Standardisierungsboard und dem föderalen IT-Architekturboard. In dieser Abstimmung wurde das breite Themenfeld der B2G- und G2G-Kommunikation auf typische Anwendungsfälle der Innenverwaltung und der Justiz eingegrenzt. Zugleich wurde die Auswahl der zu betrachtenden Technologien auf OSCI, XTA 2, FIT-Connect, eDelivery AS4, NOOTS, ZaPuK und X-Road beschränkt.

Da sich die betrachteten Technologien sowohl in ihrer Natur als auch in ihren Reifegraden erheblich unterscheiden, wurde ein ausgewogenes System zur allgemeinen und speziellen Technologiebewertung für grundlegende Kommunikationsszenarien erarbeitet. Die allgemeinen Bewertungskriterien berücksichtigen dabei internationale Standards und föderale Standard-, Service- und Architekturvorgaben in den grundlegenden Dimensionen der Standard-Spezifikationen und -Governance, Implementierungen und Developer Experience, Kommunikations- und Infrastrukturmodellen sowie IT-Security. Die Analysen zeichnen für die unterschiedlichen Technologien in Hinsicht auf allgemeine Bewertung und Eignung für grundlegende Kommunikationsszenarien ein sehr differenziertes Bild.

OSCI und XTA 2 sind in der nationalen innerbehördlichen elektronischen Kommunikation sehr verbreitete Standards. Die OSCI-Infrastruktur zeichnet sich durch hohe Bewährtheit, Stabilität und Resilienz aus. Auch der Schnittstellenstandard XTA 2 hat einen hohen Verbreitungsgrad, wenn auch in deutlich geringerem Maße als OSCI. Beide Standards stellen eine breite Abdeckung verschiedenster Einsatz- und Kommunikationsszenarien bereit. So unterstützen beide Technologien generell asynchrone und synchrone Kommunikation. Trotz seiner fortgeschrittenen Reife zeigen sich beim XTA 2-Standard jedoch deutliche Defizite, die sich insbesondere in einer Unterspezifizierung, Überkomplexität und Ineffektivität hinsichtlich verschiedener Qualitäten äußern. Dies verursacht Effizienzverluste in Digitalisierungsprojekten, Markthürden und Akzeptanzprobleme. Auch der häufig mit XTA 2 assoziierte Nachrichtenstandard OSCI zeigt Defizite bei den Artefakten auf, die seine Anwendung unterstützen, wenn auch in geringerem Maße als XTA 2. Dadurch ist die Akzeptanz von OSCI bei Anwendern und Softwareherstellern insgesamt deutlich höher als die von XTA 2. Nach Analyse des Autorenteam der vorliegenden Studie sind viele der Defizite von OSCI

und XTA 2 einer fragmentierten Verteilung von Verantwortlichkeiten und Governance für Standard, Implementierungen und Infrastruktur geschuldet, woraus sich Lehren für die Governance neuerer Technologien ziehen lassen.

Die FIT-Connect-Infrastruktur stellt trotz berichteter Anfangsschwierigkeiten, die vom Autorenteam der Studie als typisch für neue Technologien eingeschätzt werden, insgesamt eine sehr gute Unterstützung von Softwareherstellern, Dienstleistern und Kommunen bereit. FIT-Connect bietet in asynchronen Kommunikationsszenarien bereits heute eine breite Funktionalität. Synchrone Kommunikationsszenarien werden hingegen derzeit noch kaum unterstützt und auch die Infrastruktur ist in Bezug auf Skalierbarkeit und Resilienz noch nicht dem Zielbild entsprechend entwickelt.

Der eDelivery-AS4-Nachrichtenstandard ist ebenfalls auf asynchrone Kommunikationsszenarien ausgerichtet und genießt nicht nur Vorteile bezüglich europäischer Anschlussfähigkeit, sondern auch ein sehr gutes, durch Quelloffenheit geprägtes Ökosystem und effektive Governance.

Ähnliche Vorteile treffen auch auf die X-Road-Technologie zu, die jedoch im Gegensatz zum eDelivery-AS4-Standard ausschließlich für synchrone Kommunikationsszenarien ausgelegt ist und mit ihrem serviceorientierten Kommunikationsparadigma weitgehend moderne Informationsarchitekturen unterstützt. Wie eDelivery AS4 unterstützt X-Road ebenfalls skalierbare und resiliente Infrastrukturen. Insgesamt beurteilt das Autorenteam der Studie X-Road als eine sehr gute Basis für generische, synchrone Kommunikationsszenarien.

Bezüglich ZaPuK und NOOTS mussten im Rahmen der Studie die meisten Annahmen und Projektionen getroffen werden. Die NOOTS-Implementierung wird derzeit nur in prototypischen Anwendungsfällen eingesetzt. Signifikante Teile der NOOTS-Infrastruktur sind noch nicht fertiggestellt oder noch nicht vollständig konzipiert. Das Release der ersten Version für den Produktivbetrieb liegt jenseits des Erscheinens der vorliegenden Studie. Aus diesem Grund konnten die technischen Konzepte von NOOTS nur teilweise bewertet werden.

Der Fokus der einsehbaren NOOTS-Konzepte liegt derzeit auf dem Registerabruf, der einen Spezialfall von nur einem der im Rahmen der Studie ermittelten vier Kommunikationsszenarien darstellt. Für diesen Spezialfall des Registerabrufs sieht NOOTS jedoch eine im Vergleich zu allen anderen betrachteten Technologien sehr mächtige funktionale Unterstützung rechtlicher und verwaltungstechnischer Anforderungen vor: die Prüfung, ob eine Kommunikation zwischen zwei authentifizierten Teilnehmern aus fachlicher Sicht überhaupt berechtigt ist, und die Sicherstellung der Anforderungen des Identifikationsnummerngesetzes. Für diese speziellen Anforderungen des Registerabrufs bieten die einsehbaren NOOTS-Konzepte eine angemessene Funktionalität und BSI-konforme

Konzeption der Kommunikationssicherheit. Eine darüberhinausgehende funktionale Abdeckung breiterer Kommunikationsszenarien mittels NOOTS ist zwar denkbar, aber im Rahmen dieser Studie wegen fehlender Konzeption nicht bewertbar.

ZaPuK ist die für den Deutschland-Stack beschlossene »Zielarchitektur für Postfach- und Kommunikationslösungen«. Dieses Architekturkonzept ist sowohl aufgrund seiner Technologieentscheidung zugunsten der Matrix-Technologie als auch aufgrund des Fokus auf Postfachlösungen in gewisser Weise ein Außenseiter in der vergleichenden Analyse. Denn sowohl Matrix als auch Postfächer adressieren in besonderer Weise nicht nur B2G- und G2G-Kommunikation, sondern auch Government-to-Citizen-Datenaustausch (G2C). Das Autorenteam der Studie erachtet Matrix und die bekannten Kernkonzepte von ZaPuK in Summe als angemessen. ZaPuK wird als Zielarchitektur jedoch erst nach dem Erscheinen der vorliegenden Studie finalisiert und ist deshalb nicht vollständig bewertbar.

Im Rahmen der Recherchen und Interviews wurden jenseits der rein technischen Eigenschaften einzelner Technologien eine Reihe von Erkenntnissen zu übergreifenden organisatorischen und technischen Problemfeldern gesammelt und in Handlungsempfehlungen adressiert.

1 Untersuchungsgegenstand

Die digitale Transformation der öffentlichen Verwaltung setzt einen sicheren, interoperablen und effizienten Austausch von Daten zwischen Behörden (Government-to-Government, G2G) sowie zwischen Unternehmen und Verwaltung (Business-to-Government, B2G) voraus. Gleichzeitig steigen die Anforderungen an die Digitalisierung von Verwaltungsleistungen, die Registermodernisierung und den medienbruchfreien Datenaustausch kontinuierlich. Vor diesem Hintergrund gewinnt die Leistungsfähigkeit der zugrunde liegenden Kommunikationsinfrastrukturen und -standards zunehmend an Bedeutung.

Die gegenwärtige Situation der B2G- und G2G-Kommunikation in Deutschland ist jedoch durch eine Diskrepanz zwischen den funktionalen Anforderungen einer modernen digitalen Verwaltung und den technischen Eigenschaften der bestehenden Infrastruktur geprägt. Die historisch gewachsene IT-Landschaft wird dabei maßgeblich durch föderale Strukturen geprägt. Getrennte Verantwortlichkeiten mit eigenen IT-Systemen, Schnittstellen und Betriebsmodellen ermöglichen zwar die Wahrung der digitalen Souveränität der einzelnen Ebenen, führen jedoch gleichzeitig zu einer hohen Heterogenität, die interoperablen Digitalisierungslösungen im Wege steht.

1.1 Zielsetzung der Studie

Vor diesem Hintergrund untersucht die vorliegende Studie die B2G- und G2G-Kommunikation mit besonderem Fokus auf Nachrichten-, Transport- und Verschlüsselungsprotokollen. Ziel ist es, den aktuellen Stand der eingesetzten und vorgesehenen Technologien zu analysieren, bestehende Herausforderungen hinsichtlich Interoperabilität, Sicherheit und Zukunftsfähigkeit zu identifizieren sowie Handlungsempfehlungen aus den Analysen abzuleiten. Dazu betrachtet die Studie, inwieweit die eingesetzten oder geplanten Kommunikationsstandards geeignet sind, die relevanten Kommunikationsszenarien technisch abzubilden, und welche Herausforderungen sich dabei für die verschiedenen Lösungsoptionen stellen.

Neben der technischen Eignung der Kommunikationsprotokolle untersucht die Studie auch, welche Governance-Mechanismen erforderlich sind, um eine koordinierte und verbindliche Weiterentwicklung der Kommunikationslandschaft zu unterstützen.

1.2 Methodisches Vorgehen

Das methodische Vorgehen zur Bestandsaufnahme basiert auf einer Desk Research. Dabei wurden insbesondere öffentlich zugängliche Architektur- und Konzeptbeschreibungen relevanter, derzeit eingesetzter Kommunikationstechnologien sowie verfügbarer oder in Entwicklung befindlicher Alternativlösungen ausgewertet. Zusätzlich wurden zur Vertiefung des Informationsgewinns 21 Interviews (siehe Liste der Interviews im Anhang) mit Personen geführt, die über ausgewiesene Expertise in der Verwaltungsdigitalisierung und der betrachteten Technologien verfügen.

In Verbindung mit einem Stakeholder-Workshop wurde die Bestandsaufnahme der Kommunikationstechnologien genutzt, um grundlegende B2G- und G2G-Kommunikationsszenarien zu identifizieren. Diese Kommunikationsszenarien wurden während der Experteninterviews validiert und verfeinert.

Aus den Anforderungen dieser Szenarien und unter Berücksichtigung verbindlicher europäischer Standards sowie föderaler Service- und Architekturvorgaben leitet die Studie ein Bewertungsschema ab, das die vergleichende Evaluation der sehr unterschiedlichen Kommunikationstechnologien ermöglicht. Mittels dieses Schemas werden die spezifischen Stärken, Schwächen, Chancen und Risiken der betrachteten Technologien in SWOT-Analysen herausgearbeitet und Einschätzungen zu deren Tauglichkeit in verschiedenen Kommunikationsszenarien gegeben.

Aus den Untersuchungsbefunden ergeben sich technische Handlungs- sowie Governance-Empfehlungen, die den verantwortlichen Planungsgremien Entscheidungshilfen für die Technologieauswahl, die strategische Neuausrichtung der föderalen Kommunikationsarchitektur sowie für die Steuerung der Verwaltungsdigitalisierung bieten.

Die Studie vermittelt somit Handlungsmöglichkeiten und Gestaltungsansätze in Bezug auf die Harmonisierung der Nachrichten-, Transport- und Verschlüsselungsprotokolle im Sinne der ermittelten Anforderungen an eine zukunftsfähige behördliche Kommunikationsinfrastruktur. Zugleich deckt sie bestehende Lücken und Unzulänglichkeiten auf, die einer leistungsfähigen Digitalisierungslösung potenziell im Wege stehen.

1.3 Scope und Betrachtungsgegenstände

Die vorliegende Studie konzentriert sich auf die Analyse von Nachrichten-, Transport- und Verschlüsselungsprotokollen im Kontext der B2G- und G2G-Kommunikation. Bestimmte Themenbereiche liegen außerhalb des Untersuchungsumfangs und werden daher nicht vertieft betrachtet.

Nicht Gegenstand der Studie sind:

- Wirtschaftlichkeitsbetrachtungen, insbesondere quantitative Analysen zu Kosten, Finanzierung, Beschaffung oder betriebswirtschaftlichen Auswirkungen einzelner Kommunikationslösungen und Infrastrukturansätze
- Rechtliche Analysen von Gesetzen, Verordnungen oder Verwaltungsvorschriften hinsichtlich bestehender oder möglicher Technologievorgaben. Insbesondere wird nicht untersucht, inwieweit der Einsatz bestimmter Technologien oder Standards durch normative Regelungen vorgeschrieben oder eingeschränkt wird.
- Kommunikationsszenarien im Bereich des Internet of Things (IoT), insbesondere die Kommunikation von Sensoren, Aktoren oder anderen vernetzten Geräten mit spezifischen Anforderungen an Protokolle und Infrastrukturen
- Fachspezifische Kommunikationslösungen des Gesundheitswesens, da dieser Bereich aufgrund seiner besonderen regulatorischen, organisatorischen und technischen Rahmenbedingungen eigene Kommunikationsstandards und Infrastrukturkomponenten aufweist
- Kommunikationsanforderungen des Militärs und von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) wie Polizei, Feuerwehren, Rettungsdienste, das Technische Hilfswerk oder der Katastrophenschutz, da BOS-Kommunikationstechnik häufig besonderen Anforderungen an Verfügbarkeit, Geheimschutz, Resilienz und Einsatzfähigkeit unter außergewöhnlichen Rahmenbedingungen unterliegt

Der Fokus der Studie liegt damit auf allgemeinen Kommunikationsszenarien der öffentlichen Verwaltung im B2G- und G2G-Kontext sowie den hierfür relevanten Nachrichten-, Transport- und Verschlüsselungsstandards.

2 Kommunikationsmodelle im B2G- und G2G-Kontext

Das Kommunikationsmodell einer Technologie definiert die verschiedenen Rollen, die bei der Erstellung und Übertragung von Nachrichten involviert sind, sowie ihre jeweiligen Aufgaben. In jedem Kommunikationsszenario sind mindestens die Rollen des Autors einer Nachricht und des Lesers einer Nachricht involviert. Das Kommunikationsmodell entscheidet darüber, welche Anforderungen diese Kommunikationspartner selbst erfüllen müssen und welche Aufgaben an weitere Rollen, wie etwa einen digitalen Zustelldienst, zugewiesen werden.

Für die Kommunikation zwischen Autor und Leser sind unter anderem folgende Aufgaben relevant, wobei nicht bei jedem Kommunikationsvorgang alle Aufgaben anfallen müssen (So ist z. B. Rechtssicherheit nicht immer erforderlich, sondern bei einem synchronen Nachweisabruf genügt die Übermittlung der gewünschten Daten oder die Meldung eines Fehlschlags.):

- Identitätsbestimmung und Adressierung: Die Identität des vorgesehenen Lesers der Nachricht muss bestimmt und auf eine Adresse innerhalb der Kommunikationsinfrastruktur bezogen werden.
- Sicherstellung von Authentizität und Integrität: Die Nachricht muss an die Identität des Autors gebunden sein. Es muss sichergestellt werden, dass die Nachricht nicht verändert werden kann.
- Berechtigungsprüfung: Es muss geprüft werden, ob eine Kommunikation zwischen Autor und Leser aus Sicht beider Parteien zulässig ist.
- Zustellung der Nachricht: Der Transportweg von Autor zu Leser muss bestimmt werden (Routing). Danach muss die Nachricht bis zum Leser transportiert werden. Fehler in der Zustellung müssen überwacht und behandelt werden.
- Gewährleistung von Vertraulichkeit: Es muss sichergestellt werden, dass die Nachricht nur von berechtigten Kommunikationsteilnehmern gelesen werden kann. Dazu werden in der Regel Verschlüsselungsverfahren verwendet.
- Rechtssicherheit der Kommunikation: Der Austausch der Nachricht muss protokolliert werden. Ein Autor sollte das Verfassen einer Nachricht nicht abstreiten können. Die fehlerfreie Zustellung der Nachricht sowie der Versands- und Zustellzeitpunkt sollten verifiziert werden können.

Diese Aufgaben können in verschiedenen Kommunikationsmodellen verschiedenen Rollen zugeordnet werden. Auch bei Verwendung desselben grundlegenden Kommunikationsmodells können verschiedene Technologien die Aufgaben

unterschiedlich auf die Rollen verteilen. Ebenfalls macht das Kommunikationsmodell keine Aussage darüber, auf welcher technischen Ebene (z. B. Datenformat oder Transportprotokoll) die Aufgaben umgesetzt werden.

Jedes Kommunikationsszenario stellt verschiedene Anforderungen an die genutzte Technologie und ihr Kommunikationsmodell. So kann ein Modell mit einer direkten Kommunikation zwischen Autor und Leser nur synchrone Kommunikationsszenarien abbilden, in denen Autor und Leser gleichzeitig verfügbar sind. Asynchrone Kommunikationsszenarien benötigen mindestens einen weiteren Teilnehmer, der Nachrichten zwischenspeichert und ausliefert.

2.1 4-Corner-Modell

In der Beschreibung der Kommunikation elektronischer Systeme im G2X-Kontext wird in Architekturdokumenten (sowohl national als auch europäisch, z. B. im Kontext eDelivery) häufig das 4-Corner-Modell (auch »Vier-Ecken-Modell«) verwendet [1]. Im Folgenden wird in dieser Studie der deutsche Sprachgebrauch für die vier Ecken des Modells verwendet: Autor, Sender, Empfänger und Leser.

Abbildung 1 zeigt das 4-Corner-Modell am Beispiel der OSCI / XTA-Kommunikation. Dieses Modell findet aber auch in anderen Kontexten Anwendung, wie etwa NOOTS. Ziel des Modells ist es, Fachsysteme der öffentlichen Verwaltung von der sicheren Übermittlung von Daten im Sinne der Informations- und Rechtssicherheit zu entlasten. So heißt es dazu bei [1, S. 9]:

»Bereits vor der Umstellung von Briefpost auf den elektronischen Datenaustausch ist von den Beteiligten festgestellt worden, dass die professionelle Organisation des Nachrichtentransports als eigenständige Aufgabe von darauf spezialisierten Stellen wahrgenommen werden muss. Zwar hätte der dem Datenaustausch zugrunde liegende OSCI-Standard grundsätzlich auch die bilaterale Datenübermittlung zwischen je zwei Meldebehörden erlaubt. Allerdings ist die verlässliche, elektronische Datenübermittlung mit einer Vielzahl von Administrations- und Überwachungsaufgaben verbunden, die keinen unmittelbaren Bezug zu den Fachaufgaben der Behörde haben. Hierzu gehören beispielsweise die Organisation der Pflege und der regelmäßigen Erneuerung digitaler Zertifikate, kryptografischer Schlüssel und sonstiger digitaler Identitäten, die Überwachung der Übermittlungen und die rechtzeitige Reaktion auf Fehler oder die regelmäßige Integration neuer Kommunikationspartner.«

Im 4-Corner-Modell verfasst ein Autor (Corner 1) – häufig ein Fachverfahren – eine Nachricht, die einem Sender-System übergeben wird. Das Sender-Empfänger-Paar (Corner 2 und 3) stellt die informations- und rechtssichere Übertragung sicher. Der Empfänger stellt schließlich die Nachricht dem Leser (Corner 4) zu.

Typische Aufgaben, die Sender und Empfänger im 4-Corner-Modell übernehmen, sind

- Identitätsbestimmung und Identitätsprüfung
- Berechtigungsprüfung
- Routing der Nachricht
- Verschlüsselung
- Ausstellen einer Zustellbestätigung
- Sicherstellung von Nichtabstreitbarkeit
- Überwachung der korrekten Übermittlungen
- Überprüfung der Nachrichten auf Integrität und Freiheit von Schadinhalten
- Fehlerbehandlung

Das 4-Corner-Modell trifft selbst keine Aussage darüber, wie die Kommunikation zwischen Sender und Empfänger stattfindet.

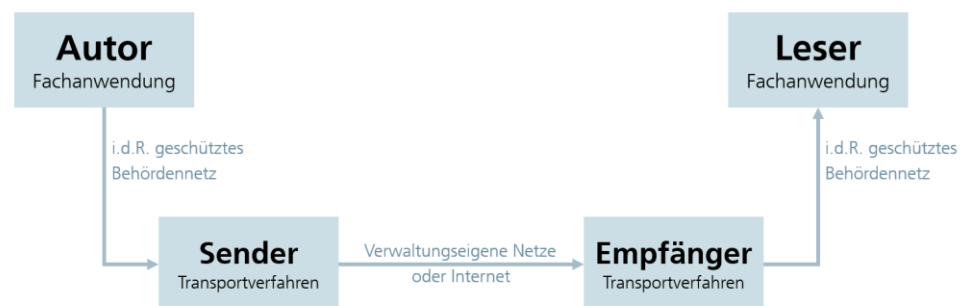


Abbildung 1 4-Corner-Modell (Quelle: Fraunhofer IESE)

2.2 3-Corner-Modell

Im Gegensatz zum 4-Corner-Modell existiert beim 3-Corner-Modell eine zentrale Nachrichtentransport-Infrastruktur. In diesem Fall kommuniziert der Autor (Corner 1) direkt mit der Transport-Infrastruktur (Corner 2), welche die Nachricht an den Leser (Corner 3) zustellt.

In diesem Modell müssen Autor und Leser also bereits grundlegende Fähigkeiten für eine sichere Identifizierung und verschlüsselte Kommunikation mit Corner 2 besitzen. Die anderen Aufgaben wie Routing, Berechtigungsprüfung, Überwachung und dergleichen gewährleistet Corner 2.

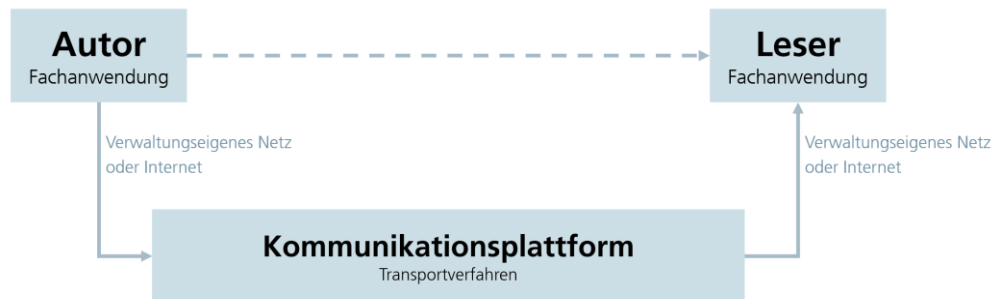


Abbildung 2 3-Corner-Modell (Quelle: Fraunhofer IESE)

2.3 2-Corner-Modell

Das 2-Corner-Modell sei hier nur der Vollständigkeit halber genannt. In diesem Modell kommunizieren Autor (Corner 1) und Leser (Corner 2) direkt. Dieses Kommunikationsszenario wird jedoch im Rahmen dieser Studie nicht betrachtet, da es bei keiner der untersuchten Datentransport-Lösungen Verwendung findet.

2.4 Überlegungen zur Ende-zu-Ende-Verschlüsselung (E2EE)

Bei Abwägungen technologischer Vor- und Nachteile im Rahmen dieser Studie nahm der Begriff der Ende-zu-Ende-Verschlüsselung (End-to-End Encryption, E2EE) einen zentralen Stellenwert ein. Dieser Begriff wurde in den Diskussionen, Dokumenten und Interviews jedoch nicht in einheitlicher Weise verwendet.

In der IT wird E2EE generell als die durchgängige, ununterbrochen verschlüsselte Kommunikation von Anwender zu Anwender verstanden.

Im Kontext dieser Studie machen die Begriffe *Business-to-Government* (B2G) und *Government-to-Government* (G2G) jedoch klar, dass die Enden der Kommunikation in erster Linie nicht als natürliche Personen verstanden werden, sondern als privatwirtschaftliche oder öffentliche Stellen.

In der B2G- und G2G-Kommunikation ist in vielen Fällen mindestens einer der Kommunikationsteilnehmer ein technisches System, wie ein Fachverfahren oder ein Register. Unabhängig davon, ob eine menschliche Person die Nachricht verfasst oder liest, wird oft das System als Autor oder Adressat der Nachricht angesehen. Diese Sichtweise ist vor allem durch verschiedene organisatorische Anforderungen an die Kommunikation mit öffentlichen Stellen, wie Funktionspostfächer, Vertretungsregelungen und Personalwechsel, geprägt. Die Mehrzahl der befragten Personen hat die Wahrnehmung des Fachverfahrens oder Registers als einen der Kommunikationsendpunkte bestätigt.

Ein weiteres Motiv für diese Betrachtungsweise ist die angestrebte Automatisierung der Verwaltungsprozesse. In mehreren Interviews wurde die Vollautomatisierung von Verwaltungsprozessen als explizites Ziel der Verwaltungsdigitalisierung genannt, wie etwa die Gewährung eines Online-Antrags, dessen Voraussetzungen automatisch geprüft werden können. Wird die Bearbeitung eines Vorgangs über Maschine-zu-Maschine-Kommunikation abgewickelt, fungiert ein IT-System als Kommunikationsendpunkt.

Insbesondere bei Verwendung eines 4-Corner-Modells wird der E2EE-Begriff teilweise noch weiter gefasst. Während nach obiger Beschreibung ein Fachverfahren oder Register als Autor beziehungsweise Leser der Nachricht als Endpunkt auftritt, betrachten einige Technologien die Rollen Sender und Empfänger als Endpunkte der Kommunikation. Dabei werden Nachrichten zum Beispiel auf einem vorgeschalteten Anschlussknoten vor dem Fachverfahren oder Register entschlüsselt, um sie dann über eine neu verschlüsselte Verbindung an das eigentliche Kommunikationsziel auszuliefern.

Diese Verwendung des E2EE-Begriffs unterscheidet sich in ihren Sicherheitseigenschaften grundsätzlich von der Betrachtung der Verschlüsselung von Anwender zu Anwender oder von Register zu Fachverfahren. Während angenommen werden kann, dass ein Fachverfahren unter der vollständigen Kontrolle der jeweiligen juristischen Person steht, sind Sender und Empfänger oftmals als Teil der Kommunikationsinfrastruktur zu betrachten und stehen gegebenenfalls unter Kontrolle einer dritten Partei. Da die Verschlüsselung im Anschlussknoten aufgebrochen wird, könnte ein Angreifer oder der Betreiber an dieser Stelle Einblick in die Nachrichten nehmen.

Um die Vertraulichkeit der Nachricht zwischen Autor und Leser sicherzustellen, ermöglichen diese Technologien teilweise eine zusätzliche Inhaltsverschlüsselung einer übertragenen Nachricht. Dabei verschlüsselt der Autor den Inhalt der Nachricht bereits vor der Übertragung zum Sender. Dazu muss er aber mit dem Leser einen zusätzlichen, gemeinsamen Schlüssel vereinbaren. Zudem entstehen durch die doppelte Verschlüsselung Effizienzeinbußen. Der Anschlussknoten verliert hierbei einen Teil seiner Schutzfunktionen (z. B. den Virenschutz). Zudem erlaubt die verbleibende Einsicht in die Metadaten bei der Umverschlüsselung potenziellen Angreifern weiterhin die Durchführung von sogenannten Verkehrsanalysen. Auch die angestrebte Komplexitätsreduzierung für den Anschluss von Autoren und Lesern an die Transportinfrastruktur wird durch die zusätzliche Verschlüsselung teilweise konterkariert.

Der Begriff E2EE sollte aus Sicht dieser Studie nur dann verwendet werden, wenn die unverschlüsselten Inhalte und die Metadaten der Nachricht nur für die (juristischen) Personen einsehbar sind, die als Autor und Leser der Nachricht auftreten. Zur Lösung der Herausforderungen durch Personalwechsel, Vertretungs-

regelungen und zur Unterstützung der Automatisierung können dabei – im Gegensatz zur klassischen Definition der Verschlüsselung von Endanwender zu Endanwender– auch technische Systeme wie Fachverfahren und Register als Endpunkte der Kommunikation auftreten. Den Zugriff auf die vertraulichen Daten durch verschiedene natürliche Personen (z. B. Sachbearbeitende) kann die Berechtigungsverwaltung der Fachverfahren kontrollieren und Daten können über Transportverschlüsselung bei der Übertragung zum Endgerät des Nutzens geschützt werden. Zentral für diese Betrachtung ist, welche Parteien die Kontrolle über ein technisches System besitzen und wer Zugriff auf die Daten hat.

2.5 Implikationen eines 3- oder 4-Corner-Modells

Die Wahl zwischen den verschiedenen Kommunikationsmodellen hat Implikationen für die technische Umsetzung und den Betrieb der Kommunikationsinfrastruktur. Im Folgenden werden primär das 3- und 4-Corner-Modell anhand verschiedener Aspekte verglichen. Das 2-Corner-Modell wird dabei nicht genauer betrachtet, da die vollständige Verantwortung immer bei den Kommunikationsendpunkten liegt und diese die Umsetzung der Anforderungen des Kommunikationsszenarios teilweise individuell entscheiden können.

Aufgabenverteilung: Grundsätzlich können die Aufgaben in der Kommunikation bei beiden Modellen unterschiedlich auf die jeweiligen Rollen verteilt werden. So kann, unabhängig vom Modell, die Technologie bei der Umsetzung entscheiden, welche Rolle für die Reaktion auf einen Zustellfehler oder für die Prüfung der Berechtigungen zuständig ist. Einige Aspekte sind jedoch durch das Kommunikationsmodell vorgegeben. In einem 3-Corner-Modell kann die Protokollierung des Eingangszeitpunktes und Zustellzeitpunktes der Nachricht vollständig durch die zentrale Infrastruktur erfolgen, während im 4-Corner-Modell der Autor nur über den Empfänger erfahren kann, wann der Leser die Nachricht empfangen hat. Die Verteilung der Aufgaben auf die verschiedenen Rollen hat in beiden Modellen Implikationen für die Sicherheit der Kommunikation und die Betriebskomplexität für Autor und Leser.

Sicherheit der Kommunikation: Die Sicherheitseigenschaften unterscheiden sich zwischen 3-Corner und 4-Corner nicht grundlegend. Es gibt in beiden Fällen Kommunikationsteilnehmer, die nicht der Autor oder Leser der Nachricht sind. Zur Wahrung der Vertraulichkeit ist in beiden Fällen eine Ende-zu-Ende-Verschlüsselung notwendig. Bei einem 3-Corner-Modell ist typischerweise nur eine weitere Partei, der Betreiber der zentralen Infrastruktur, involviert. Bei einem 4-Corner-Modell kann das Vertrauensmodell aufgrund verschiedener Betreiber von Sendern und Empfänger komplexer sein. Die Sicherheit hängt maßgeblich vom Vertrauen in die einzelnen Parteien und der Aufgabenverteilung ab. Ein Leser, der die Integritätsprüfung dem Empfänger überlässt, muss diesem entsprechend vertrauen können. Während im 3-Corner-Modell sowohl Autor als auch Leser

der gemeinsamen Infrastruktur vertrauen müssen, besteht bei einem 4-Corner-Modell unter Umständen die Freiheit, unterschiedliche vertrauenswürdige Instanzen für Sender und Empfänger zu wählen.

Betriebskomplexität: Eine zentrale Entscheidungsgrundlage bei der Wahl eines Kommunikationsmodells ist die gewünschte Komplexität und Kontrolle über die Kommunikation für die Rollen Autor und Leser. Je mehr Aufgaben und Vertrauen an andere Rollen abgegeben werden, desto einfacher ist die Implementierung und der Betrieb des technischen Systems, das als Autor oder Leser der Nachricht agiert. Das 4-Corner-Modell wird in vielen Fällen genutzt, um die Komplexität der Kommunikation in den Sender und Empfänger zu verlagern und somit die Anforderungen an Fachverfahren und Register zu verringern. Dies setzt jedoch auch entsprechendes Vertrauen in Sender und Empfänger voraus. Auf Seiten der Kommunikationsinfrastruktur entsteht durch die Aufteilung beim 4-Corner-Modell zusätzliche Betriebskomplexität. So kann ein Fehler bei der Zustellung einer Nachricht im 3-Corner-Modell zentral analysiert werden, während beim 4-Corner-Modell möglicherweise ein Austausch zwischen Sender und Empfänger notwendig ist. Generell kann gesagt werden, dass im 4-Corner-Modell Komplexität vom Autor und Leser an den Sender und Empfänger verlagert werden, während das 3-Corner-Modell mehr Kontrolle für Autor und Leser begünstigt. Im Hinblick auf den Betrieb der Kommunikationsinfrastruktur wird im 3-Corner-Modell die gesamte Komplexität beim zentralen Provider gebündelt, während im 4-Corner-Modell eine komplexe Governance des Ökosystems der Sender und Empfänger benötigt wird.

Ausfallsicherheit der Kommunikationsinfrastruktur: Die tatsächliche Ausfallsicherheit hängt nicht vom Kommunikationsmodell, sondern vom Betriebsmodell der Infrastruktur ab. Das 4-Corner-Modell bestimmt nicht, wie viele Betreiber von Sender- und Empfänger-Infrastruktur es gibt und wie sich Störungen zwischen diesen auswirken. Gleichermäßen bedeutet eine 3-Corner-Struktur nicht zwingend, dass es einen zentralen Single Point of Failure gibt: Durch eine geeignete redundante Auslegung kann die Ausfallsicherheit von Corner 2 – der zentralen Infrastruktur – auf das erforderliche Maß angehoben werden. Beide Modelle können darüber hinaus von zusätzlichen Diensten (z. B. Verzeichnisdienst, PKI) abhängen, die unabhängig von der Kommunikationsstruktur ausfallen können. Eine generelle Aussage über die technische Ausfallsicherheit kann nicht getroffen werden, jedoch bietet das 4-Corner-Modell eine bessere organisatorische Resilienz durch die Aufteilung der Verantwortung. Bei entsprechender Verteilung der Nutzenden auf verschiedene Provider von Sendern und Empfängern sind die Auswirkungen von Störungen im 4-Corner-Modell zudem geringer, da ein Ausfall bei einem Provider nur eine Teilmenge der Nutzenden betrifft.

Nachrichtenfluss und Firewall-Friendliness: Ein oft diskutiertes Thema im Bereich der B2G- und G2G-Kommunikation ist die Übertragung der Nachrichten

über öffentliche Netze und die Erreichbarkeit der Kommunikationsteilnehmer. *Firewall-Friendliness* bezeichnet dabei das Maß an erforderlichen Firewall-Freigaben für Verbindungen aus einem unsicheren Netz (z. B. dem Internet), um eine Nachricht an einen Leser zustellen zu können. Die Fachverfahren und Register, die als Leser agieren, werden dabei in der Regel in internen, abgeschotteten Netzen betrieben. Eine Freigabe für die eingehende Kommunikation aus dem Internet in diese Netze ist oft nicht möglich. Sowohl im 3-Corner- als auch im 4-Corner-Modell gibt es jedoch technische Möglichkeiten, solche Freigaben zu vermeiden. Generell sind ausgehende Verbindungen, also vom Fachverfahren im abgeschotteten Netz zu einem Server im Internet, als weniger sicherheitskritisch zu betrachten. In beiden Kommunikationsmodellen ist die Verwendung von *Polling* (Abfrage nach neuen Nachrichten durch den Leser in regelmäßigen Zeitabständen) oder *Long-Polling* (Verbindungsaufbau und Abfrage neuer Nachrichten durch den Leser mit einem blockierenden Abruf; Rückmeldung mit Reaktivierung des blockierten Lesers durch den Empfänger bei neuer Nachricht) üblich. Die Leser müssen in beiden Modellen nicht zwingend extern erreichbar sein. Sie müssen lediglich mit ihrem Empfänger oder der zentralen Infrastruktur kommunizieren können. Die Anforderungen an die Erreichbarkeit der Kommunikationsinfrastruktur unterscheiden sich zwischen den Modellen. Im 3-Corner-Modell muss die zentrale Infrastruktur lediglich für alle Autoren und Leser erreichbar sein, während im 4-Corner-Modell mehr Kontrolle möglich ist, dazu jedoch auch komplexe Freigaberegeln zwischen allen Sendern und Empfängern notwendig sind.

Unterstützte Kommunikationsszenarien: Ein Ausschlusskriterium für das 2-Corner-Modell in vielen Anwendungsfällen ist die erzwungene Synchronität der Kommunikation. In diesem Modell müssen Autor und Leser zwangsweise gleichzeitig anwesend und aktiv sein, um Nachrichten auszutauschen. Sowohl im 3-Corner- als auch im 4-Corner-Modell ist stattdessen die Zwischenspeicherung der Nachrichten durch die Kommunikationsinfrastruktur möglich. Dabei unterscheiden sich jedoch die Modelle in ihrer Eignung, vor allem für die synchrone Kommunikation. Als synchron betrachten wir dabei Kommunikation, die bestimmte Antwortzeiten einhalten muss. Bei einem 4-Corner-Modell fließen die Nachrichten über mindestens drei Verbindungen – vom Autor über den Sender zum Empfänger und von dort zum Leser. Dabei entstehen zusätzliche Latenzen, größere Timeout-Intervalle und zusätzliche Fehlerquellen. Eine synchrone Kommunikation ist generell möglich, jedoch schwieriger einzuhalten. Primär entscheidend für die Antwortzeiten einer Kommunikationsinfrastruktur ist jedoch nicht das Modell, sondern dessen technische Implementierung. Falls ein 3-Corner-Modell Polling mit großen Zeitabständen für den Abruf der Nachrichten durch den Leser verwendet, können die Anforderungen der synchronen Kommunikation auch in diesem Fall nicht erfüllt werden.

Zusatzfunktionen: Als Erweiterung der Aufgabenverteilung kann die Umsetzung von zusätzlichen Aufgaben in der Kommunikation gesehen werden. Ein oft diskutiertes Beispiel dafür ist die Prüfung von Nachrichteninhalten auf Viren und Schadcode. Prinzipiell können Funktionen, die den Inhalt der Nachrichten prüfen, sowohl im 3-Corner- als auch im 4-Corner-Modell an verschiedenen Stellen umgesetzt werden. In beiden Fällen wird Vertrauen in die prüfende Instanz, also etwa den Empfänger oder die zentrale Infrastruktur, und eine Berechtigung zum Einsehen des Inhaltes der Nachricht vorausgesetzt. Bei der Verwendung von E2EE ist eine Verarbeitung des Inhaltes durch die Kommunikationsinfrastruktur in beiden Modellen nicht möglich.

Abschließend ist es wichtig zu betonen, dass die Wahl des Kommunikationsmodells allein nicht darüber entscheidet, wie sicher, komplex oder resilient eine Kommunikationsinfrastruktur ist. Die technische Umsetzung, Verteilung der Aufgaben und das Betriebsmodell können die Eigenschaften der Kommunikationsmodelle unterstützen oder abschwächen. Die wichtigsten Unterschiede zwischen 3-Corner- und 4-Corner-Kommunikation betreffen das Vertrauensmodell und die Verteilung der Komplexität. Im 4-Corner-Modell können Autoren und Leser durch die Sender und Empfänger entlastet werden, wenn sie diesen vertrauen. Durch die Verteilung der Aufgaben ist der Betrieb eines Ökosystems aus verschiedenen Providern möglich. Diese Faktoren erhöhen die Komplexität des Vertrauensmodells, wodurch eine komplexe Governance für die Beziehungen zwischen den Providern notwendig wird. Im 3-Corner-Modell hingegen müssen alle Teilnehmer einem zentralen Provider vertrauen, der entsprechend mehr Kontrolle und Betriebskomplexität für sich vereinnahmt. Zusammenfassend kann man damit sagen, dass die Anforderungen an Autoren und Leser im 3-Corner-Modell generell höher sind.

2.6 Szenarien in der B2G- und G2G-Kommunikation

In der B2G- und G2G-Kommunikation gibt es eine Vielzahl verschiedener Kommunikationsszenarien, die jeweils eigene Anforderungen mit sich bringen. Beispiele für diese fachlichen Kommunikationsszenarien sind das Antrags- und Meldewesen, die Zustellung von Nachweisen und Bescheiden, die Übertragung hoheitlicher Dokumente und weitere.

Auf fachlicher Ebene werden diese Anforderungen durch die Verwaltungsleistung geprägt, die durch das Kommunikationsszenario abgebildet wird. Dabei geht es unter anderem darum, wer die Kommunikation initiiert, welche Arten von Nachrichten ausgetauscht werden und wie viele Schritte im Prozess durchlaufen werden. Je nach Fachbereich der Verwaltungsleistung können weitere Anforderungen hinzukommen, wie etwa die Referenzierbarkeit von Nachrichten oder die rechtssichere Protokollierung der Kommunikation.

Diese fachlichen Anforderungen münden in technischen Anforderungen, die entweder der Kommunikationstechnologie, die für den Austausch der Nachrichten verwendet wird, oder den elektronischen Fachverfahren zugeordnet werden müssen. Typische technische Anforderungen an die Kommunikationstechnologie sind beispielsweise eine Bidirektionalität des Nachrichtenkanals oder spezielle Anforderungen an die Sicherheit, Latenz, Protokollierung oder Synchronität der Übertragung.

Anhand dieser resultierenden, technischen Anforderungen lassen sich grundlegende, abstrakte Kategorien von Kommunikationsszenarien identifizieren.

2.6.1 Systematik

Der Austausch formaler Nachrichten (z. B. Dokumente, Anträge, Belege, strukturierte Datensätze) zwischen IT-Systemen im B2G- und G2G-Kontext wird in dieser Studie in zwei abstrakten Haupt-Kommunikationsszenarien betrachtet, die sich jeweils in zwei Unterszenarien gliedern. Die Kommunikationsszenarien wurden auf Basis der Erkenntnisse eines Kickoff-Workshops entwickelt und in Interviews mit Gesprächspartnern, die über einen breiten Überblick über B2G- und G2G-Nachrichtenaustausch verfügen, als grundlegende Kommunikationsszenarien validiert.

Die beiden Hauptszenarien betreffen *fachlich* asynchrone und synchrone Kommunikation. Fachlich asynchrone Kommunikation über einen technischen Kommunikationskanal liegt vor, wenn für eine vom Autor gesendete Nachricht eine mögliche Fachantwort zeitversetzt erfolgt. Gründe für diesen Zeitversatz können unbestimmte, möglicherweise weit auseinanderliegende Zeitpunkte des Empfangs oder langwierige Verarbeitungs- und Geschäftsprozesse beim Leser sein. Synchrone Kommunikation liegt vor, wenn eine Nachricht empfangen und unmittelbar maschinell verarbeitet wird, sodass der Leser innerhalb einer garantierten, kurzen Zeit (typischerweise innerhalb weniger Sekunden) eine zugehörige Fachantwort erstellen und zurücksenden kann.

Als *Kommunikationskanal* oder kurz *Kanal* wird im Folgenden eine Technologie mit zugehöriger Infrastruktur zur standardisierten Übertragung von Nachrichten und Daten zwischen Kommunikationspartnern bezeichnet, einschließlich der dafür bereitgestellten Protokolle, Dienste und Betriebsmechanismen.

Tabelle 1

Grundlegende Kommunikationsszenarien für die B2G- und G2G-Kommunikation

Haupt-Szenario	Unterszenario	Beispiel
(fachlich) asynchron	Nachrichtenversand ohne Antwort / mit Antwort über separaten Kanal	Gewerbeanmeldung; Bauantrag
	Nachrichtenversand mit asynchroner Antwort über denselben Kanal	Fortschreibungsrückmeldung; zeitlich entkoppelte Status- oder Ergebnismitteilung
(fachlich) synchron	Abruf	Registerabruf; vorausgefüllter Meldeschein; Identitätsdatenabruf
	Nachrichtenversand mit synchroner Rückmeldung	Strukturierter Antrag mit direkter Rückmeldung über Vollständigkeits-/Plausibilitätsprüfung; Übermittlung von Daten für hoheitliche Dokumente

In allen Szenarien muss der Kommunikationskanal Identifizierungs- und Routingmechanismen bereitstellen sowie sichere Übertragung hinsichtlich der drei Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit gewährleisten.

2.6.2 Szenario »Asynchron, mit oder ohne Antwort über separaten Kanal«

In diesem Szenario sendet der Autor eine Nachricht von der Kategorie Antrag, Meldung oder dergleichen an den Leser. Diese Nachricht wird durch einen Geschäftsprozess verarbeitet, der entweder keine Fachantwort produziert oder eine Fachantwort, die auf andere Weise zugestellt wird (z. B. Senden eines Antrags über Kommunikationskanal X, Antwort als elektronischer Bescheid im Unternehmenskonto des Unternehmens über Kanal Y).

Es besteht nicht die Erwartung, dass die Nachricht direkt zugestellt werden kann, da der Zeitpunkt der Zustellung unter Kontrolle des Empfängers beziehungsweise des Lesers steht. Es besteht ebenfalls keine Erwartung, dass für die zugestellte Nachricht eine Fachantwort über denselben Kanal erfolgt.

Anforderungen

- Da der Empfänger oder der Leser den Zeitpunkt der Zustellung kontrolliert, sollte der Kommunikationskanal die Nachrichten über definierte Zeiträume zwischenspeichern können.

- Der Sender benötigt in der Regel Methoden des Kommunikationskanals, um auf rechtssichere Weise bestimmte Ereignisse im Kommunikationsverlauf oder ein gesamtes Protokoll belegen zu können. Dies ist zum Beispiel notwendig, um das rechtzeitige Einreichen eines Antrags oder die erfolgte Zustellung einer Fachnachricht im Justizwesen nachweisen zu können. Das Führen von Protokollen hat datenschutzkonform zu erfolgen.
- In bestimmten Fällen können Anforderungen an Durchsatz, Latenz oder besondere Nachrichtengrößen vorliegen. Aus der reinen Asynchronität darf nicht geschlossen werden, dass der Kommunikationskanal keine angemessenen Leistungsmerkmale bereitstellt oder garantiert.

2.6.3 Szenario »Asynchron, mit asynchroner Antwort über denselben Kanal«

In diesem Szenario sendet der Autor eine Nachricht an den Leser, die auf Seiten des Lesers eine fachliche Verarbeitung erfordert und ein Ergebnis produziert. Der Verarbeitungsprozess kann eine unbestimmte Zeit in Anspruch nehmen.

Beispiele für diese Kategorie des Nachrichtenaustauschs sind Fortschreibungsrückmeldungen. Die Meldung über einen Wohnsitzwechsel von einer Meldebehörde zu einer anderen Meldebehörde wird zum Beispiel nach Prüfung als erfolgreich angenommen, ablehnend beantwortet, oder es wird eine Inkonsistenz deklariert, die weitere fachliche Klärung erfordert.

Es besteht weder für die erste noch für die zweite Nachricht die Erwartung, dass die Nachricht direkt zugestellt werden kann, da der Zeitpunkt der Zustellung unter Kontrolle des jeweiligen Empfängers oder Lesers steht. Es besteht keine Erwartung, dass für die zugestellte Nachricht zeitnah die Rückmeldung erfolgt, da der Verarbeitungsprozess langwierig sein kann.

Anforderungen

- Es gelten in beiden Richtungen alle Anforderungen aus dem ersten asynchronen Szenario.
- Zusätzlich besteht im Allgemeinen der Bedarf für die Referenzierbarkeit von Folgekommunikation, etwa über Referenz- oder Transaktions-IDs, deren Gesamtverlauf ebenfalls rechtssicher protokolliert wird. Das Führen von Protokollen hat datenschutzkonform zu erfolgen.

2.6.4 Szenario »Synchron, Abruf«

In diesem Szenario sendet ein (*Daten-*)*Abrufer* eine Abruf-Anforderung (*Request*) für einen spezifischen Datensatz an einen (*Daten-*)*Bereitsteller*. Die Abruf-Anforderung wird vom Bereitsteller – wenn verfügbar – mit dem angefragten Datensatz beantwortet (*Response*). Wenn die Anforderung nicht bedient werden kann,

ist auch dies zurückzumelden. Beispiele für diese Kategorie des Nachrichtenaustauschs sind Abrufe von Identitätsdaten im IDA-Verfahren oder Registerabrufe in NOOTS.

Es besteht die Erwartung, dass der Request direkt an den Bereitsteller zugestellt werden kann, das heißt dass der Bereitsteller immer erreichbar ist. Es besteht die Erwartung, dass der Datenabruf sofort beantwortet wird, das heißt die Response wird nach einer kurzen Verarbeitungszeit ohne Verzögerung an den Abrufer gesendet.

Anforderungen

- Der Kommunikationskanal unterstützt synchrones Request/Response mit kontrollierten Zeitlimits (Timeouts). Geht nach Verstreichen eines Zeitlimits keine Antwort auf eine Anfrage ein, kann diese beispielsweise mehrfach wiederholt werden, bis entweder eine Antwort eingeht oder der Anfrageprozess mit einer Fehlermeldung abbricht.
- Unter der Annahme, dass der Bereitsteller stets erreichbar ist, erfolgt die Zustellung des Requests ohne Verzögerung, im Folgenden als *Callback-* oder *Push-Unterstützung* bezeichnet. Der Kommunikationskanal muss eine API oder ein SDK zur Verfügung stellen, mit dem dies Firewall-verträglich umsetzbar ist.
- Die Response – sofern durch den Bereitsteller sofort angestoßen – erreicht den Abrufer typischerweise innerhalb weniger Sekunden. Das heißt der *Round-Trip* wird innerhalb kurzer Zeit beendet.
- Ob eine Protokollierung erwünscht oder unerwünscht ist, hängt vom konkreten Anwendungsfall ab. Es existieren beispielsweise Situationen, in denen eine Protokollierung in der Infrastruktur unerwünscht ist, um mögliche Profilbildungen zu verhindern.

2.6.5 Szenario »Synchron, Nachrichtenversand mit synchroner Rückmeldung«

In diesem Szenario sendet der Autor eine Nachricht an den Leser (*Request*), die auf Seiten des Lesers eine fachliche Verarbeitung mit einem Ergebnis erfordert oder die in der Verarbeitung Widerspruchsgründe erzeugen kann. Der Verarbeitungsprozess kann in kurzer Zeit maschinell durchgeführt werden. Der Leser sendet sofort nach dem Ergebnis eine Antwort (*Response*). Diese Antwort ist nicht gleichzusetzen mit der vollständigen fachlichen Ver- oder Bearbeitung der empfangenen Nachricht. Dies wäre nur dann der Fall, wenn der vollständige fachliche Geschäftsprozess sofort maschinell komplett durchlaufen werden kann. Möglicherweise ist die Response deswegen jedoch nur die Bestätigung – oder Ablehnung – im Rahmen eines ersten, automatisierbaren Schritts des fachlichen Geschäftsprozesses.

Beispiele für diese Kategorie des Nachrichtenaustauschs sind etwa Anträge oder bestimmte Formen des Datenaustauschs im Bereich »hoheitlicher Dokumente«, die vollständig oder in einem ersten Teilschritt unmittelbar maschinell verarbeitet werden können. Dass für einen Antrag eine positive Response erfolgt, bedeutet nicht, dass der Verwaltungsvorgang selbst vollständig abgeschlossen ist. Im Falle eines online eingereichten Antrags ist hier zum Beispiel nur eine Eingangsprüfung als abgeschlossen signalisiert. Die komplette Antragsbearbeitung mündet dann wie im ersten asynchronen Szenario in einem Bescheid, der über einen anderen Kommunikationskanal zu einem Postfach der antragsstellenden Person gesendet wird.

Anforderungen

- Der Kommunikationskanal unterstützt synchrones Request/Response mit kontrollierten Timeouts wie im vorangegangenen Abschnitt beschrieben.
- Unter der Annahme, dass der Leser stets erreichbar ist, erfolgt die Zustellung der Anfrage ohne Verzögerung, per Callback oder Push. Der Kommunikationskanal muss eine API oder ein SDK zur Verfügung stellen, mit dem dies Firewall-verträglich umsetzbar ist.
- Die Response mit der Auskunft über Erfolg oder Misserfolg – sofern direkt vom Leser angestoßen – erfolgt typischerweise innerhalb weniger Sekunden. Das heißt, dass der Round-Trip innerhalb kurzer Zeit beendet wird.
- Der Kommunikationskanal muss im Allgemeinen ähnliche Methoden wie bei den asynchronen Szenarien für den Abruf rechtssicherer Kommunikationsprotokolle bereitstellen. Das Führen von Protokollen hat datenschutzkonform zu erfolgen.

2.6.6 Unstrukturierte Formate

Unstrukturierte Datenformate geben keine inhaltliche Struktur der übertragenen Nachricht vor. Die meisten E-Mails, Chatnachrichten und viele textbasierte Dokumente können als unstrukturiertes Datenformat betrachtet werden. Unstrukturierte Datenformate bieten den Vorteil der unbegrenzten Flexibilität und eines theoretisch minimalen Overheads, sind jedoch in der Regel nicht maschinenlesbar und können schwer automatisiert verarbeitet oder validiert werden.

2.6.7 Passive und aktive Empfänger

In synchronen Szenarien wird auf Seite des Lesers, beziehungsweise des Datenbereitstellers, als technische Komponente generell der Einsatz eines sogenannten *passiven Empfängers* vorausgesetzt. Man beachte, dass mit »Empfänger« in diesem Fall nicht der Empfänger im 3- oder 4-Corner-Modell gemeint ist, sondern die technische Komponente im IT-System des Lesers, das die eingehenden

Nachrichten entgegennimmt. »Passiv« bedeutet, dass dieser (technische) Empfänger selbst keine Anfragen bei der Kommunikationsinfrastruktur durchführen muss, um eine Nachricht zugestellt zu bekommen.

Folglich erfordert dies von der Kommunikationsinfrastruktur die Fähigkeit, diesen (technischen) Empfänger für die Nachrichtenzustellung aufzurufen. Dies impliziert, dass die Kommunikationsinfrastruktur den Zeitpunkt der Zustellung bestimmt, was für die Erfüllung von Zeitlimits in einer synchronen Kommunikation eine notwendige Voraussetzung ist. Die Tatsache, dass dieser Empfänger von der Kommunikationsinfrastruktur aus erreichbar sein muss, stellt die Systemadministration und IT-Sicherheit in bestimmten Konstellationen vor Herausforderungen, etwa beim Einsatz von *Webhooks*.

Aktive Empfänger stellen hingegen Anfragen an die Kommunikationsinfrastruktur (Polling), um bereitstehende Nachrichten abzurufen. Da auf diese Weise der Empfänger den Zeitpunkt einer Nachrichtenzustellung bestimmt, ist diese Form der Infrastruktur-Empfänger-Konstellation im Allgemeinen nicht für synchrone Kommunikationsszenarien geeignet. Aktive Empfänger kommen deswegen vorwiegend in asynchronen Szenarien zum Einsatz. Da in diesem Fall die Zustellung stark zeitversetzt erfolgen kann, erfordert dies, dass die Kommunikationsinfrastruktur Nachrichten über längere Zeiträume zwischenspeichern muss. Die aktive Kontaktaufnahme vom Empfänger zur Kommunikationsinfrastruktur ist in der Regel unkritischer für Systemadministration und IT-Sicherheit, erfordert jedoch höhere Rechenressourcen.

Ein Sonderfall liegt bei der *Initiativumkehr* vor. In diesem Fall erfolgt der Verbindungsaufbau wie beim aktiven Empfänger von Seiten des Lesers oder Daten-Bereitstellers. Nach dem erfolgreichen Verbindungsaufbau geht der (technische) Empfänger im Leser / Daten-Bereitsteller jedoch in einen blockierten Zustand, bis eine Nachricht von der Kommunikationsinfrastruktur eintrifft. Dies schont die Rechenressourcen bei Kommunikationsinfrastruktur und (technischem) Empfänger durch die Vermeidung unnötiger Anfragen. Außerdem verbindet es die Vorteile des aktiven Empfängers bezüglich Systemadministration und IT-Sicherheit mit den Vorteilen der schnellen Reaktion eines passiven Empfängers auf eingehende Kommunikation. Beispiele für solche Technologien sind HTTPS »Long Polling«.

2.7 Deutschland-Stack

In der 49. Sitzung des IT-Planungsrats¹ wurde als »Plattformkern« der zukünftigen deutschen Verwaltungsdigitalisierung der sogenannte Deutschland-Stack

¹ Nachzulesen unter: <https://www.it-planungsrat.de/beschluesse-informationen/sitzungen-it-planungsrat/49-sitzung> Abruf 29.07.2026

(D-Stack) beschlossen, wie folgendes Zitat aus einer Pressemitteilung zu der Sitzung verdeutlicht [2]:

»Der Deutschland-Stack wird federführend durch den Bund aufgebaut und bildet künftig den gemeinsamen Plattformkern der Verwaltungsdigitalisierung. Der IT-Planungsrat verpflichtet sich auf die portfolio-orientierte, schrittweise Entwicklung und setzt dabei klare Prioritäten auf zentrale Basiskomponenten sowie zentrale Lösungen für Identität, Datenaustausch, Datenabruf, Zahlungsabwicklung und Kommunikation. Bund, Länder und Kommunen werden Lösungen, die im Rahmen des Deutschland-Stacks entwickelt werden, bei Neu- und Weiterentwicklungen konsequent nutzen.«

Laut der Portfolio-Beschreibung des Deutschland-Stacks umfassen die oben genannten Basisdienste derzeit die folgenden konkreten Projekte oder Produkte [3]:

- Identität & Vertrauen: eID, EUDI-Wallet
- Postfach: ZaPuK
- Datenaustausch: FIT-Connect
- Datenabruf: NOOTS
- Zahlungsabwicklung: ZBDS (ePayBL inkludierend)

Der Fokus dieser Studie ist auf Technologien gerichtet, die Abruf und Transport von Daten in den zuvor beschriebenen Kommunikationsmodellen ermöglichen. In den Komponenten des D-Stacks sind damit insbesondere die Projekte beziehungsweise Produkte ZaPuK, FIT-Connect und NOOTS von Interesse.

3 Technische Grundlagen des Nachrichtenaustauschs

Die in dieser Studie betrachteten Kommunikationstechnologien sind aus technischer Sicht aus verschiedenen Basistechnologien auf mehreren Ebenen aufgebaut. Zur Realisierung der zuvor beschriebenen Kommunikationsszenarien sind unter anderem folgende Bausteine notwendig:

Datenformate bestimmen die innere Struktur einer Nachricht. Sie legen fest, welche Arten von Daten, etwa Texte, Bilder oder Dateianhänge, darin enthalten sein können. Zudem beeinflussen sie die Maschinenlesbarkeit der ausgetauschten Nachrichten.

Schnittstellenstandards definieren, wie die Systeme der Kommunikationsinfrastruktur miteinander interagieren. Sie beschreiben die angebotenen Funktionen und geben vor, wie eine Nachricht verpackt werden soll. Darüber hinaus regeln sie, welche Metadaten zusätzlich zu den eigentlichen Inhalten übertragen werden und wie empfangende Nachrichten zu verarbeiten sind.

Transportprotokolle sind für die eigentliche Übertragung der Daten verantwortlich. Sie sorgen dafür, dass die gesendeten Daten vollständig und fehlerfrei beim gewünschten Zielsystem ankommen.

Sicherheitsprotokolle werden genutzt, um die Authentizität, Vertraulichkeit und Integrität der übertragenen Informationen sicherzustellen. Sie regeln die Verwendung von Verschlüsselung und digitalen Signaturen sowie die Verwaltung der notwendigen Schlüssel.

Eine *Kommunikationstechnologie* umfasst die Auswahl, Kombination, Anpassung und Erweiterung dieser und weiterer Basistechnologien. Dieselben Basistechnologien können in verschiedenen Kommunikationstechnologien auf unterschiedliche Weise eingesetzt werden und somit zur Realisierung diverser Kommunikationsszenarien geeignet sein.

3.1 Datenformate

Datenformate bestimmen die innere Struktur einer Nachricht. Sie legen fest, in welchem Format die Informationen in eine Nachricht verpackt werden. Das Format muss in der Kommunikation bekannt sein und von beiden Seiten unterstützt werden. Damit ist die Auswahl eines geeigneten Datenformats bereits ein erster Faktor bei der Interoperabilität verschiedener Lösungen.

Prinzipiell kann zwischen strukturierten und unstrukturierten Datenformaten unterschieden werden. Die Wahl des Datenformats beeinflusst die Menge der zu übertragenden Zusatzdaten (Overhead) und die Möglichkeit, Zusatzinformationen (Metadaten) zu übertragen, sowie die Maschinenlesbarkeit und Möglichkeit zur automatisierten Verarbeitung einer Nachricht. Bei der folgenden Betrachtung von Datenformaten beschränkt sich die Darstellung auf das Format der Inhaltsdaten (Payload) einer Nachricht, unabhängig vom Format der Übertragungstechnologie.

3.1.1 Strukturierte Formate

Strukturierte Datenformate geben eine feste Struktur für Nachrichten vor. Die in der Nachricht enthaltenen Informationen werden in der Regel auf verschiedene Attribute aufgeteilt, ähnlich wie bei einem Formular. Der primäre Vorteil dabei ist, dass die Struktur der Nachricht einem erwarteten Muster folgt. Es kann definiert werden, welche Arten von Daten in einer Nachricht enthalten sein dürfen und müssen. Die Validität der Daten, zum Beispiel die Angabe eines Datums im korrekten Format, kann automatisch geprüft werden. Benötigte Informationen können einfach über das jeweilige Attribut aus der Nachricht extrahiert werden. Zur Strukturierung der Daten müssen jedoch zusätzliche Informationen übertragen werden und das vorgegebene Format schränkt die Flexibilität der Nachricht ein.

3.1.2 Streaming Formate

Streaming-Formate dienen der Übertragung von Audio- oder Video-Datenströmen.

Bei *interaktiven Anwendungen* zeichnen sich diese Datenströme durch Echtzeitanforderungen aus und erfordern eine kontinuierliche Übermittlung mit gleichmäßiger Übertragungsrate, um die Ton- und Videoqualität zu gewährleisten. Andererseits bieten solche Anwendungen Spielräume, die Datenqualität an die verfügbare, mitunter schwankende Bandbreite des Übertragungskanals anzupassen. So kann etwa die Bild- oder Tonqualität reduziert werden, um eine Übermittlung des Datenstroms in Echtzeit zu gewährleisten. Es können beispielsweise auch einzelne Bildframes ausgelassen werden, um insgesamt eine ausreichende Übertragungsqualität zu erzielen. In solchen Anwendungsszenarien muss das Protokoll nicht verlustfrei sein, sondern die Echtzeitfähigkeit hat hier oft Vorrang.

Bei *Anwendungen ohne interaktiven User*, wie beispielsweise der Übertragung von Archivmaterial von Maschine-zu-Maschine, erwartet man in der Regel hingegen verlustfreies Streaming ohne Abstriche an der Datenqualität. Hier muss das Streaming-Format eine unverfälschte Datenübertragung garantieren.

3.2 Schnittstellenstandards

Die folgenden Schnittstellenstandards kommen bei den im Rahmen dieser Studie untersuchten Nachrichtentransporttechnologien zum Einsatz.

3.2.1 REST

REST steht für »Representational State Transfer« und ist ein Architekturstil für Web-Schnittstellen (APIs), der festlegt, wie Systeme über ein IP-basiertes Netzwerk miteinander kommunizieren. REST wurde von Roy Fielding ausgearbeitet und in seiner Dissertation im Jahr 2000 veröffentlicht [4]. Es handelt sich dabei nicht um ein fest definiertes Protokoll wie SOAP, sondern um eine Menge von Designprinzipien, die auf bestehenden Standards wie HTTP aufbauen.

Im Zentrum von REST stehen Ressourcen, die jeweils über eine eindeutige URI adressiert werden. REST baut im Wesentlichen auf bestehenden Web-Standards auf: HTTP(S) als Protokoll, URI/URL zur Adressierung, Medien-/MIME-Typen wie JSON oder XML zur Repräsentation der Daten sowie HTTP-Statuscodes zur Rückmeldung von Ergebnissen. RESTful Services sind idealerweise zustandslos: Jeder Request enthält alle notwendigen Informationen, damit der Server ihn ohne gespeicherten Sitzungszustand verarbeiten kann.

Die Interaktion mit Ressourcen erfolgt über HTTP-Verben, die unterschiedliche Aktionen ausdrücken: GET liest eine Ressource, POST legt eine neue Ressource an oder löst eine serverseitige Aktion aus, PUT ersetzt eine Ressource vollständig, PATCH ändert eine Ressource teilweise und DELETE entfernt eine Ressource.

3.2.2 SOAP

SOAP (ursprünglich als Akronym für *Simple Object Access Protocol* benutzt, heute als Eigenname) ist ein Netzwerkprotokoll, um Daten zwischen Systemen auszutauschen oder *Remote Procedure Calls (RPC)* durchzuführen. SOAP ist ein industrieller Standard des World Wide Web Consortiums (W3C).

SOAP ist ein XML-basiertes Protokoll für den Nachrichtenaustausch zwischen verteilten Systemen. Es definiert eine standardisierte Nachrichtenstruktur (Envelope, Header, Body) und basiert typischerweise auf XML-Schemata (XSD) zur Beschreibung der Daten sowie häufig auf WSDL (Web Services Description Language) zur formalen Beschreibung der verfügbaren Webservice-Schnittstellen. Als Transport wird meist HTTP(S) eingesetzt, es können aber auch andere Protokolle wie SMTP verwendet werden.

Unterschiedliche Operationen auf einem Webservice werden bei SOAP über im WSDL definierte Operationen realisiert, die jeweils eigene Request- und Response-Nachrichtenstrukturen besitzen. WSDL ist dabei eine XML-basierte

Beschreibungssprache, mit der Schnittstellen, Operationen, Datentypen und Endpunkte eines Webservices maschinenlesbar spezifiziert werden. Der gewünschte Dienstaufwurf wird durch die Kombination aus SOAP-Body-Inhalt und optionalen Metadaten wie dem *SOAPAction*-HTTP-Header eindeutig identifiziert.

Die SOAP-Spezifikation des W3C basiert zwingend auf XML [5].

3.2.3 XTA 2

XTA steht für »XML in der öffentlichen Verwaltung Transport Adapter« und ist ein nachrichtenbasierter Interoperabilitätsstandard der öffentlichen Verwaltung zur Vereinheitlichung der Schnittstelle zwischen Fachverfahren und Transportverfahren. Ziel von XTA 2 ist die Entkopplung von Fachanwendungen von den technischen Details der jeweils eingesetzten Transportverfahren. XTA 2 definiert dabei nicht das eigentliche Transportprotokoll, sondern die Funktionen und Datenstrukturen für die Übergabe von Nachrichten zwischen Anwendungsebene und Transportebene.

Der Standard definiert die Schnittstellen zwischen Anwendungs- und Transportebene für XML-basierte Nachrichtenstrukturen als Webservices, die in der Referenzspezifikation mittels SOAP und WSDL beschrieben werden. Die auszutauschenden Informationen werden in standardisierten Transportnachrichten gekapselt, die Transportmetadaten sowie die eigentliche Fachnachricht enthalten. Zusätzlich definiert XTA 2 sogenannte Service Profile, mit denen Anforderungen an Datenschutz, Informationssicherheit, Kryptografie, Protokollierung und weitere Transportqualitäten maschinenlesbar beschrieben werden können. Für die eigentliche Übertragung können beliebige Transportverfahren wie OSCl-Transport oder andere sichere Kommunikationsinfrastrukturen genutzt werden.

Die Semantik der XTA-2-Schnittstellen orientiert sich an den Aufgaben des Nachrichtentransports. Zentrale Funktionen sind die Erzeugung eindeutiger Nachrichtenkennungen, die Prüfung der Verfügbarkeit eines Kommunikationspartners, die Ermittlung von Erreichbarkeitsinformationen, der synchrone oder asynchrone Versand von Nachrichten sowie die Zustellung eingegangener Fachnachrichten an das empfangende Fachverfahren. Ergänzend können Statusinformationen, Transportberichte, Quittungen und Ereignisprotokolle abgerufen werden. Die Schnittstellen beschreiben damit nicht fachliche Operationen, sondern standardisierte Transportaufträge und Transportereignisse, die unabhängig vom Inhalt der eigentlichen Fachnachricht verarbeitet werden.

XTA 2 wird in Abschnitt 4.3 ausführlicher betrachtet.

3.3 SOAP versus REST

SOAP wird gerade im Vergleich mit REST oft als »veraltet« bezeichnet. Im Folgenden wollen wir daher einen Vergleich von REST und SOAP anstreben, bei der wir die technischen Eigenschaften, Unterschiede sowie die Vor- und Nachteile beider Ansätze darstellen. Dabei werden wir auch auf die im Kontext REST und SOAP verwendeten gängigen Datenformate JSON und XML eingehen, die oft zur (standardisierten) Darstellung der kommunizierten Daten verwendet werden.

3.3.1 Interoperabilität

Während REST einen flexiblen Architekturstil basierend auf Richtlinien beschreibt, ist SOAP ein strikt definiertes standardisiertes Protokoll. REST fokussiert auf Einfachheit und Schnelligkeit, SOAP auf Sicherheit, Zuverlässigkeit und formale Standards.

REST kann auch mit XML-Daten eingesetzt werden. Es gibt keinen technischen Zwang, JSON als Datenformat zu verwenden. Obwohl dies heute als De-facto-Standard für öffentliche APIs gilt, ist die REST-Architektur grundsätzlich *format-neutral* konzipiert. Das bedeutet, man kann jedes textbasierte Format (u. a. XML, aber auch CSV) nutzen, um Daten (z. B. in einem standardisierten Format) zu kommunizieren.

3.3.2 Vergleich von XML und JSON

Verglichen mit JSON zeichnet sich XML durch folgende Merkmale aus:

- XML bietet mittels XSD-Schemas ein im Vergleich zu JSON und JSON-Schema stärkeres Validierungsframework, beispielsweise mit Unterstützung von Identity Constraints, kontextsensitiver Validierung, dokumentenweiter referenzieller Integrität und einem reichhaltigeren Klassenmodell. Zu diesen Merkmalen finden sich keine gleichwertigen Entsprechungen in JSON-Schema [6].
- XML unterstützt komplexe Metadaten direkt in den Tags [7].
- XML ist »wortreicher« als JSON (größeres Dateivolumen) und das Parsen der Daten ist in der Regel langsamer als bei JSON [7].

3.3.3 Performanz und Effizienz von REST und SOAP

Zahlreiche wissenschaftliche Arbeiten vergleichen SOAP und REST (oft auch in Kombination mit den Datenformaten XML und JSON) systematisch hinsichtlich ihrer Performanz [8] [9] [10]. In diesen Studien werden meist Metriken wie Antwortzeit, Durchsatz, Bandbreitenverbrauch und Ressourcenbelastung (Rechenaufwand und Speicherbedarf) gemessen [8] [11] [12] [13].

In den genannten wissenschaftlichen Arbeiten ist man sich im Wesentlichen in folgenden Punkten einig:

- **Effizienzvorteil für REST:** In fast allen Benchmarks schneidet REST besser ab, da es weniger Overhead (Zusatzdaten) hat. Während SOAP jede Nachricht in einen komplexen XML-»Umschlag« (*Envelope*) verpacken muss, nutzt REST direkt die schlanken Strukturen von HTTP.
- **Datenmenge:** Untersuchungen zeigen, dass SOAP-Nachrichten signifikant größer sind als REST-Nachrichten. In einigen Tests war die Datenmenge bei REST-JSON nur etwa halb so groß wie bei einer funktionsgleichen SOAP-Anfrage.
- **Rechenaufwand:** Das Parsen von XML-Strukturen (die SOAP zwingend nutzt) ist rechenintensiver als das Verarbeiten von JSON. In Studien auf mobilen Geräten oder IoT-Sensoren führt dies bei REST zu einer spürbar längeren Akkulaufzeit und geringeren Latenzzeiten.
- **Stabilität versus Geschwindigkeit:** REST bietet zwar wesentliche Vorteile bei Geschwindigkeit und Skalierbarkeit gegenüber SOAP, allerdings weist eine aktuelle Studie aus dem Jahr 2024 [14] darauf hin, dass SOAP selbst in Netzwerkeumgebungen, in der die zugrunde liegende Infrastruktur Störungen aufweist, durch seine strengen Standards (wie *WS-Reliability* oder *WS-ReliableMessaging*) oft eine höhere Stabilität und Zuverlässigkeit beim Datentransfer bietet. Unter *Stabilität* eines Kommunikationsprotokolls verstehen wir dabei die Eigenschaft, unter variierenden oder fehlerbehafteten Bedingungen einen definierten, deterministischen und sicheren Betriebszustand aufrechtzuerhalten.

3.3.4 Einsatz in der Behördenkommunikation

- **Eindeutigkeit durch Verträge (WSDL):** SOAP nutzt WSDL-Dateien. Dies ist ein maschinenlesbarer »Vertrag«, der exakt festlegt, wie Daten aussehen müssen. In Behörden verhindert dies Missverständnisse zwischen verschiedenen Abteilungen oder Registern.
- **Transaktionssicherheit:** SOAP unterstützt durch den Standard *WS-AtomicTransaction* komplexe Abläufe, bei denen entweder alle Schritte erfolgreich sein müssen oder keiner (Alles-oder-Nichts-Prinzip). Das ist essenziell für verbindliche Behördenvorgänge, wie Grundbucheinträge oder Steuerangelegenheiten.
- **Integrität und Verbindlichkeit (WS-Security):** Während REST meist auf die Verschlüsselung des Transportwegs (HTTPS) vertraut, bietet SOAP mit *WS-Security* Sicherheit auf Nachrichtenebene. Das bedeutet, ein Dokument bleibt auch nach dem Empfang digital signiert und damit rechtlich nachweisbar unverändert, selbst wenn es über mehrere Zwischenstationen (Proxies) geleitet

wurde. Das ist für Behörden entscheidend, da eine Nachricht so über mehrere Zwischenstationen (Hops) geleitet werden kann, ohne dass die digitale Signatur oder die Verschlüsselung des Inhalts verloren geht – im Gegensatz zu REST, das meist nur die Punkt-zu-Punkt-Verschlüsselung (von Hop zu Hop) via HTTPS nutzt. Weiterhin zeigt die Analyse in [15], wie SOAP-Protokolle garantieren können, dass Nachrichten genau einmal (*exactly-once*) ankommen und in der richtigen Reihenfolge verarbeitet werden. Das ist die technische Basis für Verbindlichkeit bei Behördenvorgängen.

- **Fehlerbehandlung:** SOAP hat standardisierte »Fault«-Strukturen. Wenn ein Fehler auftritt, erhält die Behörde eine präzise, protokollkonforme Fehlermeldung, was die Fehlersuche in kritischen Infrastrukturen erleichtert.

3.3.5 Fazit SOAP versus REST

Während REST aufgrund seiner Geschwindigkeit insbesondere für Bürgerportale und mobile Anwendungen geeignet ist, bleibt SOAP für den rechtssicheren Backend-Datenaustausch, wie beispielsweise zwischen Behördenregistern, oft die erste Wahl [16]. Die Studie kommt zu dem Ergebnis, dass SOAP trotz der Geschwindigkeitsvorteile von REST in Bereichen wie dem Finanz- und Regierungswesen weiterhin bevorzugt wird. Die Studie zeigt ferner, dass SOAP durch seine strikten Datenvalidierungen eine höhere Datenintegrität in kritischen Systemen gewährleistet. Des Weiteren wird in der Fallstudie geschlussfolgert, dass viele Organisationen hybride technologische Ansätze wählen, die die Zuverlässigkeit von SOAP mit der Flexibilität von REST kombinieren, um den gestellten Anforderungen gerecht zu werden.

3.4 Transport- und Nachrichtenprotokolle

Transport- und Nachrichtenprotokolle definieren die Regeln für den Austausch von Nachrichten. Aus klassischer Sicht des ISO/OSI-Modells [17] sind Transportprotokolle auf Layer 4 (Transport-Layer) einzuordnen. Im Rahmen dieser Studie werden jedoch primär Protokolle zur Übertragung von Anwendungsnachrichten auf Layer 5 bis 7 des Modells betrachtet. Dabei bauen alle betrachteten Protokolle für den Nachrichtenaustausch auf das Layer-4-Protokoll TCP auf, das eine verlässliche Übertragung von Datenströmen in der korrekten Reihenfolge garantiert. Die betrachteten Protokolle definieren darüber hinaus, wie Kommunikationskanäle aufgebaut und verwaltet werden, welche Arten von Nachrichten existieren, welche Inhaltsdaten übertragen werden können und viele weitere Aspekte der Kommunikation. Da die betrachteten Protokolle sich in ihrem Funktionsumfang stark unterscheiden, ist eine einheitliche Beschreibung beziehungsweise ein direkter Vergleich nicht möglich.

3.4.1 HTTP/S

Hypertext Transfer Protocol (HTTP) ist ein Anwendungsschichtprotokoll, das vor allem zur Übertragung von Hypermedia-Dokumenten wie HTML-Seiten sowie JSON- oder XML-Daten zwischen Client und Server verwendet wird. Es nutzt typischerweise das Transmission Control Protocol (TCP) und ist zustandslos, das heißt, jede Anfrage wird unabhängig von vorherigen behandelt.

Hypertext Transfer Protocol Secure (HTTPS) ist die durch Transport Layer Security (TLS) abgesicherte Variante von HTTP und gewährleistet zusätzlich Vertraulichkeit, Integrität und Authentizität der Verbindung. In modernen Fachanwendungen und APIs ist HTTPS praktisch verpflichtend, insbesondere bei der Verarbeitung sensibler oder personenbezogener Daten. HTTP/HTTPS bildet die technische Grundlage vieler darüberliegender Protokolle und Standards.

HTTP folgt einem klassischen Client-Server-Modell. Ein Client stellt eine Verbindung her, sendet eine Anfrage und wartet auf die Antwort des Servers.

Das Protokoll ist erweiterbar und kann durch zusätzliche Header, Methoden und Erweiterungen an neue Anforderungen angepasst werden.

3.4.2 AS2

Applicability Statement 2 (AS2) ist ein Übertragungsprotokoll für den sicheren Austausch von Dateien und strukturierten Geschäftsdokumenten (EDI-Nachrichten, *Electronic Data Interchange*) über HTTP oder HTTPS. Es ermöglicht eine Punkt-zu-Punkt-Verbindung zwischen Geschäftspartnern und bietet Funktionen wie digitale Signatur, Verschlüsselung und elektronische Zustellbestätigung.

Der Nachrichtenaustausch erfolgt über das Internet. AS2 nutzt HTTP als Transportprotokoll, erweitert dieses jedoch um starke Verschlüsselung und digitale Signaturen. Die Nachrichten werden in einen »digitalen Briefumschlag« verpackt, signiert und anschließend verschlüsselt übertragen. Durch die Signatur kann der Empfänger die Authentizität des Absenders prüfen und die Integrität sicherstellen, also feststellen, ob die Nachricht unverändert geblieben ist. Die Verschlüsselung schützt die Inhalte vor unbefugtem Zugriff.

Als Empfangsbestätigung erhält der Absender eine MDN (Message Disposition Notification). Diese dient als elektronische Empfangsquittung und dokumentiert, dass die Nachricht beim Empfänger eingegangen und verarbeitet wurde. Der Einsatz von AS2 erfordert jedoch ein entsprechendes Management von Partnerbeziehungen, Firewalls und Zertifikaten.

In der Praxis wird AS2 vor allem dort eingesetzt, wo bereits viele Partner angebunden sind oder bestehende EDI-Infrastrukturen darauf aufbauen. Dadurch ist AS2 insbesondere im B2B-Umfeld weit verbreitet, etwa im Handel oder in der Industrie.

3.4.3 Matrix

Matrix ist ein offener Standard, der ein Protokoll zur Kommunikation über eine dezentrale Infrastruktur definiert. Der Standard wird durch die Matrix.org-Foundation verwaltet und durch ein offenes internationales Ökosystem über einen kollaborativen Matrix-Spec-Change-Prozess gemeinsam weiterentwickelt. Im Kontext dieser Studie ist Matrix vor allem durch den Einsatz als technische Basis in ZaPuK relevant. Dieser Abschnitt gibt eine kurze Einführung in die technischen Grundlagen und die Architektur von Matrix, um die Erklärungen in Abschnitt 4.6 übersichtlicher zu gestalten.

Matrix baut eine dezentrale Kommunikationsinfrastruktur aus mehreren *Homeservern* auf. Jeder Endnutzer hat eine Adresse bei einem Homeserver, ähnlich wie bei E-Mail. Nachrichten können zwischen Nutzern desselben Homeservers direkt über den Server ausgetauscht werden. Homeserver können sich über die öffentliche *Föderation* mit anderen Homeservern vernetzen, sodass Nachrichten zwischen den Endnutzern dieser Homeserver ausgetauscht werden können. Server können dabei frei entscheiden, mit welchen Homeservern sie föderieren. So können verschiedene Netzwerke von Homeservern aufgebaut werden; auch ein völlig privater Homeserver ist realisierbar, der nur die Kommunikation zwischen seinen lokal registrierten Nutzern ermöglicht.

Matrix organisiert Nachrichten in sogenannten *Räumen*. Ein Raum kann aus beliebig vielen Teilnehmern bestehen. *Raum-Events* beschreiben und verändern den Status des Raums, zum Beispiel den Beitritt und Austritt von Mitgliedern, die Verschlüsselungseinstellungen oder Berechtigungsvergaben, Nachrichten in den Raum zu senden. Nachrichten, die Teilnehmer versenden, sind ebenfalls Raum-Events. Alle Events eines Raums werden durch den Homeserver in einer Historie verwaltet. Bei der Kommunikation über verschiedene Homeserver synchronisieren die Server den Raumstatus untereinander und verwalten je eine lokale Kopie.

Die Übertragung von Events und Nachrichten erfolgt via HTTPS über REST-Schnittstellen. Es gibt verschiedene Schnittstellen für den Austausch zwischen Client und Homeserver, zwischen Homeservern untereinander oder zwischen Servern und externen Anwendungen. Die Kommunikation ist immer über TLS abgesichert. Zur Authentifizierung der Verbindung wird jeweils das Zertifikat des Zielservers verwendet. Der Client authentifiziert sich auf Anwendungsebene über ein Token.

Bei den übertragenen Daten handelt es sich immer um Events im JSON-Format. Es gibt verschiedene Eventtypen, um Aktivitäten im Raum, Statusnachrichten oder Fehlermeldungen zu übertragen. Die Nachrichten der Nutzer sind Events eines Nachrichtentyps. Es gibt verschiedene Nachrichtentypen, wie Textnachrichten, Bilder, Dateianhänge oder Emojis. Der Matrix-Standard ermöglicht die Spezifikation individueller neuer Event- und Nachrichtentypen für alle Implementierungen. Der Standard selbst garantiert dabei die Interoperabilität, da Server jegliche JSON-Daten transportieren können, auch wenn der Event- oder Nachrichtentyp unbekannt ist. Die korrekte Interpretation und Darstellung der Daten obliegen dem Client des Endnutzers.

Die Identitätsverwaltung und Anmeldung bei Matrix übernimmt der jeweilige Homeserver. Endnutzer können lokale Accounts bei ihrem Homeserver registrieren oder sich über einen externen Identitätsservice via OAuth 2.0 authentifizieren. Innerhalb der Kommunikation identifiziert Matrix die Nutzer anhand ihrer Matrix-Adresse. Zur Bestätigung der Authentizität von Nachrichten verwaltet der Homeserver öffentliche Schlüssel.

Die Kommunikation in Matrix-Räumen kann durch die Protokolle Olm und Megolm Ende-zu-Ende-verschlüsselt werden. Dabei verschlüsselt der Client des Nutzens alle Nachrichten-Events. Der private Schlüssel zur Herstellung des Kommunikationskanals wird durch das Endgerät des Nutzens erstellt und verlässt dieses nie. Der Homeserver speichert für verschlüsselte Räume weiterhin die Raumhistorie, kann den Typ oder Inhalt der Nachrichten jedoch nicht einsehen.

Neben der Übertragung von JSON-Nachrichten via HTTP unterstützt Matrix außerdem das Streaming von Audio und Video in Echtzeit über webRTC, sodass auch Anrufe und Videoanrufe durch Matrix übertragen werden können.

3.4.4 OSCI

OSCI steht für *Online Services Computer Interface* und ist ein Kommunikationsprotokoll der öffentlichen Verwaltung für den Austausch elektronischer Nachrichten und Dokumente. Ziel von OSCI ist die Gewährleistung von Vertraulichkeit, Integrität, Authentizität und Nachweisbarkeit bei der elektronischen Kommunikation zwischen Behörden und Unternehmen. OSCI definiert dazu ein standardisiertes Nachrichtenformat einschließlich Vorgaben für die Verschlüsselung und die Protokollierung für den Transport von Daten über offene Netze.

Der Standard spezifiziert XML-basierte Nachrichtenstrukturen, die Fachdaten und transportbezogene Informationen in einer OSCI-Nachricht zusammenfassen. Für die Übertragung werden in der Regel Webservice-Technologien auf Basis von HTTPS und SOAP eingesetzt. Zentrale Bestandteile des Standards sind Mechanismen zur Verschlüsselung, elektronischen Signatur, Zeitstempelung sowie zur Erstellung von Transport- und Zustellnachweisen. OSCI verwendet hierzu das 4-

Corner-Modell, bei dem Nachrichten über einen Vermittler (OSCI-Intermediär) geleitet werden, der Transportfunktionen übernimmt, ohne auf die geschützten Fachinhalte zugreifen zu können.

Die Semantik der OSCI-Nachrichten orientiert sich an den Anforderungen eines rechtssicheren elektronischen Nachrichtenverkehrs. Dazu unterstützt der OSCI-Standard verschiedene Modi des Nachrichtenaustauschs: asynchron (Store-and-Forward) sowie synchron (Request/Response), wobei Nachrichten entweder vom Empfänger »aktiv« abgeholt (Polling) oder bei dauerhaft erreichbaren Endpunkten direkt zugestellt werden können (»passiver Empfänger«), siehe Abschnitt 2.6.6. Zentrale Funktionen umfassen die Einlieferung von Nachrichten beim Intermediär, die Weiterleitung an den Empfänger, die Abholung bereitgestellter Nachrichten sowie die Erstellung und Übermittlung von Quittungen, Empfangsbestätigungen und weiteren Nachweisen. Ergänzend definiert der Standard die Verwendung von Zertifikaten, Signaturen und Verschlüsselungsinformationen für die Absicherung des Nachrichtenaustauschs. Der Protokollstandard beschreibt damit keine fachlichen Geschäfts- und Verwaltungsprozesse, sondern standardisierte Abläufe des sicheren und nachvollziehbaren Nachrichtentransports, unabhängig vom Inhalt der übertragenen Fachnachricht.

OSCI wird in Abschnitt 4.2 näher beschrieben.

3.4.5 ebMS 3.0 / AS4

Der Standard ebXML Messaging Services (ebMS) [18] definiert ein speziell für B2B-Geschäftsprozesse entwickeltes Nachrichtenprotokoll, das vor allem für den geschäftlichen Nachrichtenaustausch eingesetzt wird und synchrone, asynchrone sowie quasi-synchrone Kommunikation unterstützt. Das Protokoll unterstützt digitale Signaturen, Zeitstempel und die Korrelation von Nachrichten. Auf europäischer Ebene soll im Once-Only Technical System (EU-OOTS) ebMS 3.0 mit einer eDelivery-AS4-Profilierung eingesetzt werden. Ein Vorteil von ebMS ist die Möglichkeit zur Weiterleitung von Nachrichten, da Routing-Informationen in der Nachricht sichtbar sind.

Abschnitt 4.8 geht näher auf eDelivery AS4 ein.

3.5 Verschlüsselungs- und Sicherheitsprotokolle

Transport Layer Security (TLS) bildet die Basis der Verschlüsselung von Nachrichten bei der Übertragung zwischen zwei Kommunikationsteilnehmern. TLS wird in verschiedenen Transportprotokollen wie HTTPS und SMTPS (E-Mail) verwendet. Viele der betrachteten Technologien (OSCI, Matrix, FIT-Connect, NOOTS) verwenden TLS beziehungsweise HTTPS zur verschlüsselten Übertragung von Nachrichten zwischen jeweils zwei »Zwischenstopps« in der Kommunikation. TLS

basiert auf einem Handshake-Verfahren, bei dem der Client und Server sich über die zu verwendenden Algorithmen austauschen und Schlüssel aushandeln. Der Handshake ist notwendig, um sich bei jedem Nachrichtenaustausch auf neue, exklusive Schlüssel zu einigen. Die Authentifizierung der Kommunikationspartner erfolgt bei TLS in der Regel über Zertifikate, die einen öffentlichen Schlüssel an einen Namen binden und von einer vertrauenswürdigen Stelle signiert sind. In der Regel wird nur der Server über ein Zertifikat authentifiziert. In Kommunikationsszenarien, in denen auch die Identität des Clients geprüft werden muss, beispielsweise zur Prüfung von Berechtigungen, kann mTLS (Mutual TLS) verwendet werden. In dieser Version präsentiert auch der Client ein Zertifikat, das durch den Server geprüft werden kann. Zur Verbesserung der Interoperabilität und Sicherstellung von Kryptoagilität können in TLS mehrere verschiedene *Cipher-Suites*, d. h. Kombinationen aus Schlüsselaustausch-, Verschlüsselungs-, und Signaturalgorithmen verwendet werden. Server können entscheiden, welche Cipher-Suites sie anbieten und handeln die Verwendung einer bestimmten Suite im Handshake mit dem Client aus.

Durch den Handshake ist TLS ein synchrones, 2-Corner-Protokoll. Daher kann die *Transportverschlüsselung* mit TLS in 3- und 4-Corner-Modellen nicht die Kommunikation zwischen den Rollen Autor und Leser absichern. Die Nachrichtenübertragung erfolgt zunächst zwischen Autor und einer vermittelnden Stelle. Im Routing der Nachricht können weitere Zwischenstopps eingelegt werden. Jede dieser Übertragungen kann durch eine individuelle TLS-Session verschlüsselt werden. Zur Wahrung der Vertraulichkeit der Nachricht zwischen Autor und Leser bieten viele Technologien neben der Transportverschlüsselung auch eine Möglichkeit zur *Inhaltsdatenverschlüsselung*. Dabei bedienen sich unterschiedliche Technologien an verschiedenen Verschlüsselungs- und Sicherheitsprotokollen.

3.5.1 S/MIME

S/MIME wird primär für die Verschlüsselung und Signatur von E-Mails verwendet. Dabei werden Schlüssel aus X.509-Zertifikaten zur Authentifizierung der Kommunikationspartner und Signatur der Nachrichten genutzt. Die Zertifikate werden über eine Public-Key-Infrastruktur (PKI) validiert.

3.5.2 PGP

Pretty Good Privacy (PGP) wird ebenfalls primär zur Verschlüsselung und Signatur von E-Mails verwendet. Ähnlich wie *S/MIME* basiert die Prüfung der Authentizität und Integrität der Nachrichten auf Public-Key Kryptografie, wobei jedoch die benötigten Schlüssel bei PGP nicht über eine PKI, sondern über Keyserver in einem dezentralen Web of Trust bezogen werden.

3.5.3 XML-Encryption

XML-Encryption ermöglicht die Verschlüsselung von kompletten XML-Dokumenten oder einzelnen, sensiblen Elementen. Der Standard wird vom W3C verwaltet und definiert dabei, wie die verschlüsselten Inhalte in das Dokument eingebunden werden und wie Informationen über die genutzten Verschlüsselungsverfahren und Schlüssel ausgetauscht werden. Prinzipiell können dabei verschiedene symmetrische, asymmetrische und hybride Verfahren genutzt werden. In der Regel wird ein symmetrischer Schlüssel zur Verschlüsselung der Inhaltsdaten genutzt, mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und als Teil der Nachricht übertragen. XML-Encryption findet insbesondere im Kontext von Webservices und SOAP-Verwendung.

3.5.4 JSON Web Encryption

JSON Web Encryption (JWE) ist ein Standard der IETF und ermöglicht die Verschlüsselung von Nachrichten im JSON-Format. Der Standard definiert Header zur Übertragung der Informationen über das verwendete Verschlüsselungsverfahren, den genutzten Schlüssel und eines Authentication-Tags zur Sicherung der Integrität der Nachricht. Auch in JWE können dabei verschiedenen symmetrische Verfahren zur Verschlüsselung der Inhaltsdaten und verschiedene Verfahren zum Schutz des Schlüssels bei der Übertragung genutzt werden. Anders als XML-Encryption bietet JWE auch die Möglichkeit einen Schlüssel über ECDH-ES gemeinsam zu berechnen. JWE wird üblicherweise bei REST-APIs unterstützt.

3.5.5 Olm und Megolm

Olm und *Megolm* sind Verschlüsselungsverfahren, die auf dem Double-Ratchet-Mechanismus des Signal Protokolls basieren. Das Signal Protokoll ermöglicht die Ende-zu-Ende verschlüsselte Echtzeitkommunikation und wird in Messengern wie Signal und WhatsApp verwendet. Es basiert auf einem Double-Ratchet-Algorithmus, der die Schlüsselgenerierung und den Schlüsselaustausch zwischen Kommunikationspartnern synchronisiert. Es bietet starke kryptografische Garantien wie Post-Compromise Security, da für jede Nachricht neue Schlüssel verwendet werden. Olm und Megolm werden für die Ende-zu-Ende Verschlüsselung im Matrix Standard genutzt, wobei Olm für die direkte Kommunikation zwischen zwei Teilnehmern und Megolm für die Kommunikation in Gruppen genutzt wird.

3.5.6 Message Layer Security (MLS)

Message Layer Security (MLS) ist ein Standard der IETF, der ein Protokoll zur Ende-zu-Ende-Verschlüsselung von Nachrichten in großen Gruppen definiert. Es verwendet eine Baumstruktur zur Schlüsselverwaltung, wodurch Mitglieder effizienter zu Gruppen hinzugefügt und entfernt werden können als bei Megolm. Das Verfahren bietet starke kryptografische Garantien, wie Post-Compromise

Security und Perfect Forward-Secrecy. Die Implementierung des Verfahrens in Matrix wird aktuell angestrebt.

4 Transportarchitekturen und -standards

Dieses Kapitel widmet sich der Beschreibung der Kommunikationstechnologien, die in der vergleichenden Bewertung im Fokus dieser Studie liegen. Zweck dieses Kapitels ist es, die Leserschaft mit den Eigenschaften der Technologien vertraut zu machen, um die folgenden Bewertungen einordnen zu können.

4.1 Analyisierte Technologien

Dieser Abschnitt beschreibt die Auswahl der im Rahmen dieser Studie näher betrachteten Kommunikationstechnologien und die Struktur der Analysen.

4.1.1 Betrachtungsgegenstände

Um die Studie im Umfang beherrschbar zu halten, wurden die Betrachtungsgegenstände in enger Abstimmung mit der Auftraggeberin auf folgende Technologien mit den jeweiligen Begründungen festgelegt:

- **OSCI / XTA** ist ein verbreiteter Kommunikationsstandard in vielfältigen Kommunikationsszenarien der öffentlichen Verwaltung, der damit unerlässlich für eine Betrachtung in dieser Studie ist.
- **FIT-Connect** ist Gegenstand der Analyse, da die Kommunikationsinfrastruktur ursprünglich der vereinfachten Anbindung von OZG-Leistungen diene und zudem in den Deutschland-Stack aufgenommen wurde.
- **NOOTS**, als Kommunikationsinfrastruktur der Registermodernisierung und Teil des Deutschland-Stacks, ist ebenfalls unerlässlicher Betrachtungsgegenstand.
- **ZaPuK** ist die Zielarchitektur für Postfach- und Kommunikationslösungen (ZaPuK) im Deutschland-Stack und damit ebenfalls Gegenstand der Analyse.
- **X-Road** ist eine Datenaustauscharchitektur, die national (z. B. in Schleswig-Holstein) und international im G2G- und B2G-Kontext im Einsatz ist und in Europa häufig als mögliche Zukunftsarchitektur diskutiert wird.
- **eDelivery AS4** ist ein Nachrichtenprotokoll, das national und international domänenübergreifend sehr verbreitet ist und insbesondere auf europäischer Anschlussebene Anwendung findet.

4.1.2 Getrennte Betrachtung von OSCI und XTA 2

Insbesondere die Befürwortenden von OSCI oder XTA 2 haben sich in den Interviews überwiegend für eine getrennte Betrachtung der beiden Technologien OSCI und XTA 2 in der Studie ausgesprochen.

Gründe, die in den Interviews dafür genannt wurden, waren:

- Interviewte, die OSCI – aber nicht XTA 2 – einsetzen oder für die Standards in einer Fachdomäne zuständig sind, argumentierten, dass Vor- und Nachteile von OSCI und XTA 2 nicht in der Analyse miteinander vermischt werden sollten. In Interviews wurde von Teilnehmenden bestätigt, dass es ganze Anwendungsfelder von OSCI-Nachrichtentransporten (z. B. in der Justiz) gebe, in denen XTA 2 keine oder kaum eine Rolle spiele.
- XTA 2 sei eine Technologie, die vom eingesetzten Nachrichtenprotokoll abstrahiere. Sie sei also potenziell mit einer Vielzahl verschiedener Protokolle einsetzbar. Es wurde auf ein Beispiel verwiesen, in dem XTA 2 zur Anbindung an Peppol/AS4 statt an OSCI eingesetzt wird. Auch Informationsseiten der FITKO enthalten dieses Argument [19].

Gründe, die aus Sicht des Autorenteam gegen eine getrennte Betrachtung sprechen, sind:

- Die XTA-2-Spezifikation in der Version 3.1.1 erläutert in einem einleitenden Kapitel im Abschnitt 1.1.2.4 [20] ausführlich, dass XTA 2 den OSCI-Standard ergänzt.
- Die XTA-2-Spezifikation in ihrer neuesten Version 5.1.1 enthält diese Bemerkung nicht mehr, gibt aber in der technischen Spezifikation keinen Hinweis darauf, dass ein anderes Nachrichtenprotokoll als OSCI vorgesehen ist, siehe Näheres dazu in Abschnitt 4.3.1.3.
- Auf den Webseiten der zuständigen Koordinierungsstelle für IT-Standards (KoSIT) werden die beiden Standards zusammen aufgeführt. In den Erklärungen auf dieser Webseite findet sich keine relevante Erwähnung des potenziellen Einsatzes von XTA 2 mit anderen Nachrichtenprotokollen [21].
- Außer dem Beispiel mit dem Nachrichtenstandard Peppol/AS4 in der spezialisierten Edition eines Softwareprodukts der Firma Governikus [22] sind keine weiteren Beispiele für den Einsatz von XTA 2 mit anderen Nachrichtenprotokollen offensichtlich auffindbar.

Ergebnis der Abwägung:

Nach Abwägung der genannten Argumente entschied sich das Autorenteam für eine getrennte Analyse von OSCI und XTA 2. Insbesondere der – laut Mitgliedern der Arbeitsgruppe »IT-Standards in der Justiz« der Bund-Länder-Kommission

(BLK) – quasi exklusive Einsatz von OSCI ohne XTA 2 im Justizbereich und die Eigenschaften der technischen Umsetzung von XTA-2-Kommunikation in OSCI-Nachrichten (siehe auch Abschnitt 4.3.2) waren für diese Entscheidung des Autorenteam ausschlaggebend.

4.1.3 Struktur der Analysen

Eine Schwierigkeit in der Erstellung der Studie bestand darin, dass die aufgezählten Technologien zwar im Kern dasselbe Ziel verfolgen: den sicheren Transport von Informationen entsprechend den drei Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit [23]. Darüber hinaus spielen bei den betrachteten Technologien jedoch teilweise sehr unterschiedliche Aspekte eine Rolle:

- Manche der betrachteten Technologien (z. B. OSCI / XTA) sind gezielt sehr generisch ausgelegt, um möglichst viele Szenarien abdecken zu können. Andere wiederum wurden für begrenzte Zwecke und Herausforderungen entworfen.
- Einige der betrachteten Technologien entfalten bestimmte Stärken in Szenarien, die außerhalb des Studienfokus liegen. Hier ist insbesondere Matrix zu nennen, welches eine Reihe von Eigenschaften bereitstellt, die im G2C-Kontext wichtig sind, jedoch in geringerem Maße für B2G- oder G2G-Szenarien.
- Die aufgeführten Technologien sind sehr divers, was ihren *Typ* angeht. OSCI, XTA 2 und AS4 sind Standards – aber teilweise auf unterschiedlichen Ebenen des Datentransports. Für sich geben sie jedoch wenig Auskunft über die physische Infrastruktur, die notwendig ist, um Daten mittels dieser Standards auszutauschen. FIT-Connect, NOOTS, Matrix und X-Road haben jeweils Merkmale einer Architektur oder Plattform, während Matrix dazu auch ein Nachrichtenprotokoll definiert. ZaPuK ist hingegen »nur« eine »Zielarchitektur« und beschreibt damit lediglich Anforderungen an eine konkrete Architektur.
- Die betrachteten Technologien besitzen sehr unterschiedliche Reifegrade: Während OSCI seit Jahren im bewährten Praxiseinsatz ist, existieren von anderen Technologien nur erste Versionen, eventuell Prototypen – und ZaPuK wird sogar erst nach Beendigung der vorliegenden Studie als Architekturvorgabe finalisiert.

Um der Leserschaft eine möglichst gute Vergleichbarkeit zu ermöglichen, wird im Folgenden stets auf die Anwendungsbereiche und das Kommunikationsmodell einer betrachteten Technologie eingegangen. Anschließend werden jeweils die im Kontext der Technologie eingesetzten Kommunikations- und Schnittstellenstandards erörtert, danach gegebenenfalls existierende Implementierungen und Infrastrukturen oder deren Anforderungen. Da sich die IT-Sicherheit aus der Gesamtheit von Standards, Implementierungen und Infrastrukturen ergibt, wird dieses Thema jeweils zum Ende eines Technologiekapitels behandelt.

Da es ein expliziter Wunsch der Auftraggeberin war, auch Technologien in die vergleichende Betrachtung einzubeziehen, die derzeit noch nicht im großflächigen Einsatz oder auch nur final definiert sind, erforderte dies in vielen Fällen die Analyse von Konzepten anstelle existierender Software- oder Infrastruktur-Dokumentation. Sofern diese Konzepte vorlagen, hat das Autorenteam diese evaluiert. Reine Absichtserklärungen ohne vorliegendes Konzept wurden jedoch von einer Betrachtung ausgeklammert, um einen fairen Vergleich zu ermöglichen.

4.2 OSCI

Im Folgenden wird das Protokoll *OSCI* (Online Services Computer Interface) erläutert. Der Fokus liegt dabei auf der Vorstellung der Kernkonzepte und gegebenenfalls identifizierten Problemstellungen, die im Rahmen von Interviews und Spezifikationsanalyse festgestellt wurden.

4.2.1 Anwendungsbereich

Bei OSCI-Transport² handelt es sich um einen Standard zum inhaltsagnostischen Austausch von Nachrichten [24, S. 11]. Der Austausch dieser Nachrichten folgt dem Konzept von Aufträgen und Auftragsantworten, wobei es sich bei der Auftragsantwort auch um eine Fehlermeldung handeln kann [24, S. 13].

4.2.2 Kommunikationsmodell

4.2.2.1 Teilnehmer

Die OSCI-Spezifikation unterscheidet bei einer Kommunikation zwischen unterschiedlichen logischen Betrachtungsebenen (dargestellt in Abbildung 3). Es handelt sich hierbei um die *Geschäftsvorfallenebene* (Autor, Leser), *Auftragsebene* und eine *Nachrichtenebene* (Sender, Empfänger). OSCI orientiert sich hierbei grundsätzlich an dem in Abschnitt 2.1 vorgestellten 4-Corner-Modell. Die Wegstrecke von Autor zu Sender, bei der die Systemgrenze zu OSCI überschritten wird, definiert die Spezifikation an dieser Stelle nicht [24, S. 12–13].

4.2.2.2 Intermediär

Innerhalb der *Auftragsebene* (dargestellt in Abbildung 3) treten die OSCI-spezifischen Rollen eines *Clients* und *Suppliers* in Erscheinung. Client und Supplier sind dabei als Endpunkte der Zwischenkommunikation vom *Sender* zu *Intermediär* und *Intermediär* zum *Empfänger* zu betrachten. Beim Intermediär handelt es sich um eine dritte Instanz, die als vermittelnder Knoten der Kommunikation zwischen Sender und Empfänger dient. Sender und Empfänger tauschen

² vorliegend in Version 1.2 mit Korrigenda 1 bis 10 und Erweiterung zur Verwaltung großer Datenmengen [44], nachfolgend nur »OSCI« genannt

Nachrichten über OSCI nie direkt aus, sondern nutzen einen Intermediär [24, S. 12–13].

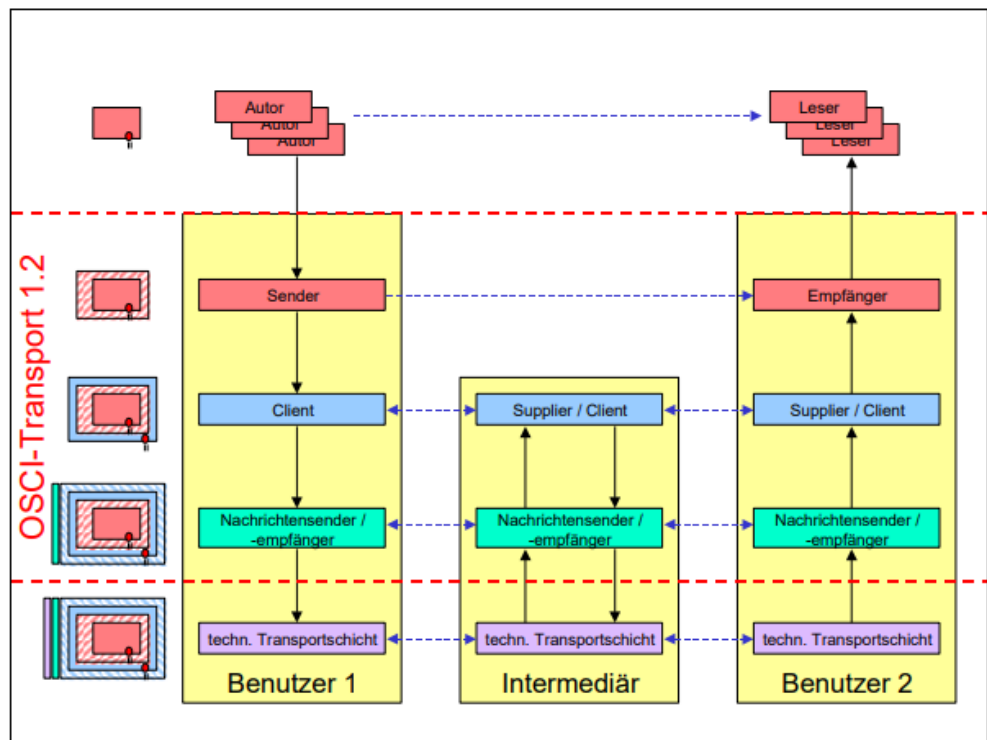


Abbildung 3

Darstellung der Kommunikationsebenen durch die OSCI-Spezifikation [24]

Der Intermediär übernimmt auch Aufgaben abseits des reinen Nachrichtentransports, etwa in Form von Protokollierung oder Zertifikatsüberprüfung sowie so genannter »Mehrwertdienste« [24, S. 11]. Was die Spezifikation unter dem Begriff Mehrwertdienst vorsieht, bleibt unspezifiziert. Zusätzlich werden an den Intermediär eine Reihe von Anforderungen gestellt, die über die Rolle eines Vermittlers im Sinne einer Übertragung hinausgehen, etwa in Form von Schemaprüfungen und inhaltlichen Validierungen [24, S. 37].

Innerhalb des OSCI-Spezifikationsdokuments wird eine Verzahnung mit XTA, insbesondere im Hinblick auf das in Kombination von XTA und OSCI auf der Website vorgestellte 4-Corner-Modell [25], nicht behandelt. Implizit muss hier der Bedarf weiterer Technologien und Infrastruktur angenommen werden, insbesondere im Hinblick auf XTA, dessen Rolle sich erst durch Begutachtung getrennter Dokumentation ergibt.

4.2.2.3 Dialog

Die Kommunikation zwischen Teilnehmern wird in OSCI in Auftrag-Antwort-Paaren betrachtet. Eine oder mehrere dieser Nachrichtenrundstrecken kann mittels eindeutiger Kennung zu einem *Dialog* zusammengefasst werden. Die OSCI-Spezifikation unterscheidet hierbei zwischen einer expliziten und impliziten Erzeugung eines Dialogs, der zum einen über einen Dialoginitialisierungsauftrag explizit oder durch einen anderen Auftrag implizit zustande kommt [24, S. 13].

Wird keine explizite Dialoginitialisierung durchgeführt, hat dies Auswirkungen auf den Kommunikationsablauf, etwa im Szenario einer One-Way-Message mit aktivem Empfänger durch den Bedarf zusätzlicher, sich wiederholender Zertifikatsprüfungen [24, S. 21]. Auf Basis der Spezifikation wird zwar erkennbar, dass die implizite Dialoginitialisierung bei Bedarf dynamisch für ein Auftrag-Antwort-paar genutzt werden kann [24, S. 13], was allerdings zu Lasten einer Implementierungskomplexität geht. Hierdurch wird den Implementierenden de facto die Umsetzung beider Dialoginitialisierungspfade vorgeschrieben, wenn auch Empfehlungen für eine explizite Dialoginitialisierung vorliegen [24, S. 22].

4.2.3 Kommunikationsstandards

OSCI baut zentral auf dem Konzept von SOAP auf [24, S. 8]. Daher wird der OSCI-Standard eng mit den XML-(Sub)-Standards, etwa für Signaturen und Verschlüsselung, verknüpft [24, S. 8].

Als Trägermedium für die Datenübertragung wird HTTP benannt [24, S. 38].

4.2.4 Schnittstellenstandard

OSCI definiert in erster Linie Nachrichtenformate, die hierbei in die Gruppen der Geschäftsvorfallenebene, Auftrags- und Nachrichtenebene untergliedert sind [24, S. 12].

Die *Geschäftsvorfallenebene* umfasst durch Autoren definierte, inhaltsagnostische Nachrichten, die dort als *Inhaltsdaten* beschrieben werden, wie diese Daten zustande kommen und zur Verfügung gestellt werden, wird dabei von der Spezifikation nicht definiert [24, S. 12].

Die zu übertragenden Daten werden im Sinne einer durch die Spezifikation definierten OSCI-Nachricht auf der *Nachrichtenebene* verortet [24, S. 13].

4.2.5 Implementierungen

Das Webangebot der Koordinierungsstelle für IT-Standards umfasst primär die Spezifikation von OSCI. Governikus selbst bietet auf der openCode-Plattform

eine quelloffene Java-Clientbibliothek an [26]. Eine .NET-basierte Edition der Clientbibliothek wurde zwar auf der Governikus-Website gelistet, deren öffentliche Verfügbarkeit konnte im Rahmen dieser Studie jedoch nicht verifiziert werden [27]. Auf openCode listet die Gitlab-Untergruppe *OSCI* der Governikus-Gruppe lediglich auf, dass diese »demnächst« auch eine .NET-Edition umfassen wird [28].

Auf der Website der Koordinierungsstelle für IT-Standards sind verschiedene (Infrastruktur-)Implementierungen unterschiedlicher Marktteilnehmer gelistet, deren Konformität nicht geprüft wird [29].

4.2.6 Infrastruktur

Teilnehmer in einer OSCI-basierten Infrastruktur sind grundsätzlich dezentral strukturiert. Wie die Knoten (in ihren Rollen als Intermediär) logisch verortet werden, bleibt frei. Es wird in der Spezifikation lediglich darauf hingewiesen, dass Intermediäre auch beim Nutzenden physisch verortet sein können [24, S. 11].

OSCI selbst betrachtet den Aspekt des Routings zwischen Kommunikationspartnern (unabhängig ob Client/Supplier oder Intermediär) nicht. Die Spezifikation betrachtet die Teilnehmer als bekannt, setzt aber die Existenz eines *Chiffrierzertifikates* voraus [24, S. 11]. Der Bezug dieser Zertifikate, etwa für die Rolle Autor, wird nicht spezifiziert [24, S. 31].

OSCI wird in der etablierten Kommunikationsinfrastruktur der Innenverwaltung und Justiz mit externen Verzeichnisdiensten wie DVDV oder SAFE verzahnt [30]. Ein konkretes Zusammenspiel zwischen OSCI und den Verzeichnisdiensten wird in der Spezifikation nicht genauer definiert.

4.2.7 Sicherheit

4.2.7.1 Signaturen

Inhalts- und Auftragsebene können digital signiert werden. Wie die Verschlüsselung ist auch das Signieren nur als Option spezifiziert und nicht verbindlich vorgeschrieben [24, S. 29].

Die Notwendigkeit von Signaturen auf *Inhaltsebene* wird durch die OSCI-Spezifikation lediglich als »nicht verpflichtend« festgehalten [24, S. 29]. Durch die Spezifikation wird kein einheitliches Verfahren zur Reaktion auf fehlende oder fehlerhafte Signaturen auf Leserseite definiert [24, S. 29], wodurch sich die Gefahr heterogenen Verhaltens auf Implementierungsseite ergibt.

4.2.7.2 Signaturalgorithmen der OSCI-Spezifikation

Die vorliegende Spezifikation von OSCI 1.2 lässt die Nutzung von SHA-1 für die Erzeugung von Signaturen »bis auf Weiteres« zu [24, S. 214], obwohl die Verwendung dieses Hashalgorithmus für kryptografische Anwendungsgebiete durch das BSI auf Basis bekannter Angriffsszenarios nicht empfohlen wird [31, S. 51]. Gleichzeitig wird in der Spezifikation widersprüchlich empfohlen, auf SHA-1 (mit einer Schlüssellänge von 1024 Bit) zu verzichten, allerdings wird deren Unterstützung weiterhin vorgeschrieben [24, S. 216].

Innerhalb der Spezifikation werden die in Tabelle 2 gelisteten Algorithmen explizit als zu nutzend deklariert [24, S. 215].

Tabelle 2

Unterstützte Signaturalgorithmen der OSCI-Spezifikation

Algorithmus	Hash-algorithmus	Schlüssellänge lt. Standard	Bemerkung
RSASSA-PKCS1-v1_5	SHA-256, SHA-512	Mind. 2048 Bit	BSI empfiehlt Nutzung nur bis 2025 und Migration auf RSASSA-PSS oder ECDSA [32, S. 26].
RSASSA-PKCS1-PSS	SHA-256, SHA-512	Mind. 2048 Bit	BSI empfiehlt Schlüssellängen von mind. 3000 Bit für RSASSA-PSS [31, S. 12].
ECDSA-SHA	SHA-256, SHA-384, SHA-512	Spezifikation verweist keine Schlüssellängen mit Verweis auf RFC6931 angegeben.	BSI empfiehlt bei ECDSA-konfigurationen spezifische Schlüssellängen [31, S. 12].
RSASSA-PKCS1-PSS	SHA3-256, SHA3-384, SHA3-512	Mind. 2048 Bit	SHA-3 Familie als geeignet zu betrachten [33, S. 51]. Schlüssellänge siehe vorherigen Eintrag zu RSASSA-PKCS1-PSS

»Um Komptabilität mit im Markt eingesetzten Implementierungen zu gewährleisten« [24, S. 215–216] gestattet die Spezifikation die Verwendung von RSASSA-PKCS1-v1_5 mit SHA-1 und einer Länge von 1024 Bit. Damit entspricht die Spezifikation nicht den aktuellen Empfehlungen des BSI, die die Nutzung sowohl von RSASSA-PKCS1-v1_5 und SHA-1 für kryptografische Anwendungen nicht mehr empfiehlt [32, S. 26] [31, S. 51].

4.2.7.3 Verschlüsselung

OSCI schreibt für Verschlüsselungsvorgänge X.509v3 als Basisformat vor [24, S. S.33]. Der Bedarf der Umsetzung einer Verschlüsselung von Aufträgen und deren Antworten wird in der Spezifikation lediglich als optional festgehalten [24, S. 13], während individuelle Auftragsantworten verpflichtend zu verschlüsseln sind [24, S. 31].

Auf der Inhaltsebene sieht die Spezifikation eine Verschlüsselung lediglich als möglich, aber nicht erzwungen vor. Ebenso wird auch kein einheitliches Verhalten im Falle von Verschlüsselungsproblemen definiert [24, S. 31–32].

Vergleichbar mit der in Abschnitt 4.2.2.2 beschriebenen fehlenden architekturglobalen Betrachtungsweise mit XTA lässt die Spezifikation frei, wie in einem Betriebsumfeld die notwendigen Zertifikate bezogen werden können [24, S. 32]. Durch die fehlende Referenzierung notwendiger Abhängigkeiten auf Infrastrukturebene wird das Verständnis erschwert, wie sich OSCI in ein Gesamtsystem der B2G- und G2G-Kommunikation integrieren lässt.

4.2.7.4 Ende-Zu-Ende-Verschlüsselung

Die OSCI-Spezifikation definiert die Möglichkeit einer Ende-Zu-Ende-Verschlüsselung, bei der die Verschlüsselungsstrecke von Autor zu Leser reicht. Beide Rollen sind allerdings in der Spezifikation explizit außerhalb von OSCI verortet [24, S. 12].

Hierdurch wird implizit notwendig, dass das einliefernde Fachverfahren die in OSCI geltenden Verschlüsselungs- und Signieranforderungen unterstützen muss, um kryptografisch geeignete Nachrichten im Sinne einer Ende-Zu-Ende-Verschlüsselung erzeugen zu können. Gleiches gilt für die konsumierende Fachanwendung auf Leserseite.

OSCI betrachtet Verschlüsselungen sowohl auf der Antrags- als auch der Nachrichtenebene. Es findet hier das Konzept eines inneren und äußeren Umschlags Anwendung, welches durch Nachricht und Auftrag in OSCI repräsentiert wird. Hierdurch wird insbesondere für neue Umsetzungen die notwendige Implementierungskomplexität erhöht.

Gleichzeitig eröffnet die Ausführung der Kryptografie auf Auftrags- und Nachrichtenebene eine durchgängige Verschlüsselung der eigentlichen Inhaltsdaten. Unabhängig von der Öffnung des äußeren Umschlags der Auftragsebene bleibt die Vertraulichkeit des inneren Umschlags unversehrt, da die Nachricht durch den Intermediär grundsätzlich nicht gelesen werden muss.

Eine globale Secure-By-Default-Policy liegt in OSCI nicht vor. Der Bedarf der Verschlüsselung wird anhand der Ausprägung des eingehenden Auftrags oder der individuellen Standardkonfiguration des Intermediärs bestimmt (siehe Abschnitt 4.2.7.3).

4.2.7.5 Verschlüsselungsalgorithmen der OSCI-Spezifikation

Die Spezifikation weist die in Tabelle 3 gelisteten symmetrischen Verfahren zur Verschlüsselung im Rahmen eines Hybridverschlüsselungsvorgangs aus [24, S. 31] [24, S. 220–221].

Tabelle 3 In OSCI-Spezifikation erlaubte Verschlüsselungsalgorithmen

Verschlüsselungsalgorithmus	Bewertung
Two-Key-Triple-DES	Angreifbar gegenüber CVE-2016-21 83 [34]
AES-128 mit CBC	Folgt aktuellen Empfehlungen des BSI aus [31, S. 46]
AES-192 mit CBC	
AES-256 mit CBC	
AES-128 mit GCM	Folgt aktuellen Empfehlungen des BSI aus [31, S. 46]
AES-192 mit GCM	
AES-256 mit GCM	

4.2.7.6 Fehlermanagement

Die OSCI-Spezifikation definiert zur Benennung von Fehlern beim Nachrichtenaustausch numerische Statuscodes (»osci:Code«), die auf die Ebenen der Nachricht und des Auftrags verteilt sind. Die Statuscodes erinnern funktional an HTTP-Statuscodes, basieren aber auf den fachlichen Anforderungen im Kontext der OSCI-Kommunikation.

Die Fehlercodes sind durch Kodiertabellen fixiert und infolgedessen nicht variabel. Auf Basis der Kodiertabellen entfallen insbesondere auf die Auftragsebene eine hohe Anzahl zu beachtender Fehlercodeszenarien für die Behandlung von Signier- und Zertifikatsfehlern [24, S. 39–42].

Der Bedarf an dem Niveau dieser Granularität der Fehlercodes rein für Signier- und Zertifikatsfehler wird im Kontext der Spezifikation nicht erkennbar und erhöht die Komplexität der Implementierungen, welche Konformität zur Spezifikation anstreben.

Im Rahmen von Interviews wurden Anforderungen an die Rechtssicherheit als Grund für die Menge an Fehlercodes im Zertifikatsumfeld aufgeführt. Allerdings ist für den erfolgreichen Nachrichtenaustausch für individuelle Teilnehmer der Kommunikation im Grunde nur das binäre Ergebnis einer Zertifikatsprüfung, im Sinne von Erfolg oder Fehlschlag, von Interesse.

4.2.7.7 Rechtsicherheit

OSCI verfügt über keine eigene Benutzerverwaltung [24, S. 11], erfordert aber ein Zertifikat, über das Teilnehmer identifiziert werden [24, S. 35 u. 206]

Die Spezifikation stellt an den Intermediär zur Laufzeit Aufgaben, die über die reine Vermittlung von Daten hinausgehen. Es handelt sich hierbei etwa um die Verifikation der Integrität des Zertifikats und dessen Gültigkeitsprüfung [24, S. 33–34].

Darüber hinaus werden zusätzliche Protokolldaten erzeugt, die in einem »Laufzettel« vereint werden. Es handelt sich hierbei insbesondere um Informationen zur Einreichung, Weiterleitung und Empfangsbestätigung [24, S. 33], denen insbesondere im Hinblick auf die Rechtssicherheit und der Beweisbarkeit einer Übertragung eine hohe Bedeutung zukommt.

4.2.8 Governance

4.2.8.1 Bereitstellung der OSCI-Spezifikation

Die OSCI-Spezifikation umfasst Schriftstücke und die XSD-Schemata, welche die Nachrichtenformate beschreiben [35]. Die Schemata werden in einem Archiv zum Download angeboten, eine Versionsübersicht existiert nicht, Angaben zu Lizenzen externer, im Download enthaltener Schemata sind nicht beigefügt [24].

Das reine Dokument der Spezifikation wird durch mehrere ergänzenden Schriftstücke erweitert, die als Korrigenda, nummeriert von eins bis zehn, und Ergänzungen bezeichnet werden [35].

Zusätzlich existiert die Spezifikation als zusammengefasstes Dokument, das allerdings als »nicht normatives Hilfsmittel« bezeichnet wird. Betrachtet man die Spezifikationsdokumente einzeln (hier Kernspezifikation, Korrigenda und Ergänzungen), bleibt unklar, welche Gültigkeit die einzelnen Schriftstücke aufweisen [35].

Die Korrigenda eins bis acht weisen den Status »Final« auf. Korrigenda neun und zehn werden als »Entwurf« [35] gelistet, die anwendbare Gültigkeit bleibt unklar. Das als nicht normatives Hilfsmittel beschriebene, zusammenfassende Dokument beinhaltet allerdings auch die nicht-finalen Dokumente.

4.2.8.2 Versionierung der OSCI-Spezifikation

Die OSCI-Spezifikation trägt eine Versionsnummer 1.2 [24]. Die Version OSCI 2.0 wurde nicht finalisiert und zugunsten von OSCI 1.2 eingestellt [36].

Eine fortlaufende, nachvollziehbare Top-Level-Version wird nicht geführt, auch mit Erweiterungen verbleibt die OSCI-Versionsnummer auf 1.2: Marktübliche Ansätze wie etwa semantische Versionen [37] werden nicht genutzt. Zum Zeitpunkt der Studie war die Versionsnummer 1.2 fixiert, die durch aufsteigend nummerierte Korrigenden erweitert werden [38].

Die Abweichung von marktüblichen Versionierungsansätzen erschwert die Identifikation des inhaltlichen Standes der Spezifikation. Implementierungen können keine genaue OSCI-Version ausweisen, gegen die sie umgesetzt wurden.

4.2.8.3 Lifecycle-Management

Die Spezifikation verweist mehrfach auf die Problematik der Nutzung von SHA-1 und dessen kurzen Schlüssellänge [24, S. 216]. Eine klare Exit-Strategie für gebrochene Kryptografiealgorithmen wird jedoch nicht erkennbar. Die weitere Verwendung von SHA-1 muss laut Spezifikation lediglich mit einem Warnhinweis »deutlich« in einer Fehlerantwort ausgewiesen werden [24, S. 216].

4.2.8.4 Referenzimplementierung

Es wird auf der OSCI-Website der KoSIT im OSCI-Kontext auf XTA-Referenzimplementierungen für Version 3 und 5 verwiesen, in denen OSCI-Funktionalitäten laut schematischer Darstellung integriert sind [39]. Die Systemgrenzen zwischen OSCI und XTA wird hierbei insbesondere für neue Implementierende nur bedingt erkennbar. Für OSCI selbst existiert jedoch auf den KoSIT-Webseiten kein Verweis auf eine eigene Referenzimplementierung.

Der Reifegrad dieser Referenzimplementierungen wird in beiden Fällen nur als »Entwurf« im Repository dargestellt; die Dokumentation ist laut Projekt-Readme-Datei unvollständig [40] [41].

4.2.8.5 Referenzumgebung

Auf der Website zur Referenzimplementierung wird auf den möglichen Bezug einer separaten Referenzumgebung über die Firma Governikus verwiesen [39],

deren Zugriff zum Zeitpunkt dieser Studie nur über den Bezug über einen vierstelligen Eurobetrag möglich ist [42].

4.2.8.6 Konformitätsprüfung

Auf der Website der Koordinierungsstelle für IT-Standards sind verschiedene Implementierungen unterschiedlicher Marktteilnehmer gelistet. Es handelt sich dabei um eine kuratierte Liste, die von der Koordinierungsstelle für IT-Standards gepflegt wird. Allerdings wird im Rahmen einer Eintragung keine Konformitätsprüfung durchgeführt: »Für die Eintragung muss die Implementierung keine Konformität nachweisen« [29].

Hierdurch verbreiten sich möglicherweise auch nur teilkompatible Lösungen, die zu einer langfristigen Dialektbildung führen können. Auf der zentralen Website zu OSCI wird kein dedizierter Konformitätstester angeboten, wie er etwa für die XTA 2 Versionen 3 [20] und 5 [43] zur Verfügung gestellt wird.

4.2.8.7 Zugänglichkeit und Ökosystem

Die Website der Koordinierungsstelle für IT-Standards³ wird durch die dort zugängliche Spezifikation [24], Dokumentationen durchaus als zentraler Anlaufpunkt für OSCI wahrgenommen.

Es gibt Funktionspostfächer, die für Anfragen genutzt werden können, allerdings existiert kein offener Austausch für Implementierende oder solche, die eine Anbindung an das OSCI-Ökosystem anstreben. Hierdurch wird die Aufklärung von Unstimmigkeiten, die etwa durch eine öffentliche Diskussion transparent gestaltet werden könnten, hinter geschlossenen E-Mail-Kommunikationen versteckt. Eine fehlende transparente Diskussion von Implementierenden fördert selektive, bilaterale Abstimmungen zwischen Teilnehmern und provoziert somit ebenfalls die Dialektbildung innerhalb des OSCI-Ökosystems.

Eine Bearbeitung der Spezifikation wird explizit rechtlich limitiert [24, S. 2], so dass bei der OSCI-Spezifikation zwar von einer öffentlich zugänglichen Spezifikation, aber nicht von einer Open-Source-Spezifikation im engeren Sinne gesprochen werden kann.

Die Spezifikation selbst wird nicht im Rahmen eines transparenten Entwicklungsprozesses, etwa durch Versionskontrollsysteme, verwaltet und zugänglich gemacht. Der Download erfolgt über das Content-Management-System der Koordinierungsstelle für IT-Standards [44].

³ <https://www.xoev.de/> Abruf 17.07.2026

In jüngster Vergangenheit wurde zunehmend die Plattform openCode⁴ für Verwaltungs-Digitalisierungsprojekte positioniert. Sie wird aber im Kontext OSCI nur zum Teil ausgereizt, etwa durch [26]. Die Koordinierungsstelle für IT-Standards legt Projekte hingegen auf einer eigenen GitLab-Instanz⁵ ab, die über eine eigene Benutzerverwaltung verfügt und somit über separate, genehmigungspflichtige Accounts verfügt.

Eine zentrale Nutzung von Plattformen wie openCode könnte den Einstieg und Möglichkeiten zur Diskussion bieten, die auch zu einer transparenten Weiterentwicklung der Spezifikation beitragen können. Die Zersplitterung von auswertbaren Spezifikationsbestandteilen und (nicht normativen) Hilfsmitteln zwischen xoev.de, projekte.kosit.org und Governikus erschweren die Zugänglichkeit und die Zuordnung von Zuständigkeiten.

4.3 XTA

Wir analysieren im Folgenden den Standard XTA 2 in der aktuell empfohlenen Version 5.1.1 [43] und untersuchen dabei insbesondere dessen funktionale Ausgestaltung, semantische Eindeutigkeit sowie die Umsetzung von Sicherheits- und Qualitätsanforderungen.

4.3.1 Anwendungsbereich

Der XTA 2-Standard dient als zentrale Grundlage für den standardisierten Datentransport in der öffentlichen Verwaltung.

4.3.1.1 Hintergrund und Entwicklung von XTA

XTA ist die Abkürzung für *XML in der öffentlichen Verwaltung Transport Adapter*. Die Bezeichnung XTA 2 verweist auf die zweite Generation des Standards (Version 2), die eine weiterentwickelte und stärker standardisierte Form des ursprünglichen XTA-Ansatzes darstellt und insbesondere auf höhere Interoperabilität sowie einheitliche Schnittstellen abzielt. XTA 1 existiert seit den 2000er-Jahren im Zuge des Aufbaus der OSCI-basierten E-Government-Infrastruktur. Es war die erste Generation des XTA-Standards und wurde später durch XTA 2 abgelöst (politisch ab 2017 konsolidiert [45]). Wie in der technischen Konversation über XTA 2 üblich, verwenden wir im Folgenden das Akronym XTA synonym für XTA 2.

⁴ <https://opencode.de/> Abruf 07.07.2026

⁵ <https://projekte.kosit.org/transport-public/> Abruf 07.07.2026

4.3.1.2 Ziele von XTA

Ein wesentliches Ziel von XTA ist die Vereinheitlichung der Schnittstellen zwischen behördlichen Fach- und Transportverfahren. Dadurch soll die verteilte, fachliche Bearbeitung von (behördlichen) Geschäftsprozessen, auch innerhalb überregionaler Kommunikationsverbünde, digital unterstützt werden.

In [20] wird ausführlich auf die Motivation für den Entwurf von XTA erläutert:

» [...] Durch die Vielzahl der Einsatzgebiete und durch wechselnde rechtliche Rahmenbedingungen sind die Anforderungen an den Schnittstellen zwischen den Fachverfahren der öffentlichen Verwaltung und der Transportinfrastruktur der öffentlichen Verwaltung stark gestiegen.

Es hat sich gezeigt, dass in manchen komplexen E-Government-Anwendungen eine Aufteilung zwischen fachlichen IT-Verfahren und einer spezialisierten Transport-Infrastruktur sinnvoll sein kann. In solchen Fällen wird eine standardkonforme Kommunikation zumeist nur zwischen den 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.

Diese Lücken sollen durch XTA 2 geschlossen werden, indem die (funktionalen) Schnittstellen zwischen Fach- und Transportverfahren definiert werden [...] und indem durch die Service Profile ein Instrument zur Verfügung gestellt wird, durch das die (modalen) Anforderungen an den Transport einheitlich definiert und konfiguriert werden können [...] «

Ausführlich wird in dieser Motivation auf die Probleme und Herausforderungen spezialisierter Betreiber von Transportverfahren – insbesondere die Betreiber sogenannter Clearing- oder Vermittlungsstellen – sowie der Hersteller von Fachverfahren eingegangen. Ziele, die durch XTA adressiert werden sollten, sind unter anderem:

- Aufwandsreduktion für die Betreiber von zentralisierten Transportverfahren (z. B. zentral in einem Bundesland) durch Vereinheitlichung unterschiedlicher proprietärer Fachverfahrensschnittstellen, wie in Abbildung 4.
- Aufwandsreduktion für die Softwarehersteller überregional eingesetzter Fachverfahren durch Vereinheitlichung der Schnittstellen zu unterschiedlichen

Betreibern von Transportverfahren (z. B. in unterschiedlichen Bundesländern), wie in Abbildung 5.

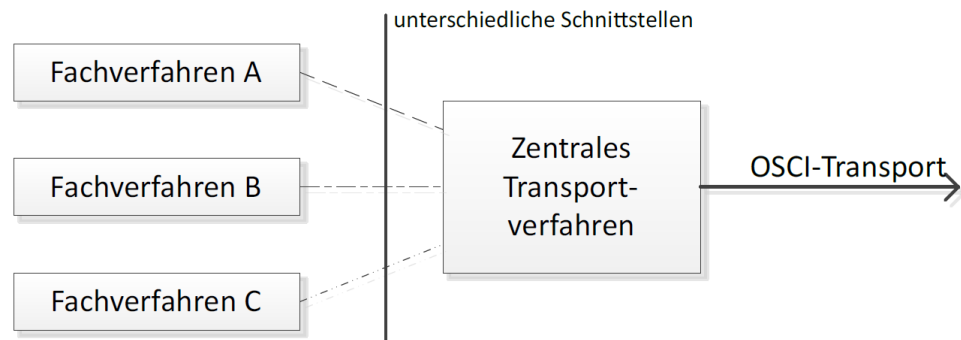


Abbildung 4

Heterogene Anbindung von kommunalen Fachverfahren an einen Betreiber von Transportverfahren ohne vereinheitlichte XTA-Schnittstelle [20]

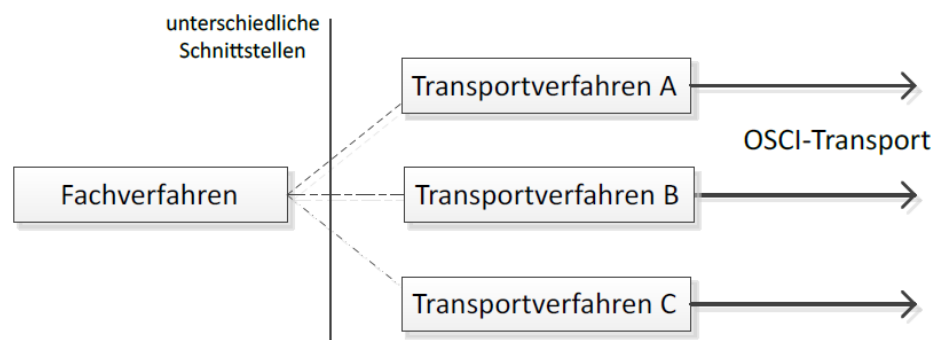


Abbildung 5

Heterogene Anbindung eines Fachverfahrens zu den zentralen Transportverfahren in unterschiedlichen Bundesländern [20]

Dazu werden mit XTA einheitliche Vorgaben für Transportverfahren und ihre Schnittstellen zu den Fachverfahren definiert. Dies beinhaltet sowohl eine Festlegung der Funktionen eines konkreten Transportverfahrens als auch das technische Format der Schnittstelle. Die Formulierung der technischen Eigenschaften in einem einheitlichen Standard – XTA – sollte folglich eine bessere Interoperabilität zwischen den Fach- und den Transportverfahren herstellen.

4.3.1.3 Einsatz von XTA 2

XTA ist als Kommunikationsstandard verbindlich in bestimmten Kontexten von G2G-Kommunikation vorgeschrieben, z. B. in der XBasisdaten-Verordnung [46]. Der Anteil der in der öffentlichen Infrastruktur ausgetauschten OSCI-Nachrichten, die mittels XTA verarbeitet werden, war im Rahmen dieser Studie

nicht zu ermitteln. In einem Interview mit der Firma Governikus wurde der Anteil der mittels XTA übermittelten Nachrichten am Gesamtvolumen von ca. 2 Milliarden OSCI-Nachrichten (siehe [22]) auf zwischen 15 und 25 Prozent geschätzt.

Es gibt Bereiche der öffentlichen Verwaltung, in denen XTA kaum oder gar nicht zum Einsatz kommt. Laut Auskunft von Mitgliedern der Arbeitsgruppe »IT-Standards in der Justiz« der Bund-Länder-Kommission (BLK) basiert der elektronische Nachrichtenverkehr im Justizbereich aufgrund einer weitgehenden Standardisierung des Datenaustauschs fast ausschließlich direkt auf OSCI.

In der Praxis werden beispielsweise von der Firma Governikus und Procilon XTA-Server mit Unterstützung von OSCI als Nachrichtenprotokoll zur Verfügung gestellt. Der XTA-Server COM Despina der Firma Governikus existiert darüber hinaus in einer spezialisierten Edition, der über das XTA-Protokoll auch Zugang zu Peppol/AS4 Kommunikation ermöglicht [22]. Dies ist ein Beispiel für die Fähigkeit von XTA, vom konkreten Transportverfahren abstrahieren zu können. In der XTA-Spezifikation selbst findet sich jedoch außer der Beschriftung »OSCI, etc.« in einer Abbildung kein Hinweis auf die Unterstützung solcher Szenarien (siehe auch Abbildung 6). In den Codelisten auch der aktuellen XTA-Spezifikation zu Transportnachrichtenformat, Transportprotokoll oder Verzeichnisdienst finden sich lediglich Codes zu im OSCI / XTA-Umfeld üblichen Methoden. Der Einsatz von XTA in Konstellationen mit anderen Transportverfahren als OSCI ist zwar als Aspiration z. B. auf Informations-Webseiten der FITKO genannt [19]. Ein tatsächlicher Einsatz von XTA in diesen Kontexten findet damit jedoch außerhalb der konkreten XTA-Spezifikation statt. Es ist unbestreitbar, dass eine Erweiterung von XTA um solche Einsatzszenarien möglich ist, sie hat jedoch bis jetzt noch keinen Eingang in die offizielle Spezifikation gefunden.

OSCI / XTA wurde durch das Bundesverwaltungsamt (BVA) für den Einsatz im Nationalen Once-Only-Technical-System (NOOTS) erwogen, aber zugunsten einer Eigenentwicklung der Transportschicht verworfen. Abschnitt 4.5.3 geht näher auf die Gründe dieser Entscheidung ein.

4.3.2 Kommunikationsmodell

4.3.2.1 4-Corner-Modell

Das XTA-Rollenmodell bestehend aus Autor, Sender, Empfänger und Leser ist grundlegend, um den XTA-Standard zu verstehen. Es basiert auf dem abstrakten 4-Corner-Modell (siehe Abschnitt 2.1), das über einer Transportschicht und einer darüberliegenden Anwendungsschicht angeordnet ist: Auf der Anwendungsschicht überträgt ein Autor eine Nachricht, die aus strukturierten Daten besteht, an einen Leser. Für die technische Abwicklung bedient sich der Autor eines auf der Transportschicht befindenden Senders, der die Nachricht an einen

geeigneten Empfänger, ebenfalls auf der Transportschicht, schickt, welcher wiederum die Nachricht dem Leser auf der Anwendungsschicht bereitstellt. Zur eigentlichen Datenübertragung zwischen Sender und Empfänger werden weitere Infrastrukturdienste und Technologien genutzt (Abbildung 6).

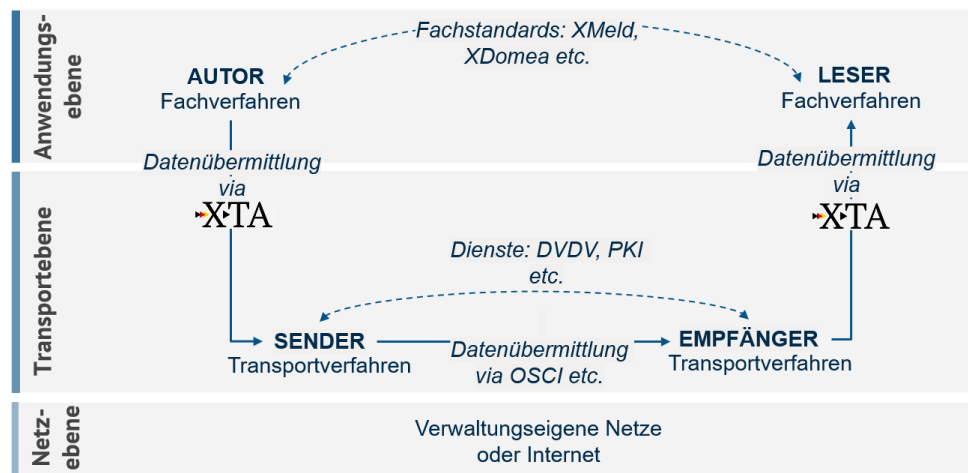


Abbildung 6 Datenübertragung mittels XTA zwischen Sender und Empfänger [43]

4.3.2.2 Kernkonzepte

Die Verwendung des XTA-Schnittstellenstandards soll zwischen Fachdatenaustausch und Transportverfahren trennen, wie es in verteilten (digitalen) Systemen allgemein üblich ist (vergleiche TCP/IP-Referenzmodell [47]).

Die KoSIT-Webseiten schreiben dazu in [21]:

»Die Spezifikation umfasst die Methoden für den Austausch von Nachrichten zwischen Fach- und Transportverfahren in Form einer einheitlichen Webservice-Schnittstelle. Neben Kernfunktionen zur Übergabe der zu transportierenden Daten, stehen auch zusätzliche Funktionen zur Verfügung. Zum Beispiel für den parallelen Abruf von Nachrichten, Benachrichtigungen von Transportverfahren an Fachverfahren und den zeitgesteuerten Versand. Begleitend zur Webservice-Schnittstelle, definiert XTA in Form der Service-Profile eine einheitliche Beschreibung für Anforderungen an den Transportdienst. Dadurch werden sowohl die notwendigen, einheitlichen Mittel für eine funktionale Steuerung des Transports (Daten, Adressierung) als auch für Anforderungen an den Transportdienst (Servicequalitäten) zur Verfügung gestellt. Die Spezifikation des XTAService-Profils und des XTA-Webservice beziehen sich konzeptionell stark aufeinander, sie können trotzdem unabhängig voneinander eingesetzt werden.«

Der letzte Satz des Zitats kann als ein weiteres Indiz interpretiert werden, dass zumindest die Aspiration bestand, XTA auch für die Anwendung mit anderen Nachrichtenprotokollen einzusetzen. Dies lässt sich auch aus Abbildung 7 erkennen, die den »XTA-Rahmenbedingungen« [48] entnommen ist:

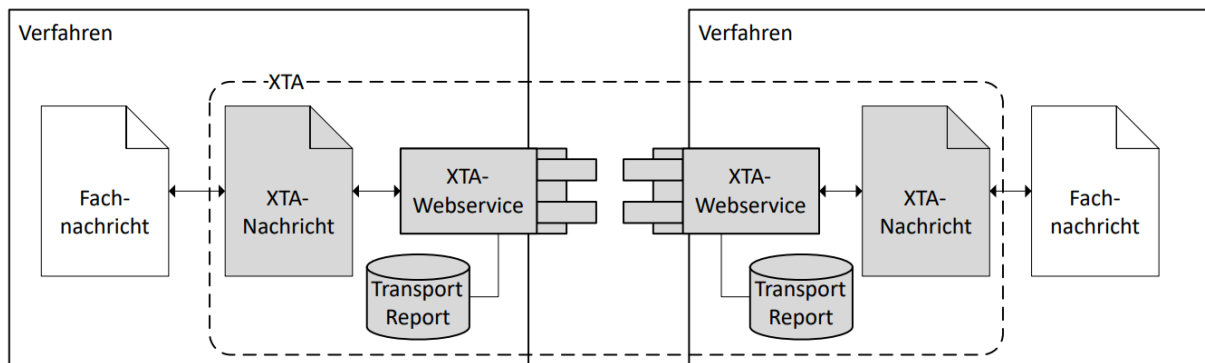


Abbildung 7

Datenübertragung zwischen Autor und Leser über das XTA-Protokoll [48]

Das Bild suggeriert, dass die Fachverfahren lediglich die XTA-Schnittstelle kennen müssen und nicht das zum Transport genutzte Nachrichtenprotokoll. Auf diesen Punkt kommt diese Studie zu einem späteren Zeitpunkt zurück.

Die XTA-Spezifikation bezeichnet den Sender als »XTA-Server« und das angebundene Fachverfahren als »XTA-Client«. Der XTA-Server nimmt im 4-Corner-Modell die Stelle des Senders und Empfängers ein.

Wie im Zitat oben ausgeführt, besteht der XTA-Standard im Wesentlichen aus den beiden Komponenten:

- Definition der XTA-Webservices (Modul *XTA-Webservices*, XTA-WS)
- Definition der XTA-Service-Profile (Modul *XTA-Service-Profile*, XTA-SP)

Auf Basis dieser Module lassen sich mit XTA folgende Entitäten und Anforderungen definieren:

- Transportnachrichten bestehend aus Transportauftrag und Fachnachricht
- Methoden zum Versand und Empfang von Transportnachrichten
- Berichte inklusive Ereignisprotokolle und gesonderte Quittungen zur Überprüfung des Transports
- 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

XTA unterstützt sowohl asynchrone als auch synchrone Zustellprozesse. Dies bedeutet, dass Nachrichten nicht nur zeitversetzt zum Versand zugestellt werden können (*Store-and-Forward*), sondern XTA unterstützt auch die Definition sogenannter *Callbacks* über die Methode *deliverMessage*, über die ein XTA-Server eine direkte Reaktion des angesprochenen Fachverfahrens erwirken kann, sofern das Fachverfahren einen entsprechenden Webservice implementiert hat.

4.3.2.3 Einsatz von XTA 2 in Verbindung mit OSCI

Wichtig für das Verständnis des XTA-Standards ist, dass XTA nur die Schnittstelle zwischen Fachverfahren und Transportverfahren mittels der oben gelisteten Funktionen standardisiert, aber selbst keinen eigenen Nachrichtenstandard festlegt. Dies bedeutet, dass eine Nachricht, die mittels XTA »aufgegeben« wurde, nicht notwendigerweise mittels XTA wieder »abgenommen« werden muss. In der Praxis werden sowohl Nachrichten, die rein mittels OSCI aufgegeben wurden, per XTA abgenommen, als auch umgekehrt. Abbildung 8 zeigt ein Kommunikationsszenario aus einem Bericht des Landes NRW über die Übertragung von Daten eines Online-Portals zu unterschiedlichen Fachverfahren, die entweder über XTA oder direkt über OSCI angebunden sind. Dieses Szenario gilt aber auch umgekehrt, d. h. eine OSCI-Nachricht kann auch – sofern sie dem eigentlichen Fachstandard entspricht – an einen XTA-Empfänger zur Weiterleitung an den Leser geschickt werden.

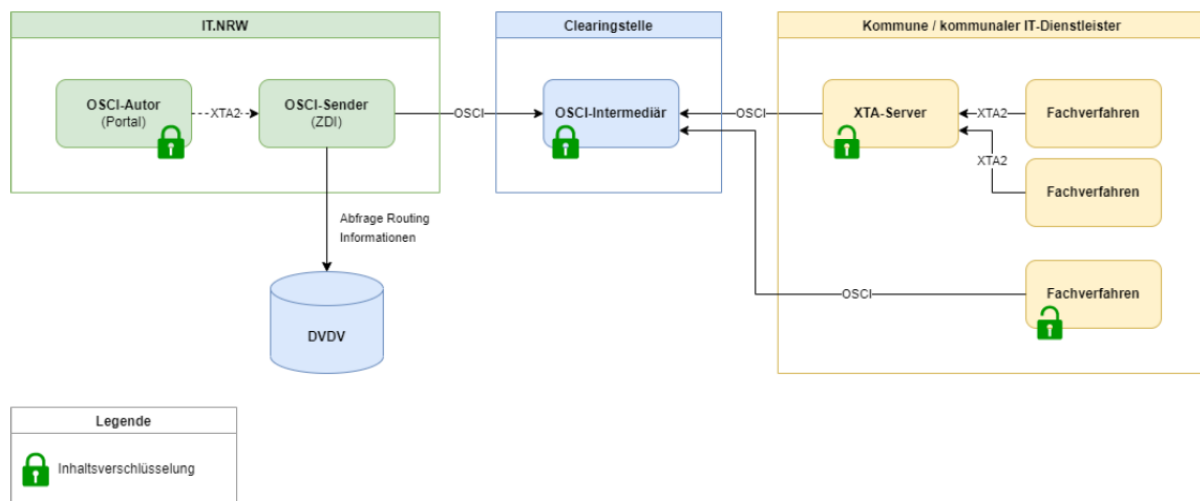


Abbildung 8 Szenario einer testweisen Übertragung von Daten eines Portals über XTA an die OSCI-Infrastruktur zu entweder XTA- oder OSCI-Abnehmern [49]

4.3.3 Kommunikationsstandards

XTA wird in erster Linie mit OSCI eingesetzt. In Interviews wurde von einigen Gesprächspartnern argumentiert, dass XTA als Abstraktionsschicht des konkreten Nachrichtenprotokolls eingesetzt werden kann – z. B. mit Verweis auf die COM Despina Peppol/AS4 Edition des XTA-Servers der Firma Governikus [22].

Hervorzuheben ist hierbei, dass der XTA-Standard gewisse Freiräume für proprietäre Anpassungen lässt. Dokumentation und Codelisten des Standards beziehen sich jedoch ausschließlich auf Mechanismen des OSCI-Protokolls und darauf basierender Infrastruktur. Um Interoperabilität von XTA-Servern zu anderen Nachrichtenprotokollen wie AS4 oder FIT-Connect herzustellen, müsste zwingend der XTA-Standard erweitert und die Infrastruktur von XTA-Servern aktualisiert werden, die auch für andere Nachrichtenprotokolle genutzt werden sollen.

4.3.4 Schnittstellenstandard

4.3.4.1 Allgemeines

Der XTA-Standard basiert auf XML und WSDL und damit auf industriellen Standards des World Wide Web Consortiums (W3C). WSDL spezifiziert allerdings nur die syntaktischen Elemente eines Webservices. Die darüberhinausgehende semantische Spezifikation eines Webservices erfolgt daher durch die Erläuterungen in der XTA-Spezifikation und den XTA-Rahmenbedingungen [48]. Die Semantik von XML-Spezifikationen könnte zumindest teilweise in eingeschränkter Weise mit Hilfe von *XML-Schema*, einem weiteren W3C-Standard, formal festgelegt werden, wird jedoch bei der Definition des XTA2-Standards *nicht* eingesetzt. Auch wenn heutzutage meist JSON statt XML zur syntaktischen Definition von Datenstrukturen zu Einsatz kommt, sind XML und WSDL etablierte und erprobte W3C-Standards (siehe zum Vergleich von REST und SOAP auch den Abschnitt 3.3).

Der XTA2-Standard ermöglicht eine hohe Flexibilität bei der Definition von Anforderungen hinsichtlich Schutzbedarf, Verschlüsselung und Löschung der zu transportierenden (Fach-)Daten sowie der Protokollierung (mit temporärer Archivierung) und Quittierung des Datentransports selbst. Damit bietet der XTA2-Standard, insbesondere die XTA-Service-Profile, die einen großen Teil des Standards ausmachen, viele Möglichkeiten, behördliche Prozesse hinsichtlich rechtlicher Nachvollziehbarkeit, Fälschungssicherheit von Dokumenten und den standardisierten Austausch von Nachweisen zu unterstützen.

Während die standardisierte Schnittstelle von XTA-Webservice (XTA-WS) den fachlichen Datenaustausch zwischen XTA-Anwendern vereinfachen soll, können mit XTA-Service-Profilen (XTA-SP) in standardisierter Form Anforderungen an die Art und Weise des Transports von Fachnachrichten formuliert und ausgetauscht

werden. Das Modul *XTA Service Profile* dient dabei der einheitlichen Definition und Konfiguration der regelgeleiteten Anforderungen an den Transport (fachlicher/ behördlicher) Nachrichten. Das Modul *XTA Webservice* vereinheitlicht die funktionalen Schnittstellen der Webservices zwischen Fach- und Transportverfahren, um die Übermittlung von Nachrichten vor allem im Behördenkontext zu standardisieren.

4.3.4.2 XTA Service Profile

Der Standard *XTA Service Profile* spezifiziert XML-Datenstrukturen, die wir im Folgenden XTA-Service-Profile oder nur Service-Profile nennen. In einem solchen Service-Profil werden generelle fachliche – und auch technische – Rahmenbedingungen festgelegt. Die Service-Profile unterteilen sich in die in dargestellten Klassen.

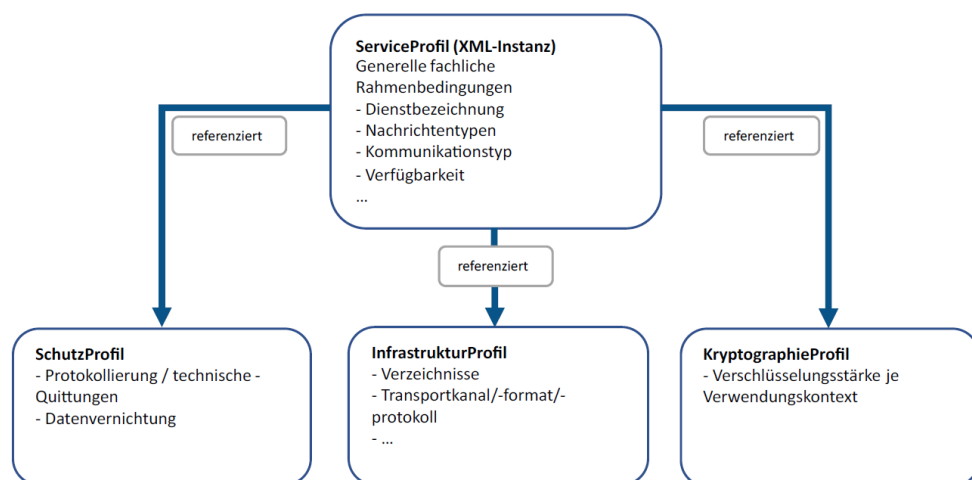


Abbildung 9 Unterteilung der Service-Profile [43]

XTA lässt genau ein Schutzprofil, ein oder mehrere (1..n) Infrastrukturprofile sowie gegebenenfalls mehrere (0..n) Kryptographieprofile in den Service-Profilen zu.

4.3.4.2.1 XTA-Schutzprofil

Im Schutzprofil können detaillierte Angaben zu Schutz und Sicherheit gemacht werden. Beim Schutz geht es darum, die Nachrichtenübermittlung transparent und somit nachvollziehbar zu gestalten. Dazu können Angaben gemacht werden, welche Protokollierungen und Quittungen von welcher Rolle erstellt werden sollen. Weiterhin können Vorgaben zum Löschen der Daten und Protokollierungen gemacht werden. Diese Definitionen werden ergänzt durch die Angabe eines Abweichverhaltens, das festlegt, wie zu verfahren ist, wenn die Protokollierung, Quittierung oder das Löschen nicht umgesetzt wurde, d. h. die Vorgabe

nicht erfüllt ist. Definierbar sind die Verhalten *Abbrechen* oder *Fortsetzen* der Nachrichtенbearbeitung.

In puncto Sicherheit können eine oder mehrere Vorgaben gemacht werden:

- Zur Vertraulichkeit der Daten/Nachricht,
- zur Integrität (Unversehrtheit der Daten/Funktionieren des Systems),
- zur Authentizität (d. h. Identität des Kommunikationspartners),
- zur Unveränderbarkeit der übertragenen Daten sowie
- zum zu verwendenden Zertifikat, beispielsweise beim Identitätsnachweis.

Zu den Vertraulichkeitsqualitäten können mehrere Angaben für unterschiedliche *Geltungsbereiche* gemacht werden. Der Geltungsbereich eines Vertraulichkeits-Parametersatzes bezieht sich auf eine der folgenden Kommunikationsstrecken im 4-Corner-Modell: Autor – Leser, Autor – Sender, Autor – Empfänger, Sender – Empfänger, Empfänger – Leser.

4.3.4.2.2 Infrastrukturprofil

In einem Service-Profil können mehrere Infrastrukturprofile für – ebenfalls so benannte *Geltungsbereiche* angegeben werden. Bei Infrastrukturprofilen beziehen sich die Geltungsbereiche auf:

- bundesweiter Nachrichtenaustausch
- länderübergreifender Nachrichtenaustausch
- landesinterner Nachrichtenaustausch
- kein Geltungsbereich definiert

In einem Infrastrukturprofil können die Eigenschaften der für einen Transport benötigten Infrastrukturkomponente festgelegt werden. Dazu gehören die Übertragungskанäle zwischen Sender und Empfänger. Dabei kann zwischen einer Übermittlung über das Internet, das Verbindungsnetz, das NotarNet oder einer rechenzentrums- oder systeminternen Übermittlung gewählt werden. Zudem muss das Transportnachrichtenformat, das Transportprotokoll und die beiden Verzeichnisdienste zur Adressierung und zur Identifikation von Teilnehmern eindeutig vorgegeben werden. Diese beiden Verzeichnisdienste können gleich sein (z. B. DVDV oder SAFE), wobei zur Identifikation andere Dienste als bei Adressierung genutzt werden können (z. B. IDA-BHVZ). Mögliche Werte für das Transportnachrichtenformat sind OSCI 1.2, XTA 1.1, XTA 2, systemintern und OSCI 2. Für das Transportprotokoll sind http, https, ftp, sftp, smtp und *systemintern* mögliche Werte, wobei in beiden Fällen die Konstante *systemintern* vermutlich eigene Anpassungen am XTA-Standard vorbei ermöglichen soll. Weiterhin sind

eindeutige Vorgaben zum Zertifikat, zur Protokollführung, zur Datenhaltung, zur Abgabestation und zur maximalen Nachrichtengröße zu machen.

Bei der Protokollführung gibt es eindeutige Vorgaben zur Vorhaltdauer und zur Löschfrist, wobei die Qualität des Löschvorgangs im Schutzprofil zu definieren ist. Bei der Datenhaltung ist als Vorgabe die Löschfrist zu definieren. Bei der Abgabestation ist festzulegen, ob die Direktzustellung zum Empfänger oder zum Leser oder in ein Postfach des Empfängers erfolgt. Wie im Schutzprofil sind auch hier Abweichverhalten zu definieren.

4.3.4.2.3 Kryptografieprofil

Im Kryptografieprofil als Teil des Serviceprofils können in mehreren sogenannten Krypto-Suiten sehr detaillierte Angaben zur Verschlüsselungsqualität korrespondierend zum benötigten Schutzbedarf, zu den entsprechenden Algorithmen und ihren Parametern (Herkunft, Schlüssellängen etc.) gemacht werden. Der Einsatz von Verschlüsselung im XTA-Standard kann zwar definiert werden, muss es aber nicht.

4.3.4.2.4 Ereignisprotokollierung und Nachweise

Neben eher statischen Anforderungen an die Art und Weise der Dienstleistung *Datentransport* lassen sich in den Serviceprofilen auch die tatsächlichen Servicequalitäten im Verlauf der Datenübertragung protokollieren und dabei auftretende Ereignisse – auch ungewollte wie Fehler – dokumentieren. Die Struktur und Semantik dieser Protokolle und Ereignisse sind im Abschnitt 1.2 der XTA-Spezifikation [43] definiert. Diese Ereignisse und Nachweise dienen vor allem dazu, die einzelnen Prozessschritte und dabei genutzten Methoden der Nachrichtenübertragung vom Sender zum Empfänger sehr detailliert zu dokumentieren.

4.3.4.3 XTA-Webservice

4.3.4.3.1 Bezug zum Kommunikationsmodell

Der XTA-Webservice als Teil des XTA2-Standards spezifiziert die Schnittstellen der Webservices bei Sendern und Empfängern zum Daten-/Nachrichtentransport zwischen den Rollen: *Autor* und *Leser* auf Anwendungsebene, über *Sender* und *Empfänger* auf Transportebene im zugrunde gelegten 4-Corner-Modell. Neben der XTA-Spezifikation gehört im XTA-Standard auch »[...] eine WSDL-Datei *xta-core.wsdl*, die alle benötigten XTA-Schemata einbindet« [43, S. 37]. WSDL (*Web Services Description Language*) ist ein XML-Format und ein Industriestandard, der Webdienste und deren Endpunkte dokumenten- und prozedurorientiert beschreibt, siehe [50].

Um ausreichende Sicherheit in der Kommunikation zwischen den *XTA-Clients*, also den Fachverfahren, und einem XTA-Server, zu gewährleisten, ist eine Kontenführung der XTA-Clients auf dem Server und die Authentifizierung mittels Client-Zertifikaten vorgeschrieben [43, S. 37].

4.3.4.3.2 Transportauftrag

Der Nachrichtenaustausch zwischen Autoren, Sendern, Empfängern und Lesern mittels XTA-Webservices wird im Wesentlichen durch sogenannte *Transportaufträge* bestimmt. Eine detaillierte Beschreibung der einzelnen Prozessschritte ist im Abschnitt 4.2 der XTA-Rahmenbedingungen [48, S. 18ff] dargestellt.

Ein Transportauftrag enthält neben der gegebenenfalls verschlüsselten Fachnachricht weitere (Meta-)Daten zur Fachnachricht und zur Art und Weise des Transports, sowie zur Autorisierung von Methodenaufrufen. In einem Transportauftrag kann auf ein Serviceprofil verwiesen werden. Dies definiert Anforderungen hinsichtlich der Art und Weise des Nachrichtentransports auf der Strecke Autor-Sender-Empfänger-Leser und damit insbesondere auch die Qualität des Dienstes (»Quality of Service«). Unabhängig von definierten Schutzbedarfen und vorgegebenen Kryptografie-Verfahren (für die Fachnachricht) »[...] muss der Kommunikationskanal [für den Nachrichtentransport zwischen Sender und Empfänger] mittels TLS/HTTPS unter Berücksichtigung von aktuellen Empfehlungen/Vorgaben des BSI abgesichert werden (Stand März 2022 mindestens TLS v1.2).« Das heißt auf Basis der vorgegebenen Schutz- und Kryptografieprofile werden die Daten bei der Übertragung zwischen Sender und Empfänger im Allgemeinen doppelt verschlüsselt.

4.3.4.3.3 Partneridentifikation

Die Kommunikationspartner sind im Transportauftrag zu benennen. Zur deren Identifikation sind zudem Verzeichnisdienste (z. B. DVDV oder SAFE) und Zertifikate anzugeben.

4.3.4.3.4 Exceptions

Die Methoden für den Datenaustausch zwischen Autor und Sender und Empfänger und Leser über die entsprechenden XTA-Webservices können beim Auftreten von Fehlern oder bei Problemen sogenannte *Exceptions* (Ausnahmeereignisse) »werfen«.

4.3.4.3.5 Inhaltsdaten

Die Inhaltsdaten enthalten die eigentliche Fachnachricht. Die Art der Nachricht ist durch die MIME-Spezifikation (RFC 2183) festgelegt. Formate sind: text/xml, text/plain, application/gzip oder application/pdf, wobei die Zeichenkodierung angegeben werden kann (z. B. UTF-8). Die Inhaltsdaten können auch einen Verweis auf eine Datei enthalten, die die Datenquelle ist.

4.3.4.3.6 Konformitätserklärung mit dem XTA-Standard

Der XTA-Transportadapter ist das Programm, das Daten normgerecht verschickt oder entgegennimmt. Die Konformitätserklärung (siehe Anhang »C Konformitätserklärung (XTA-Webservice)« [43, S. 106]) eines Herstellers von einem XTA-Transportadapter ist eine freiwillige Selbsterklärung. Ausgenommen davon ist jedoch die Umsetzung – zumindest in Teilen – von Service-Profilen. Für diese »[...] muss eine eigene Konformitätserklärung mit Angaben zur verwendeten Version und dem unterstützten Umfang des XTA Moduls Service Profile abgegeben werden.« [43, S. 58]. Für Nutzer, die einen XTA-Transportadapter auswählen, müssen hier demnach zwei Sachverhalte geprüft werden:

- Grundkonformität → erfüllt der Nutzer den XTA-Standard?
- Service-Profile → unterstützt der Nutzer die gewünschten Profile?

Das heißt, bei Einsatz eines XTA-Transportadapters ist vorab zu prüfen, ob dieser bei Verwendung von Service-Profilen per Erklärung nicht nur den grundlegenden Datentransport, sondern auch die verwendeten Service-Profile unterstützt und damit eine definierte Servicequalität mit vorgegebenen Sicherheitsanforderungen gewährleistet. Zur Überprüfung der Grundfunktionalität wird von der KoSIT ein XTA-Konformitätstester (vormals »XTA Testumgebung«) für die Version 3 von XTA 2 [51], aber auch für XTA 2 Version 5 [52] bereitgestellt.

4.3.4.3.7 Codelisten

Der XTA-Standard ist an manchen Stellen »offengelassen«, nämlich dort, wo im sogenannten *XRepository*⁶ für XÖV-Standards Codelisten abgerufen werden können. Ein Vorteil ist die flexible Anpassung an neue Gegebenheiten, ohne den Standard ändern zu müssen. Nachteilig ist jedoch, dass gegebenenfalls nicht alle Implementierungen diese Codelisten umfassend unterstützen.

4.3.5 Implementierungen

Ein in Interviews und vorangegangenen Studien wiederkehrend aufgeführtes Defizit für XTA als Standard ist, dass für die Versionen 3 und 5 laut Informationsseite der KoSIT [39] keine Referenzimplementierung existiert, lediglich »Entwürfe« von Referenzimplementierungen. Wie bereits die Studie des Bundesverwaltungsamts [53, S. 65] hält auch die Autorengruppe der vorliegenden Studie darüber hinaus die Bereitstellung eines quelloffenen XTA-Servers (analog zum Domibus Access Point für eDelivery AS4) für eine Ergänzung, die Entwickelnden den Zugang zum XTA-Standard erleichtern würde. In Interviews wurde als Grund für solche fehlenden Hilfsmittel mangelnde Finanzierung des XTA-Standards genannt.

⁶ <https://www.xrepository.de/> Abruf 29.07.2026

Es existiert für die XTA-Versionen 3 und 5 jedoch quelloffen ein sogenannter Konformitätstester. Der Konformitätstester soll es Herstellern von XTA-Produkten erlauben, die Konformität ihrer Software mit dem XTA-Standard zu testen und dokumentieren [54]. Ein Entwickler einer XTA-Anbindung berichtete in einem Interview, dass der Quellcode des Konformitätstesters in Ermangelung einer fertigen Referenzimplementierung dazu genutzt wurde, die XTA-Kommunikation so weit zu verstehen, dass die Anbindung erfolgreich durchgeführt werden konnte.

XTA-Server werden von verschiedenen Organisationen kommerziell zur Verfügung gestellt, etwa von Governikus und Procilon. Wie die Studie zum Praxistest von OSCI / XTA feststellte [49, S. 17], ist die Installation mindestens des Governikus COM Despina XTA-Servers aufwändig, was in den Interviews der vorliegenden Studie bestätigt wurde. Dem Autorenteam der Studie liegen keine Informationen vor, dass dieser Umstand für Produkte der Marktbegleiter anders gelagert ist. Dies hat für den Einsatz von XTA-Servern, insbesondere im kommunalen Umfeld Implikationen, auf die im nächsten Abschnitt näher eingegangen wird.

In Bezug auf den Funktionsumfang der verfügbaren XTA-Server hinsichtlich des XTA-Standards stellt die BVA-Studie [53, S. 65] Folgendes fest:

»Im Rahmen der OSCI-Studie konnte kein XTA-Server identifiziert werden, der den Standard vollständig implementiert.«

Die vorliegende Studie konnte zumindest durch Interviews bestätigen, dass Governikus COM Despina als verbreiteter XTA-Server bestimmte Teile des Standards gar nicht oder nicht standardkonform implementiert hatte, die zur Anbindung des IDA-Fachverfahrens (Identitätsdatenabruf) durch das BVA benötigt wurden. Die Autorengruppe geht davon aus, dass die Feststellung über die unvollständige Unterstützung des XTA-Standards auch weiterhin für die Produkte der Marktbegleiter gilt.

4.3.6 Infrastruktur

Wie im vorangegangenen Abschnitt erwähnt, sind die konkreten Implementierungen von XTA-Servern für Kommunen in vielen Fällen zu herausfordernd im Aufbau und Betrieb. In der Annahme, dass Fachverfahren (Corner 1 und Corner 4) in kommunalen Netzen betrieben werden, stellt die BVA-Studie [53, S. 22f] die Netzübergänge bei XTA-Kommunikation zusammen mit Abbildung 10 wie folgt dar:

»Die Infrastruktur erstreckt sich über viele unterschiedliche Netze auf bundes-, landes- und kommunaler Ebene, sowie dem Verbindungsnetz, dem Internet und Sondernetzen. Die Netzübergänge sind unterschiedlich gelöst: Bspw.

existiert für Governikus COM Despina die Betriebsvorgabe, dass es im gleichen Netz wie das Fachverfahren betrieben werden soll – die Kommunikation über ggf. unsichere Netze erfolgt dann ausschließlich per OSCI ([...], Szenario 1, oben). Bei Procilon wird das Fachverfahren per VPN und weiterer Sicherheitsmaßnahmen an einen entfernt stehenden XTA-Server angebunden ([...], Szenario 2, unten).«

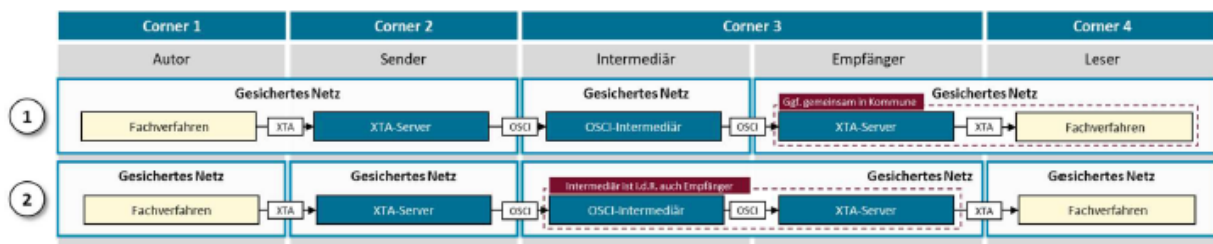


Abbildung 10 Netzübergänge bei XTA [53]

Diese Vorgaben schaffen eine teilweise sehr heterogene Landschaft von Netzübergängen, die bezüglich Administrationsaufwand und IT-Sicherheit unterschiedlich zu beurteilen sind (siehe auch nächsten Abschnitt). Man beachte in diesem Zusammenhang, dass die Inhaltsverschlüsselung der Fachdaten nach den Erkenntnissen der Studie im überwiegenden Teil der Anbindungen erst in den XTA-Servern beginnt und wieder endet. Das heißt, die Inhaltsdatenverschlüsselung liegt lediglich auf den OSCI-Transportstrecken vor.

4.3.7 Sicherheit

XTA bietet über eine Vielzahl von Vertraulichkeits-Servicequalitäten, sogar definierbar für unterschiedliche Streckenabschnitte des 4-Corner-Modells, ein sehr ausgeprägtes Konfigurationskonzept für Verschlüsselung. Wie bei der Analyse der Schwächen des XTA-Standards festgestellt, bleiben jedoch Zweifel an der Wirksamkeit dieser Konfigurationsmöglichkeiten, siehe dazu auch Abschnitt 5.2.2:

- Es besteht die Möglichkeit, dass der im Schutzprofil formulierte Schutzbedarf durch die Kryptografieprofile nicht technisch umgesetzt wird.
- Auch im neuesten XTA-Standard [43, S. 3] müssen konforme Softwareprodukte die Service-Profile nicht lesen und interpretieren können. Damit besteht keine Gewähr, dass Kryptografieprofile korrekt umgesetzt werden.
- Kein XTA-Server scheint den vollständigen Standard umzusetzen. Damit bleiben Zweifel daran, ob alle möglichen Kryptografievorgaben standardkonform umgesetzt werden.

In einem Interview im Rahmen der Studie wurde angegeben, dass fachverantwortliche Stellen ihrer Verantwortung in Bezug auf die notwendige Verschlüsselung ihrer Kommunikation in vielen Fällen nicht nachkämen. Auch [53, S. 46ff] kommt zu dem Schluss, dass Fachverfahren die Kryptografie zu XTA-Servern hin delegieren. Dies führt nach den Ergebnissen mehrerer Interviews dazu, dass in vielen Fällen die Inhaltsverschlüsselung erst im XTA-Server vorgenommen wird. Wie in Abschnitt 2.4 zum Thema fehlender Ende-zu-Ende-Verschlüsselung zwischen Autor und Leser erwähnt, führt dies zu einer gewissen Verwundbarkeit der Inhaltsdaten auf der Strecke zwischen Fachverfahren (Autor / Corner 1) und XTA-Server (Sender / Corner 2). Diese Verwundbarkeit ist im Falle der praktischen Infrastrukturgegebenheiten um XTA in manchen Fällen zusätzlich erhöht, wo die Problematik vieler Netzübergänge hinzukommt (siehe Abschnitt 4.3.6, Abbildung 10). In Fällen, wo – wie bei der Anbindung des IDA-Fachverfahrens – E2E-Verschlüsselung zwischen Autor und Leser vorliegt, ist die 4-Corner-Kommunikation über XTA als sicher anzusehen. Dies scheint nach den Erkenntnissen aus den Interviews jedoch eine Ausnahme darzustellen.

4.3.8 Governance

4.3.8.1 Pflege des Standards

Der XTA-Standard wird, wie OSCI, von der Koordinationsstelle für IT-Standards (KoSIT) gepflegt. Wie bereits in Abschnitt 4.1.2 erläutert, sind die beiden Standards auf den Informationsseiten der KoSIT nicht immer eindeutig voneinander getrennt. Es gelten für Aspekte der Bereitstellung von Spezifikationen, Lifecycle-Management und Zugänglichkeit zum Ökosystem analoge Umstände wie bei OSCI, siehe dazu die entsprechenden Unterabschnitte von Abschnitt 4.2.8. Dies äußert sich auch in der teilweise gemischten Bereitstellung von »Hilfsmitteln« für OSCI und XTA.

4.3.8.2 Referenzimplementierungen

Ein in einer vorangegangenen Studie festgestellter Mangel im Bereich XTA ist das Fehlen von Referenzimplementierungen [53, S. 65], sowohl für XTA-Clients als auch für die quelloffene Implementierung eines XTA-Servers. Möglicherweise in Reaktion auf diese Kritik finden sich unter den »XTA-Hilfsmitteln« heute ein Link auf Referenzimplementierungen für XTA-Clients [55]. Die Reife und der Umfang dieser Referenzimplementierungen für die Versionen 3 [40] und 5 [41] ist jedoch nicht klar. Beide Repositories tragen den Hinweis: *»Bei dem vorliegenden Stand der Referenzimplementierung handelt es sich noch um einen Entwurf. Der Quellcode und die Dokumentation sind unvollständig.«* Die letzten Änderungen an diesen Entwürfen stammen vom September beziehungsweise November 2025. Auf eine quelloffene Referenzimplementierung eines XTA-Servers gibt es keine Hinweise.

Eine Anmerkung zu den Repositories⁷ der KoSIT, in denen die Referenzimplementierungen verwaltet werden: Im Rahmen einer transparenten Open-Source-Softwareentwicklung ist es üblich, die Durchführung von Änderungen durch den verantwortlichen Benutzer zu dokumentieren. Für die Referenzimplementierungen sind eine große Anzahl von Git-Commits jedoch einem anonymen Nutzer zugeordnet. Es mag hier das Argument gelten, dass Änderungen unter Kontrolle der KoSIT als Organisation stattfinden, anonyme Commits entsprechen jedoch nicht Best-Practice in Open-Source-Softwareentwicklung.

4.3.8.3 Referenzumgebung

Wie schon in Abschnitt 4.2.8.5 aufgeführt, existiert ein kommerzielles Angebot für die Nutzung einer Referenzumgebung auf Basis des XTA-Servers COM Despina durch die Firma Governikus. Mit ihr kann der Versand und Empfang von XTA-Nachrichten im XMeld-Nachrichtenformat über eine gesicherte OSCI-Transportstrecke getestet werden. *Auch »weitere Standards, die von COM Despina unterstützt werden«* seien auf Anfrage möglich. Diese Beschreibung der kommerziellen Referenzumgebung lässt Zweifel daran, ob sie eine geeignete Basis für die Entwicklung der Transportadapter für einen neuen, noch nicht unterstützten Fachstandard ist. Laut den Webseiten der Firma Governikus wird jedoch nur die XTA-Version 3, nicht die aktuelle XTA-Version 5 unterstützt [42].

4.3.8.4 Konformitätsprüfung

Für die Feststellung von Konformität gelten bei XTA grundsätzlich die gleichen Bedingungen wie bei OSCI. Der Zugang zu der kuratierten Liste konformer Softwareprodukte auf den Seiten der KoSIT erfolgt per Selbsterklärung [29]. Es erfolgt keine Konformitätsprüfung und kein Nachweis ist erforderlich.

Im Gegensatz zu OSCI werden auf den Seiten der KoSIT sogenannte »Konformitätstester« für die XTA-Versionen 3 [51] und 5 [52] bereitgestellt. Der Umfang der durchgeführten Konformitätsprüfung ist nicht unmittelbar klar. In Hinblick auf die Tatsache, dass verbreitete, zentrale XTA-Produkte den XTA-Standard nur unvollständig unterstützen, wird von den Konformitätstestern offensichtlich nur eine Untermenge der Anforderungen des Standards geprüft. In den Konformitätsvorgaben zur Version 3, siehe [56, S. 13], wird klargestellt, dass von den Vorgaben nur die des XTA-Webservices verbindlich sind. Es ist zu vermuten, dass dementsprechend auch nur ein Teil der Vorgaben des XTA-WS-Moduls durch die Konformitätstester abgedeckt wird, nicht jedoch die Anforderungen der XTA-Serviceprofile.

⁷ <https://projekte.kosit.org/transport-public> Abruf 21.07.2026

4.3.8.5 Gründe für Defizite in den Standards OSCI / XTA

Viele der in den Abschnitten 4.2 und 4.3 beschriebenen Defizite in der Gesamtbetrachtung der beiden Standards sind aus Sicht des Autorenteam dieser Studie auf eine fragmentierte und nicht ausreichend ausgestattete Governance der beiden Standards zurückzuführen.

Für die Pflege der Standards ist die KoSIT zuständig, Implementierungen erfolgen zum Teil privatwirtschaftlich getrieben oder im Auftrag der KoSIT für bestimmte Artefakte. Die Infrastruktur wird dezentral gestellt, mit einer losen Zusammenarbeit der Betreiber in der *AG Clearingstellenbetreiber*. Laut Auskunft der KoSIT existierte eine implizite Erwartungshaltung, dass die KoSIT das Management dieser verschiedenen Aspekte übernehmen solle, wofür sie jedoch nie entsprechend personell ausgestattet worden sei. Auch für die vielfach geforderten Standard-Artefakte wie beispielsweise Referenzimplementierungen sei die finanzielle Ausstattung nicht gegeben gewesen.

4.4 FIT-Connect

FIT-Connect ist eine zentrale Plattform zur standardisierten und sicheren Übermittlung von Verwaltungsanträgen in Deutschland. Entwickelt und betrieben wird sie von der FITKO im Auftrag des IT-Planungsrats. FIT-Connect verfolgt das Ziel, Behördenleistungen Ende-zu-Ende (kurz E2E) zu digitalisieren und auch die Prozesse dafür zu unterstützen und zu automatisieren. Prozessunterstützung und Prozessautomatisierung sind jedoch nicht Gegenstand dieser Studie und werden deshalb im Folgenden nicht betrachtet.

4.4.1 Anwendungsbereich

FIT-Connect wurde für die standardisierte und sichere Übermittlung von Verwaltungsanträgen entwickelt. Personen aus der Bürgerschaft und Unternehmen können Anträge über ein OZG-Portal stellen. Das OZG-Portal nutzt dann im Hintergrund FIT-Connect, um die Anträge an die Behörde zu übermitteln. Unternehmen können Anträge aber auch direkt über angebundene ERP-Systeme automatisiert per API an FIT-Connect übermitteln. Die Anträge werden von FIT-Connect an das richtige System zur behördlichen Bearbeitung, im Folgenden Fachverfahren genannt, übermittelt. Das Routing von Anträgen ist eine zentrale Funktionalität von FIT-Connect.

Die Antwort der Behörde kann über unterschiedliche Kanäle erfolgen: über FIT-Connect selbst, über E-Mail (optional auch mit PGP verschlüsselt) oder auch über das Zentrale Bürgerpostfach (ZBP) der BundID. Über diesen Weg können außerdem auch Statusinformationen übermittelt werden. Unternehmen oder andere Behörden können die Statusinformationen über eine Schnittstelle abrufen, was

die Integration der Statusinformationen in ERP-Systeme und Behördensysteme zur Bearbeitung im Fachverfahren ermöglicht [57].

4.4.2 Kommunikationsmodell

Die an die FIT-Connect Plattform angeschlossenen Clients kommunizieren direkt mit der zentralen Plattform. Es gibt keine weiteren Intermediäre oder ähnliche Infrastrukturkomponenten. Das Kommunikationsmodell ist somit ein reines 3-Corner-Modell mit einer zentralen Plattform.

Die Kommunikation bei FIT-Connect erfolgt immer asynchron, das heißt der Antragsteller schickt seinen Antrag an die FIT-Connect Plattform und von dort wird er asynchron vom Fachverfahren abgerufen und bearbeitet. Das Fachverfahren kann dazu entweder Polling verwenden, d. h. es ruft in regelmäßigen Abständen einen Endpunkt auf, der ihm eine Liste mit neuen Anträgen gibt oder es kann einen Callback registrieren, den FIT-Connect dann aufruft, wenn ein neuer Antrag vorliegt. Hierdurch entsteht immer eine kleine Verzögerung, die beim Entwicklungsstand zum Zeitpunkt der Studienrecherche ungefähr 3 bis 5 Sekunden betrug. Laut neuester Information des FITKO-Produktmanagements wurden diese Werte nach Abschluss der Recherchen noch gesenkt. Wie sich die Latenzen in Lastsituationen verhalten, ist jedoch unklar. Daher ist die FIT-Connect-Plattform derzeit noch nicht für Anwendungen geeignet, die eine sehr geringe Latenz benötigen.

Durch das asynchrone Kommunikationsmodell bekommt der Antragsteller kein direktes Feedback, ob das Fachverfahren den Antrag akzeptiert hat oder nicht. In vielen Fällen rufen Fachverfahren die übermittelten Anträge in Zeitabständen von ein oder mehreren Stunden bei FIT-Connect ab. Erst zu diesen Zeitpunkten kann jeweils eine fachliche Prüfung des Antrags erfolgen. Über *Security Event Tokens* (SETs) im Event-Log von FIT-Connect ist jedoch der aktuelle Status und sämtliche Statusänderungen eines Antrags für alle beteiligten Parteien immer nachvollziehbar [58].

Das Event-Log schafft außerdem eine Voraussetzung, um Nichtabstreitbarkeit umzusetzen, da die SETs signiert und mit einem Zeitstempel versehen sind. Der Event-Log ist auch im Fehlerfall wichtig, da eine Analyse von Fehlern bei einer asynchronen Kommunikation oft aufwendiger ist als bei synchroner Kommunikation.

Durch die Pufferung in der Plattform, bedingt durch das asynchrone Kommunikationsmodell, müssen Fachverfahren keine durchgängige Verfügbarkeit sicherstellen. Da Fachverfahren oft von Kommunen in eigener Verantwortung betrieben werden und für eine Antragstellung eine solche Verzögerung im Regelfall kein Problem darstellt, ist die Wahl der asynchronen Kommunikation hier

sinnvoll. Eine synchrone Kommunikation ist bei FIT-Connect derzeit nicht vorgesehen und für das Routing von Anträgen auch nicht notwendig.

4.4.3 Kommunikationsstandards

FIT-Connect verwendet HTTPS als Transportprotokoll. Basierend auf dem HTTPS-Protokoll bietet die Plattform REST-Schnittstellen an. Andere Schnittstellen oder Protokolle, die dem Fachverfahren oder dem OZG-Portal eine eventbasierte Verarbeitung ermöglichen würden (wie zum Beispiel ein Websocket über den eine Nachricht bei Vorliegen eines neuen Antrags gesendet wird), werden nicht angeboten.

FIT-Connect erfordert die E2E-Verschlüsselung der Inhaltsdaten und der Metadaten des Antrags. Daraus ergibt sich automatisch eine strikte Trennung zwischen den E2E-verschlüsselten Daten und den unverschlüsselten Metadaten, die für das Routing und den Transport benötigt werden. Die REST-Schnittstellen sind so gestaltet, dass nur die für das Routing und den Transport an das Fachverfahren notwendigen Daten unverschlüsselt bereitgestellt werden müssen [59]. Dadurch kann es bei FIT-Connect nicht zu einer Vermischung von Inhalts- und Transportdaten kommen. Auch die zum Routing und Transport erforderlichen Metadaten, die nicht der E2E-Verschlüsselung unterliegen, sind zwischen Absender und FIT-Connect Plattform immer transportverschlüsselt.

4.4.4 Schnittstellenstandard

Die REST-Schnittstellen sind mittels OpenAPI dokumentiert und über Swagger-UIs können Endpunkte direkt im Browser ausprobiert werden. Zusätzlich ermöglicht die OpenAPI-Spezifikation, da sie eine in der Praxis sehr häufig verwendete Spezifikation zur Dokumentation von REST-Schnittstellen ist, eine automatische Generierung von Clients für sehr viele Programmiersprachen und Frameworks. Somit ist eine einfache Integration in bestehende Fachverfahren, OZG-Portale und ERP-Systeme möglich. Die OpenAPI Spezifikationen der REST-Schnittstellen sind in öffentlichen Git-Repositories auf dem Gitlab-Server der FITKO abgelegt [60] [61] [62]. Hier kann auch die Weiterentwicklung der Schnittstellen anhand der Git-History nachvollzogen werden.

Die Struktur der Inhaltsdaten kann in FIT-Connect entweder mittels eines JSON-Schemas beschrieben werden oder mittels eines XML-Schemas. Unterstützt werden dabei sowohl FIM-Fachschemata als auch XÖV-Fachschemata [63]. Die Daten können dabei entweder in XML oder in JSON vorliegen. Welches Fachschema für welchen Antrag genau unterstützt wird, legen die zuständigen Fachministerkonferenzen und Gremien fest. Eine Überprüfung der Inhaltsdaten kann durch die FIT-Connect-Plattform selbst nicht erfolgen, da die Daten E2E verschlüsselt sind. Die von FIT-Connect bereitgestellten Client-SDKs enthalten jedoch entsprechende Funktionen, mit denen ein Fachverfahren eine solche Überprüfung selbst

durchführen und fehlerhafte oder unvollständige Anträge nach dem asynchronen Abruf ablehnen kann.

Zusätzlich werden auch Anhänge in Binärformaten wie etwa PDF unterstützt. Diese können eine Größe von bis zu 5 Gigabyte [64] haben, da FIT-Connect mittels *Chunkings* eine Möglichkeit zur Übertragung großer Anhänge in der Plattform und den SDKs umgesetzt hat [65].

Für das Routing von Daten eines bestimmten Typs an die betreffende Behörde gibt es die Möglichkeit, jeweils einen per Self-Service-Portal konfigurierbaren Endpunkt anzulegen. Mit dessen Hilfe kann die Behörde eine eindeutige ID sowie weitere Informationen deklarieren, wie etwa den Leistungsschlüssel der betreffenden Verwaltungsleistung – ehemals Leika-Schlüssel - sowie der akzeptierten JSON- oder XML-Datenschemata ihres an FIT-Connect angebundenen Fachverfahrens. Das antragsende OZG-Portal kann anhand des Leistungsschlüssels der Verwaltungsleistung und des amtlichen Regionalschlüssels der Kommune die zur korrekten Datenaufbereitung und zum Routing erforderlichen Informationen zur Laufzeit bestimmen. Der amtliche Regionalschlüssel kann dabei mit Hilfe von Namen oder Postleitzahl über einen separaten Endpunkt ermittelt werden.

Für jeden Antrag, der über FIT-Connect eingereicht wird, erstellt die FIT-Connect Plattform einen Fall mit einer eindeutigen ID (in der API »Caseld« genannt). Dadurch lässt sich sämtliche Kommunikation, die rund um einen Antrag entsteht, immer eindeutig zuordnen. Auch die rechtssicheren Protokolle über SETs werden immer einer Caseld zugeordnet.

4.4.5 Implementierungen

Für Entwicklerteams von Online-Portalen oder ERP-Systemen und auch für die Entwicklung von Software für Fachverfahren stellt FIT-Connect zusätzlich zu den OpenAPI-Spezifikationen SDKs für Java, JavaScript und .NET bereit. Eine Besonderheit des JavaScript-SDKs ist dessen Fähigkeit, Antragsdaten direkt im Webbrowser zu verschlüsseln. Die SDKs sind außerdem quelloffen. Die Quellcode-Repositories befinden sich auf der Gitlab-Instanz der FITKO in der fit-connect-Gruppe [66].

Bei einem kurzen Test des Java-SDKs im Rahmen der Studie gelang es innerhalb weniger Stunden, mit Hilfe des Schnelleinstiegs, der SDK-Dokumentation und der bereitgestellten Python-Skripte zur Generierung von Self-Signed-Zertifikaten von FIT-Connect einen funktionierenden Prototyp sowohl für einen Onlinedienst also auch für ein empfangendes Fachverfahren in Java zu implementieren und mit Hilfe der frei zugänglichen Testumgebung von FIT-Connect zu testen.

Der Quellcode der FIT-Connect-Plattform selbst (inklusive des Self-Service-Portals) ist nicht quelloffen. Jenseits einer mündlichen Absichtserklärung im Interview

sind dazu keine Planungen in schriftlicher Form auffindbar. Der Entwicklungsprozess ist jedoch transparent, da die Issues und die Boards auf der Gitlab Instanz der FITKO einsehbar sind [67].

Das Self-Service-Portal ermöglicht es Kommunen oder einem von einer Kommune beauftragten IT-Dienstleister ihre Fachverfahren selbstständig anzubinden. Über die Teamfunktionalität können Kommunen auch Accounts für IT-Dienstleister hinzufügen, damit diese die Fachverfahren im Auftrag verwalten können. Für jede Leistung muss die Kommune einen Zustellpunkt im Self-Service-Portal anlegen. Dessen Spezifikation umfasst den Leistungsschlüssel, ein V-PKI Zertifikat für die Verschlüsselung (was im JWK-Format vorliegen muss, siehe Sicherheit), den Regionalschlüssel, die unterstützten Antwortkanäle und die Kontaktdaten der Kommune. Außerdem muss hier konfiguriert werden, ob das Fachverfahren Polling oder Callbacks zum Abruf verwendet. Nach erfolgreichem Anlegen bekommt die Kommune hier die Zugangsdaten für die OAuth2-Authentifizierung mittels Client Credentials Flow für die FIT-Connect REST-Schnittstellen. Für den Produktivbetrieb ist außerdem das Einpflegen der EfA-Parameter in das jeweilige Landesredaktionssystem notwendig. Darüber werden die Daten in das Onlinegateway des Portalverbunds (PVOG) eingespielt und gelangen so zum Routing-Dienst von FIT-Connect. Für die Testumgebung von FIT-Connect ist dieser Schritt nicht notwendig, dort funktioniert das Routing auch ohne Eintrag im PVOG. Auch Betreiber eines OZG-Portals können im Self-Service-Portal von FIT-Connect selbstständig ihr OZG-Portal anbinden. Bei Bedarf bietet FIT-Connect aber auch Support für die Kommunen und OZG-Portal-Betreiber bei der Anbindung an. Außerdem gibt es ein Ticketsystem, wo man Support-Tickets öffnen kann [68].

Einer der befragten Marktteilnehmer mit FIT-Connect-Anbindung und Dienstleistungsangebot für Kommunen berichtete von technischen Herausforderungen und mangelndem Komfort zumindest in früheren Entwicklungsphasen des FIT-Connect-SDKs. Im Einzelnen betraf dies

- mühsame Publikationsprozesse über das PVOG,
- die Inkompatibilität mit dem DVDV,
- eine für Dienstleister zu aufwändige Verwaltung von im Auftrag durchgeführten und gepflegten Fachverfahrensanbindungen,
- Probleme mit der Zertifikatsvalidierung bei auseinanderlaufenden Serverzeiten sowie
- die fehlende Unterstützung von Zertifikaten, die auf elliptischen Kurven basieren.

Im Interview wurde eingeräumt, dass nicht bekannt sei, welche dieser reklamierten Defizite durch aktuelle Versionen von Plattform und SDK inzwischen beseitigt sind.

Vom FIT-Connect Produktmanagement wurden diese Angaben in folgender Weise beantwortet: Das PVOG stelle gewisse Herausforderungen, die jedoch außerhalb des Einflusses von FIT-Connect lägen. Das DVDV sei bezüglich seiner Schnittstellen zumindest in der Aufbauphase von FIT-Connect nicht dazu in der Lage gewesen, die notwendigen Anforderungen zu erfüllen. Deshalb existiere heute in gewissem Maße eine parallele Verzeichnisdienstinfrastruktur für OSCI- und FIT-Connect-Transport. Probleme mit der Zeitbasis bei der Zertifikatsüberprüfung seien adressiert worden und derzeit kein Problem mehr. Bezüglich der akzeptierten Zertifikate sei es die technische Strategie gewesen, keine große Vielfalt von Zertifikatstechnologien zu unterstützen, sondern nur RSA-Zertifikate. Ansonsten würden hier die Vorgaben des BSI beachtet.

Bezüglich zu aufwändiger Auftragsverwaltung der Fachverfahrensanbindungen und Konfiguration von Kommunikationsendpunkten für Kommunen wurde von Seiten des FIT-Connect-Produktmanagements widersprochen: Das Self-Service-Portal werde permanent ausgebaut und biete schon aktuell eine breite Unterstützung sogenannter Teamfunktionen, mit denen Kommunen den Dienstleistern entsprechende Berechtigungen einräumen könnten. Für diese Verwaltungsfunktionen stünden auch APIs statt nur Portalfunktionen zur Verfügung.

Im Rahmen dieser Studie war es nicht möglich, diese Themen näher zu untersuchen und zu bewerten.

4.4.6 Infrastruktur

Die Plattform von FIT-Connect wird zentral im Auftrag der FITKO gehostet, das heißt es gibt derzeit nur eine zentrale Produktivinstanz für ganz Deutschland. Dadurch werden Kommunen entlastet, da sie sich nicht selbstständig um den Betrieb von Komponenten für FIT-Connect kümmern müssen. Laut Aussage im Interview ist die Plattform Cloud-native entwickelt, das heißt sie ist für den Betrieb in einer Cloud-Infrastruktur mit dynamischer Skalierung und Managed Services ausgelegt.

Die Nutzung der zentralen FIT-Connect-Plattform ist kostenlos für Kommunen, da die Kosten vom Bund und den Ländern getragen werden. Bundesländer können die Kommunen über eine Umlage an ihren Kosten für FIT-Connect beteiligen. Das ist jedoch von Bundesland zu Bundesland unterschiedlich. Für das benötigte V-PKI-Zertifikat entstehen Kosten, die von der Kommune getragen werden müssen.

FIT-Connect gibt jährlich eine neue Major-Version seiner Schnittstellen frei, die potenziell nicht abwärtskompatible Änderungen enthält [69]. Die alte Version der Schnittstellen wird danach noch ein Jahr unterstützt. Für die spätestens alle zwei Jahre notwendigen Aktualisierungen des Fachverfahrens mit den notwendigen Anpassungen der FIT-Connect Anbindung benötigt die Kommune einen im Regelfall kostenpflichtigen Wartungsvertrag mit dem Hersteller des Fachverfahrens.

4.4.7 Sicherheit

Unternehmen und Behörden nutzen das Elster-Unternehmenskonto, um sich im FIT-Connect Self-Service-Portal zu authentifizieren. Für IT-Dienstleister von Kommunen kann die Kommune ein Konto mit Passwort und zweitem Faktor (PIN) einrichten. Da die Mitarbeitenden von IT-Dienstleistern, die die Kommunen betreuen, im Regelfall keinen Zugriff auf ihr eigenes Elster-Unternehmenskonto haben, stellt dieser Weg eine gute praxisorientierte Lösung dar.

Da die FIT-Connect-Plattform nicht dafür gedacht ist, von der Bürgerschaft direkt verwendet zu werden, bietet sie keinen eigenen Service für die Identifikation des Antragstellers an. Stattdessen sieht sie vor, dass OZG-Portale elektronische Identitätsdaten einer Person auf anderem Weg beziehen. Diese Informationen werden dann in den verschlüsselten Metadaten des Antrags mitgeschickt.

Die Daten des Antrags, die Metadaten und auch über FIT-Connect übermittelte Antworten müssen E2E-verschlüsselt werden. Damit sind sie für den Betreiber der Plattform selbst nicht einsehbar. Nur die für das Routing notwendigen Metadaten liegen unverschlüsselt vor. Mit Hilfe des JavaScript-SDKs von FIT-Connect kann die Verschlüsselung der Antragsdaten und der nicht für das Routing benötigten Metadaten direkt im Browser des Antragstellers vorgenommen werden. Deshalb bietet FIT-Connect trotz der zentral betriebenen Plattform ein sehr hohes Datenschutzniveau.

FIT-Connect verwendet JSON Web Encryption (JWE) und Zertifikate der V-PKI zur E2E-Verschlüsselung der Antragsdaten, Metadaten und Antworten. Gemäß den Vorgaben von FIT-Connect sind dabei folgende Algorithmen zu verwenden [70]:

- Symmetrische Verschlüsselung: AES-256 mit Galois/Counter-Mode (GCM) gemäß der Empfehlung des BSI [33]
- Asymmetrische Verschlüsselung: RSA-OAEP-256 (RSA mit Optimal Asymmetric Encryption Padding (OAEP) unter Verwendung der Mask Generation Function MGF1 und der Hashfunktion SHA-256) gemäß der Empfehlung des BSI [33]. Hierbei wird in der FIT-Connect-Dokumentation jedoch auf einen Abschnitt referenziert, der in der aktuellen Version des Dokuments des BSI nicht mehr existiert. Außerdem empfiehlt das BSI in der aktuellen Version des

Dokuments auf quantensichere Algorithmen umzusteigen oder den Umstieg darauf vorzubereiten. Im Interview wurde darauf hingewiesen, dass FIT-Connect diesen Punkt bereits adressiert.

- Außerdem muss für die Inhaltsdaten und jeden Anhang jeweils ein SHA-512-Hash erzeugt und in den Metadaten mitgesendet werden, sodass der Empfänger überprüfen kann, dass die Daten vollständig und unverändert angekommen sind. Das entspricht dem aktuellen Stand der Technik. Auch die optionalen digitalen Signaturen können in den Metadaten übertragen werden. Es ist aber auch möglich, diese direkt in den Inhaltsdaten zu übertragen. Sofern die Signatur eingebettet im Inhalt übertragen wird, ist ein entsprechendes Flag in den Metadaten zu setzen, damit das Fachverfahren weiß, dass es die Signatur in den Inhaltsdaten prüfen sollte.

Die Nutzung von JWE bei FIT-Connect erfordert jedoch die Umwandlung der Zertifikate der V-PKI, die zur Verschlüsselung verwendet werden, in JSON-Web-Keys (JWKs). Das kann mit Hilfe eines Tools von FIT-Connect gemacht werden, ist jedoch mit Arbeitsaufwand für die zuständige Person innerhalb der Kommune oder beim IT-Dienstleister verbunden, da die Umwandlung nicht nur bei der Erstellung, sondern auch bei jedem Erneuern des Zertifikats erforderlich ist.

Auf Grund der E2E-Verschlüsselung kann die FIT-Connect-Plattform keinen Virensan der Inhaltsdaten oder der verschlüsselten Metadaten durchführen [71]. Die Verantwortung hierfür liegt bei den Betreibern der angebundenen Systeme (Web-Portale, ERP-Systeme und Fachverfahren), da diese die Daten im Klartext vorliegen haben. Dies entspricht den Vorgaben der BSI-Richtlinie TR-03172 Porttalverbund [72].

FIT-Connect verwendet OAuth Access Tokens in Form von JWTs für die Authentifizierung der Clients gegenüber der REST-Schnittstellen. Dabei wird ausschließlich Edwards-curve Digital Signature Algorithm (EdDSA) mit SHA-512 und Ed25519 zum Signieren der Tokens verwendet. Das entspricht dem aktuellen Stand der Technik.

Die Option, eine PGP-verschlüsselte Mail als Antwortmöglichkeit in den Metadaten zu spezifizieren, ist sehr sinnvoll für den G2C-Fall, jedoch eher ungeeignet für den B2G-Fall, da im Geschäftsumfeld eher S/MIME als PGP zur Mailverschlüsselung eingesetzt wird.

Bei Nutzung von Polling zum Abruf von Anträgen muss für das Fachverfahren bei der Nutzung von FIT-Connect kein Port freigegeben werden, über den das Fachverfahren im Internet zu erreichen ist. Allerdings muss das Fachverfahren frei mit dem Internet kommunizieren können, da sich die statischen IP-Adressen der FIT-Connect-Plattform ändern können [73]. Daher ist hier kein Whitelisting von IP-Adressen möglich, sondern es müssen entweder alle im Internet öffentlich

erreichbaren IP-Adressen freigegeben werden oder es muss ein Whitelisting auf Ebene der Subdomänen erfolgen, was jedoch nicht von allen Firewalls unterstützt wird. Das stellt ein gewisses Sicherheitsrisiko dar.

Die Nutzung von Webhooks oder HTTP-Callbacks setzt voraus, dass der entsprechende Endpunkt im Internet zu erreichen ist. Auch hier kann die Firewall kein Whitelisting vornehmen, da FIT-Connect keine Angaben macht, von welchen IP-Adressen aus die Webhooks aufgerufen werden.

Im Gegensatz zu nicht von FIT-Connect unterstützten Techniken wie Long-Polling oder Websockets sind Webhooks für die Administration von IT-Sicherheit weniger komfortabel und sicher zu handhaben (siehe auch Abschnitt 2.6.6). Im Interview wurde bezüglich dieser Kritik geäußert, dass für die asynchronen Szenarien der Antragsübermittlung für diese Techniken kein Bedarf bestanden habe. Eine Erweiterung auf Long Polling sei jedoch angedacht und werde zukünftig eingeplant.

Als Infrastruktur mit zentralem Aufbau erfordert FIT-Connect – im Gegensatz zu einer eher dezentralen Struktur wie bei OSCI – für den flächendeckenden Einsatz ein Resilienzkonzept, das sowohl Schutz gegen technische Störungen als auch gegen Angriffe wie etwa DDoS bietet. Laut Auskunft der interviewten Personen bietet die derzeit existierende Infrastruktur noch keine dafür geeignete (Geo-)Redundanz oder eine ausreichende Angriffserkennung und -abwehr. Diese Themen seien noch anzugehen. Ein Skalierungskonzept mit Anforderungen an einen hochverfügbaren Betrieb existiert zwar bereits, jedoch wurde hier der Aspekt der Abwehr von Angriffen nicht berücksichtigt [74].

4.4.8 Governance

Die FIT-Connect-Plattform und die SDKs werden von einem Produkt-Team bei der FITKO entwickelt und bereitgestellt. Dieses Team ist gleichzeitig für die REST-Schnittstellen verantwortlich, sodass hier kein Bruch zwischen Standard und Implementierung entsteht. Die zentrale Plattform vereinfacht außerdem das Durchsetzen von organisatorischen und technischen Maßnahmen zu verschiedenen Aspekten, wie zum Beispiel dem Datenschutz. Auch ist die Zuständigkeit klar geklärt, da die Steuerung der Softwareentwicklung von APIs, SDK und Plattform sowie der Aufbau der Infrastruktur an einer Stelle bei der FITKO zusammenläuft.

Die Finanzierung von FIT-Connect wird größtenteils vom Bund übernommen [75]. Die Steuerung des FIT-Connect-Produkts erfolgt durch den Bund und die Länder Baden-Württemberg, Thüringen, Sachsen-Anhalt und Hamburg.

In der openCode-Gitlab-Gruppe für FIT-Connect gibt es ein offenes Feedback-Repository, wo Fehler gemeldet und Verbesserungsvorschläge eingebracht

werden können, indem man ein GitLab-Issue erstellt [76]. Allerdings wurde diese Möglichkeit erst während der Erstellung der vorliegenden Studie geschaffen.

4.5 NOOTS

Das *Nationale Once-Only Technical System* (NOOTS) ist die nationale Ausprägung des europäischen Once-Only Technical Systems (EU-OOTS), einer digitalen Infrastruktur für den grenzüberschreitenden sicheren Austausch von Nachweisen zwischen Behörden.

4.5.1 Anwendungsbereich

Die Rolle des NOOTS bei der Digitalisierung der öffentlichen Verwaltung regelt der NOOTS-Staatsvertrag [77]. Der Staatsvertrag verfolgt das Ziel, ein gemeinsames, flächendeckendes informationstechnisches System zu etablieren, das perspektivisch den gesamten Datenaustausch zwischen öffentlichen Stellen automatisiert und damit eine reibungslose und kostengünstige Verwaltungsarbeit ermöglichen soll. In Paragraf 1 des Staatsvertrags wird konkretisiert, dass dieses System dem nationalen und grenzüberschreitenden Abruf und der Übermittlung von Nachweisen und Daten durch öffentliche Stellen zur Erfüllung öffentlicher Aufgaben dient.

Zunächst soll das Once-Only-Prinzip für Verwaltungsleistungen nach dem Onlinezugangsgesetz umgesetzt werden. Dabei wird NOOTS eingesetzt, um bei Antragstellungen erforderliche Nachweise, die den Behörden bereits vorliegen, automatisch zu beschaffen und dem Antrag beizufügen, ohne dass der Antragsteller sich um die Nachweisführung gesondert kümmern muss. Die weitere Nutzung des Systems wird durch den IT-Planungsrat nach Maßgabe des NOOTS-Staatsvertrags gesteuert.

NOOTS schafft die Voraussetzungen dafür, dass Behörden ihre Daten digital und sicher miteinander austauschen können, indem Register und Onlinedienste der Verwaltung an das NOOTS angeschlossen werden. Dies ermöglicht den rechtskonformen Abruf elektronischer Nachweise aus Registern der deutschen Verwaltung. Ein Datenabruf erfolgt dabei ausschließlich dann, wenn Personen und Unternehmen dem ausdrücklich zustimmen, was einen datenschutzkonformen Nachweisabruf ermöglicht.

Seit Ende 2025 ist eine erste Version des NOOTS verfügbar, und zum Zeitpunkt der Studie gibt es bereits Pilotanwendungen. Bis Ende 2028 müssen zudem die in Anlage 1 des ID-Nummerngesetzes (IDNrG) definierten Register an das Identitätsdaten-Abrufverfahren (IDA) und das Datenschutzcockpit (DSC) angeschlossen werden; gemäß dem NOOTS-Staatsvertrag sind diese Register darüber hinaus auch an das NOOTS anzubinden.

4.5.2 Kommunikationsmodell

Das NOOTS-Konzept strebt als Fernziel im Grundsatz eine möglichst datenzentrierte Austauschplattform für Behördeninformationen an. Statt prozess- oder fachverfahrensspezifische Kommunikationslösungen zu schaffen, soll NOOTS vor allem eine grundlegende Abstraktion bereitstellen: einen vertraulichen, integritätsgeschützten Kanal, dessen Endpunkte eine abstrakte Berechtigungsprüfung erfolgreich durchlaufen haben. Welche spezifischen Transaktionen dann über diesen Kanal abgewickelt werden, ist Sache der Endpunkte. Wenn eine sichere Transportverbindung etabliert ist, tritt NOOTS bewusst in den Hintergrund und überlässt verfahrensspezifische Besonderheiten – zum Beispiel Zustellnachweise – den involvierten Kommunikationspartnern. Diese Entwurfsphilosophie soll dazu beitragen, zentrale Performance- oder Verfügbarkeits-Engpässe zu vermeiden und die Transportschicht nicht zu überfrachten.

Die NOOTS-Architektur beruht auf dem 4-Corner-Modell. Die *nachweisbeantragende Stelle* (Corner 1 – Data Consumer) ist mittels eines *Sicheren Anschlussknotens* (Corner 2 – SAK) an die NOOTS-Infrastruktur angekoppelt. Der SAK fungiert als Sender. Er nimmt die Anfrage des Data Consumers (DC), also des Autors der Anfrage entgegen, ermittelt über Anfragen bei den zentralen Diensten der NOOTS-Infrastruktur das zuständige Register und leitet die Anfrage dorthin weiter. Der SAK, über den das Register an das NOOTS angeschlossen ist (Corner 3) dient als Empfänger des Nachweisabrufs. Er nimmt die Anfrage entgegen und stellt sie nach einer Prüfung dem Leser der Anfrage (Corner 4 – Data Provider), also dem nachweisführenden Register, bereit. Der Data Provider (DP) prüft die formale Korrektheit und Rechtmäßigkeit der Anfrage anhand der vom SAK übermittelten Token und Metadaten. Bei positivem Prüfergebnis liefert der DP den gewünschten Nachweis auf dem umgekehrten Weg – also DP → DP-SAK → DC-SAK → DC – an die anfordernde Stelle zurück. Abbildung 11 zeigt den grundlegenden Ablauf eines Nachweisabrufs.

Das NOOTS ist für fachlich *synchrone* Nachweisabrufe ausgelegt. Ein fachlich *asynchroner* Nachweisabruf, bei dem der Nachweis nicht sofort vom Data Provider bereitgestellt werden kann, wird durch einen erneuten Abruf (Retry) realisiert. Das entsprechende Nachrichtenmuster zeigt Abbildung 12.

Für den Anschluss an das europäische OOTS stellt NOOTS eine zentrale Intermediäre Plattform bereit [78] [79] [80], die wie alle sonstigen Data Consumer und Data Provider über einen SAK an NOOTS angeschlossen ist. Dieser Intermediär fungiert für nationale Anfragen ins europäische Ausland als Data Provider gegenüber der anfragenden nationalen Stelle und als Data Consumer gegenüber dem europäischen Register; für Registeranfragen europäischer Partner fungiert er als Data Consumer gegenüber dem angefragten nationalen Register und als Data Provider gegenüber dem anfragenden europäischen Partner.

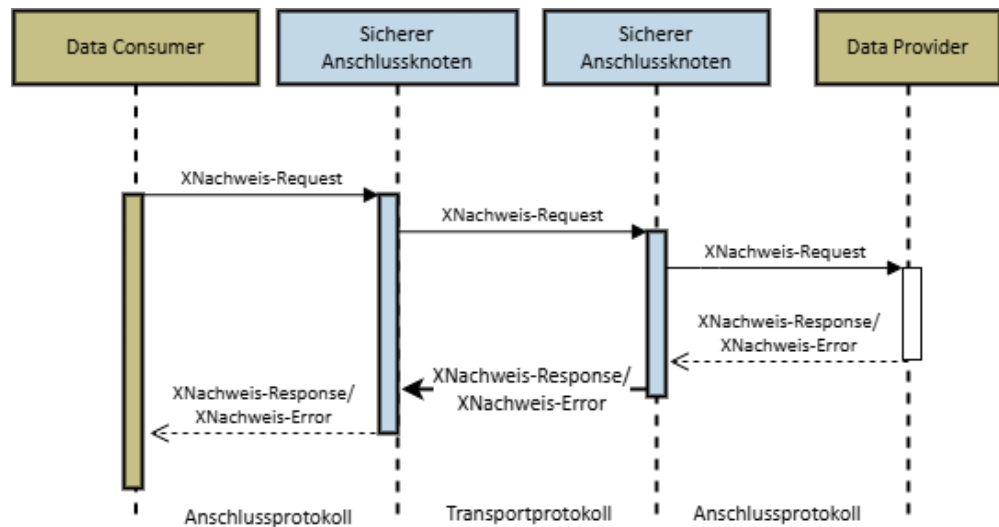


Abbildung 11 Nachrichtmuster Request-Response/Sync für fachlich synchronen Nachweisabruf [81]

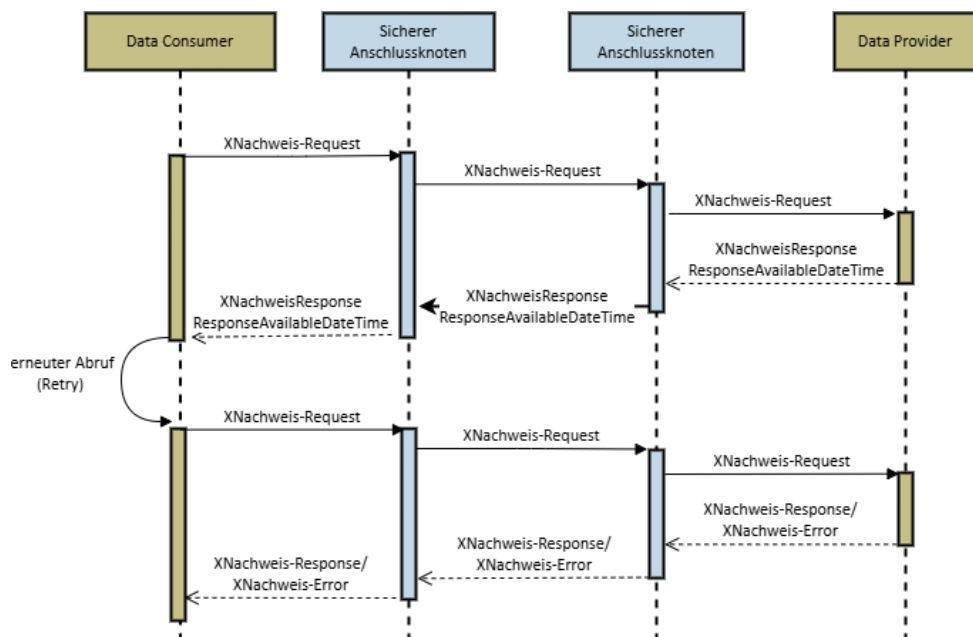


Abbildung 12 Nachrichtmuster Request-Response mit erneutem Abruf [81]

Technisch umfasst das NOOTS folgende wesentliche Elemente [82]:

- den Sicheren Anschlussknoten (SAK) [83], um teilnehmende Data Consumer (DC) und Data Provider (DP) sicher und nach einheitlichen Standards an das

NOOTS anzuschließen, um gesetzliche und sicherheitsrelevante Vorgaben zu erfüllen und insbesondere die abstrakte Berechtigungsprüfung durch die Vermittlungsstelle [84] bei jedem Nachweisabruf mit Identifikationsnummern zu gewährleisten,

- die Intermediäre Plattform (IP) [78] als bidirektionale Verbindung zum EU-OOTS,
- zentrale Komponenten, die für die Navigation, Authentisierung und Autorisierung benötigt werden:
 - Registerdatennavigation (RDN) [85] zur Ermittlung des zuständigen DP,
 - Vermittlungsstelle (VS) [84] für die abstrakte Berechtigungsprüfung, ob ein Nachweisabruf von einem Data Consumer bei einem Data Provider zu einem gegebenen Zweck zulässig ist,
 - Datenmanagementsystem (DAMAS) für die Datenpflege der NOOTS-Komponenten IAM, RDN und VS,
 - Identity- und Accessmanagement für Behörden (IAM-B) [86] für die Zuordnung und zum Abruf berechtigungsrelevanter Informationen für Zugriffe auf Ressourcen gemäß rechtlichen Vorgaben,
 - Identity Management für Personen (IDM-P) [87] für die Bereitstellung der Identifikationsnummer (IDNr) und weiterer Basisdaten natürlicher Personen,
 - Identity Management für Unternehmen (IDM-U) [88] für die Bereitstellung einer eindeutigen Identifikation von Unternehmen anhand einer bundeseinheitlichen Wirtschaftsnummer (beWiNr).⁸

Darüber hinaus benötigt NOOTS den Zugriff auf eine geeignete Public-Key-Infrastruktur, wie etwa die Verwaltungs-PKI (V-PKI) für Schlüsselmateriale und Zertifikate.

4.5.3 Kommunikationsstandard

DC und DP erreichen ihren jeweiligen SAK über eine REST-Schnittstelle. Als Kommunikationsstandards dient Mutual TLS (mTLS), also eine verschlüsselte und gegenseitig authentifizierte HTTP-Verbindung.

Was das Transportprotokoll zwischen den Anschlussknoten betrifft, so wurden mehrere technische Alternativen für den Datenaustausch geprüft und von den Fachgremien des BVA aus unterschiedlichen Gründen verworfen (siehe [89], Anhang B):

⁸ Die Umsetzung des IDM-U wurde mit Beschluss vom Januar 2025 [88] bis auf Weiteres zurückgestellt

- Eine Einführung zusätzlicher Transportknoten, die als Intermediäre den Nachrichtentransport zwischen SAKs steuern, war in früheren Architekturentwürfen [89] ursprünglich vorgesehen, wurde aber im Zuge der Weiterentwicklung des NOOTS-Konzepts verworfen. Die Transportknoten sollten insbesondere den Übergang zwischen unterschiedlichen Verwaltungsnetzen ermöglichen. Da NOOTS aber bis zur Verfügbarkeit eines umfassenden Informationsverbund der öffentlichen Verwaltung (IVÖV-Netz) aus Zeit- und Komplexitätsgründen eine Vernetzung der SAKs über das Internet vorsieht, konnten die intermediären Transportknoten entfallen [81].
- Direkte Punkt-zu-Punkt-Verbindungen (REST/SOAP) erfüllen die Anforderungen an IT-Sicherheit, Prüffunktionen und Robustheit nicht. Sie würden die Verantwortung und den Aufwand für Authentifizierung, Autorisierung und Verschlüsselung dem DC und DP aufbürden, was sehr aufwändig und unzuverlässig wäre.
- Der Aufbau einer X-Road-, eDelivery-AS4-, FIT-Connect- oder ZPS-Elster-Infrastruktur deckt nach der Einschätzung in [89], Anhang B die spezifischen nationalen NOOTS-Anforderungen (insbesondere rechtliche Vorgaben, Integration zentraler NOOTS-Komponenten, Zero-Trust und IT-Sicherheit) nur unzureichend oder zu fachspezifisch ab.
- Die ausschließliche Nutzung der bestehenden OSCI / XTA-Infrastruktur würde nach Einschätzung des BVA (siehe [89], Anhang B) zu erheblichen Verzögerungen und höheren Betriebskosten führen, und die Weiterentwicklung der Basiskomponente Nachweisabruf (BKN) wurde vom BMI eingestellt.

Da bei der Prüfung vorhandener Alternativen keines der gängigen Transportprotokolle das uneingeschränkte Placet des BVA erhalten hat, ist die endgültige Festlegung auf einen verbindlichen Transportstandard in NOOTS nicht abschließend geklärt; theoretisch wäre es auch denkbar – wenn auch nicht wünschenswert – dass der SAK mehrere Transportprotokollvarianten unterstützt. Da sich alle NOOTS-Teilnehmer verpflichtend via SAK an NOOTS ankoppeln müssen, ist eine Änderung der Transportschicht möglich, ohne dass Data Consumer oder Data Provider von der Änderung betroffen wären, vorausgesetzt, die Schnittstelle zwischen SAK und Kommunikationsendpunkt bleibt unangetastet.

Derzeit tauschen die SAK ihre Nachrichten mittels mTLS aus, wobei als Transportnetz das Internet genutzt wird. Das Routing der Nachrichten zur Gegenstelle übernimmt dabei das Internet-Protokoll.

Langfristig ist geplant, ein geschlossenes deutsches Behördennetz aufzubauen, den »Informationsverbund der öffentlichen Verwaltung« (IVÖV). Bis dieser Informationsverbund bereitsteht und alle Behörden daran angeschlossen sind, wird es jedoch noch mehrere Jahre dauern. Sobald der IVÖV verfügbar ist, soll die

NOOTS-Kommunikation durch Austausch der SAK darauf umgestellt werden, ohne dass DC oder DP angepasst werden müssen.

4.5.4 Schnittstellenstandards

Data Consumer und Data Provider nutzen die Consumer- beziehungsweise Provider-Anwendungsschnittstelle des SAK-Anschlussprotokolls, um gemäß den Nachweisabrufprozess des NOOTS Nachweise bereitzustellen. Dieses synchron arbeitende Protokoll ist zustandslos und folgt dem Stil eines *Remote Procedure Calls* (RPC). Es basiert auf *Representational State Transfer* (REST) und verwendet HTTPS als Transportmedium, unterstützt durch zusätzliche HTTP-Header-Attribute zur Übermittlung von Metainformationen.

Der jeweils aktuelle Arbeitsstand der APIs für Data Consumer und Data Provider findet sich in [90] als OpenAPI-Spezifikation. Die *README*-Datei dieser Quelle weist allerdings ausdrücklich darauf hin, dass die vorliegende Spezifikation nur den aktuellen Arbeitsstand darstellt, der als Grundlage für fachliche und technische Reviews dient, aber nicht für die Implementierung in Umsetzungsprojekten vorgesehen ist.

Das NOOTS nutzt für Registerabfragen *XNachweis*, einen XML-Standard der öffentlichen Verwaltung (XÖV) [91]. Der Standard wird durch das Bundesverwaltungsamt (BVA) herausgegeben und im Auftrag des BVA durch die KoSIT betrieben.

XNachweis ist ein Standard für die fachunabhängige Anforderung und Übermittlung von Nachweisen zu Personen und Unternehmen. Mittels XNachweis werden nationale Verwaltungsportale, registerführende wie auch weitere öffentlichen Stellen an das nationale (NOOTS) und das europäischen Once Only Technical System (EU-OOTS) angebunden. Der Standard ist interoperabel mit den europäischen Spezifikationen (EU-Technical Design Documents, kurz EU-TDD) der EU-Verordnung 2018/1724 (SDG-VO) und gleichzeitig ausgerichtet auf die spezifischen Anforderungen eines nationalen OOTS [91].

Die Transportinfrastruktur unterstützt das synchrone Request-Response-Nachrichtenaustauschmuster, wie es in der *Once-Only Technical System High Level Architecture* (EU-OOTS) Referenzarchitektur beschrieben ist. Dieses Nachrichtenaustauschmuster ermöglicht zum Beispiel sofortige Previews von Nachweisdaten in nationalen Onlinediensten.

4.5.5 Implementierungen

Die Konzepte für das NOOTS betrachten derzeit im Wesentlichen nur die Aspekte, die für den Registerdatenabruf relevant sind, da weitere Anwendungsszenarien noch nicht genauer ausgearbeitet worden sind.

Der SAK wird vom Bundesverwaltungsamt als eigenständige, perspektivisch mandantenfähige⁹ Komponente bereitgestellt, die als Java-Anwendung oder in einem OCI-konformen Container betrieben wird [83]. Der SAK stellt seine Funktionen als REST-Services auf Basis von Open-API bereit [90] [92]. Anders als eine SDK-Lösung wie etwa bei FIT-Connect bietet dies eine Programmiersprachen-unabhängige Schnittstelle für die angeschlossenen Systeme und ermöglicht zentral bereitgestellte Updates der SAK-Software. Obwohl der SAK zentral bereitgestellt wird, erfolgt der Betrieb dezentral durch die NOOTS-Teilnehmer.

Der SAK unterstützt ausschließlich den Abruf von Nachweisdaten und den entsprechenden Datenaustausch. Der aktive Versand oder Austausch anderer Daten ist derzeit noch nicht vorgesehen [83].

Was die oben genannten zentralen Komponenten des NOOTS betrifft, so ist deren Entwicklung noch nicht abgeschlossen. Zwar ist das NOOTS gemäß der *zentralen Wissensplattform der Registermodernisierung* [93] seit Ende 2025 in einer ersten Version verfügbar und seit 2026 gibt es erste Pilotanwendungen, aber Kernkomponenten wie RDN, DAMAS, VS, IDM-P, IDM-U sind derzeit noch unvollständig oder wurden noch gar nicht realisiert. Zur Umsetzung der Pilotprojekte musste daher auf provisorische Teil- oder Zwischenlösungen zurückgegriffen werden.

4.5.6 Infrastruktur

Zukünftige NOOTS-Teilnehmer betreiben ihre Online-Dienste, Fachverfahren und Register teils lokal auf eigenen Serversystemen, teils in klassischen Rechenzentrums-Umgebungen oder in DVC-konformen VerwaltungscLOUDs. Der SAK ist deshalb sowohl auf herkömmlichen Serverplattformen als auch als Container in Cloud-Infrastrukturen einsetzbar. Diese technische Offenheit soll es ermöglichen, bestehende Systeme schrittweise an NOOTS anzubinden, ohne grundlegende Infrastrukturentscheidungen revidieren zu müssen.

Die Funktionsfähigkeit des NOOTS ist von der Verfügbarkeit und dem korrekten Verhalten der zentralen Komponenten (z. B. VS, RDN, IAM, IDM-P) abhängig. Fällt eine dieser Komponenten aus oder wird kompromittiert, so könnte damit im äußersten Fall der bundesweite Registerdatenabruf außer Funktion gesetzt werden. Es ist daher essenziell, die zentralen NOOTS-Komponenten hochverfügbar (d. h. mit ausreichender Redundanz) und hochsicher (d. h. in einer besonders gehärteten, eng überwachten Umgebung) zu realisieren, um gegen Angriffsversuche gewappnet zu sein.

⁹ Zum Zeitpunkt unserer Interviews war die Mandantenfähigkeit offenbar noch nicht realisiert.

4.5.7 Sicherheit

Der SAK ist ein zentraler Baustein zur Erfüllung der Sicherheitsanforderungen auf nationaler Ebene. Insbesondere übernimmt er folgende Funktionen, um die angeschlossenen Kommunikationsendpunkte zu entlasten [94] [95] [96]:

- Verschlüsselung und Entschlüsselung von Nachrichten (neben der Transportverschlüsselung mittels mTLS sieht das NOOTS-Konzept eine zusätzliche Verschlüsselung der Inhaltsdaten vor, um Transportverbindungen gegebenenfalls aufbrechen und umverschlüsseln zu können.)
- Beschaffung der erforderlichen Authentisierungs- und Autorisierungstoken von der Vermittlungsstelle (durch den SAK-DC senderseitig)
- Prüfung der strukturellen Integrität der Nachrichten
- Durchführung der abstrakten Berechtigungsprüfung durch Validierung der vom SAK-DC gesendeten Token (SAK-DP empfängerseitig)
- Prüfung der Virenfreiheit von Nachrichten
- Zertifikat- und Schlüsselmanagement

Ungeachtet dieser Security-Prüfungen ist der Data Provider gehalten, die Berechtigung jeder eingehenden Anfrage selbst noch einmal zu prüfen (»konkrete Berechtigungsprüfung«), wobei der DP im Gegensatz zum SAK auch den Nachrichteninhalte als Prüfkriterium heranziehen kann. Neben der abstrakten Berechtigung des Abrufs, die schon der SAK validiert hat, ist so auch eine weitergehende fachliche und technische Berechtigungsprüfung möglich.

Durch die Transportverschlüsselung mittels mTLS ist gewährleistet, dass Nachrichten niemals im Klartext übermittelt werden und dass die jeweiligen Kommunikationsendpunkte authentisch sind, sowohl bei der Übertragung zwischen DC oder DP und ihrem jeweils zuständigen SAK als auch beim Transport zwischen SAK-DC und SAK-DP. Die zusätzlich geforderte Verschlüsselung des Nachrichteninhalts sorgt außerdem dafür, dass die übertragenen Inhalte auch bei einem möglichen Routing über segmentierte Verwaltungsnetze (z. B. einem künftigen IVÖV), bei denen potenziell Gateways oder Intermediäre zu passieren und die Nachrichten daher umzuverschlüsseln wären, vertraulich bleiben.

Allerdings ist die Vertraulichkeit innerhalb eines SAK nicht gewährleistet, da die Nachrichten dort im zur Prüfung im Klartext vorliegen. Deshalb ist es für die Sicherheit des NOOTS wichtig, dass SAKs nur von vertrauenswürdigen IT-Personal und in sicheren Umgebungen betrieben werden. Da Behörden den IT-Betrieb oft an Dienstleister auslagern, ist die Auswahl und die Beaufsichtigung der Dienstleister im NOOTS von besonderer Bedeutung.

Die Ende-zu-Ende-Verschlüsselung endet zudem im SAK und wird nicht bis zum Data Consumer oder Data Provider durchgereicht [96]. Dies entbindet DC und DP von Kryptooperationen und einem aufwändigen Schlüsselmanagement – insbesondere mit Blick auf Gruppenschlüssel und Vertretungsregelungen – und gewährleistet einheitliche kryptografische Mindeststandards. Andererseits schwächt es die Vertraulichkeit der Verarbeitungskette.

Der Datenaustausch findet auf nationaler Ebene ausschließlich zwischen den SAKs von Data Consumer und Data Provider statt, ohne zwischengeschaltete Intermediäre, wie es ursprünglich erwogen wurde. Dadurch bleiben Verfügbarkeitsprobleme und Sicherheitsvorfälle jeweils auf die am betroffenen SAK angeschlossenen Teilnehmer begrenzt, was die Resilienz des Gesamtsystems erhöht [92]. Sollte das NOOTS künftig nicht mehr das Internet, sondern einen geschlossenen behördlichen Informationsverbund mit abgeschotteten Netzsegmenten nutzen, könnten Intermediäre wieder ins Spiel kommen, um das Routing zwischen DC und DP zu vereinfachen oder Netzsegmentgrenzen zu überwinden. Die Resilienz des NOOTS wäre dann neu zu bewerten.

Im Gegensatz etwa zu OSCI / XTA sieht das NOOTS-Konzept keine ausdrückliche Unterstützung für Zustellnachweise vor. Synchrone Registerabfragen benötigen keinen solchen Mechanismus, aber in anderen Verwaltungskontexten, bei denen strenge gesetzliche Fristen einzuhalten sind oder die Zustellung von Informationen rechtssicher nachgewiesen werden muss, besteht ein Bedarf, die Nichtabstreitbarkeit von Nachrichten einschließlich der Nachrichten-Metadaten (z. B. Zeitstempel, Autor und Leser) zu Gewährleisten. Sofern das NOOTS perspektivisch als universelles Transportsystem für Verwaltungsdaten dienen soll, müssen entsprechende Mechanismen entweder in das NOOTS integriert werden, oder die Fachanwendungen selbst müssen geeignete Nachweise bereitstellen, etwa als Attribute des verwendeten XÖV-Standards. Zu klären wäre dann jedoch, wie solche Nachweise verwaltet und allen Bedarfsträgern auch nach Abschluss Verwaltungstransaktion zugänglich gemacht werden können.

Ein wichtiger Aspekt des NOOTS ist die Nachvollziehbarkeit von Registerabrufen im Sinne des Auskunftsrechts gemäß der Datenschutzgrundverordnung. Alle angeschlossenen Register müssen daher auch eine Schnittstelle zum Datenschutzcockpit (DSC) bereitstellen. Das DSC soll es der Bürgerschaft ermöglichen, sich über alle sie betreffenden Registeranfragen zu informieren. Anhand ihrer IDNr kann jede Person anfragen, welche Register in einem gegebenen Zeitraum Auskünfte über diese Person erteilt haben und an wen.

Eine Befragung der NOOTS-Fachleute im Rahmen dieser Studie hat allerdings ergeben, dass die Realisierung des DSC in seiner derzeitigen Form nicht wirklich praktikabel ist. Das Cockpit-Konzept – und mutmaßlich auch die Schnittstellen und Protokolle zur Erfassung und Bereitstellung der benötigten Datenschutz-

informationen – muss daher grundlegend überarbeitet werden, um zukunftsfähig für den weiteren Ausbau des NOOTS zu sein.

4.5.8 Governance

Das Bundesverwaltungsamt (BVA) steuert die Entwicklung von NOOTS und es verantwortet auch den XÖV-Standard *XNachweis*, der für alle Registerabfragen mittels NOOTS vorgesehen ist. Diese Governance umfasst die zentralen Komponenten des NOOTS (z. B. DAMAS, VS, RDN), die intermediäre Plattform zur Ankopplung des NOOTS an das EU-OOTS sowie den SAK als verbindliches Anschlusselement für alle Data Consumer, Data Provider und die Intermediäre Plattform.

4.5.8.1 Darreichungsform der NOOTS-Dokumentation

Zur Dokumentation der NOOTS-Architektur und ihres aktuellen Entwicklungsstands hat das BVA ein öffentliches Portal eingerichtet [97]. Dort finden sich die Architekturdokumente, die dokumentierten Architekturentscheidungen sowie Begleitdokumente.

Außerdem findet sich auf den Portalseiten eine Übersicht über die neuesten Versionen der SAK-APIs. Sie dient jedoch ausschließlich fachlichen und technischen Reviews und ist nicht für die Implementierung vorgesehen. Die Übersicht umfasst auch Beispieldaten, darunter auch Beispiele für das XNachweis2.0-Format sowie diverse Token-Schemata, die im Zuge einer Registerabfrage benötigt werden.

Die Dokumentation des Web-Portals ist jedoch nicht vollständig, sondern macht nur ausgewählte Dokumente öffentlich verfügbar. Einige der im Quellenverzeichnis genannten Dokumentenverweise (z. B. AD-NOOTS-DAMAS-01 und AD-NOOTS-DAMAS-10 [98]) führen nicht zum erwarteten Dokument, sondern verweisen zurück auf das Quellenverzeichnis.

Neben dem Architektur-Portal des BVA unterhält die FITKO im Auftrag des IT-Planungsrats auch eine Startseite für NOOTS-Interessierte [99]. Diese enthält neben Statusinformationen zum Stand der Registermodernisierung, Kontaktadressen von Ansprechpersonen und Erfahrungsberichten zu abgeschlossenen Pilotprojekten auch einen internen Bereich (ein Confluence-Workspace), der nur für registrierte Nutzer zugänglich ist. Dort stehen detailliertere Informationen für Softwarelieferanten, betrieblich Verantwortliche und registerführende Stellen zur Verfügung.

4.5.8.2 Versionierung

Die Dokumentation unter [97] wird in aufeinanderfolgenden Sprints fortgeschrieben und aktualisiert, wobei die Dokumente jeweils eine Änderungshistorie

enthalten. Der Name der Dokumente bleibt jedoch gleich und erfährt keine Versionierung zur Unterscheidung unterschiedlicher Entwicklungsstände.

4.5.8.3 Referenzimplementierung

Eine öffentlich verfügbare Referenzimplementierung ist uns im Rahmen der Studie nicht bekanntgeworden. Inzwischen gibt es jedoch mehrere Pilotanwendungen des NOOTS. Diese sind auf der NOOTS-Startseite [99] kurz beschrieben und mit kurzen Erfahrungsberichten hinterlegt.

4.5.8.4 Konformitätsprüfung

Da das NOOTS-Konzept noch in der Entwicklung und einige der NOOTS-Komponenten nur in provisorischer Realisierung verfügbar sind, ist eine förmliche, vollständige Konformitätsprüfung noch nicht möglich. Daher liegen uns auch keine Informationen zu einem Konformitätstest-Werkzeug vor, mit dem Softwarelieferanten die Korrektheit und Interoperabilität ihrer Software validieren könnten.

4.5.8.5 Ökosystem

Der Zeitpunkt der vorliegenden Studie ist zu früh, um die Verbreitung des NOOTS zu beurteilen. Erst seit Ende 2025 liegt überhaupt eine erste, jedoch noch unvollständige Version des NOOTS vor, und erst im Jahr 2026 wurden erste erfolgreich abgeschlossene Pilotanwendungen öffentlich bekannt.

Laut Auskunft der in den Interviews befragten Fachleute wird bis Ende des Jahres eine neue Version des NOOTS erwartet; auch diese wird aber in Teilen noch unvollständig sein.

Der aktuelle Entwicklungsstand wird via openCode im Internet für jedermann zugänglich schritthaltend dokumentiert [97]. Die Dokumentation umfasst auch die Beschreibung eines Konsultationsprozesses, bei dem Stakeholder mit Bezug zur Registermodernisierung, Unternehmen sowie Fachleute aus der Wissenschaft, Wirtschaft und Verwaltung die Möglichkeit haben, ihre Expertise und Erfahrungen einzubringen oder Bedarfe an das NOOTS vorzubringen.

Aufgrund der anhaltenden, raschen Weiterentwicklung der NOOTS-Konzepte erfordert der Anschluss von Registern derzeit noch viele individuelle Absprachen und Klärungen. Ein vollumfängliches, für jedermann problemlos einzusetzendes, vollständig spezifiziertes und gut dokumentiertes Implementierungs-Kit ist unseres Wissens noch nicht verfügbar.

4.6 ZaPuK

Die *Zielarchitektur Postfach- und Kommunikationslösungen* (ZaPuK) ist ein laufendes Projekt des Föderalen Architekturboards im Auftrag des IT-Planungsrats. Das Ziel des Projekts ist die Entwicklung einer Architektur für die Kommunikation zwischen öffentlichen Stellen sowie mit Unternehmen und Privatpersonen, insbesondere über Postfächer. Die Zielarchitektur soll mehrere bestehende Postfachlösungen aus verschiedenen Anwendungsbereichen ersetzen. Dazu zählen das zentrale Bürgerpostfach der Bund-ID, das MeinJustizPostfach sowie das ELSTER Postfach 2.0. Der Zweck des Projekts ist die Konsolidierung dieser Bestandssysteme auf einer gemeinsamen modernen technischen Basis, um den Aufwand der Parallelentwicklung zu reduzieren und die Interoperabilität zu erhöhen. ZaPuK wurde als Basisdienst *Postfach* in den Deutschland-Stack aufgenommen.

Die Zielarchitektur baut auf dem Technologiestandard Matrix auf. Der technische Austausch von Nachrichten und die Grundlagen des Kommunikations- und Betriebsmodells werden maßgeblich durch den Matrix-Standard geprägt. Die Grundlagen des Standards wurden bereits in Abschnitt 3.4.3 vorgestellt, während die Details für die Betrachtung im Rahmen dieser Studie nicht relevant sind. Die technischen Beschreibungen sind daher in diesem Kapitel bewusst kürzer gehalten. Stattdessen liegt der Fokus auf der Governance der Zielarchitektur und der Eignung der Technologie für den spezifischen Anwendungsbereich.

Es ist zu betonen, dass es sich bei der Zielarchitektur um ein laufendes Standardisierungsprojekt, nicht ein vollständiges Technologieprodukt handelt. Daher werden im Projekt verschiedene Aspekte ausgeklammert, die für den Nachrichtenaustausch in der Praxis notwendig sind, so etwa die Implementierung von Software und der Betrieb von Infrastrukturen. Da das Projekt zum Zeitpunkt dieser Studie noch nicht abgeschlossen ist, sind einige der betrachteten Aspekte zudem noch nicht finalisiert. Die Beschreibung und spätere Bewertung von ZaPuK basiert daher auf dem aktuell verfügbaren Stand der Informationen.

4.6.1 Anwendungsbereich

ZaPuK versteht sich als die Postfachlösung für die Kommunikation zwischen Behörden und Privatunternehmen (G2B), Privatpersonen (G2C) und anderen Behörden (G2G). Der Fokus liegt dabei aktuell auf dem Bereich G2C, in dem das Projekt NEO eine Pilotversion der Zielarchitektur für die Antragsfolgekommunikation mit der Bürgerschaft umsetzt.

Die Einsatzszenarien und Anforderungen der Zielarchitektur wurden dabei aus verschiedenen Gesetzen und Richtlinien zur G2X-Kommunikation sowie aus Interviews mit Stakeholdern der Bestandslösungen erhoben. Das primäre Einsatzszenario der Postfachlösungen ist die Antragsfolgekommunikation. Viele G2X-

Interaktionen basieren auf der Bearbeitung von Anträgen, die beispielsweise über ein OZG-Portal via FIT-Connect an ein Fachverfahren übertragen werden. Die Reaktion der Behörde auf diese Anträge, wie etwa die Übermittlung von Rückfragen oder die Zustellung von Bescheiden, erfolgt aktuell über verschiedene Wege und Technologien, die durch ZaPuK konsolidiert werden sollen.

Neben der Zustellung von Nachrichten und Dokumenten in ein Postfach deckt ZaPuK auch synchrone Kommunikation via Chat ab. Aus technischer Sicht ist auch die Übertragung von Audio- und Videoanrufen möglich. Im Rahmen dieser Studie wird ZaPuK jedoch primär mit anderen Lösungen zur Übertragung von (Text-)Nachrichten und Dokumenten verglichen, weshalb diese Varianten nicht genauer betrachtet werden.

4.6.2 Kommunikationsmodell

Das Kommunikationsmodell in ZaPuK ist durch die Wahl des Technologiestandards Matrix zur Übertragung der Nachrichten geprägt.

Matrix verwendet ein hybrides 3- beziehungsweise 4-Corner-Modell, bei dem die Nachrichten eines Autors zuerst an dessen Homeserver übertragen werden. Ist der Leser der Nachricht auf demselben Homeserver zu finden, so wird die Nachricht, wie in einem 3-Corner-Modell, direkt ausgeliefert. Der Leser kann sich jedoch auch auf einem anderen Homeserver befinden. In diesem Fall agiert der Homeserver des Autors als Sender und der Homeserver des Lesers als Empfänger. Die Nachricht wird zunächst vom Sender zum Empfänger übertragen und von diesem an den Leser zugestellt.

Die Art der Kommunikation hängt dabei von der Anzahl und den Beziehungen zwischen Homeservern ab. Alle Homeserver in Matrix sind Teil einer *Föderation* und können prinzipiell miteinander kommunizieren. Jedoch muss jeder Homeserver individuell entscheiden, mit welchen anderen Homeservern eine Kommunikation möglich sein soll. Somit ist auch eine Kommunikationsinfrastruktur denkbar, in der es nur einen isolierten Homeserver gibt. In dieser Ausprägung würde die Kommunikation exklusiv nach dem 3-Corner-Modell ablaufen.

Über die Entscheidung, die Kommunikation mit anderen Homeservern zu erlauben oder nicht zu erlauben, können auch die Kommunikationsberechtigungen für die Teilnehmer der Kommunikationsinfrastruktur auf dem Granularitätsniveau verschiedener Homeserver abgebildet werden. Eine rein verwaltungsinterne Behörde kann ihren eigenen Homeserver betreiben und die Kommunikation mit öffentlichen oder privatwirtschaftlichen Homeservern verbieten.

In ZaPuK ist vorgesehen, ein offenes Ökosystem zu schaffen, in dem die Endnutzer ihren Homeserver frei wählen, eigene Homeserver betreiben und frei über die Kommunikation mit anderen Homeservern entscheiden können [100, S. 15].

ZaPuK selbst macht keine Vorgaben, wie die verschiedenen Teilnehmergruppen auf Homeserver verteilt werden sollen.

Das Projekt *NEO* der FITKO erprobt die Umsetzung der Zielarchitektur am Beispiel der G2C-Kommunikation [101]. Im Projekt wurde eine Kommunikationsinfrastruktur aus zwei Homeservern aufgebaut, einem Server für Privatpersonen und einem Server für alle teilnehmenden öffentlichen Stellen. Die Kommunikation findet in dieser Umsetzung nach dem 4-Corner-Modell statt.

Im Vergleich zu anderen in dieser Studie betrachteten Technologien weist Matrix die Besonderheit auf, dass dieses Protokoll das *Konversationsmodell* der Kommunikation deutlich genauer spezifiziert. In anderen Transporttechnologien ist die Organisation der Konversation – also beispielsweise die Möglichkeit, einen Bezug zwischen verschiedenen Nachrichten herzustellen, Nachrichten nach der Übertragung zu speichern oder Nachrichten zu bearbeiten – vollständig in der Verantwortung der Autoren und Leser.

Die Kommunikation in Matrix hingegen erfolgt prinzipiell in *Räumen*, die einen Kommunikationskanal zwischen Teilnehmern beschreiben. Dabei können beliebig viele Endnutzer auf verschiedenen Homeservern an Räumen teilnehmen. Die Kommunikation ist nicht auf genau einen Autor und Leser beschränkt, sondern kann auch in Gruppen erfolgen. Dabei kann durch die Einstellungen des Raums kontrolliert werden, welche Teilnehmer Nachrichten im Raum versenden dürfen. Der Status eines Raums wird durch alle teilnehmenden Homeserver repliziert und persistent gespeichert. Alle Nachrichten in einer fachlichen Konversation sind über die Historie des Raums gespeichert. Endnutzer können den Inhalt des Raums auf verschiedenen Geräten mehrfach von ihrem Homeserver neu beziehen. Eine Persistenz der Nachrichten und ein Bezug sowie eine Historie mehrerer Nachrichten zueinander wird direkt durch die Kommunikationsinfrastruktur hergestellt.

4.6.3 Kommunikationsstandard

Im Rahmen des Projekts ZaPuK wurden verschiedene Transport- und Schnittstellenstandards als technische Basis der Zielarchitektur bewertet. Dazu zählten unter anderem die in dieser Studie betrachteten Technologien OSCI in Kombination mit XTA, FIT-Connect, eDelivery-AS4 und X-Road. Die Wahl der Projektverantwortlichen fiel auf den bereits beschriebenen Matrix-Standard. Die Gründe für diese Entscheidung waren unter anderem das Ökosystem und das Governance-Modell des Standards sowie die modernen Funktionen der Technologie. Die Bewertung der Technologien ist öffentlich in der Architekturentscheidung ADR-0011 [102] des Projekts dokumentiert.

Der Kommunikationsstandard Matrix transportiert Nachrichten mittels verschiedener REST-APIs via HTTPS, über die Events im JSON-Format übertragen werden.

4.6.4 Schnittstellenstandard

Die Schnittstellen zur Übertragung von Nachrichten zwischen Clients und Server sowie zwischen verschiedenen Homeservern werden durch den Matrix-Standard vorgegeben. Die REST-Schnittstellen zur Übertragung der Nachrichten sind bewusst generisch und erweiterbar gestaltet. Die APIs definieren lediglich die Semantik für den Austausch von Events. Der Standard definiert verschiedene Typen von Events, wie etwa die Erstellung von Räumen, den Beitritt neuer Mitglieder und den Versand von Nachrichten. Darüber hinaus können Technologien, die auf Matrix aufbauen, zusätzliche eigene Eventtypen definieren. Die Inhaltsdaten der Nachrichten können jegliche Form von JSON-Struktur enthalten. Die Matrix-Spezifikation beschreibt für einige Nachrichtentypen, wie Daten repräsentiert werden sollten, zum Beispiel als Textnachricht, Bild oder Datei. Neue Nachrichtentypen können ebenfalls frei definiert werden.

Zur Unterstützung neuer Arten von Nachrichten und Events ist daher keine Anpassung der Schnittstellen notwendig. Server und Clients, die einen neuen Event- oder Nachrichtentyp nicht kennen, können diesen weiterhin austauschen und übertragen, ignorieren diesen jedoch bei der Verarbeitung und Darstellung.

Um den fachlichen Anforderungen der Zielarchitektur gerecht zu werden, sind zusätzliche Funktionen notwendig. Der Matrix-Standard bietet aktuell keine native Unterstützung für die Verwaltung von Postfächern und die Nichtabstreitbarkeit der Kommunikation (ADR-0011 [102]). Konkrete Informationen darüber, welche Erweiterungen dafür notwendig sind und wie diese umgesetzt werden sollen, liegen zum Zeitpunkt dieser Studie nicht vor. Die zu unterstützenden Erweiterungen für Client- und Serverimplementierungen sollen in Form von Anbindungsbedingungen dokumentiert werden.

4.6.5 Implementierungen

Das Projekt ZaPuK erstellt lediglich eine Zielarchitektur für die Entwicklung von Postfachlösungen, die in einem gemeinsamen Ökosystem zusammengeschlossen werden können. Das Projekt selbst wird jedoch keine einsatzfähige Software entwickeln. In mehreren Architekturentscheidungen (ADR-0007, ADR-0009 [102]) wurde allerdings festgelegt, dass nach Fertigstellung der Zielarchitektur eine Referenzimplementierung des modifizierten Matrix-Servers und ein Software Development Kit (SDK) für die Entwicklung von Clients zentral bereitgestellt werden sollen.

Im Matrix-Ökosystem existieren verschiedene quelloffene Implementierungen der Standardspezifikation, sowohl auf Server- als auch auf Clientseite. Die Implementierungen sind in verschiedenen Programmiersprachen und Formen (z. B. als App oder Web-Client) verfügbar. Die geplanten Referenzimplementierungen der Zielarchitektur können auf diese vorhandenen Ressourcen aufbauen.

ZaPuK sieht zudem vor, dass Drittimplementierungen des Servers sowie eigene Implementierung von Clients durch Dritte bedingungslos erlaubt werden (ADR-0003, ADR-0007 [102]). Als Orientierungshilfe für die notwendigen Funktionen sollen laut Aussagen in Interviews im Rahmen dieser Studie die Referenzimplementierungen und Anbindungsbedingungen zur Verfügung gestellt werden. Die Einhaltung dieser Empfehlungen soll jedoch nicht geprüft werden (ADR-0003, ADR-0007 [102]).

In NEO, dem Pilotprojekt der Zielarchitektur, hat die FITKO ein SDK in Rust mit Bindings in anderen Programmiersprachen sowie Clients in Form einer iOS-App und einer Web-App entwickelt. Zur Anbindung von Fachverfahren wurde der Code zur Anbindung an die NEO-Infrastruktur auch in das FIT-Connect-SDK integriert.

4.6.6 Infrastruktur

Die Zielarchitektur macht keine Vorgaben für den Betrieb der Infrastruktur und stellt selbst keine Infrastruktur bereit. In verschiedenen Architekturentscheidungen werden die Topologie der Infrastruktur, die notwendige Basisinfrastruktur und die Bedingungen für die Teilnahme an der Kommunikationsinfrastruktur definiert.

Im Matrix-Ökosystem können Homeserver von jedem Teilnehmer vollständig unabhängig betrieben werden. Es gibt keine zentralen oder externen Dienste, die zum Betrieb eines Homeservers notwendig sind. Die Kommunikation zwischen Nutzern zweier verschiedener Homeserver erfolgt direkt durch die beiden Homeserver. Bei Betrieb eines öffentlichen Homeservers kann das öffentliche Domain Name System (DNS) zur Auflösung der Servernamen verwendet werden. Die Authentifizierung der Server kann über Zertifikate einer öffentlichen Public-Key Infrastructure (PKI) erfolgen. Die Authentifizierung der Nutzer kann über eine API durch externe Identity-Provider umgesetzt werden. Diese Dienste sind jedoch optional und können durch private Versionen oder manuelle Konfiguration ersetzt werden.

ZaPuK definiert eine Kommunikationsinfrastruktur, in der mehrere Homeserver miteinander vernetzt werden, um die Kommunikation zwischen deren Endnutzern zu ermöglichen. Dabei definiert ZaPuK in ADR-0003 und ADR-0004 [102] eine prinzipielle Offenheit für den Betrieb von Servern und Clients durch Drittanbieter. Zusätzlich wird in ADR-0005 und ADR-0006 [102] entschieden, dass auch jeweils ein zentraler Postfach-Zugang (Client) und ein zentrales Backend (Homeserver) bereitgestellt werden sollen. Die Zielarchitektur macht jedoch keine Aussage darüber, wer für den Betrieb dieser zentralen Infrastruktur verantwortlich ist.

Des Weiteren macht die Zielarchitektur zum Zeitpunkt der Studie keine Aussagen über die Existenz oder den Betrieb von Zusatzdiensten, wie einem Verzeichnis der Homeserver oder Systemen zur Namensauflösung und Authentifizierung der Sever. Für den Beitritt zum Ökosystem soll ein zentrales Self-Service-Portal (ADR-0008 [102]) bereitgestellt werden. Über den Betrieb dieses Portals und die notwendigen Prozesse zur Anbindung werden zum Zeitpunkt der Studie keine genauen Aussagen getroffen. Im Rahmen der Architekturentscheidung werden jedoch potenzielle Ausnahmen und Prozessvarianten für besondere Nutzergruppen eingeräumt.

4.6.7 Sicherheit

Der Nachrichtenaustausch im G2B- und G2G-Kontext unterliegt verschiedenen Anforderungen hinsichtlich der Vertraulichkeit, Integrität, Authentizität, Nachweisbarkeit und Rechtssicherheit. Um diesen Anforderungen gerecht zu werden, müssen verschiedene technische Möglichkeiten geschaffen werden.

Die Authentifizierung von Nutzern und die Sicherstellung der Authentizität und Integrität von Nachrichten in Matrix wurde bereits im Abschnitt 3.4.3 beschrieben. Da das ZaPuK-Ökosystem auch Drittanbietern offensteht, die möglicherweise bössartig agieren und allgemein nicht vertrauenswürdig sind, sieht ZaPuK eine zusätzliche Authentifizierung innerhalb eines bereits etablierten Ende-zu-Ende-verschlüsselten Kommunikationskanals vor (ADR-0013 [102]). Die Identitätsbestätigung erfolgt dabei für die verschiedenen Nutzergruppen der öffentlichen Stellen, Privatorganisationen und Privatpersonen über unterschiedliche externe Nachweise. Privatpersonen authentisieren sich wahlweise über die eID ihres Personalausweises, die BundID oder zukünftig per EUDI-Wallet (ADR-0014 [102]). Für öffentliche Organisationen sind Zertifikate aus der Verwaltungs-PKI oder das Organisationskonto nach OZG vorgesehen (ADR-0015 [102]). Privatunternehmen können ebenfalls das Organisationskonto nach OZG oder ein Zertifikat aus einer öffentlichen PKI verwenden (ADR-0016 [102]). Die Verifikation der Identität eines Kommunikationspartners muss vollständig durch den Endnutzer oder deren Client möglich sein, da die Backend-Systeme als nicht vertrauenswürdig betrachtet werden.

Die Zielarchitektur macht aktuell keine Aussagen darüber, wie die Authentifizierung des Nutzers gegenüber dem Backend-System (Homeserver) durchzuführen ist oder wie ein Client die Identität verifiziert.

Matrix stellt Mechanismen zur Verschlüsselung der ausgetauschten Nachrichten bereit. Auf unterster Ebene sind alle Verbindungen zwischen Client und Server sowie zwischen verschiedenen Homeservern durch HTTPS transportverschlüsselt. Zusätzlich können die Inhaltsdaten der ausgetauschten Nachrichten durchgängig über die Algorithmen Olm beziehungsweise Megolm Ende-zu-Ende verschlüsselt

werden. Die Ver- und Entschlüsselung übernehmen dabei die Clients, wodurch Inhaltsdaten nicht durch Homeserver eingesehen werden können. Die Verschlüsselung beruht auf Public/Private-Schlüsselpaaren, die der Client generiert und an die Identität des Matrix-Nutzers bindet.

Die Ende-zu-Ende-Verschlüsselung und die Rolle der Endgeräte in der Kommunikation bergen jedoch verschiedene Herausforderungen für die Schlüssel- und Identitätsverwaltung, insbesondere in Anwendungsfällen wie Funktionspostfächern. Diese Herausforderungen liegen vor allem in der Implementierung der Postfachfunktionalität und in der Verwaltung von Clients. Der Betrieb und die Verwaltung von Clients und ihres Schlüsselmaterials sind jedoch nicht Gegenstand der Zielarchitektur.

In Interviews wurden verschiedene Ansätze zur Lösung dieser Herausforderungen geäußert, beispielsweise der Betrieb eines Clients auf einem Server, der die betroffene Organisation repräsentiert. Dieser Client könnte die Nachrichten empfangen und verwalten. Menschliche Endnutzende, beispielsweise Sachbearbeitende einer Behörde, könnten Zugriff auf die Nachrichten durch eine zusätzliche Softwarelösung oder die Bildung von Gruppen innerhalb von Matrix erhalten. Dieses Vorgehen deckt sich mit der allgemeinen Auffassung von E2EE im G2G und G2B Bereich, wie in Abschnitt 2.4 beschrieben.

Bei der G2X-Kommunikation spielt auch die Rechtssicherheit eine wichtige Rolle. Rechtssicherheit kann als eine Kombination aus Nachweisbarkeit und Nichtabstreitbarkeit der Kommunikation, Protokollierung, Authentizität und Integrität der Nachrichten angesehen werden. Zur technischen Umsetzung von Rechtssicherheit sind typischerweise Elemente wie digital signierte Nachrichten, signierte Zeitstempel und eine Protokollierung der Nachrichtenübermittlung notwendig. Aktuell bietet der Matrix-Standard keine direkte Umsetzung von Rechtssicherheit, wobei einzelne Elemente, wie die digitale Signatur von Nachrichten, bereits vorhanden sind. ADR-0017 und ADR-0018 [102] stellen ein Konzept zur Definition der spezifischen Anforderungen an Rechtssicherheit und Vorgaben zur Implementierung der Funktionalität im Kontext von ZaPuK in Aussicht. Dieses Konzept ist jedoch zum Zeitpunkt dieser Studie noch nicht verfügbar.

4.6.8 Governance

Im Kontext von ZaPuK muss zwischen der Governance des Matrix-Standards und der Governance der Zielarchitektur unterschieden werden.

Der Matrix-Standard wird durch die *Matrix.org-Foundation* verwaltet, einer Community Interest Company mit Sitz im Vereinigten Königreich [103]. Die Foundation übernimmt die Pflege des Standards und des Ökosystems. Die Weiterentwicklung der technischen Spezifikation übernehmen verschiedene Teams. Änderungen an der Spezifikation können über den Matrix-Specification-Change-

Prozess von der Öffentlichkeit vorgeschlagen werden. Die Spezifikation und die technische Dokumentation des Standards sind in aktueller und in historischen Versionen auf einer Webseite kostenlos verfügbar. Es existieren keine offiziellen Referenzimplementierungen des Standards unter Verwaltung der Foundation. Stattdessen existiert ein Ökosystem verschiedener Implementierungen, die teilweise quelloffen und unter offenen Lizenzen wie MIT oder Apache 2.0 veröffentlicht werden [104]. Eine Testsuite zur Prüfung der Konformität einer Implementierung zur Spezifikation existiert und wird durch die Foundation gepflegt.

Die Zielarchitektur wird aktuell durch das Architekturboard der FITKO im Auftrag des IT-Planungsrats entwickelt. Die bestehenden Architekturentscheidungen wurden durch das Projektteam in Abstimmung mit verschiedenen Fachleuten und Stakeholdern der Bestandslösungen getroffen. Die Dokumentation der Zielarchitektur ist über die Plattform Open Code öffentlich und kostenlos einsehbar, einschließlich der Änderungshistorie.

Da sich die Zielarchitektur noch in der Ausarbeitung befindet, existiert aktuell keine Versionierung. Die derzeit verfügbaren ADRs [102] der Zielarchitektur beschreiben die generelle Topologie des Ökosystems und den Beitritt über ein geplantes Self-Service-Portal. Die Kommunikationsinfrastruktur wird offen für Dritte gestaltet. Eine Konformitätsprüfung der Implementierungen oder Betriebsplattformen Dritter durch eine zentrale Stelle ist nicht vorgesehen. Die Zielarchitektur sieht eine Bereitstellung einer quelloffenen Referenzimplementierung der Software und von zentralen Infrastrukturen vor, die allen Nutzern zur Verfügung stehen. Die Verantwortlichkeiten für den Betrieb dieser Infrastruktur und für die Entwicklung der Implementierungen sind bisher jedoch nicht festgelegt.

Die Governance-Struktur, die Verantwortlichkeit und die Finanzierung der Pflege und Weiterentwicklung der Zielarchitektur sind zum Zeitpunkt dieser Studie noch offen. Diese und weitere Aspekte der Pflege der Zielarchitektur sollten ursprünglich im Rahmen der zweiten Phase des Projekts im zweiten Quartal 2026 entschieden werden [105]. In einem Beschluss der 50. Sitzung des IT-Planungsrats [106] vom 17. Juni 2026 wird die Vorlage eines Betriebs- und Finanzierungsmodells zur 52. Sitzung (voraussichtlich im März 2027) vorgegeben.

4.7 X-Road

X-Road ist eine quelloffene, cloudfähige Infrastruktur für den sicheren synchronen Datenaustausch über das Internet. Die Technologie stammt aus Estland und wird dort von der Verwaltung erfolgreich eingesetzt. Auf Basis von X-Road betreibt (oder nutzt) jede dazugehörige Organisation einen sogenannten Security Server, über den ihre Fachsysteme Dienste (APIs) bereitstellen und anfragen. Die Security Server kommunizieren untereinander über standardisierte, signierte und verschlüsselte Nachrichten, die protokolliert werden und damit Nachweisbarkeit

sowie Datenhoheit sicherstellen. Die zentrale X-Road-Konfiguration hält die Metadaten darüber, welche Organisationen und Diensten existieren und wie sie sicher miteinander verbunden werden.

4.7.1 Anwendungsbereich

X-Road ermöglicht sichere Datenübertragung zwischen Behörden (G2G) und Unternehmen (B2G). Dabei werden typische Funktionalitäten einer Daten-Transportinfrastruktur bereitgestellt. Zu diesen gehören Routing, Zugriffsmanagement, Authentifizierung, Signatur und Protokollierung.

Der Schwerpunkt von X-Road liegt auf Vernetzung, ohne dass zentrale Datenbanken oder ein zentraler Datenaustauschpunkt für die ausgetauschten Daten erforderlich sind. Typische Anwendungsbereiche sind der Austausch von Verwaltungsdaten, die Anbindung von Registern und Fachverfahren sowie die Bereitstellung digitaler Dienste zwischen Organisationen.

4.7.2 Kommunikationsmodell

X-Road setzt technisch auf eine Request-Response-basierte, serviceorientierte Kommunikation zwischen Fachsystemen, die überwiegend im Machine-to-Machine-Betrieb erfolgt. Dazu gehören beispielsweise proaktive und antragslose Verwaltungsleistungen sowie regelmäßige automatisierte Anspruchsprüfungen [107].

Technisch ist X-Road als dezentrale Architektur konzipiert, bei der jede teilnehmende Organisation einen eigenen Security Server betreibt oder einen Security-Server-Dienst nutzt. Diese Security Server bilden die verbindliche Schnittstelle zwischen internen Fachsystemen und der externen X-Road-Kommunikation. Der Central Server fungiert als Vertrauensanker und hält die globale Konfiguration, etwa die Liste der Mitglieder, Security Server, vertrauenswürdigen Zertifikatvergabestellen und Zeitstempeldienste. Ein Configuration Proxy, der als vermittelnde Instanz dient, verteilt die Konfiguration in großen Umgebungen. Fachsysteme selbst implementieren das X-Road-Protokoll nicht, sondern kommunizieren über Standardverfahren (HTTPS, SOAP, REST) mit ihrem jeweiligen Security Server, wodurch Transportlogik und Fachlogik klar getrennt bleiben.

Der Central Server ist die sicherheitstechnische Grundlage einer X-Road-Instanz. Er verwaltet die Datenbank der X-Road-Mitglieder und Security-Server. Diese Datenbank umfasst unter anderem die Liste der vertrauenswürdigen Zertifikatvergabestellen, die Liste der vertrauenswürdigen Zeitstempeldienste sowie anpassbare Parameter wie die maximal zulässige Gültigkeitsdauer einer Online-Certificate-Status-Protocol-Antwort. Mit diesem Protokoll wird der aktuelle Status eines digitalen Zertifikats bestätigt. Damit definiert der Central Server das übergreifende Sicherheits- und Vertrauenskonzept der Instanz und sorgt für die

interoperable Einbindung aller beteiligten Organisationen, ohne selbst operative Fachdaten zu transportieren [108].

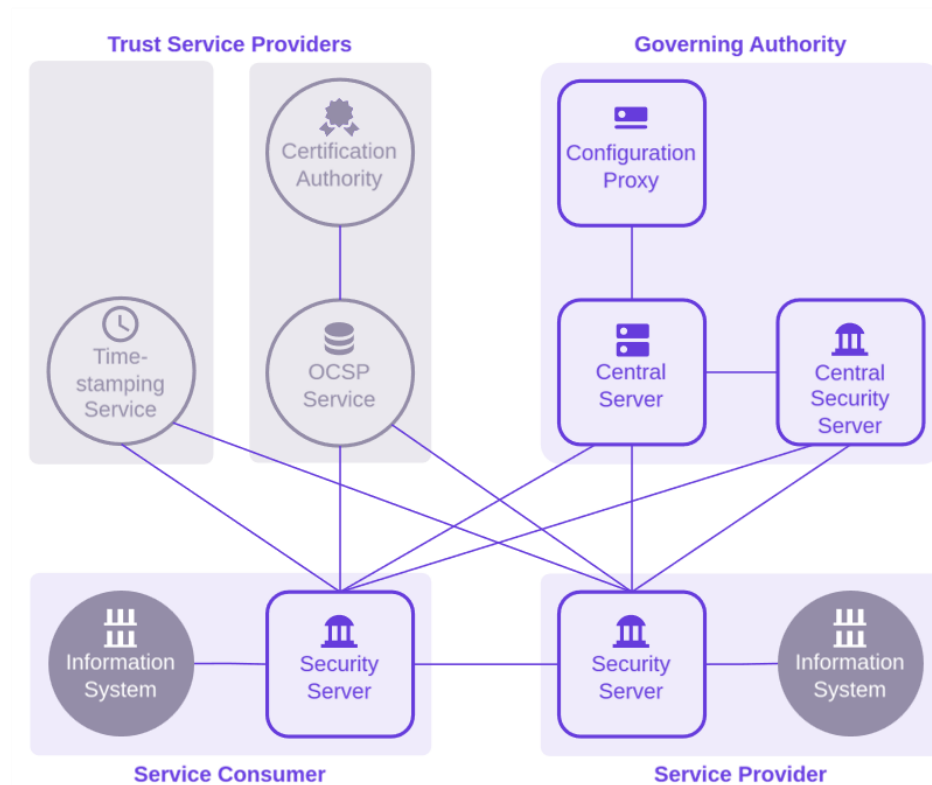


Abbildung 13 Übersicht über die X-Road-Architektur [109]

Der Security Server ist der verpflichtende Anschlussknoten und dedizierter Zugriffspunkt zwischen den angeschlossenen Informationssystemen. Er vermittelt Dienstaufrufe und -antworten, stellt die Punkt-zu-Punkt-Kommunikation zu anderen Security-Servern her und führt OCSP-Abfragen zur Zertifikatsprüfung durch. Dabei kapselt er alle sicherheitsrelevanten Funktionen, unter anderem die Verwaltung von Schlüsseln für Signatur und Authentifizierung, den Aufbau kryptografisch gesicherter Kanäle zu anderen Security Servern, das Signieren der Nachrichten durch den Client (Signaturschlüssel) sowie das Zeitstempeln, die Protokollierung, den Nachweisabruf und die Durchsetzung strenger Zugriffskontrollen. So bleibt die Datensouveränität der Behörden gewahrt, da keine zentralen Datenkopien entstehen, jede Organisation nur ihren relevanten Datenausschnitt freigibt und der Security Server als kontrollierbare Vermittlungsschicht zwischen internen Fachsystemen und der externen X-Road-Kommunikation dient [108].

Die Information Systems sind Fachanwendungen der Nutzer von X-Road, die über ihren Security Server Dienste bereitstellen oder konsumieren. Mithilfe des

X-Road-Metadatenprotokolls können registrierte Mitglieder sowie deren angebotene Dienste ermittelt werden. Diese Dienste setzen das X-Road-Protokoll nicht selbst um, sondern kommunizieren in der Regel über standardisierte Verfahren wie HTTPS, REST oder SOAP mit ihrem zuständigen Security Server [108].

Die Time-Stamping Authority stellt Zeitstempel aus, die die Existenz von Datenobjekten zu einem bestimmten Zeitpunkt nachweisen, und reduziert durch die Verwendung von Batch-Zeitstempeln die Last des Zeitstempeldienstes [108].

Die Certification Authority stellt die Authentifizierungszertifikate für die Security Server aus. Diese Zertifikate werden verwendet, um die sichere Kommunikation zwischen zwei Security Servern zu ermöglichen und die Identität der Kommunikationspartner zu überprüfen. Zusätzlich stellt die Certification Authority Signierzertifikate für X-Road-Mitglieder bereit, die zur digitalen Signatur von ausgetauschten Nachrichten verwendet werden. Die Gültigkeit der Zertifikate wird von den Security Servern mithilfe des Online Certificate Status Protocols (OCSP) überprüft. Nur Security Server mit gültigen und vertrauenswürdigen Zertifikaten können am sicheren Datenaustausch innerhalb der X-Road-Infrastruktur teilnehmen [108].

Der Configuration Proxy fungiert als Vermittler zwischen X-Road-Servern beim Austausch globaler Konfigurationen. Der Operational Monitoring Daemon sammelt und speichert Betriebsdaten des X-Road-Security-Servers und stellt sie über entsprechende Schnittstellen externen Monitoringsystemen zur Verfügung, während der Environmental Monitoring Daemon Informationen über die Betriebsumgebung des Security-Servers erfasst und diese ebenfalls über geeignete Schnittstellen für externe Monitoringsysteme bereitstellt [108].

X-Road ermöglicht dezentrale Kommunikation zwischen unabhängigen Informationssystemen. Während des Datenaustauschs werden Daten dezentral gespeichert und verbleiben daher dort, wo sie entstehen, statt in einer zentralen Datenplattform. Diese Funktion soll Flexibilität und Datensouveränität erhöhen. Zusätzlich bleibt so die Data Ownership immer gleich und es gibt keine Datendoppelungen.

Das effiziente Governance-Modell ermöglicht den Mitgliedsorganisationen eine weitgehend eigenständige Einrichtung und Verwaltung ihrer Datenaustauschdienste. Service Provider stellen Daten oder Funktionen bereit, legen Zugriffsrechte fest und entscheiden selbst, welche Informationen sie mit welchen Organisationen teilen. Der zentrale Betreiber einer X-Road-Instanz verwaltet die Mitgliedschaften und die gemeinsame Infrastruktur, greift jedoch nicht in den Datenaustausch zwischen den Mitgliedern ein [107] [108].

X-Road bleibt auch bei einem Ausfall des Central Servers weitgehend funktionsfähig. Der Central Server unterstützt Hochverfügbarkeit durch Clustering,

wodurch Resilienz und Skalierbarkeit verbessert wird. Ein Central-Server-Cluster besteht aus zwei oder mehr Serverknoten und arbeitet nach dem Prinzip, dass alle Knoten sowohl Lese- als auch Schreibzugriffe verarbeiten können. Fällt ein Knoten aus, können die Security Server automatisch auf einen anderen verfügbaren Knoten umschalten [110].

X-Road definiert einheitliche Identifikationskonzepte für Organisationen, Subsysteme und Dienste, sodass Aufrufe eindeutig zugeordnet werden können. Der Security Server übernimmt das Routing von eingehenden Serviceaufrufen zu den richtigen internen Fachsystemen (»Member Information Systems«). Anhand der Dienstkennung entscheidet der Security Server, welches Fachverfahren den Aufruf verarbeiten soll. Wenn ein Fachsystem einen Dienst einer anderen Organisation nutzen will, schickt der eigene Security Server die Anfrage zum passenden fremden Security Server. Die Zielorganisation und der gewünschte Dienst sind in der X-Road-Konfiguration eindeutig beschrieben und werden im Central Server gespeichert; der Security Server greift auf diese Information zu, indem er Global Configuration Files, die vom Central Server generiert werden, runterlädt. Die Information von diesen Global Configuration Files nutzt der Security Server dann, um die Anfrage an den richtigen Gegensever zu schicken.

4.7.3 Kommunikationsstandard

Der Security Server stellt Informationen über neue Informationssysteme und deren Schnittstellen automatisch bereit. Die Kommunikation mit den Informationssystemen erfolgt standardmäßig über eine mTLS-gesicherte Verbindung.

Die Kommunikation zwischen den Security Servern erfolgt direkt über ein IP-Netzwerk und wird durch eine HTTPS-Verbindung mit mTLS zum Security Server des Service Providers abgesichert.

4.7.4 Schnittstellenstandard

X-Road unterstützt sowohl SOAP- als auch REST-Schnittstellen und nutzt HTTPS als Transportprotokoll für den sicheren Datenaustausch zwischen den Sicherheitsservern. Dadurch können bestehende Servicelandschaften mit überschaubarem Anpassungsaufwand integriert werden, sofern sie bereits über REST- oder SOAP-Schnittstellen verfügen. X-Road unterstützt beide Diensttypen, führt jedoch keine automatische Konvertierung zwischen unterschiedlichen Nachrichten- oder Serviceformaten durch.

Ein dienst anbietendes Informationssystem implementiert REST- oder SOAP-Dienste und veröffentlicht diese über X-Road. Bestehende REST-Dienste können dabei ohne Anpassungen eingebunden werden, während SOAP-Dienste das X-Road-Nachrichtenprotokoll für SOAP implementieren müssen. Die Beschreibung von REST-Diensten erfolgt mithilfe der OpenAPI-3-Spezifikation, die von SOAP-

Diensten mittels WSDL. Service Consumer können diese Dienstbeschreibungen über das X-Road-Metadatenprotokoll abrufen und auf dieser Grundlage die angebotenen Schnittstellen sowie deren Struktur und Spezifikation nachvollziehen.

Standardisierte APIs ermöglichen die interoperable Anbindung verschiedener Fachverfahren und bilden damit eine wesentliche Grundlage für den Datenaustausch in X-Road.

4.7.5 Implementierung.

Die X-Road-Software ist quelloffen mit freier Verfügbarkeit [111].

Die Anbindung an X-Road erfolgt entweder über einen selbst betriebenen Security Server oder über die Infrastruktur eines IT-Dienstleisters. In Schleswig-Holstein wird zusätzlich eine Sandbox betrieben, um X-Road-Anbindungen testen zu können [112].

Die Größe eines X-Road-Ökosystems unterliegt keinen festen Begrenzungen. Daher kann X-Road sowohl für landesweite Infrastrukturen als auch für kleinere organisationsbezogene Lösungen eingesetzt werden. Für die Implementierung unterscheidet X-Road vier Modelle: nationale, regionale, geschäftliche und organisationsbezogene Ökosysteme [112].

Bei nationalen Implementierungen liegt der Schwerpunkt auf dem organisationsübergreifenden Datenaustausch zwischen verschiedenen Verwaltungsbereichen und Geschäftsdomänen. Dabei können sowohl öffentliche Einrichtungen als auch private Unternehmen in ein gemeinsames X-Road-Ökosystem eingebunden werden [112].

Darüber hinaus unterstützt X-Road den grenzüberschreitenden Datenaustausch zwischen verschiedenen Ländern. Hierfür können unabhängige X-Road-Ökosysteme mithilfe der Föderationsfunktion miteinander verbunden werden. Dadurch können Mitgliedsorganisationen unterschiedlicher Ökosysteme Daten austauschen, als wären sie Teil einer gemeinsamen X-Road-Umgebung [112].

4.7.6 Infrastruktur

X-Road basiert auf dem Prinzip der dezentralen Datensouveränität. Kommunikation läuft über Security Server, die bei den einzelnen Organisationen liegen. So behalten Organisationen die alleinige Kontrolle über ihre Schnittstellen.

Die Kommunikation zwischen den Security Servern erfolgt über IP-basierte Netzwerke, beispielsweise das öffentliche Internet oder geschlossene Verwaltungnetze.

4.7.7 Sicherheit

X-Road bietet verschiedene Schutzmechanismen für einen sicheren Datenaustausch. Durch Zugriffskontrollen wird sichergestellt, dass nur authentifizierte Mitglieder auf Daten Zugriff haben. Die Kommunikation zwischen Security Servern erfolgt verschlüsselt über mTLS, ergänzt durch eine PKI-basierte Authentifizierung der beteiligten Organisationen und Server [113].

Der Client signiert jede Nachricht, wodurch sichergestellt wird, dass sie unverändert vom identifizierten Absender stammt.

X-Road verlangt eine verbindliche Protokollierung aller Dienstaufrufe, sodass für jede Transaktion nachvollziehbar ist, welcher Client wann welchen Dienst mit welchen Parametern aufgerufen hat. Diese Audit-Trails werden vom Security Server dezentral geführt und sind ein wesentliches Element für Nichtabstreitbarkeit, Datenschutzkontrolle und forensische Analysen. Die Protokollierung von X-Road ermöglicht es grundsätzlich, nachzuvollziehen, welche Organisation wann auf welche Daten zugreift. In Estland kann beispielsweise die Bürgerschaft über eigene Portale Einsicht in viele dieser Zugriffe nehmen.

Beim Datenaustausch zwischen registrierten X-Road-Mitgliedern übernimmt der Sicherheitsserver die Zugriffskontrolle auf Organisationsebene. Das zentrale Prinzip von X-Road besteht darin, dass jeder Service Provider Eigentümer seiner Daten bleibt und selbst für die Verwaltung der Zugriffsrechte auf seine Dienste verantwortlich ist. Die Veröffentlichung eines Dienstes über X-Road gewährt anderen Mitgliedern daher nicht automatisch Zugriff darauf. Ein Zugriff ist nur möglich, wenn der Service Provider die entsprechende Berechtigung erteilt hat.

Zur laufenden Prüfung der Zertifikatsgültigkeit wird Online Certificate Status Protocol (OCSP) eingesetzt, sodass kompromittierte oder abgelaufene Zertifikate erkannt werden. Zusätzlich kommt eine Time-Stamping Authority zum Einsatz, die Zeitstempel vergibt und damit beweisbar macht, dass eine bestimmte Nachricht zu einem bestimmten Zeitpunkt existierte und verarbeitet wurde.

Die Ende-zu-Ende-Verschlüsselung ist in X-Road nicht vorgegeben, sie liegt in den Händen der Service Provider und Service Consumer.

4.7.8 Governance

Die Infrastruktur wird durch das *Nordic Institute for Interoperability Solutions* (NIIS), eine Zusammenarbeit von Estland und Finnland, entwickelt. Estland nutzt X-Road als Basis für eine vollständige Digitalisierung seiner Verwaltung, die trotz häufiger Cyberattacken zuverlässig funktioniert.

X-Road wird international eingesetzt. Die Infrastruktur wird in zahlreichen Ländern benutzt. Auch in Deutschland wird X-Road seit April 2020 von der Kassenärztlichen Vereinigung Hessen als Pilotprojekt für Videosprechstunden und digitale Rezepte genutzt. In Schleswig-Holstein wird X-Road nun erstmals in Deutschland in der Verwaltung eingesetzt für ein landesweites Behördenetz. Die Entscheidung für X-Road in Schleswig-Holstein fiel unter anderem wegen des bewährten Einsatzes in Estland.

4.8 eDelivery AS4

4.8.1 Anwendungsbereich

Das eDelivery-AS4-Profil ist eine offene technische Spezifikation für den sicheren, nutzdatenunabhängigen Nachrichtenaustausch. Es legt fest, wie mit dem AS4-Nachrichtenprotokoll zu kommunizieren ist und ermöglicht so einen interoperablen Datenaustausch über Organisations- und Landesgrenzen hinweg.

Das Profil ist für 4-Corner-Netzwerktopologien (siehe Abschnitt 2.1) konzipiert, gleichzeitig kann es auch bei Punkt-zu-Punkt-Austauschen eingesetzt werden, je nachdem, ob der Nachrichtenaustausch über Dienstleister oder direkt erfolgt. eDelivery AS4 unterstützt einen sicheren Nachrichtenaustausch, asynchrone und synchrone Kommunikationsmuster, einen nutzdatenunabhängigen Nachrichtenaustausch, ohne Betrachtung oder Interpretation der Inhalte sowie digitale Signaturen und Verschlüsselung auf Basis kryptografischer Zertifikate.

Die aktuelle Version des CEF¹⁰-Standards eDelivery AS4 ist die Version 2.0 vom Dezember 2024 [114]. Sie ist unter der *European Union Public License* (EUPL), Version 1.2 – einer Open-Source-Lizenz der europäischen Union – lizenziert. Die aktuelle Version 2.0 ist allerdings nicht mit früheren Versionen kompatibel, da sie inkompatible Sicherheitsalgorithmen verwendet. Der Standard basiert auf dem AS4-Profil 1.0 der ebMS 3.0-Spezifikation [115], das 2021 sogar ISO-Standard wurde. Dieser Standard wurde entwickelt, um Einfachheit zu gewährleisten und eine bessere Konformität mit den Webservice-Standards (u. a. SOAP, WSDL und WSS) sowie Funktionen wie die Möglichkeit zum Abrufen von Nachrichten und einen integrierten Empfangsbestätigungsmechanismus zu gewährleisten. AS4 steht dabei für *Applicability Statement 4*, wobei die 4 für die vierte Version in einer Entwicklungsreihe sicherer B2B-Kommunikationsprotokolle steht.

AS4 eignet sich insbesondere für den zuverlässigen Austausch großer Dateien und Massendaten, einschließlich Quittungen, Wiederholungsversuchen und

¹⁰ Connecting Europe Facility

definiertem Ablauf- und Fehlerhandling. Es ist außerdem für dokumentenorientierte Anwendungen geeignet, etwa für den Austausch strukturierter Nutzdaten.

Das eDelivery-AS4-Profil konkretisiert den allgemeinen AS4-Standard für den interoperablen Einsatz. Hierzu definiert es ein verbindliches »Common Profile«, welches eine einheitliche und zu unterstützende Teilmenge der AS4-Funktionalitäten festlegt. Das Profil basiert auf dem AS4-ebHandler-Konformitätsprofil, präzisiert dessen Nutzung und ergänzt zusätzliche Anforderungen für den sicheren und interoperablen Nachrichtenaustausch. Dadurch entsteht ein gemeinsames Nutzungsprofil (»Usage Profile«), welches technische Interoperabilität zwischen unterschiedlichen AS4-Implementierungen sicherstellt. Es ist mit dem vom ENTSG (dem Europäischen Netzwerk der Fernleitungsnetzbetreiber für Gas) entwickelte AS4-Profil für Übertragungsnetzbetreiber abgestimmt und entspricht einer Teilmenge davon.

Das eDelivery-AS4-Profil konkretisiert den allgemeinen AS4-Standard für den interoperablen Einsatz. Hierzu definiert es ein verbindliches Common Profile, das eine einheitliche und zu unterstützende Teilmenge der AS4-Funktionalitäten festlegt. Das Profil basiert auf dem AS4-ebHandler-Konformitätsprofil, präzisiert dessen Nutzung und ergänzt zusätzliche Anforderungen für den sicheren und interoperablen Nachrichtenaustausch. Dadurch entsteht ein gemeinsames Nutzungsprofil (»Usage Profile«), das die technische Interoperabilität zwischen unterschiedlichen AS4-Implementierungen sicherstellt. Es ist mit dem vom ENTSG (dem Europäischen Netzwerk der Fernleitungsnetzbetreiber für Gas) entwickelte AS4-Profil für Übertragungsnetzbetreiber abgestimmt und entspricht einer Teilmenge davon.

Das BDEW-AS4-Profil wiederum ist ein AS4-Nutzungsprofil zum Datenaustausch für regulierte Prozesse in der Energiewirtschaft im deutschen Strom- und Gasmarkt [116]. Es basiert auf dem eDelivery-AS4-Profil, allerdings auf der Version 1.15. Mit dem BDEW-AS4-Profil wurde eine größtmögliche Kompatibilität mit dem eDelivery-AS4-Profil 1.15 angestrebt und erweitert dieses technisch, wo es aus regulatorischen Gründen notwendig ist.

Zusätzlich zum Common Profile enthält die eDelivery-AS4-Spezifikation eine Reihe optionaler Profilerweiterungsmodule, die Funktionserweiterungen festlegen, die den AS4-Nachrichtenaustausch in 4-Corner-Topologien, das Verhalten von dynamischen Empfängern und Sendern, die Unterstützung der Pull-Funktion, das Zerlegen und Wiederzusammensetzen von großen Nachrichten sowie alternative Sicherheitsalgorithmen abdecken.

Der Hauptanwendungsbereich von eDelivery-AS4-Profilen liegt im sicheren, rechtsverbindlichen und nutzdatenunabhängigen B2B-, B2G- und G2G- Datenaustausch.

Als Standard der Europäischen Kommission wird eDelivery-AS4 vor allem für die länderübergreifende Interoperabilität in der öffentlichen Verwaltung sowie in streng regulierten Branchen wie der Energiewirtschaft (ENTSO-G, BDEW) genutzt. Der Standard wird in folgenden Bereichen angewendet:

- Im E-Government ermöglicht er den elektronischen Datenaustausch in der öffentlichen Verwaltung von EU-Staaten.
- Zur Verbindung der EU-Staaten wird eDelivery-AS4 für den Austausch zwischen den europäischen Verwaltungen im Rahmen der Connecting Europe Facility (CEF) genutzt.
- Im Kontext B2G und C2G sorgt der Standard dafür, dass Personen und Unternehmen den Behörden Daten (wie Urkunden oder Nachweise) gemäß dem Once-Only-Prinzip (EU-OOTS) nur einmal übermitteln müssen.

Während eDelivery-AS4 auf EU-Verwaltung und die Energiebranche fokussiert, wurde AS2 eher für den globalen Handel entwickelt, insbesondere für den Bereich B2B-E-Commerce. Zudem benötigt AS4 im Gegensatz zu AS2 keine dauerhaft geöffneten Firewall-Ports für den Empfang (durch den Pull-Modus) von Nachrichten. Zudem bietet AS4 flexiblere Kompressions- und Signatur-Mechanismen. AS4 ist vollständig nutzdatenunabhängig, wobei AS2 oft auf EDIFACT-Nutzdaten fokussiert.

4.8.2 Kommunikationsmodell

Das eDelivery-AS4-Profil unterstützt vor allem den asynchronen Datenaustausch. Synchroner Datenaustausch kann mittels asynchroner Kommunikation nachgebildet werden, wird jedoch technisch nicht direkt unterstützt. Die direkte Kommunikation ist zwar eine Punkt-zu-Punkt-Kommunikation, jedoch wird oft ein Kommunikationsmodell realisiert, das auf dem 4-Corner-Modell beruht, wie in Abbildung 14 dargestellt.

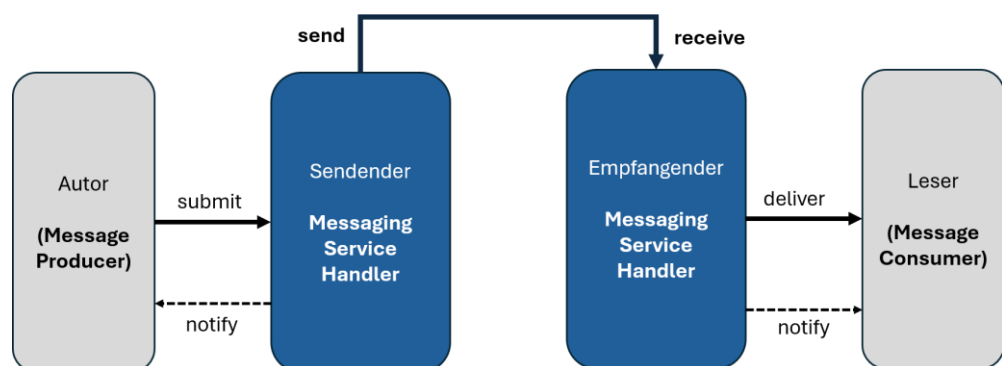


Abbildung 14 Kommunikationsmodell des eDelivery-AS4 in Anlehnung an die Darstellung in [18]

Der Transportstandard eDelivery AS4 benötigt nicht zwingend Intermediäre, da er für eine direkte Peer-to-Peer-Kommunikation (Punkt-zu-Punkt) zwischen Sender und Empfänger konzipiert ist. Die Adressierung und das Auffinden der Kommunikationspartner erfolgen standardisiert über das sogenannte Dynamic Discovery-Modell mittels Metadaten-Registern. Die Identifikation der Partner im eDelivery-Netzwerk basiert dabei auf eindeutigen Kennungen innerhalb des Nachrichtenkopfs (d. h. im Message Header). Das heißt, Sender und Empfänger werden über standardisierte Identifikatoren eindeutig identifiziert. Um eine Nachricht ohne zentralen Intermediär direkt an die richtige IP-Adresse des Empfängers zu senden, nutzt eDelivery ein zweistufiges Suchverfahren (Dynamic Discovery):

Der Sender nutzt dazu den zentralen sogenannten *Service Metadata Locator* (SML, vergleichbar mit einem DNS-Verzeichnis), um herauszufinden, in welchem regionalen oder sektoralen Register die Details des Empfängers liegen. Der SML verweist den Sender an den sogenannten *Service Metadata Publisher* (SMP) des Empfängers. Dieses SMP ist dezentral und enthält die exakte URL des Access-Points (Endpunkt) des Empfängers sowie dessen unterstützte Zertifikate und Prozesse. Dann wird im Access-Point des Senders die Nachricht verschlüsselt, signiert und direkt an die ermittelte URL des Access-Points des Empfängers geschickt. Wird eDelivery AS4 im 4-Corner-Modell betrieben, übernimmt ein Dienstleister, der den Access-Point des Senders bereitstellt, die Rolle eines technischen Vermittlers (Intermediärs). Der finale Leser der Nachricht wird dabei nicht durch das AS4-Protokoll selbst adressiert. Die Weiterleitung vom Empfänger an den Leser erfolgt über die Auswertung der angehängten XML-Metadaten durch die nachgelagerte Software des Empfängers.

4.8.3 Kommunikationsstandard

Eine AS4-Nachricht setzt sich von außen nach innen aus den folgenden Schichten zusammen:

- *HTTP-Transport-Umschlag*: Die äußere Hülle für die Übertragung per Webprotokoll (HTTP(S) 1.1).
- *MIME-Multipart-Container*: Bündelt die XML-Metadaten und die eigentlichen Nutzdaten.
- *SOAP-Umschlag (Envelope)*: Enthält den strukturellen XML-Code, welcher UTF-8-kodiert sein muss. Für Nachrichtenverpackung und Nutzdatenkompression wird SOAP 1.2 »with attachments« genutzt.
 - *SOAP-Header*: Enthält Routing-Informationen, Absender, Empfänger sowie *WS-Security*-Elemente wie digitale Signaturen und Zertifikate zur Verifizierung.

- *SOAP-Body*: Bleibt bei der Nutzung von Anhängen oft leer oder enthält Verweise.
- *Anhänge*: Die eigentlichen Fachnachrichten oder Geschäftsdaten (z. B. EDIFACT- oder XML-Dateien) werden separat komprimiert, signiert und verschlüsselt angehängt.

4.8.4 Schnittstellenstandards

Da SOAP und HTTPS zur Kommunikation verwendet werden, kommen XML und WSDL zum Einsatz, wobei letzteres XML-basiert ist und beide W3C-Standards sind.

4.8.5 Implementierungen

Für das Nachrichtenprotokoll AS4 (Applicability Statement 4) existieren standardisierte Referenzimplementierungen und etablierte Testumgebungen, die primär durch die Europäische Kommission im Rahmen der eDelivery-Initiative sowie für spezifische Branchen (wie die deutsche Energiewirtschaft oder das Peppol-Netzwerk) bereitgestellt werden:

- Die zentrale und offizielle Referenzimplementierung (der europäischen Kommission) für den AS4-Standard in Europa ist *Domibus* [117]. Diese Open-Source-Messaging-Software dient als Standard-Zugangspunkt (Access Point) für den sicheren und zuverlässigen B2B-, B2G- und G2G-Datenaustausch im eDelivery-Netzwerk. Diese Software nutzt das AS4-Profil und fungiert als universelle Schnittstelle zur Anbindung von Backend-Systemen und setzt das eDelivery-AS4-Profil vollständig um. Sie dient Softwareherstellern als technischer Maßstab und kann direkt als funktionstüchtiger *Access Point*, also in der Rolle eines Senders oder Empfängers gemäß 4-Corner-Modell, in Test- und Produktivumgebungen integriert werden. Die Software ist unter der bereits genannten EUPL-Lizenz frei verfügbar.
- *phase4 (phax)* ist eine einbettbare Java-Bibliothek für AS4-Clients und AS4-Server [118]. Sie ist modular aufgebaut und bietet dedizierte Profile für das europäische Peppol-Netzwerk, eDelivery sowie das deutsche BDEW-AS4-Profil.
- *Oxalis-NG* (ehemals *Oxalis-AS4*) wurde ursprünglich von der norwegischen Digitalisierungsbehörde entwickelt [119]. Es ist eine verbreitete Open-Source-Komponente für den Dokumentenaustausch im Peppol-Ökosystem via AS4-Protokoll [120].
- *Holodeck B2B* ist eine robuste, eigenständige Open-Source-AS4-Implementierung unter GPLv3-Lizenz, die ebenfalls vollständig konform zu den eDelivery-Spezifikationen ist [121].

- Die quellenoffene .NET-Implementierung *AS4.NET* implementiert OASIS ebMS 3.0 und AS4 vollständig und wurde von der Europäischen Kommission (u. a. im Rahmen von eDelivery) auf Konformität getestet. Weiterhin wurde sie erfolgreich gegen Domibus oder Holodeck B2B getestet [122].

Um die Interoperabilität und Standardkonformität eigener AS4-Systeme zu prüfen, stehen verschiedene Plattformen bereit. Im europäischen Raum:

- Die Europäische Kommission betreibt den zentralen (offiziellen) *eDelivery Conformance Testing Service*. Nach erfolgreichem Durchlauf aller Pflichttests wird ein offizielles *eDelivery Conformance Certificate* ausgestellt, und das Produkt wird in der Liste konformer Lösungen geführt [123].

Ergänzend gibt es weitere nationale und branchenspezifische Testumgebungen:

- Das internationale Peppol-Netzwerk nutzt eine eigene, auf den eDelivery-Spezifikationen aufbauende Testumgebung (*Peppol Testbed*), um den sicheren Nachrichtenaustausch zwischen den zertifizierten *Access Points* (Sender – Corner 2 und Empfänger – Corner 3) zu validieren.
- Für den regulierten Datenaustausch – die *sichere Marktkommunikation* auf Basis von AS4 – im *deutschen Strom- und Gasmarkt* (festgelegt durch die Bundesnetzagentur) organisieren Verbände wie der EDNA-Bundesverband und Marktteilnehmer eigenständige Interoperabilitätstests (1:1-Hersteller-tests). Hierbei testen Hersteller ihre AS4-Gateways direkt gegeneinander auf Basis der BNetzA-Vorgaben.

4.8.6 Infrastruktur

Voraussetzung für einen Datenaustausch auf Basis von eDelivery-AS4 ist ein TCP/IP-Netzwerk, wobei für ein funktionierendes HTTP/TLS-System, wie es bei eDelivery-AS4 eingesetzt wird, sowohl ein DNS-System (Domain Name System) als auch eine Public-Key-Infrastruktur (PKI) bereitzustellen sind. Ersteres, damit IP-Adressen in lesbare Namen übersetzt werden können, da TLS-Zertifikate fast immer auf Domainnamen und nicht auf IP-Adressen ausgestellt werden. Letzteres, um Verbindungen zu Zertifikatvergabestellen (CAs) aufzubauen und die Gültigkeit der TLS-Verschlüsselung zu verifizieren.

4.8.7 Sicherheit

AS4 bietet ein sicheres Austauschprotokoll für die Nutzung über das Internet, das die MIME-Umschlagstruktur nutzt, um beliebige Nutzdaten zu übertragen. Die Unterstützung für Nachrichtensicherheit wird von AS4 über ebMS 3.0 sowie die Spezifikationen WS-Security 1.1 und 1.1.1 bereitgestellt. Dazu gehören Kombinationen aus XML-Digital-Signature- und XML-Encryption-X.509-Sicherheitstoken zum Signieren und Verschlüsseln als primäre Mittel zur Authentifizierung

von Nachrichten, zur Gewährleistung des Datenschutzes und zur Sicherstellung einer sicheren Datenübertragung. Darüber hinaus unterstützt AS4 die Verwendung von Benutzername-/Passwort-Token als Zugriffskontrolle für Message-Pull-Kanäle. Dabei ist Transport Layer Security und WS-Security obligatorisch, und die verwendete Version der WS-Security-Spezifikation ist 1.1.1.

Bei der Verwendung von AS4 gewährleistet *Transport Layer Security* (TLS) die Vertraulichkeit der Inhalte und die Authentifizierung. Die Serverauthentifizierung mithilfe eines Serverzertifikats ermöglicht es dem Client, sicherzustellen, dass die HTTPS-Verbindung mit dem richtigen Server hergestellt wird. Wenn eine Nachricht gesendet wird, authentifiziert der Sender den HTTPS-Server des Empfängers.

TLS-Versionen und Verschlüsselungssuiten müssen internationalen und nationalen Mindestanforderungen sowie Best Practices genügen. Implementierungen, die diesem AS4-Profil entsprechen, dürfen SSL 3.0, TLS 1.0 und 1.1 nicht verwenden. Sie müssen mindestens TLS 1.2 (RFC 5246¹¹) unterstützen und sollen die Verwendung von TLS 1.3 (RFC 8446¹²) unterstützen (u. a. schreibt das US-amerikanische National Institute of Standards and Technology seit dem 1. Januar 2024 die Unterstützung von TLS 1.3 vor [124]). Ferner sollen Implementierungen bestimmte als sicher geltende TLS 1.3-Verschlüsselungssuiten unterstützen. eDelivery-AS4 2.0 zeichnet sich damit besonders durch höchste Sicherheit durch modernisierte Kryptografie (u. a. elliptische Kurven) aus und erfüllt die Sicherheitsanforderungen der eIDAS-Verordnung [125].

Des Weiteren bietet eDelivery-AS4 2.0 durch Empfangsbestätigungen, d. h. automatisch generierte Belege, die den Versand und den Erhalt einer Nachricht eindeutig beweisen, Rechtssicherheit und gewährt durch automatisch generierte Eingangsbestätigungen und durch Erkennung von Duplikaten Verbindlichkeit.

Ende-zu-Ende-Verschlüsselung, also die Verschlüsselung der Nutzdaten vom initialen Autor zum finalen Leser, muss außerhalb von eDelivery AS4 erfolgen, sofern im 4-Corner-Modell betrieben. Das ist dann der Fall, wenn sich Sender/Empfänger nicht direkt in geschützten Bereichen beim Autor/Leser befinden. Dazu verschlüsselt der Autor (Corner 1) an einem Ende die eigentliche Nachricht (Nutzlast), noch bevor diese an den Sender (Corner 2) und dessen Access-Point übergeben wird. Dazu benötigt der Autor den öffentlichen Schlüssel (Public Key) des Lesers (Corner 4). Dabei ist zu beachten, dass der Access-Point des Senders die Informationen zur korrekten Adressierung des Empfängers und für das korrekte Routing diese Metadaten unverschlüsselt und separat benötigt. Der Access-Point beim Sender signiert die Nachricht und verschlüsselt sie nach AS4-Vorgaben. Die

¹¹ <https://datatracker.ietf.org/doc/html/rfc5246> Abruf 20.07.2026

¹² <https://datatracker.ietf.org/doc/html/rfc8446> Abruf 20.07.2026

Nutzdaten sind somit auf dem Transportweg doppelt verschlüsselt. Der Access-Point beim Empfänger (Corner 3) validiert nach Erhalt der Nachricht die AS4-Signatur, entfernt die AS4-Transportverschlüsselung und leitet die immer noch verschlüsselten Nutzdaten an den Leser (Corner 4) weiter (bzw. der Leser holt sie bei Corner 3 ab). An diesem Ende werden die Daten mit dem privaten Schlüssel (Private Key) des Lesers entschlüsselt.

4.8.8 Governance

Die Europäische Kommission pflegt die offiziellen Spezifikationen eDelivery AS4 über die Connecting Europe Facility (CEF) und sorgt für die Weiterentwicklung (wie z. B. auf die Version 2.0, um neue Sicherheitsstandards wie TLS 1.3 oder ECDSA zu unterstützen). Nationale Organisationen adaptieren diese Spezifikationen von eDelivery AS4 für die nationale E-Government-Landschaft. In der deutschen Energiewirtschaft wird im Rahmen der Marktkommunikation das eDelivery-AS4-Profil in angepasster Form genutzt und durch Institutionen wie die Bundesnetzagentur und den BDEW reguliert. Informationen zum Konformitätstest und anerkannten (getesteten) Software-Lösungen für eDelivery-AS4 bietet eine Webseite der Europäischen Kommission [126].

Die offizielle Open-Source-Referenzimplementierung für einen eDelivery-AS4-Zugangspunkt Domibus wird von der Generaldirektion für Informatik (kurz DIGIT) der Europäischen Kommission entwickelt und gepflegt. Es handelt sich dabei um eine Software, die sichere, standardisierte und zuverlässige Nachrichtenübermittlungen gemäß der eDelivery-AS4-Spezifikation in ganz Europa ermöglicht. Der Quellcode und die offiziellen Komponenten sind für die Öffentlichkeit frei zugänglich und werden aktiv weiterentwickelt. Domibus dient als Open-Source-Musterlösung, die von Mitgliedsstaaten, Behörden und Unternehmen nutzbar ist oder als Vorlage für eigene eDelivery-AS4-konforme Systeme dient. Die Europäische Kommission bietet Support, stellt regelmäßige Updates, Sicherheits-Patches sowie Long-Term-Support (LTS)-Versionen und Dokumentationen bereit und hilft mit Antworten auf häufig gestellte Fragen [117].

5 Technologiebewertung

5.1 Bewertungsmodell

Die Bewertung der betrachteten Technologien erfolgt auf zwei getrennten Ebenen. Zunächst werden die Technologien isoliert anhand ihrer Stärken und Schwächen auf Grundlage der in diesem Kapitel aufgeführten Kriterien in Form einer SWOT-Analyse bewertet. Anschließend erfolgt ein Vergleich aller betrachteten Technologien in Bezug auf die Anforderungen der verschiedenen Kommunikationsszenarien aus Abschnitt 2.6.

Dieses Vorgehen wurde gewählt, da die betrachteten Technologien starke Unterschiede in ihrem Anwendungsbereich, Umfang und Reifegrad aufweisen, die eine vergleichende Bewertung auf technologischer Ebene unmöglich machen. Während OSCI ursprünglich einen Standard für ein Nachrichtenprotokoll darstellt, werden in dieser Studie auch externe Implementierungen, der Betrieb des OSCI-Ökosystems und Erfahrungswerte von Nutzenden und Entwickelnden im Umgang mit der Dokumentation des Standards einbezogen. Im Vergleich dazu wird in ZaPuK aktuell eine Zielarchitektur definiert, die lediglich Regeln für die Verwendung des Technologiestandards Matrix und den Betrieb eines Ökosystems definiert. NOOTS hingegen kann als eine Beschreibung einer Kommunikationsinfrastruktur verstanden werden, in deren Rahmen verschiedene zentrale Dienste und Implementierungen zur Anbindung an die Infrastruktur bereitgestellt werden sollen. Sowohl bei NOOTS als auch bei ZaPuK bestehen bisher in vielen Aspekten nur Pläne – konkrete Umsetzungsentscheidungen und prüfbare Spezifikationen stehen aktuell oft noch aus. FIT-Connect umfasst die Governance, den Betrieb und die Bereitstellung von Implementierungen für eine 3-Corner-Kommunikationsinfrastruktur mit bestehenden Erfahrungswerten, definiert im Vergleich zu OSCI auf technologischer Ebene jedoch kein eigenes Protokoll.

Aufgrund dieser Unterschiede ist die Definition von Bewertungskriterien, die auf alle betrachteten Technologien angewendet werden können, nicht möglich. Stattdessen werden die Technologien in Abschnitt 5.2 in einer SWOT-Analyse anhand ihrer individuellen Stärken und Schwächen bewertet. Die Bewertung orientiert sich dabei an den Bewertungsdimensionen in Tabelle 4.

Für die Erstellung der grundlegenden Liste von Kriterien wurden in erster Linie der Standard ISO/IEC 25010 [127], der Servicestandard für die digitale Verwaltung [128], die Vorgaben des föderalen Standardisierungsboards zur Bewertung von IT-Standards [129], die föderalen Architekturrichtlinien [130] und die

Architekturprinzipien des Deutschland-Stacks [131] herangezogen, sofern jeweils in Bezug auf die Fragestellungen der Studie anwendbar. Konkrete Bewertungen richten sich nach einer Vielzahl konkreter IT-Standards, technischer Richtlinien und anderer Artefakte, die in den beschreibenden und bewertenden Kapiteln 4 und 5 direkt im jeweiligen technologischen Kontext begründet werden.

Tabelle 4

Bewertungsdimensionen und Bewertungskriterien

Bewertungsdimension	Beispielhafte Bewertungskriterien
Standard-Governance	• Offenheit und Transparenz des Standards • Status und Reifegrad des Standards (national oder international etabliert) • Klare Zuständigkeit und Governance-Strukturen für den Standard • Konzepte für die Beteiligung von Stakeholdern und Regelungen für die Teilnahme an der Weiterentwicklung • Aktive Pflege und Weiterentwicklung des Standards • Verwaltung der Dokumentation • Digitale Souveränität
Standard-Spezifikation	• Vollständigkeit der Spezifikation • Eindeutigkeit der Beschreibungen, Vermeidung von Widersprüchen • Verbindlichkeit der Spezifikation und Vermeidung von Dialektbildung • Erweiterbarkeit und Anpassbarkeit der Spezifikation • Effektivität und Effizienz • Interoperabilität • Marktakzeptanz
Implementierungen und Developer Experience	• Verfügbarkeit von offiziellen Referenzimplementierungen als Open Source • Verfügbarkeit von Testsuiten und Testumgebungen • Verfügbarkeit von technischer Dokumentation und Anleitungen • Verwendung von etablierten Technologien, Paradigmen und Befolgen von Best Practices
Kommunikations- und Infrastrukturmodell	• Klare Governance für die Teilnahme an der Kommunikationsinfrastruktur

Bewertungsdimension	Beispielhafte Bewertungskriterien
	• Klare Verteilung der Aufgaben im Kommunikationsmodell • Klare Verteilung der Verantwortlichkeiten im Infrastrukturmodell • Bevorzugung von Open Source in allen zentralen Komponenten • Abdeckung verschiedener Kommunikationsszenarien • Abhängigkeit von externen Komponenten und Diensten • Anforderungen an Betreiber der Infrastruktur • Anforderungen an Nutzende (Autoren und Leser, z. B. Self-Service) • Zuverlässigkeit • Resilienz • Skalierbarkeit • Effizienz
Security	• Verschlüsselung nach Stand der Technik • Kryptoagilität • Fähigkeit zur Ende-zu-Ende-Verschlüsselung • Rechtssicherheit der Kommunikation • Authentifizierung und Berechtigungsmanagement • Vertrauensmodelle

Die Bewertungsdimensionen und –kriterien liefern aus unserer Sicht eine angemessene Grundlage für die Bewertung der betrachteten Technologien. Allerdings besteht kein Anspruch auf Vollständigkeit und nicht alle Kriterien sind für die individuelle Bewertung verbindlich. Über Bewertungsdimensionen, die auf eine Technologie nicht zutreffen oder über die keine verlässlichen Informationen bekannt sind, wird für die jeweilige Technologie in der SWOT-Analyse in Abschnitt 5.2 keine Aussage getroffen, es sei denn, daraus ergibt sich ein noch zu adressierendes Risiko.

In den Abschnitten 5.3 und 5.4 werden die Technologien im Hinblick auf ihre Eignung für die betrachteten Kommunikationsszenarien (siehe Abschnitt 2.6) eingeordnet. Dies ermöglicht einen Vergleich und die Ableitung von Handlungsempfehlungen für die Auswahl. Die Bewertung erfolgt in Form von jeweils einer Matrix pro Kommunikationsszenario. Die Bewertungskriterien werden dabei individuell durch die Anforderungen des jeweiligen Szenarios bestimmt.

5.2 Allgemeine Technologiebewertung mittels SWOT-Analyse

Zur strukturierten Bewertung der betrachteten Kommunikationstechnologien wird im Rahmen dieser Studie die SWOT-Analyse eingesetzt. SWOT steht für *Strengths* (Stärken), *Weaknesses* (Schwächen), *Opportunities* (Chancen) und *Threats* (Risiken). Die Methode dient dazu, interne Eigenschaften einer Technologie von externen Einflussfaktoren zu unterscheiden und dadurch ein ganzheitliches Bild ihrer Eignung und Zukunftsfähigkeit zu gewinnen.

Auch wenn insbesondere die unterschiedlichen Reifegrade der Technologien eine Gegenüberstellung erschweren, so lassen sich selbst aus noch nicht ausgereiften Technologien anhand der existierenden Konzepte bestimmte Eigenschaften der späteren physischen Infrastruktur extrapolieren. Sofern sich daraus noch zu adressierende Risiken ergeben, so werden diese bei Weakness oder Threat der betreffenden Technologien aufgeführt.

Stärken und Schwächen beschreiben technologieimmanente Merkmale, beispielsweise hinsichtlich Funktionalität, Standardisierung, Interoperabilität, Sicherheit oder Implementierungsaufwand. Chancen und Risiken ergeben sich hingegen aus dem technologischen, organisatorischen oder regulatorischen Umfeld und umfassen beispielsweise auch strategische Entwicklungen, gesetzliche Rahmenbedingungen oder Abhängigkeiten von externen Akteuren. Die SWOT-Analyse ermöglicht damit eine systematische Einordnung der Potenziale und Herausforderungen einer Technologie und bildet die Grundlage für die anschließende vergleichende Bewertung.

Basis der im Folgenden aufgeführten SWOT-Analysen bildet die ausführliche Darstellung der Technologien und die Liste der Bewertungskriterien aus den vorangegangenen Kapiteln.

5.2.1 OSCI

Die SWOT-Analyse bezieht sich auf OSCI-Version 1.2, siehe Abschnitt 4.2.

5.2.1.1 Stärken

OSCI profitiert von einem hohen Verbreitungsgrad, insbesondere im Hinblick auf die Kommunikation zwischen Behörden. Durch den fortgeschrittenen Stand der Spezifikation sind bereits viele funktionale Anforderungen integriert, etwa im Bereich der Nachweisbarkeit von Nachrichtenübertragungen. Dadurch ist OSCI in vielen Kontexten einsetzbar. Durch die Kapselung auf der Auftrags- und Nachrichtenebene kann durch OSCI eine Ende-zu-Ende-Verschlüsselung grundsätzlich ermöglicht werden.

Durch die Ausrichtung als dezentrales Konzept vermeidet OSCI aus konzeptioneller Sicht Single-Point-of-Failure-Problemstellungen, sodass eine Skalierung auf Lastspitzen auf Basis dezentraler Infrastrukturkomponenten möglich wird.

S – Strengths (Stärken)

- Vielseitige Einsetzbarkeit
- Bewährtheit, hohe Verbreitung, Ausgereiftheit
- Rechtssicherheit, Nachweisbarkeit
- Kapselung auf Auftrags- und Nachrichtenebene ermöglicht durchgängige Vertraulichkeit
- Skaliert im bisherigen Ausbau
- Resilienz aufgrund der dezentralen Funktionsweise

5.2.1.2 Schwächen

Die Governance der OSCI-Spezifikation ist trotz zentraler Website fragmentiert, die Versionierung der Spezifikation ist unüblich und schwer nachvollziehbar. Das spezifikationsseitige Handling von Deprecations, insbesondere im Hinblick auf Kryptografie, wird nicht konsequent umgesetzt. Kryptografische Algorithmen, die als nicht sicher bekannt sind, werden aus Gründen der Abwärtskompatibilität weiter in der Spezifikation aufgeführt. Die OSCI-Spezifikation definiert nicht, wie Zertifikate durch Teilnehmer bezogen werden können, wodurch die Umsetzung einer durchgängigen Verschlüsselung erschwert wird.

Ein inhaltlicher Austausch wird durch intransparente, nicht offene Kommunikationskanäle auf bilaterale Kommunikation limitiert und bekannte Implementationen der OSCI-Spezifikation werden nicht auf deren Konformität hin überprüft. Es besteht hier die Gefahr einer Dialektbildung. Test- und Referenzumgebungen sind teilweise mit XTA vermischt oder nicht frei zugreifbar. Zudem entspricht die Offenheit der Implementierungen im OSCI-Ökosystem (z. B. kein quelloffener OSCI-Intermediär) nicht den aktuellen Vorgaben der föderalen Richtlinien [130].

W – Weakness–(Schwächen)

- Fragmentierte Governance
- Teilweise vage Vorgaben
- Marktunübliche Versionierung

W – Weakness–(Schwächen)

- Unübersichtliche Dokumentation
- Konformität bekannter Implementierungen wird trotz Listing auf Spezifikationswebsite nicht von Spezifikationsausgeber sichergestellt
- Mangelnde Open-Source-Abdeckung im OSCI-Ökosystem
- Begrenzte Test- und Referenzimplementierungen und -umgebungen
- Trennung zu XTA nicht immer klar dokumentiert, hierdurch hohe Komplexität, nicht komplett umgesetzt in Implementierungen

5.2.1.3 Chancen

OSCI weist ein bestehendes, sich in Produktion befindliches Ökosystem aus Software-Lieferanten und Infrastrukturbetreibern auf. Das Ökosystem bedient bereits verschiedene Nutzergruppen, die zum Teil OSCI in ihrem fachlichen Kontext erfolgreich integriert haben.

Eine Substitution von OSCI mit einem anderen Protokoll birgt damit das Risiko eines erheblichen Bedarfs an monetären und personellen Ressourcen.

O – Opportunities (Chancen)

- Software-Lieferanten für erprobte OSCI-Lösungen, etabliertes »Ökosystem«
- Etablierte Nutzerbasis

5.2.1.4 Risiken

Die Schwächen bei der Dokumentation, Test- und Referenzimplementierungen führen zu Hürden für die Umsetzung durch neue Teilnehmer. Im Hinblick auf europäische Kommunikation stellt OSCI eine nationale Insellösung dar. OSCI wurde bis jetzt auch nicht in den Deutschland-Stack aufgenommen.

Das von OSCI verwendete Protokoll SOAP wird häufig als veraltet wahrgenommen und gilt nicht mehr als Stand der Technik. Die heute bevorzugte Nutzung von REST bei Client-Server-Anwendungen, insbesondere bei neuem Fachpersonal, birgt ein Risiko für eine Kompetenzlücke, die den Umgang mit der Spezifikation und Implementierung weiter erschwert.

T – Threats (Risiken)

- Hohe Verständnishürde für neue Implementationen
- Dialektbildung wegen fehlender Eindeutigkeit, etwa beim Kryptografiemanagement
- Teilnehmer müssen sich an den Implementierungen einiger weniger Software-Anbieter ausrichten
- Technologieverbreitung (SOAP vs. REST) gering: wenig erfahrenes Fachpersonal marktvfugbar
- Nur national verbreitet und keine Aufnahme im Deutschland-Stack

5.2.2 XTA 2

Die SWOT-Analyse bezieht sich auf XTA 2 Version 5.1.1 [43], siehe Abschnitt 4.3.

5.2.2.1 Stärken

Der XTA2-Standard zielt auf hohe Flexibilität und eine breite funktionale und rechtliche Abdeckung von Kommunikationsszenarien. Durch die vielfältigen Möglichkeiten in Service-Profilen können detaillierte Vorgaben zu Protokollierung, Schutz und Sicherheit gemacht werden, die auf die Erfüllung von Anforderungen nach Rechtssicherheit, Nachvollziehbarkeit, Nachweisbarkeit abzielen. Der Standard ist daher in vielfältigen behördlichen Kontexten einsetzbar. Er unterstützt sowohl asynchrone als auch synchrone Kommunikationsszenarien durch eine einheitliche Schnittstelle auf Basis von SOAP-Webservices.

S – Strengths (Stärken)

- Vielfältige Möglichkeiten zu Vorgaben bezüglich Protokollierung, Schutz und Sicherheit in Service-Profilen, damit im behördlichen Kontext vielseitig einsetzbar
- Einheitliche XTA-Webservices für die Anbindung von Fachverfahren

5.2.2.2 Schwächen

Eine Analyse des XTA2-Standards zeigt, dass durch seine hohen Freiheitsgrade und teilweise vagen Definitionen ein hohes Risiko für Mehrdeutigkeit, Dialektbildung und nicht-interoperable sowie fehleranfällige Implementierungen besteht.

Diese ungünstige Situation wird dadurch verschärft, dass für den Standard keine fertige Referenzimplementierung existiert, an der sich Softwarehersteller in den Lücken und Unschärfen der Spezifikation orientieren könnten.

Die hohe Flexibilität des XTA-Standards birgt nicht nur die Gefahr von schwerer Handhabbarkeit, sondern erfordert insbesondere in den Service-Profilen eine hohe, teilweise sehr technische und fachliche Expertise. Damit ergibt sich das Risiko, dass Schutz- und Sicherheitsaspekte sowie die dazu einzusetzenden Methoden unter-, über- oder gar widersprüchlich definiert sind. Die in mehreren Interviews geforderte Erleichterung durch »Standardprofile«, die auch in Dokumenten des XTA-Standards als Erwartungshaltung geäußert wird [48, S. 14], hat sich im Standard nicht materialisiert. Die fehlende Verbindlichkeit im Bereich der Service-Profile, verbunden mit vielen Unklarheiten und Freiheitsgraden, ist aus Sicht des Autorenteam nicht nur der Grund für Probleme in der Interoperabilität, sondern auch insgesamt für eine Ineffektivität des XTA-Standards hinsichtlich seiner expliziten Ziele für eindeutige, überprüfbare Steuerung der Service-Qualitäten des Transports, siehe [48, S. 13]. Auch finden sich Hinweise auf eine Vermischung von Fach- und Transportlogik sowie einer engen Kopplung an Mechanismen der OSCI-Kommunikation. Dies widerspricht den formulierten Zielen der »Abtrennung von der Technik«.

Folgende Teile der Spezifikation sind dafür aus Sicht des Autorenteam Belege:

- *Zu Service-Profilen:* Im einleitenden Kapitel der XTA-Spezifikation [43, S. 3] wird auf folgendes hingewiesen: »In der vorliegenden Version sind die Profile und die zugehörige Protokollierung optional und müssen nicht vom implementierten XTA-System les- und interpretierbar sein.« Dies lässt also für eine XTA-Implementierung unverbindlich, dass z. B. mittels Kryptografieprofilen der Einsatz einer vorgegebenen Verschlüsselung der Daten gesteuert und sichergestellt wird. Selbst wenn eine profilkonforme Umsetzung des Profils »hart codiert« vorliegt, bedarf eine mit dem Schutzbedarf korrespondierende Definition des Kryptografieprofils einer hohen fachlichen Kryptokompetenz. Zudem birgt dies in Abwesenheit von standardisierten Profilen für unterschiedliche Schutzbedarfe ein hohes Risiko für inadäquate Vorgaben. Auch die Umsetzung der Vorgaben für Rechtssicherheit in Schutz- und Infrastrukturprofilen sind durch die mangelnde Verbindlichkeit nicht gewährleistet. Aus Sicht der Autorengruppe der vorliegenden Studie ist es unverständlich, dass ein Standard mit hohem Reifegrad (Version 5) zwar die maschinenlesbare Formulierung von Servicequalitäten in Service-Profilen unterstützt, aber nicht die maschinelle Interpretation und Konfiguration einfordert. Der Standard stellt also frei, ob eine Software die Servicequalitäten auf Basis der Profile konfiguriert oder für einen bestimmten Fachstandard »hart codiert«. Auch die vorangegangene BVA-Studie stellt dieses Defizit in Standard und Implementierungen fest [53, S. 65] und fordert diesbezüglich eine entsprechende

Umsetzung. Die fehlende Verbindlichkeit hinsichtlich Service-Profilen stellt die tatsächliche Interoperabilität und Verlässlichkeit der Einhaltung der Vorgaben an Servicequalitäten – und damit die generelle Effektivität des Standards – für existierende Implementierungen in Frage.

- *Zu Infrastruktur- und Kryptografie-Profilen:* Sind mehrere Verweise auf Infrastruktur- oder Kryptografieprofile angegeben, so »[...] liegt es in der Zuständigkeit der Rolle des Senders, das für einen gegebenen Transportauftrag geeignete [...] Profil aus den referenzierten [...] Profilen auszuwählen« [43, S. 5]. Es gibt für den jeweiligen Profiltyp in den spezifischen Beschreibungen Hinweise auf einzelne Daten, die Entscheidungsmerkmale sein könnten. Generell bleibt jedoch unklar, was die Kriterien für ein »geeignetes« Profil sind und nach welchen es ausgewählt werden soll. Umgekehrt gesprochen bleibt unklar, wann es notwendig ist, mehrere Infrastruktur- und Kryptografieprofile anzugeben.
- *Zu Infrastrukturprofilen:* Laut [43, S. 16] kann nur für eine der vier Rollen (Autor, Sender, Empfänger, Leser) eine Zertifikatsvorgabe bestehend aus Zertifikatsherausgeber (z. B. PKI1-Verwaltung), gemacht werden. Die Spezifikation lässt im Unklaren, wie mehr als eine Vorgabe umgesetzt werden kann.
- *Zur Partneridentifikation:* »Die Prüfung der Zertifikate [...] ist eine optionale Serviceleistung der Transportinfrastruktur.« [43, S. 61]. Es ist unklar, warum dies hervorgehoben und die Prüfung der Zertifikate nur als eine optionale Serviceleistung der Transportinfrastruktur dargestellt wird. Eine Prüfung sollte standardmäßig ausgeführt werden, da ansonsten grundlegende Sicherheitsqualitäten in Frage gestellt sind. Aus der Dokumentation erschließt sich eine Begründung nicht.
- *Qualitätsangaben generell:* Relevante Begriffe sind häufig nicht klar definiert. Obwohl im Anhang A.2.10 des XTA-Standards bei den verwendeten qualitativen Schutzbedarfen »normal« und »hoch« auf die vom BSI definierten Begriffe zum IT-Grundschutz Bezug genommen wird, fehlt im Anhang A.2.11 eine eindeutige Definition der verwendeten qualitativen Begriffe. Es ist lediglich von »einfachem« und »sicherem« Löschen die Rede, ohne dass die Begriffe näher definiert werden. Gleiches gilt im Anhang A.2.12 für die Qualitätsanforderung »hoch«. Diese verlangt eine »revisionssichere Protokollierung«, was jedoch nicht weiter ausgeführt wird und damit unbestimmt bleibt. Ähnliches gilt in den weiteren Anhängen A.2.9, A.2.13 und A.2.15, in denen qualitative Angaben gemacht werden.

Der XTA-Standard wirkt darüber hinaus an verschiedenen Stellen überkomplex:

- *Zu (mehrfach definierbaren) Infrastruktur- und Kryptografieprofilen:* Wie oben bereits ausgeführt, ergeben sich hohe Freiheitsgrade durch die Möglichkeit der Vorgabe mehrerer Infrastruktur- und Kryptografieprofile ohne klare

Vorgaben, zu welchem Zweck mehrere Vorgaben gemacht werden oder wie das »geeignete« Profil ausgewählt werden soll.

- *Zu Schutzprofilen:* Es existiert ein hoher Freiheitsgrad in der Definition unterschiedlicher Vertraulichkeits-Parametersätze für unterschiedliche Abschnitte der Gesamtkommunikationsstrecke zwischen Autor und Leser. Es ist unklar, ob diese Mittel in der Praxis ausgeschöpft werden.
- *Zu Infrastrukturprofilen:* Die Löschfristen laut XTA-Spezifikation sind nicht im Schutzprofil, sondern in den Infrastrukturprofilen festzulegen. Die Sinnhaftigkeit, an verschiedenen Stellen unterschiedliche Löschfristen für Daten- und Protokollinhalte zu definieren, erschließt sich allenfalls durch das »Hindurchsickern« von Transportlogik konkreter Infrastrukturen in das jeweilige Infrastrukturprofil. Wenn Löschfristen in erster Linie fachlich begründet sind, sollte es idealerweise nur eine Vorgabe geben.
- In Bezug auf den Funktionsumfang der verfügbaren XTA-Server hinsichtlich des XTA-Standards stellt die BVA-Studie [53, S. 65] Folgendes fest: *»Im Rahmen der OSCI-Studie konnte kein XTA-Server identifiziert werden, der den Standard vollständig implementiert.«* Als Begründung dafür wurde in der Studie und in Interviews angegeben, dass die Entwicklung der XTA-Server bedarfsgetrieben erfolge. Da es am Markt nicht viele Implementierungen für XTA-Server gibt, aber keiner davon den XTA-Standard vollständig umsetzt, ist dies ein klares Indiz für eine Überkomplexität des Standards. Dieser stellt offensichtlich Anforderungen, die sich nicht in den realen Bedarfen ausdrücken.

Eine Vermischung von Fach- und Transportlogik – womit der XTA-Standard aus Sicht des Autorenteam nicht dem Anspruch einer Abstraktionsschicht gerecht wird [48, S. 13ff] – äußert sich gemäß unserer Analyse in folgenden Punkten:

- *Fehlender Hinweis im XTA-Standard auf Schemavalidierung und andere Mehrwertdienste in den praktischen XTA-Server-Implementierungen:* Die BVA-Studie zu OSCI / XTA [53, S. 46ff] weist darauf hin, dass XTA häufig dazu verwendet wird, bestimmte Aufwände von den Fachverfahren zu den XTA-Servern zu verlagern, beispielsweise zur Delegation der Inhaltsdatenverschlüsselung oder der Schemavalidierung. Demnach erfordert auch die Übersetzung der Fachnachricht vom XTA-Standard nach OSCI die Kenntnis des diesbezüglichen Fachstandards durch den XTA-Server. Deswegen ist diese Validierungs- und Transformationslogik fest in den XTA-Servern implementiert und muss für jeden neuen Fachstandard ergänzt werden. Dadurch ergibt sich laut der BVA-Studie eine Kopplung der XTA-Server-Implementierung an die XÖV-Fachstandards, also eine Vermischung von Fach- und Transportlogik in den XTA-Servern [53, S. 65f], sowie ein Hindernis für eine Ende-zu-Ende-Verschlüsselung zwischen Autor und Leser. Zwangsweise Folge dieser Kopplung ist, dass bei Aktualisierung oder Einführung eines neuen Fachstandards auch die existierenden XTA-Server aktualisiert werden

müssen.

Dies wurde in eigenen Interviews der vorliegenden Studie bestätigt. So wurde beispielsweise bei Kommunikationstests neuer XÖV-Fachstandards der Transport durch den eingesetzten XTA-Server unerwartet wegen einer fehlgeschlagenen Schemavalidierung des für den Server noch unbekannten Fachstandards abgelehnt.

Diese fehlende Entkopplung des XTA-Standards von der Transportebene liegt – wie auch schon in [53] festgehalten – teilweise in der Verantwortung der Softwarehersteller der XTA-Server. Andererseits, wie in derselben Studie festgehalten [53, S. 40], ergibt sich diese Notwendigkeit aus fehlenden Möglichkeiten im Standard, die exakte Übersetzung einer XTA-Fachnachricht in bereits existierende OSCI-XÖV-Fachstandards konfigurieren zu können. Dies befördert die ohnehin schon hohe Komplexität von XTA.

Da OSCI-Nachrichten aber sowohl auf Sender- wie auf Empfängerseite mit und ohne XTA-Server erstell- und lesbar sein müssen, ergibt sich durch dieses Defizit im XTA-Standard vermutlich der Zwang für die Hersteller, die Logik aus den Fachstandards in die XTA-Server mit aufzunehmen.

Ein Ausweg aus dieser Situation wäre möglicherweise die Festlegung von XTA-Standardprofilen und eine Anpassung der Fachstandards gewesen. Dies ist jedoch nie erfolgt – vermutlich aufgrund des hohen Einigungs- und Aktualisierungsbedarfs.

- *Verwendung der Service-Profile in XTA:* Die XTA-Profile abstrahieren zwar in Teilen von technischen Eigenschaften und zielen laut XTA-Rahmenbedingungen [48] auf eine »technikneutrale« Formulierung der Servicequalitäten ab. In Abschnitt 4.1.1 der XTA-Rahmenbedingungen wird jedoch klar, dass dies nicht vollständig in den Service-Profilen umgesetzt wird. Stattdessen setzt der XTA-Standard auf die Kooperation zwischen »Fachverantwortlichem« und »Transportzuständigem« bei der Erstellung der Profile. Der Fachverantwortliche erstellt dazu die fachlichen Anforderungen, die von dem auf technischer Transportebene versierten Transportzuständigen in die eher technischen Parameter der Kryptografie- und Infrastrukturprofile umgesetzt werden.
Die XTA-Service-Profile abstrahieren folglich nicht die Vorgabe der Servicequalitäten, sie trennen lediglich die Zuständigkeit für das Ausfüllen unterschiedlicher Teile desselben XML-Dokuments zwischen verschiedenen Personen, wie in Abbildung 15 dargestellt.
- *Zu Infrastrukturprofilen:* Die in den Codelisten des Infrastrukturprofils aufgeführten Codes – z. B. zu Nachrichtenformat oder Verzeichnisdiensten – sind in erster Linie auf die existierende OSCI-Infrastruktur angepasst. Auch hier besteht eine klare Verbindung zu technischen Eigenschaften der Transportstrecke.

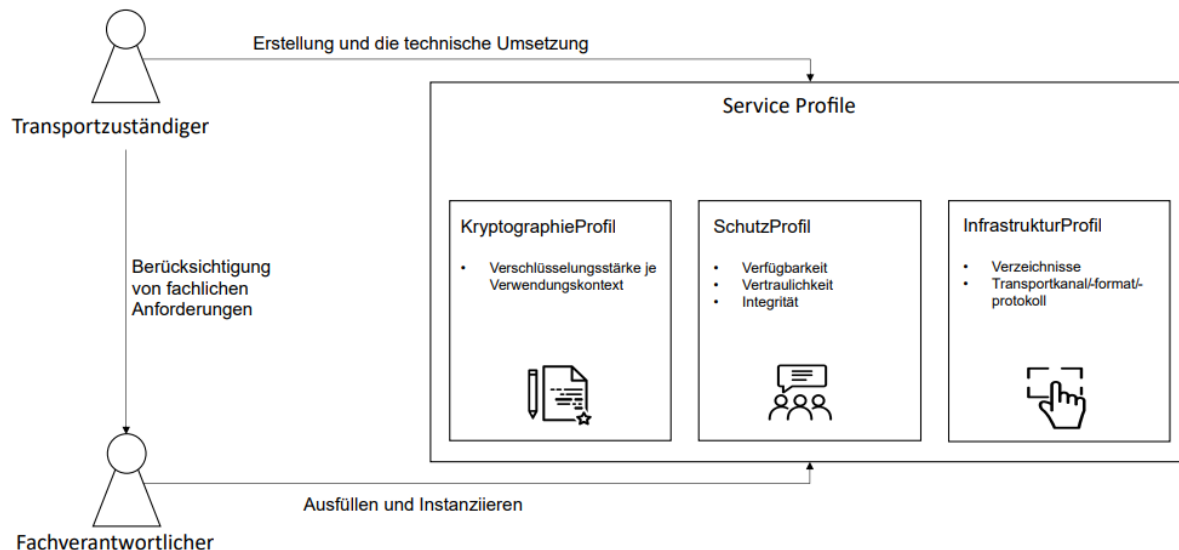


Abbildung 15 XTA-Kooperationsmodell für die Definition von Service-Profilen [48]

- Zu Kryptografieprofilen: Die unabhängige Definition von widersprüchlichen Sicherheitseigenschaften im XTA-Standard belegt beispielhaft sowohl eine Unterspezifizierung als auch Vermischung von Fach- und Transportlogik: Verschlüsselungsqualität und Schutzbedarf lassen sich getrennt voneinander definieren. So kann etwa der Schutzbedarf »hoch« eingestuft werden, aber die gewählten Algorithmen oder deren Parameter dem Schutzbedarf nicht genügen (z. B. bei hohem Schutzbedarf aber zu kurzen Schlüssellängen). Natürlich ist hier der Transportzuständige in der Verantwortung, die korrekten technischen Servicequalitäten zu bestimmen. Andererseits ändert sich die Einschätzung der Sicherheit dieser technischen Parameter über die Zeit, nicht aber die fachliche Anforderung eines hohen oder normalen Schutzbedarfs. Bei XTA sind beide jedoch in einem Dokument vermisch.
- Zu Transportaufträgen: Laut Abschnitt 2.3.1.6 des XTA-Standards können im Transportauftrag Metadaten zur fachlichen Nachricht eingetragen werden: »Die Struktur [...] bietet für die Weiterverarbeitung Aspekte der fachlichen Einordnung der Fachnachricht an. Dies gilt auch für Transportprozesse, die nicht auf die Fachnachricht zugreifen sollen.« Damit werden Anwendungs- und Transportebene vermisch. Diese Vermischung wird mit höherem Komfort begründet, was aus unserer Perspektive keine ausreichende Begründung für dieses Konstrukt darstellt: »Der Zweck der durch den Autor an dieser Stelle einzufüllenden Information des Transportauftrags ist, dass der Leser bereitliegende Fachnachrichten filtern kann, ohne sie lesen bzw. analysieren zu müssen. Er kann die Information beispielsweise als Suchfeld für den Abruf aus dem Postfach einsetzen.« [43, S. 57].

Wie in den Abschnitten 4.3.1.2 und 4.3.2.2 aus den XTA-Dokumenten zitiert, ist eines der Hauptziele von XTA, eine einheitliche Definition und Konfiguration für die funktionale Steuerung der Servicequalitäten auf der Transportstrecke durch Service-Profile zu ermöglichen. Da es jedoch auch in der aktuellen Version 5.1.1 weitgehend an einer Verbindlichkeit hinsichtlich der Konfigurierbarkeit und Umsetzung mittels Service-Profilen fehlt, leidet nicht nur die Interoperabilität, sondern der Standard selbst ist in diesen Teilen aus Sicht des Autorenteam der Studie ineffektiv.

Wie in Abschnitt 4.3.5 festgestellt, sind die am Markt befindlichen XTA-Server insbesondere für Kommunen im Betrieb eine Herausforderung. Die Überkomplexität gepaart mit der Unterspezifizierung des Standards führen zu sehr diversen Betriebsszenarien, wie in Abschnitt 4.3.6 beschrieben, wodurch sich eine sehr heterogene Infrastruktur ergibt.

Existierende Fachstandards delegieren die Verschlüsselung der Inhaltsdaten in den allermeisten Fällen zum XTA-Server, um Mehrwertdienste in Anspruch zu nehmen. Dies verhindert eine Ende-zu-Ende-Verschlüsselung (E2EE). Generell fördern die Konzepte des XTA-Standards nicht den Einsatz von E2EE, weswegen sie auch nur in Ausnahmefällen angewendet werden.

W – Weaknesses (Schwächen)

- Fragmentierte Governance (analog OSCI)
- Unterspezifiziert, nicht eindeutig
- Überkomplex, dadurch schwer zu handhaben
- Ineffektiv hinsichtlich der datenschutztechnischen und rechtlichen Servicequalitäten durch Unverbindlichkeit von Service-Profilen
- Vermischung von Applikations- und Transportlogik
- Keine Referenzimplementierung (lediglich Entwurf)
- Keine frei verfügbare Referenzumgebung
- Verbreitete XTA-Server sind nicht quelloffen
- Schwache Konformitätsprüfung und -regelung
- Fokussierung auf OSCI als Nachrichtenprotokoll
- Herausforderungen im Betrieb der XTA-Server für kleine Kommunen und Organisationen, daraus resultierend heterogene Infrastruktur
- In der Praxis Hindernis für Ende-zu-Ende-Verschlüsselung

5.2.2.3 Chancen

Der XTA-Standard ist in Teilen der Innenverwaltung etabliert mit einem existierenden Ökosystem von Software-Lieferanten und -Nutzern. Dieses Ökosystem könnte für eine Weiterentwicklung und -verbreitung des Standards genutzt werden. Obwohl OSCI und XTA oft miteinander assoziiert werden, ist die Nutzerschaft von XTA deutlich kleiner als die Nutzerschaft von OSCI. XTA besitzt also nicht in allen Teilen des OSCI-Ökosystems dieselbe Akzeptanz wie OSCI selbst. Über die OSCI-Nutzerschaft hinaus ist XTA jedoch kaum verbreitet. Die punktuell hohe Akzeptanz von XTA in der Verwaltung äußert sich beispielsweise in der Tatsache, dass XTA in manchen Verordnungen als verbindlich genannt wird.

Aus Sicht des Autorenteam ist der Einsatz von XTA in Verbindung mit anderen Nachrichtenprotokollen und -infrastrukturen wie etwa AS4 oder FIT-Connect eine Chance, XTA über eine reine OSCI-Abstraktionsschicht hinaus als einheitliche, technologie neutrale Schnittstelle für Fachverfahren zu etablieren. Wie in Abschnitt 5.2.2.2 dargelegt, würde das jedoch die Beseitigung vieler Defizite im XTA-Standard erfordern. Auch wären im Sinne einer stärkeren Abstraktion und Vereinfachung für die Nutzenden die Definition von Standardprofilen ein echter Mehrwert.

O – Opportunities (Chancen)

- Existierendes »Ökosystem« von Software-Lieferanten und -Usern
- Hohe Akzeptanz in Teilen der Verwaltung
- Möglichkeit höherer Technologie neutralität im Nachrichtenprotokoll
- Möglichkeit höherer Akzeptanz durch Definition von Standardprofilen

5.2.2.4 Risiken

Die hohe Komplexität sowie zahlreiche Unklarheiten im XTA-Standard, verbunden mit vielen Freiheitsgraden erklären, warum der XTA-Standard in der Vergangenheit nicht flächendeckend angenommen wurde. Wie durch Interviews und auch in einer vorangegangenen Studie [49, S. 18] festgestellt, sind insbesondere die Defizite in der Klarheit des Standards nicht nur eine Markthürde für Softwarehersteller ohne Erfahrung mit OSCI / XTA, sondern fördern gemeinsam mit schwacher Konformitätsregelung auch eine Dialektbildung. Auch aus dem Kreis der Interviewpartner, die OSCI mit oder ohne XTA einsetzen, wurde Zurückhaltung oder Ablehnung beim Einsatz von XTA mit dem Argument bekundet, dass XTA für sie in Summe keinen oder wenig Mehrwert erbringe. Der Einsatz der notwendigen XTA-Server verursache hingegen zusätzliche Komplexität und Kosten.

Folgende Indizien stützen diese Befunde:

- In den XTA-Rahmenbedingungen [48] wird der Bereich der Justiz als besonders geeignet für die Anwendung von XTA genannt. In einem Interview mit Mitgliedern eines Standardisierungsgremiums in der Justiz wurde jedoch festgestellt, dass XTA im Justizbereich praktisch nicht zum Einsatz komme. Als Grund wurde der hohe Grad an Standardisierung der eingesetzten OSCI-Fachstandards genannt. Dadurch werde eine darüberliegende Entkopplungs- oder Abstraktionsschicht nicht als mehrwertstiftend angesehen.
- Ein besonderer Fall ergab sich bei der Anbindung des IDA-Fachverfahrens durch das BVA. Hier ist der Einsatz von XTA per Verordnung vorgeschrieben (siehe XBasisdaten-Verordnung [46]). Laut Interviews hatten sich Beteiligte im Konsultationsprozess aus Gründen der Reduktion von Komplexität für die Anbindungsoption mittels OSCI, ohne XTA, ausgesprochen. Gemäß diesen Interviewteilnehmern wurde eine Änderung der Verordnung jedoch als unerwünscht angesehen. Einen Teil der Gründe, warum sich die Umsetzung des Projekts stark verzögerte, sieht das BVA in Herausforderungen mit der XTA-Anbindung selbst begründet (z. B. fehlende oder nicht-standardkonforme Unterstützung bestimmter XTA-Funktionen durch den ausgewählten XTA-Server). Als Fazit sieht das BVA für zukünftige Anbindungen eine Option über REST als bevorzugte Lösung an.
- In den XTA-Rahmenbedingungen [48, S. 14] wird als voraussichtlicher Mehrwert von XTA Folgendes angegeben: *»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.«* Im Rahmen dieser Studie konnte nicht im Detail geklärt werden, ob sich wiederkehrende Konfigurationen ergaben. Das Fehlen von Standardkonfigurationen auch für Version 5 wurde jedoch in Interviews als versäumter Mehrwert genannt. Die Standardisierung von Konfigurationen wäre auch aus Sicht des Autorenteam eine Chance für die Überleitung in echte Abstraktion von der Transportebene gewesen. Sie ist jedoch bis heute nicht im Standard selbst angelegt.
- Einer der weiteren fehlenden Mehrwerte ist, dass sich der Standard nie entschieden in Richtung anderer unterstützter Transportprotokolle als OSCI entwickelt hat. Die Unterstützung von Peppol/AS4 durch eine spezialisierte Version des COM Despina der Firma Governikus scheint hier eine Ausnahme zu sein, die sich jedoch nicht im XTA-Standard manifestiert hat. In einem Interview eines Herstellers von OZG/EfA-Leistungen wurde berichtet, dass ihre

Software die Anbindung zu Fachverfahren über FIT-Connect und XTA an die OSCI-Infrastruktur umsetzt. In einer idealen Konstellation müsste der Softwarehersteller lediglich die XTA-Schnittstelle implementieren und der XTA-Server würde für den Adressaten den korrekten Nachrichtenkanal wählen.

Die Risiken beim Einsatz von XTA lassen sich in folgenden Punkten zusammenfassen:

Insbesondere die Defizite und mangelnde Verbindlichkeit von Teilen des XTA-Standards, siehe auch Abschnitt 5.2.2.2, führen zu einer mangelnden funktionalen Abdeckung und geringen Interoperabilität der existierenden Implementierungen, siehe dazu auch Abschnitt 4.3.5. Der aus den Defiziten des Standards resultierende hohe Aufwand bei der Anbindung neuer Fachverfahren über XTA führt zu einer zurückhaltenden Akzeptanz bei den potenziellen Nutzern des Standards, insbesondere den Fachverfahrensherstellern. Auch die Fokussierung auf OSCI als Nachrichtenprotokoll und fehlende Unterstützung weiterer Protokolle schmälern dessen Attraktivität. Diese Umstände in Summe werden von Entscheidungsgremien wahrgenommen und führen zu einer Zurückhaltung bei Entscheidungen zugunsten des Einsatzes von XTA.

Gegen eine hohe Akzeptanz bei unterschiedlichen Gruppen spricht außerdem die nur nationale Verbreitung von XTA und die technologische Basis von SOAP, XML und WSDL, deren Verbreitung am Markt schwindet.

T – Threats (Risiken)

- Basiert auf Technologie mit abnehmender Verbreitung (SOAP, XML, WSDL), dadurch potenzieller Engpass bezüglich Fachpersonal
- Gefahr der Dialektbildung, geringe Interoperabilität existierender Implementierungen
- Geringe Akzeptanz seitens der Fachverfahrenshersteller wegen der Komplexität neuer Anbindungen, unter anderem bedingt durch das Fehlen von Standardprofilen
- Geringe Attraktivität mangels Unterstützung anderer Transportprotokolle als OSCI
- Nur nationale Verbreitung, keine Aufnahme in den Deutschland-Stack

5.2.3 FIT-Connect

Die SWOT-Analyse bezieht sich FIT-Connect Version 2, siehe Abschnitt 4.4.

5.2.3.1 Stärken

Die frei zugängliche Dokumentation von FIT-Connect ist sehr umfangreich und gut strukturiert. Außerdem existieren kleine Video-Tutorials für jeden Schritt und jeden Stakeholder, der an der Anbindung eines Clientsystems an FIT-Connect beteiligt ist. Das macht es sehr einfach, die Anbindung vorzunehmen. Auch die Nutzung des Self-Service-Portals und der SDKs ist in den Video-Tutorials mit Screencasts gut erklärt.

Mittels der regelmäßig angebotenen virtuellen Austauschformate des FIT-Connect-Teams können sich die unterschiedlichen Stakeholder rund um FIT-Connect austauschen und vernetzen. Das trägt zur Bildung einer Nutzer-Community bei, in der sich die Teilnehmer gegenseitig helfen und unterstützen können. FIT-Connect unterliegt in der Weiterentwicklung von Infrastruktur und Software einer effektiven, zentralen Governance.

Die regelmäßig aktualisierten SDKs für die im Enterprise und Web-Umfeld gängigen Programmiersprachen Java, .NET und JavaScript erleichtern Entwicklerteams die Arbeit. Sie ermöglichen es, die FIT-Connect Plattform mit nur wenigen Zeilen Code anzubinden, sodass sich die Entwickelnden darauf konzentrieren können, die eigentliche Fachlichkeit für die Antragserstellung und Antragsbearbeitung umzusetzen. Auch das Debugging und die Fehlersuche gestaltet sich relativ einfach, da die SDKs quelloffen sind und im Fehlerfall ein Debugging ermöglichen.

Die frei zugängliche Testumgebung ermöglicht ein schnelles Testen der FIT-Connect Anbindung mit nur wenig Aufwand, sodass FIT-Connect insgesamt eine sehr gute Developer-Experience bietet.

Die quelloffenen SDKs und die modernen REST-Schnittstellen ermöglichen eine einfache Integration in Software von Drittanbietern oder Unternehmen. Auch ist die Verfügbarkeit von Entwickelnden mit Erfahrung bezüglich REST-Schnittstellen und den Programmiersprachen der SDKs hoch.

FIT-Connect ist bereits bei einigen Kommunen und Behörden im Produktivbetrieb. Dadurch verfügt das Team über Praxiserfahrung und konnte bereits testen, ob die Konzepte von FIT-Connect in der Praxis funktionieren. Auch erste »Kinderkrankheiten«, die häufig bei der Einführung eines neuen Softwaresystems auftreten, wie zum Beispiel Problemen mit der Zertifikatsvalidierung aufgrund falscher Server-Zeitbasis, wurden laut Aussagen im Interview bereits behoben.

Das Self-Service-Portal ermöglicht eine selbstständige Anbindung von OZG-Portalen oder Fachverfahren. Dies vermeidet organisatorische »Flaschenhälse«, da Kommunen und Portalbetreiber zur Konfiguration von Anbindungen nicht auf Sachbearbeitende für FIT-Connect angewiesen sind. Im Self-Service-Portal

existieren außerdem Teamfunktionen, die Dienstleistern die Durchführung entsprechender Konfigurationsaufgaben im Auftrag ermöglichen. Für Dienstleister bietet FIT-Connect spezielle APIs, um diese Aufgaben zu automatisieren. Diese Funktionen tragen zur Skalierbarkeit von FIT-Connect bei. Im Interview wurde außerdem auf die Möglichkeit hingewiesen, den Status von Übertragungen im Self-Service-Portal einsehen zu können, was eine Fehlersuche unterstützen kann.

Ende-zu-Ende-Verschlüsselung wird über das SDK direkt unterstützt. Lediglich Metadaten zur Adressierung und zum Routing liegen innerhalb der Plattform unverschlüsselt vor.

S – Strengths (Stärken)

- Zentrale Governance von FIT-Connect über die FITKO
- Sehr gute Dokumentation inklusive Video-Tutorials
- Virtuelle Austauschformate (Videokonferenzen) für unterschiedliche Stakeholder (User, Entwicklerteams etc.)
- Nutzung moderner REST-Schnittstellen
- Client-SDKs für Java, .NET und JavaScript verfügbar und quelloffen
- Testumgebung frei zugänglich
- Erste Praxiserfahrung aus dem Produktivbetrieb
- Self-Service für Teilnehmer in der FIT-Connect-Infrastruktur
- Integrierte Ende-zu-Ende-Verschlüsselung der Inhaltsdaten

5.2.3.2 Schwächen

Da FIT-Connect noch nicht in allen Bundesländern und bei allen Kommunen und Behörden im Einsatz ist, fehlt noch Praxiserfahrung, wie gut die Plattform mit einer solchen Last umgehen kann. Dies gilt nicht nur für die IT-Systeme, sondern auch für den Support und die Organisation dahinter, die ja auch entsprechende personelle Kapazitäten (z. B. Supportmitarbeiter) bereitstellen muss.

Im Interview wurde bestätigt, dass die zentrale FIT-Connect-Plattform im Moment noch nicht geo-redundant betrieben wird. Wenn es also zu einem großen technischen Problem oder zu einem groß angelegten DDoS-Angriff käme, ist ein Ausfall der FIT-Connect Plattform sehr wahrscheinlich. Solch ein Ausfall führt dazu, dass keine Anträge über FIT-Connect an die zuständigen Fachverfahren übermittelt werden können. Insbesondere im Hinblick auf die zunehmende Nutzung von FIT-Connect und auch die zunehmende Anzahl an Cyberangriffen ist dies ein erhebliches Risiko.

Die zentrale Plattform ist nicht quelloffen. Sollte es zu einer Einstellung der Finanzierung der Entwicklung vom Bund kommen, gibt es im Moment für die Bundesländer oder einen von den Bundesländern beauftragten IT-Dienstleister keine Möglichkeit, die Plattform eigenständig zu betreiben und weiterzuentwickeln. Auch Sicherheitsaudits der Plattform können von unabhängigen Dritten nicht ohne weiteres durchgeführt werden. Außerdem ist eine einfache Nachnutzung der durch Steuergelder finanzierten FIT-Connect-Plattform in anderen Kontexten somit nicht möglich.

W – Weaknesses (Schwächen)

- Unsicherheiten bei der Skalierbarkeit der zentralen Plattform bei großflächigem Rollout von FIT-Connect in ganz Deutschland
- Ausfall des gesamten Dienstes durch Angriff oder technische Störung der zentralen Plattform
- Zentrale Teile der Plattform sind nicht Open-Source, dadurch Risiken beim Übergang von Verantwortlichkeiten und fehlende Möglichkeit unabhängiger Sicherheitsaudits und Nachnutzung

5.2.3.3 Chancen

Der enge Austausch mit dem Projekt ZaPuk (Abschnitt 4.6) und die anlaufende Integration von Matrix in FIT-Connect bietet das Potenzial, die einheitliche Postfachinfrastruktur von ZaPuk für die Kommunikation rund um einen Antrag zu nutzen. Mit Hilfe von Matrix ist auch eine einfache Integration von Audio- und Videostreaming möglich.

Die Roadmap von FIT-Connect ist transparent und für jeden einsehbar, sodass sowohl User als auch Entwickelnde wissen, an was FIT-Connect gerade arbeitet. Das ermöglicht Herstellern von Fachverfahren und OZG-Portalen einen Abgleich ihrer internen Feature-Roadmaps mit der FIT-Connect-Roadmap. Auch jede interessierte Privatperson kann sich ein Bild machen, wofür die Mittel bei der Entwicklung für FIT-Connect verwendet werden.

Die Möglichkeit, Feedback über Issues in einem openCode-Repository Feedback an das FIT-Connect Team heranzutragen, bietet die Chance, die Anforderungen von Nutzenden, Entwickelnden und Entscheidenden in der FIT-Connect-Roadmap frühzeitig zu berücksichtigen.

Die Aufnahme von FIT-Connect in den Deutschland-Stack als Basisdienst für Datenaustausch fördert die Verbreitung von FIT-Connect und sichert perspektivisch den Betrieb dieser Plattform.

O – Opportunities (Chancen)

- Austausch mit ZaPuK für die Integration von Matrix
- Transparente Roadmap
- Möglichkeit für externes Feedback auf openCode
- Entscheidung zur Aufnahme in den Deutschland-Stack

5.2.3.4 Risiken

FIT-Connect ist eine rein nationale entwickelte und eingesetzte Plattform. Damit ist FIT-Connect nicht direkt anschlussbereit an europäische Infrastruktur, auch besteht keine direkte Möglichkeit zur internationalen Kooperation zur Weiterentwicklung der Plattform.

T – Threats (Risiken)

- Nur nationale Verbreitung

5.2.4 NOOTS

Die SWOT-Analyse bezieht sich auf das NOOTS und seine offen einsehbare Dokumentation zum Entwicklungszeitpunkt Juli 2026, siehe Abschnitt 4.5.

5.2.4.1 Stärken

Die Entwicklung des NOOTS setzt von Beginn an auf eine *zentrale Steuerung* durch das Bundesverwaltungsamt (BVA). Eine klare Governance ist wichtig, um für einheitliche, interoperable Lösungen Sorge zu tragen und einer »Dialektbildung« durch inkompatible Protokollimplementierungen oder auseinanderdriftende Protokollversionen vorzubeugen. Insbesondere wird der SAK, ein Kernelement der NOOTS-Architektur, den NOOTS-Teilnehmern als verbindliches Anschlusselement bereitgestellt, und das BVA verantwortet auch die zentralen Komponenten des NOOTS (z. B. DAMAS, VS, RDN).

Das Sicherheitskonzept des NOOTS ist so gestaltet, dass eine kompromittierte einzelne Systemkomponente nicht das System als Ganzes kompromittieren kann. Das Konzept beruht auf einem *Zero-Trust-Paradigma* [132] mit mehreren Verteidigungslinien, bei dem sich die beteiligten Architekturkomponenten sowie die Datenkonsumenten und Datenregister gegenseitig rückversichern, dass sie mit

einer authentischen Gegenstelle integritätsgesicherte Daten austauschen. Dadurch sind punktuelle Angriffe auf NOOTS nicht ausgeschlossen, aber eine flächendeckende Unterwanderung des Systems kann so unterbunden werden.

Zur Resilienz des NOOTS trägt auch die Gestaltung Anschlussknoten bei. Ein Entwurfsziel war eine möglichst *leichtgewichtige, zustandslose SAK-Realisierung*. Das Vermeiden von dynamischen Zustandsdaten vereinfacht die Fehlerbehandlung beim SAK-Betrieb und erleichtert die Umsetzung von Redundanzmechanismen (z. B. Stand-by-Komponenten), um eine hohe Verfügbarkeit des Systems zu gewährleisten. Die Reduzierung von Komplexität vereinfacht zudem das Testen und Validieren der SAK-Software.

Der verpflichtende, zentral vorgegebene Anschlussknoten setzt darüber hinaus *einheitliche Mindeststandards*, da der SAK wichtige Sicherheitsmechanismen in geprüfter Qualität bereitstellen kann, wie etwa Schema-Validierung und Virenprüfung übertragener Nachrichten oder Ver- und Entschlüsselung. Dies entlastet die Fachverfahren-Software von Routineaufgaben und vermeidet eine fehlerhafte Umsetzung kritischer IT-Sicherheitsfunktionen.

Ein Alleinstellungsmerkmal des NOOTS-Konzepts im Vergleich zu den anderen betrachteten Technologien ist *umfassende Berechtigungsprüfung*. Abstrakt gesehen ist eine Berechtigung ein 3-Tupel bestehend aus Rolle, Nachweistyp und Verarbeitungszweck mit der Bedeutung »Die <Rolle> darf zum angegebenen <Verarbeitungszweck> auf den <Nachweistyp> zugreifen«. Das NOOTS-Konzept sieht vor, dass jeder Data Provider (DP) die Nachweisangebote seines Registers per Self-Service mittels DAMAS einpflegt – einschließlich der Zugriffsberechtigungen. Aufgrund der vorherrschenden großen Heterogenität bestehender behördlicher Register und dem Bestreben, einen möglichst schlanken Anschlussknoten bereitzustellen, bietet NOOTS nur den »kleinsten gemeinsamen Nenner«¹³. Zum Beispiel prüft der SAK nur die abstrakte Berechtigung einer Anfrage (siehe [84], Abschnitt 6.1.4), nicht aber konkrete, also fachliche (bzgl. Datenattributen) und technische (bzgl. Schnittstellenfunktionen) Berechtigung des individuellen Data Consumers (DC). Diese Prüfung obliegt dem DP, doch NOOTS stellt dafür unseres Wissens kein SDK oder vergleichbare Hilfsmittel bereit.

Für die Nutzung dieser technischen Möglichkeiten sind bundesweit eine Reihe von Herausforderungen zu bewältigen: Soll der DP die konkrete Berechtigung prüfen, so müssen sich alle NOOTS-Beteiligten über die verwendeten Rollen-, Nachweistyp- und Verarbeitungszweck-Bezeichnungen einig sein. Dies setzt aber bei Hunderten von Verarbeitungszwecken und Nachweistypen sowie möglicherweise Hunderten von Verwaltungsrollen entsprechende bundeseinheitliche Ontologien voraus, zu deren Existenz die vorliegende Studie keine näheren

¹³ Die Formulierung »SAK als kleinster gemeinsamer Nenner« stammt aus einem Experteninterview, das im Rahmen dieser Studie geführt wurde

Informationen ermitteln konnte. Wenn einheitliche Begrifflichkeiten bei allen NOOTS-Teilnehmern etabliert sind, ergeben sich durch die Vielzahl möglicher Berechtigungsstapel womöglich sehr aufwändige Berechtigungskonfigurationen. Dies stellt eine mögliche Herausforderung an die organisatorische Skalierbarkeit dar, die jedoch nicht Teil der technischen Betrachtung im Rahmen dieser Studie ist. Auch für den DP ist eine detaillierte fachliche Berechtigungsprüfung eine herausfordernde Aufgabe, solange das NOOTS kein standardisiertes, geprüftes SDK mit entsprechender Funktionalität bereitstellt.

Das NOOTS-Konzept für den Registerabruf wahrt die Datenhoheit der registerführenden Stelle. Die registerführende Stelle nutzt dazu das ausgeklügelte abstrakte und fachliche Berechtigungskonzept dieser Transporttechnologie und kann mittels DAMAS selbst spezifizieren, welche Daten sie für einen Registerabruf überhaupt freigibt und unter welchen Voraussetzungen und an welche Data Consumer er einen angefragten Nachweis ausliefert. Die Registerdaten verbleiben lokal beim DP, und der DP setzt die gewünschten Zugriffsbeschränkungen technisch durch.

Um den Anschluss an das NOOTS zu vereinfachen, ist der *SAK als Containerlösung mit REST-Schnittstelle* konzipiert. Dies bietet eine Programmiersprachen-unabhängige Lösung, vereinfacht die Wartung des SAK sowohl für das BVA als auch für den SAK-Betreiber und reduziert mögliche Fehlerquellen bei Installation, Konfiguration und Betrieb.

Das NOOTS erfordert kein gesondertes Verwaltungsnetz als Kommunikationsinfrastruktur. Es wird über das öffentliche Internet betrieben [81], ohne die Vertraulichkeit und Integrität der transportierten Daten zu kompromittieren. Sobald der geplante Informationsverbund der öffentlichen Verwaltung (IVÖV) flächendeckend verfügbar ist, kann NOOTS durch entsprechende Anpassung der SAK-Software mit geringem Aufwand auf die IVÖV-Infrastruktur umgestellt werden.

Das Eingliedern von Registern in das NOOTS wird durch ein *Self-Service-Konzept für Data Provider* vereinfacht. Jeder DP registriert dazu sein Informationsangebot im zentralen Datenmanagementsystem (DAMAS). Dabei legt der DP fest, welche Datenattribute in welchem Format von welchen Datenkonsumenten abgerufen werden dürfen. Der dezentral nutzbare Self-Service vermeidet einen bürokratischen Flaschenhals bei der Registrierung.

S – Strengths (Stärken)

- Zentrale Governance des NOOTS durch das BVA
- Zero-Trust-Paradigma mit mehreren Verteidigungslinien

S – Strengths (Stärken)

- Resilienzgewinn durch leichtgewichtiges, zustandsloses SAK-Design
- Durchsetzung von Sicherheitsmindeststandards durch verbindliche Nutzung eines SAK
- Umfassendes Berechtigungskonzept als Alleinstellungsmerkmal unter den betrachteten Technologien
- Wahrung der Datenhoheit des Data Providers
- Unkomplizierte Anbindung mittels offener REST-Schnittstelle, wahlweise über das Internet oder eine künftige IVÖV-Infrastruktur
- Self-Service für Data Provider zur Registrierung neuer Register

5.2.4.2 Schwächen

Da jeder Data Consumer (DC) jeden Data Provider (DP) erreichen können muss, müssen die SAK über das Internet erreichbar sein, was bedeutet, dass sie nicht in einem abgeschotteten Verwaltungsnetz platziert werden können. Die *SAK müssen in einer ans Internet angeschlossenen demilitarisierten Zone betrieben werden*. Dort sind sie Angriffen aus dem Internet ausgesetzt, da die Anzahl aller möglichen Kommunikationspartner (alle anderen SAKs) so hoch ist, dass die Einschränkung der Erreichbarkeit eines SAKs mit legitimen Gegenstellen bei Anbindungen über IPv4 nur schwerlich per IP-Adress-Whitelisting erzielt werden kann – was in vielen anderen in dieser Studie betrachteten Technologien möglich ist. Da der SAK absichtlich leichtgewichtig entwickelt wurde, um ihn auch durch kleinere Organisationen betreiben zu können, muss im Endausbau der NOOTS-Infrastruktur von einem Betrieb in lokalen IT-Netzen der unterschiedlichsten Professionalisierungsgrade ausgegangen werden, was in weiteren Angriffsvektoren auf einzelne SAK resultieren kann.

Auch wenn ein Angreifer sich aufgrund des Zero-Trust-Prinzips vermutlich nicht erfolgreich als behördliche Gegenstelle ausgeben kann, erleichtert die exponierte Lage der SAK zumindest Denial-of-Service-Angriffe sowie unter Umständen die Platzierung von Angriffen mittels sogenannter »Zero-Day-Exploits« und damit potenziell die Kompromittierung von SAKs. Da die SAK-Software zentral bereitgestellt und damit homogen ist, ließe sich ein erfolgreicher Angriff auf einen SAK voraussichtlich auch auf andere SAKs übertragen und könnte dann auch großflächige Störungen zu verursachen.

Wegen fehlender Erfahrung oder Dokumentation der Umsetzungskonzepte der zentralen Dienste wie VS, DAMAS und RDN ist derzeit *keine Aussage über die Resilienz einer resultierenden NOOTS-Infrastruktur möglich*. Die eigentliche

Kommunikation findet zwar dezentral über den direkten Datenaustausch zwischen den SAK statt. Das Zustandekommen dieses Datenaustauschs hängt jedoch von der Verfügbarkeit der zentralen NOOTS-Dienste ab. Für eine Bewertung der konkreten Ausgestaltung und zeitlichen Planung von Maßnahmen, um eine Resilienz dieser zentralen Dienste gegen Angriffe oder technische Störungen sicherzustellen, liegt in der verfügbaren Dokumentation keine Grundlage vor.

Eine weitere Schwäche des derzeitigen SAK-Konzepts ist die Wahl der *SAK als Endpunkte der Ende-zu-Ende-Verschlüsselung*. Obwohl NOOTS neben der Transportverschlüsselung mTLS zusätzlich noch eine Inhaltsverschlüsselung vorsieht, werden beide Verschlüsselungen im SAK aufgehoben, so dass dort die ausgetauschten Daten vollständig im Klartext vorliegen [84]. Dies beeinträchtigt die Vertraulichkeit insbesondere dann, wenn SAKs von privaten Dienstleistern im Auftrag der Behörde betrieben werden: Dann haben Dritte potenziellen Einblick in vertrauliche behördliche, oft personenbezogene Daten. Auch die weiter oben beschriebene netzwerktechnische Exponiertheit des SAK bietet hier zusätzliche Angriffsfläche in Bezug auf den Datenschutz.

Die geplante, derzeit offenbar noch *fehlende Mandantenfähigkeit* der SAK [133] [83] bedeutet, dass Behörden mit verschiedenen Fachverfahren viele isolierte SAK-Instanzen betreiben müssen, was den Betriebs- und Überwachungsaufwand erhöht und Ressourceneinsparungspotenziale vernichtet.

Die Präambel des NOOTS-Staatsvertrags sieht das NOOTS als die künftige Lösung für den gesamten Datenaustausch zwischen allen öffentlichen Stellen in Deutschland. Der *Fokus der Betrachtung liegt bisher auf dem Registerabruf* mittels XNachweis, was nur einen Teil relevanten Kommunikationsszenarien abdeckt. Einige der NOOTS-Konzepte könnten sich schließlich als unzureichend für gewisse Anwendungsfälle erweisen. So handelt es sich bei Abrufen zum Beispiel um synchrone Lesezugriffe, die mit einem aktiven DP (Long-Polling-Verfahren) oder einem passiven DP (Weiterleiten der Anfrage vom SAK an das Service-Provider-Interface des DP) realisiert werden (siehe [83], Abschnitt 7.5.1). Abzuwarten bleibt, ob die bestehenden NOOTS-Konzepte auch für fachlich asynchrone Transportszenarien oder gar für Änderungstransaktion, also Schreibzugriffe, tragfähig sein werden.

Da die NOOTS-Infrastruktur noch im Aufbau ist und die dahinterstehenden Konzepte zum Teil erst noch verfeinert werden müssen, ist die *verfügbare Dokumentation noch lückenhaft* und unterliegt beständigen Anpassungen und Erweiterungen. Zudem entspricht der Stand des Konzepts nicht immer dem Stand der Realisierung. Dies erschwert zum einen verbindliche Aussagen über das NOOTS und eine abschließende Bewertung; zum anderen stellt es eine Herausforderung für Fachverfahren und Anschlussknotenbetreiber dar, sich in die Infrastruktur zu integrieren. Konzeptionelle Missverständnisse können leicht zu Sicherheits-

schwachstellen, zumindest aber zu Inkompatibilitäten führen, die durch die zugrundeliegende Registermodernisierung ja gerade verhindert werden sollen.

W – Weaknesses (Schwächen)

- Exponiertheit des SAK in der Demilitarisierten Zone (DMZ) des Internetanschlusses aufgrund beschränkter Möglichkeiten zur Einschränkung der Erreichbarkeit aus dem Internet
- Ungewisse Resilienz zentraler NOOTS-Dienste gegen Angriffe und technische Störungen
- SAK als Endpunkt der Ende-zu-Ende-Verschlüsselung (Sender und Empfänger anstelle von Autor und Leser gemäß 4-Corner-Modell)
- Konzept zur Berechtigungsprüfung (Alleinstellungsmerkmal) noch wenig erprobt und Details teilweise ungeklärt
- Vorgesehene Mandantenfähigkeit derzeit noch nicht realisiert
- Enger Fokus des NOOTS-Konzepts auf Registerabfragen (XNachweis)
- Dokumentation noch lückenhaft und im Fluss

5.2.4.3 Chancen

NOOTS als bundesweit einheitliche Infrastruktur für die Registermodernisierung schafft die technischen Voraussetzungen zur *Bereinigung kleinteiliger, mitunter wenig professionell betriebener kommunaler Register*. Mit dem SAK wurde ein Cloud-fähiger Schlüsselbaustein geschaffen, um künftig »Register as a Service« an zentraler Stelle als sicheren Dienst zu betreiben, dem kleine Behörden ohne eigenes IT-Fachpersonal ihre Daten anvertrauen können. Zwar ist die geforderte Mandantenfähigkeit der SAK (funktionale Anforderung NOOTS-1281 in [83]) zurzeit noch nicht umgesetzt, die ein wichtiger Aspekt bei einer Cloud-Service-Lösung ist. Überlegungen dazu finden sich aber zum Beispiel im Whitepaper »Mandantenfähigkeit SAK« [134].

Für das NOOTS spricht auch der Beschluss der 49. IT-Planungsrats-Sitzung [106], das NOOTS in das Basisdienste-Portfolio als *Komponente des Deutschland-Stacks* aufzunehmen. Dies verleiht der Technologie zusätzliche Sichtbarkeit und Relevanz und steht im Einklang mit der Präambel des NOOTS-Staatsvertrags.

O – Opportunities (Chancen)

- Bundeseinheitliche Governance und Infrastruktur als günstige Ausgangsposition für »Register as a Service« zur Bereinigung kleinteiliger kommunaler Register
- Aufnahme von NOOTS in das Portfolio der Basisdienste des Deutschland-Stacks

5.2.4.4 Risiken

Generell birgt die *eingeschränkte Konzeptreife des NOOTS-Ansatzes* Risiken. Obwohl laut der NOOTS-Homepage [93] das NOOTS seit Ende 2025 in einer ersten Version verfügbar ist und inzwischen auch bereits verschiedene Pilotprojekte einzelne XNachweis-Szenarien erfolgreich mittels NOOTS realisiert haben, sind viele Details noch ungelöst. So wird etwa erst in Kürze eine erste, noch rudimentäre Version von DAMAS erwartet, zu der zum Studienzeitpunkt noch keine genaueren Informationen ermittelt werden konnten. Ähnliches gilt für die NOOTS-Vermittlungsstelle (VS), und auch über die genaue Gestaltung einer Private-Key-Infrastruktur, die sowohl Behörden als auch Dienstleister angemessen und möglichst hochautomatisiert bedienen kann, herrschen noch Unklarheiten. Da DAMAS und VS grundlegende Kernelemente des NOOTS-Ansatzes sind, birgt es erhebliche Risiken, wenn die Konzeption dieser Komponenten noch nicht vollständig abgeschlossen und validiert ist.

Ein Risiko für die Beurteilung ist auch die *mangelnde Praxiserfahrung und Bewährung des NOOTS in der Anwendung*. Zwar wurden inzwischen mehrere Register an das NOOTS angeschlossen und der Nachweisabruf in Pilotprojekten erfolgreich demonstriert – darunter auch grenzüberschreitend im EU-OOTS-Kontext. Diese Pilotanwendungen arbeiten jedoch noch mit zahlreichen provisorischen Lösungen, da an den Realisierungen von VS, DAMAS, RDN und PKI nach Auskunft unserer Interviewten noch gearbeitet wird. Zudem ist das Lastaufkommen und die Lastheterogenität in den betreffenden Anwendungen zu gering, um daraus belastbare Rückschlüsse auf die Skalierbarkeit des NOOTS und die Performanz im Vollausbau zu ziehen. Auch organisatorisch spiegeln die punktuellen Pilotszenarien die Herausforderungen eines flächendeckenden Realbetriebs nur ungenügend wider, denn für die ausgesuchten Sonderfälle waren im Zweifelsfall bilaterale Absprachen zwischen DC und DP möglich, was in einem vollumfänglichen n:m-Szenario mit hunderten angeschlossenen Registern und tausenden anfragenden Stellen nur sehr eingeschränkt möglich ist.

Viele Interviewte äußerten Bedenken, was den eigenverantwortlichen Betrieb der Anschlussknoten betrifft: *Der Konfigurations- und Wartungsaufwand der SAK*

überfordert voraussichtlich die Ressourcen und Kompetenzen kleinerer Standorte. Diese Einschätzung deckt sich mit den persönlichen Projekterfahrungen des Autorenteam der Studie im kommunalen Bereich. Dem lässt sich grundsätzlich begegnen, indem kleine Register in einem Standort-übergreifenden Rechenzentrum im Modus »Register as a Service« professionell betrieben werden. Entsprechende technische, politische und gesetzliche Weichenstellungen wären dazu aber erst noch zu treffen.

Ein weiteres Risiko ist die *unveränderte Übertragung veralteter, nicht-digitalisierter Verwaltungsprozesse in das Digitalzeitalter*, ohne die technischen Möglichkeiten einer digitalen Lösung auszuschöpfen. Dies kann zum einen zu Systemanforderungen führen, die bei geeigneter Prozessmodernisierung vermeidbar wären. Zum anderen ist zu bedenken, dass NOOTS als Transportinfrastruktur für Registeranfragen nur einen begrenzten Teil der Registermodernisierung abdecken kann: Eine mindestens ebenso große Herausforderung wie die Bereitstellung der technischen NOOTS-Infrastruktur ist die Anpassung der Register, die man sich im Allgemeinen nicht als einfache monolithische Datenbanksysteme vorstellen darf, sondern die oft aus einem Konglomerat von IT-Systemen, Fachverfahrenssoftware und Verwaltungsprozessen bestehen. Daher ist es ohne grundlegende Modernisierung der Data-Provider-IT nur schwer möglich, Registeranfragen in Übereinstimmung mit den NOOTS-Vorgaben korrekt und in den vorgegebenen Zeitschranken zu bedienen, weil eine XNachweis-Anfrage unter Umständen beim Register eine komplexe Prozesskaskade auslösen kann, bis die gewünschten Informationen bereitgestellt sind [135].

T – Threats (Risiken)

- Eingeschränkter Reifegrad der NOOTS-Konzepte
- Mangelnde Praxiserfahrung und Bewährung des NOOTS in der Anwendung
- Überforderung der Ressourcen und Kompetenzen kleinerer Standorte durch den notwendigen Konfigurations- und Wartungsaufwand der SAK
- Gefahr unnötiger Komplexität durch die Übertragung analoger, nicht-digitalisierter Verwaltungsprozesse in digitale Systeme
- Mangelhafte Modernisierung und Anpassung der IT-Fachsysteme der Data Provider für eine erfolgreiche Integration in das NOOTS

5.2.5 ZaPuK

Bei der Bewertung von ZaPuK gilt es zu beachten, dass viele der Bewertungsdimensionen durch die Wahl von Matrix als Technologiestandard geprägt werden. Die Begründung der Wahl von Matrix als Transportschicht der Zielarchitektur kann der offiziellen Dokumentation (ADR-0011 [102]) entnommen werden.

Die Eigenschaften, die vollständig oder primär durch Matrix geprägt sind, werden in dieser Bewertung durch ein (M) gekennzeichnet. Die Unterscheidung zwischen den Eigenschaften der Transporttechnologie und den Architekturentscheidungen der Zielarchitektur ist deshalb wichtig, weil die Eigenschaften der Transporttechnologie gegebenenfalls auch auf andere betrachtete Technologien und Governance-Modelle übertragen werden können. Beispielsweise findet im Rahmen des Projekts NEO aktuell eine Integration der Anbindung an Matrix im FIT-Connect-SDK statt. In Interviews wurde von involviertem Fachpersonal eine potenzielle Umstellung der Kommunikation in FIT-Connect auf den Matrix Standard erwogen. Daher sind Bewertungsdimensionen gekennzeichnet, um das Potenzial von Matrix als Transportschicht in verschiedenen Anwendungsbereichen aufzuzeigen und gleichzeitig die spezifischen Eigenschaften der Zielarchitektur hervorzuheben.

5.2.5.1 Stärken

Dezentrales Ökosystem (M) und offene Infrastrukturtopologie: Matrix ermöglicht die Realisierung einer vollständig dezentralen Kommunikationsinfrastruktur. Es gibt prinzipiell keine zentralen Dienste, von denen die Kommunikation abhängig ist. Ausgetauschte Daten werden nur durch die direkt in der Kommunikation involvierten Homeserver verarbeitet. Das dezentrale Betriebsmodell von Matrix bietet verschiedene Freiheiten im Betrieb der Infrastruktur, die die Resilienz, Sicherheit und das Vertrauen in die Kommunikation verbessern können. ZaPuK baut auf diesem Modell auf und ermöglicht eine sehr flexible Infrastrukturtopologie, die es verschiedenen Fachbereichen, Berufsverbänden und anderen Organisationsgruppen ermöglicht, sich selbst zu organisieren und eigene Modelle für die Anbindung an ZaPuK auszuwählen. Die Topologie der Infrastruktur kann sich kontinuierlich verändern, ohne dass zentrale Anpassungen oder Freigaben erforderlich wären.

Offener, internationaler Standard (M): Matrix ist ein international etablierter Standard, der offen zugänglich und nutzbar ist. Der Standard verfügt über eine Nutzerbasis, die aktiv zum Ökosystem der Implementierungen und der Weiterentwicklung des Standards beiträgt.

Etablierte Technologiebasis (M): Matrix baut auf modernen und weit verbreiteten Basistechnologien wie HTTPS, REST und JSON auf. Die Basistechnologien sind flexibel anpassbar.

Starke funktionale Basis (M): Die Matrix-Spezifikation und ihre verfügbaren Implementierungen bieten direkte Unterstützung für viele moderne Funktionen, wie etwa Kompatibilität mit Mobilgeräten, Nutzung von mehreren verschiedenen Geräten, Push-Benachrichtigungen und Long-Polling.

Moderne Kryptografie mit E2EE (M): Matrix verfügt mit Olm und Megolm über eine starke kryptografische Basis mit Ende-zu-Ende-Verschlüsselung. Die Algorithmen können bei korrekter Konfiguration und Anwendung moderne Sicherheitsgarantien wie Forward Secrecy und Post-Compromise Security bieten.

Interoperabilität und Anpassbarkeit: Als technologische Basis der Zielarchitektur bietet Matrix ein sehr flexibles Protokoll, das durch neue Event- und Nachrichtentypen beliebig erweitert werden kann. Die Zielarchitektur soll Bestandslösungen aus verschiedenen Fachbereichen ersetzen, die teilweise spezielle fachliche Anforderungen an die Kommunikationsstruktur mitbringen. Durch die Erweiterbarkeit von Matrix ist die technische Umsetzung dieser Anforderungen grundlegend möglich. Durch die Fähigkeit von Matrix, auch unbekannte Events zu transportieren, kann die Interoperabilität verschiedener Fachlösungen sichergestellt werden. Die Zielarchitektur sieht des Weiteren auch vor, über Protocol-Converter auf Basis des EU Digital Markets Act die Interoperabilität mit anderen Kommunikationstechnologien herzustellen.

Offenes, flexibles Ökosystem: Die Zielarchitektur plant den Aufbau eines offenen und sehr flexiblen Ökosystems auf mehreren Ebenen. Die Flexibilität der Infrastrukturtopologie ermöglicht es den Endnutzern, sich eigenständig in verschiedenen Infrastrukturen und Gruppen zu organisieren und bestimmte Aspekte der Governance zur Nutzung der Kommunikationsinfrastruktur eigenständig zu regeln. Die Flexibilität der technologischen Basis und Offenheit des Ökosystems für Implementierungen und Betrieb durch Dritte ermöglicht es, das Kommunikationsprotokoll und die genutzte Software auf die jeweiligen Bedürfnisse der verschiedenen Nutzergruppen anzupassen, ohne die Kommunikation zwischen verschiedenen Gruppen grundsätzlich zu verhindern.

S – Strengths (Stärken)

- Dezentrales Ökosystem (M)
- Offene Infrastrukturtopologie
- Offener, international etablierter Standard (M)
- Etablierte Technologiebasis (M)
- Starke funktionale Basis (M)
- Moderne Kryptografie mit E2EE (M)

S – Strengths (Stärken)

- Offenes, flexibles Ökosystem

5.2.5.2 Schwächen

Mangelnde Kryptoagilität (M): Matrix ist aktuell nur für die Verwendung von Olm und Megolm als Verschlüsselungsalgorithmen aufgebaut. Die geplante Migration auf Message Layer Security (MLS), das auch in der Zielarchitektur verwendet werden soll (ADR-0012 [102]) ist komplex und aufwendig. Bei Schwächen in den verwendeten Algorithmen wäre ein direkter Wechsel der Algorithmen auf Protokollebene deutlich aufwendiger als beispielsweise in TLS.

Komplexität und Offenheit des Ökosystems: Durch die vielen Freiheitsgrade und die Offenheit des geplanten Ökosystems, sowohl auf Ebene von Matrix als auch bezüglich der Zielarchitektur, entsteht eine zusätzliche Verwaltungskomplexität. Eine Übersicht über Teilnehmer, Kommunikationsregelungen und Topologie ist schwer möglich. Aufgrund der Dezentralität der Infrastruktur und Offenheit der Implementierungen können Anforderungen und Richtlinien nicht zentral technisch durchgesetzt werden.

Früher Projektstatus: Aufgrund des aktuellen Status der Zielarchitektur sind viele Details der Architekturvorgaben bisher noch nicht bekannt oder noch nicht finalisiert. Es fehlen an verschiedenen Stellen detaillierte Konzepte zu den geplanten Maßnahmen, etwa bezüglich der Liste der Anbindungsbedingungen, der Organisation des Self-Service-Portals, der Durchführung der Authentizitätsprüfung auf E2EE-Ebene (ADR-0013 [102]) und der Unterstützung für öffentliche PKIs (ADR-0016 [102]). Geplante ADRs zu Kernthemen der Kommunikation wie Adressierung und Nutzerverwaltung sind aktuell nicht vorhanden. Des Weiteren entsprechen die aktuell veröffentlichten ADRs laut Aussagen in Interviews nicht in allen Fällen den neusten Erkenntnissen zu verschiedenen Aspekten der Zielarchitektur.

Fehlende Funktionen der Technologiebasis (M): Matrix bietet aktuell nicht alle notwendigen Funktionen zur Umsetzung der geplanten Kommunikation in Za-PuK. Unter anderem sind Erweiterungen des Standards für die Postfachverwaltung notwendig. Matrix bietet derzeit ebenfalls keinen Mechanismus, um die Rechtssicherheit der Kommunikation zu gewährleisten. Da insbesondere diese Anforderung auch den Einsatz von Matrix in anderen Kommunikationsszenarien betrifft, wird die Schwäche Matrix zugeschrieben.

Vermischung von Transportfunktionalität und Fachlichkeit (M): Mit seinem Konzept der Raum-Historie und der Verwaltung von Räumen durch die Homeserver übernimmt das Kommunikationsmodell von Matrix teilweise die Gestaltung der *Konversation*. Während die Kommunikation über Postfächer von dieser Persistenz der Nachrichten potenziell profitiert, ist diese Vermischung von Transportfunktionalität und der anschließenden Verwaltung der Nachrichten in anderen Kommunikationsszenarien möglicherweise nicht angebracht.

Begrenzter Scope und fehlende Konzepte: Die veröffentlichten oder geplanten Architekturentscheidungen adressieren in aktueller Form nicht alle erhobenen Anforderungen an Postfach- und Kommunikationslösungen. Verschiedene Bereiche, in denen für den Betrieb einer Kommunikationsinfrastruktur Konzepte und Entscheidungen notwendig sind, liegen außerhalb des Betrachtungshorizonts des aktuellen Zielarchitekturprojekts. Nach eigener Beschreibung stellt die Zielarchitektur lediglich ein Steuerungsinstrument mit einem idealisierten Greenfield Ansatz dar [100]. Des Weiteren werden sogenannte »weitere Handlungsfelder«, die sich »unterhalb der architektonischen Relevanzschwelle einer föderalen Zielarchitektur« befinden, im Architekturkonzept nicht adressiert. Es ist unklar, welche Aspekte zukünftig durch ADRs adressiert werden sollen. So existieren derzeit beispielsweise keine Konzepte für die Umsetzung der identifizierten Anforderungen in den Bereichen Speicherung und Funktionspostfach. Es besteht die Gefahr, dass technische Details der Zielarchitektur in die Umsetzung der Referenzimplementierung verlagert werden. Dies erzeugt eine Bindung zwischen Spezifikation und Implementierung, vor der die befragten Fachleute in Interviews gewarnt haben.

Unklarheiten bezüglich Governance, Betrieb und Finanzierung: Aktuell sind verschiedene Aspekte der Langzeitpflege der Zielarchitektur ungeklärt. Es ist beispielsweise unklar, welche Stelle für den Betrieb und die Finanzierung der geplanten zentralen Infrastruktur (ADR-0005 und ADR-0006 [102]) sowie für die Entwicklung der Referenzimplementierungen (ADR-0007 [102]) verantwortlich sein wird. Eine Planung sollte in Arbeitspaket 2.6 des Projekts bis zum Ende des zweiten Quartals 2026 erfolgen [105], wird voraussichtlich jedoch erst zur 52. Sitzung des Planungsrats vorliegen [106].

W – Weaknesses (Schwächen)

- Mangelnde Kryptoagilität (M)
- Komplexität und Offenheit des Ökosystems
- Früher Projektstatus
- Fehlende Funktionen der Technologiebasis (M)

W – Weaknesses (Schwächen)

- Vermischung von Transportfunktionalität und Fachlichkeit (M)
- Begrenzter Scope und fehlende Konzepte
- Unklarheiten bezüglich Governance, Betrieb und Finanzierung

5.2.5.3 Chancen

Konsolidierung verschiedener Bestandslösungen: Die Zielarchitektur hat das Potenzial, die Komplexität der Interaktion zwischen der öffentlichen Verwaltung mit Privatpersonen (G2C), der Privatwirtschaft und Standesorganisationen (G2B) durch die Konsolidierung verschiedener Bestandslösungen deutlich zu reduzieren. Insbesondere die Unterstützung für G2C-Kommunikation bietet eine Chance, die Anzahl der notwendigen Technologien, die durch Behörden betreut werden müssen, zu verringern.

Aktive Community und vorhandene Expertise (M): Der Matrix-Standard hat eine sehr aktive internationale Community, die den Standard und das Ökosystem kontinuierlich weiterentwickelt. Nutzer des Standards können von Weiterentwicklungen, wie etwa der aktuell laufenden Integration von MLS, profitieren, ohne selbst in die Entwicklung investieren zu müssen. Durch die internationale Verbreitung und Nutzung von Matrix in anderen Kommunikationssystemen (z. B. den TI-Messenger der Gematik oder den BW-Messenger der Bundeswehr) sind Erfahrungswerte und qualifiziertes Fachpersonal am Markt verfügbar. Aus Sicht der Zielarchitektur bietet sich auch die Chance, den Standard aktiv mitzugestalten, beispielsweise durch die Umsetzung der Rechtssicherheit und einer Postfachverwaltung.

Bestandteil des Deutschland-Stacks: ZaPuK wurde bereits als Basisdienst »Postfach« in den Deutschland-Stack aufgenommen. Diese Position erhöht die Bekanntheit des Projekts und kann die Akzeptanz und das Vertrauen in die Lösung im Nutzerkreis verbessern.

Effiziente Methoden im Rollout: Die vorhandenen Implementierungen von Matrix und die Möglichkeiten zu deren Integration in bestehende Software – wie aktuell durch die Integration von NEO in das FIT-Connect SDK demonstriert – sowie die geplanten zentralen Infrastrukturkomponenten bieten sehr effiziente und einfache Wege zur Anbindung an ZaPuK. Insbesondere realisiert das FIT-Connect-SDK aktuell eine gewisse Abstraktion zwischen der API und der Integration in Fachverfahren, sodass laut Auskunft der befragten Personen eine nahezu transparente Nutzung verschiedener Transporttechnologien vorstellbar wäre.

Erschließung neuer Kommunikationsszenarien (M): Matrix bietet Unterstützung für Kommunikationsszenarien, die bisher im Kontext anderer betrachteter Technologien nicht beachtet wurden. Dazu zählen die Kommunikation über Echtzeit-Chat sowie Audio- und Videostreaming. Diese neuen Kommunikationsformen eröffnen Chancen für die Verbesserung der G2X Kommunikation. Insbesondere die Kommunikation über Chats wird bereits in anderen Bereichen genutzt (z. B. im TI-Messenger sowie im BW-Messenger).

O – Opportunities (Chancen)

- Konsolidierung verschiedener Bestandslösungen
- Aktive Community und vorhandene Expertise (M)
- Bestandteil des Deutschland-Stacks
- Effiziente Methoden im Rollout
- Erschließung neuer Kommunikationsszenarien (M)

5.2.5.4 Risiken

Mangelnde Nutzerakzeptanz: Jeder neuen Technologie im G2X-Umfeld steht eine Resistenz der Zielgruppe gegen Veränderungen entgegen. In vielen Bereichen gibt es etablierte Lösungen, die in vielen Fällen durch Dienstleister genau auf die Bedürfnisse der jeweiligen Nutzer zugeschnitten sind. Die Zielarchitektur versucht eine Reihe von Bestandslösungen abzulösen, so etwa das ZBP, das MJP oder das ELSTER-Postfach 2.0. Während die Bedürfnisse der Stakeholder bereits bei der Anforderungserhebung mit einbezogen wurden, gibt es nach den Erkenntnissen aus Interviews weiterhin Uneinigkeiten und Diskussionsbedarf, die einer flächendeckenden Verwendung der Zielarchitektur entgegenstehen könnten.

Dialektbildung und Inkompatibilität: Aufgrund der Flexibilität der technologischen Basis, dem Fehlen detaillierter Konzepte für die Implementierung zusätzlicher Funktionen und den noch ungeklärten Anbindungsbedingungen besteht das Risiko der Dialektbildung und damit einer Inkompatibilität verschiedener Implementierungen und Lösungen im ZaPuK-Ökosystem. Während Matrix und die Offenheit des Ökosystems eine Konsolidierung der Bestandslösungen fördern, indem sie den Teilnehmergruppen die Implementierung spezifischer fachlicher Anforderungen in ihren Homeservern und Clients ermöglichen, besteht dadurch eine Gefahr einer nur scheinhaften Interoperabilität. Matrix ermöglicht zwar den Austausch von Nachrichten eines unbekannten Typs zwischen verschiedenen Homeservern, jedoch kann dies bei verschiedenen Clients und Fachverfahren zu Problemen bei der Darstellung der Inhalte führen. Konzepte zur Eindämmung

einer solchen Dialektbildung existieren aktuell nicht. Das Umsetzungsprojekt der Zielarchitektur, NEO, hat beispielsweise eigenständig die Definition einer neuen Multi-Event-Struktur beschlossen (NEO ADR-0004 [136]), die nicht Teil der Zielarchitektur ist. Zwar stellt dies aufgrund der frühen Projektphase und des Bezugs zwischen den Projekten noch keine Inkompatibilität zur finalen Version der Zielarchitektur dar, weist aber auf mögliche zukünftige Risiken hin.

Fehlende Governance und Verbindlichkeit: Wie bereits in den *Schwächen* in Abschnitt 5.2.5.2 erwähnt, ist die Governance der Zielarchitektur selbst derzeit noch unklar. Aber auch auf einer weiteren Ebene ist die interne Governance und Verbindlichkeit der Architekturentscheidungen des Standards innerhalb des ZaPuK-Ökosystems unklar. Bisher existieren keine Vorgaben dazu, ob und wie die Einhaltung der Architekturentscheidungen bei Implementierungen der Zielarchitektur kontrolliert werden soll. Die Veröffentlichung von Anbindungsbedingungen ist zwar vorgesehen, jedoch ist keine Verifikation der Einhaltung geplant und der Umfang der Bedingungen ist bisher unklar. Das Projekt NEO hat sich beispielsweise gegen die Öffnung der NEO-Infrastruktur für Drittbetreiber entschieden (NEO ADR-0003 [136]), obwohl die Offenheit durch die Zielarchitektur zugesichert wird (ADR-0004 [102]). In Interviews wurde diskutiert, mit Hinweis auf laufende Überlegungen die Offenheit des Ökosystems zumindest für den Kreis der Privatpersonen auch in ZaPuK einzuschränken. Dieses Beispiel verdeutlicht, dass es bisher ungeklärte Aspekte in der Governance des Ökosystems gibt, die adressiert werden müssen, um eine Fragmentierung zu vermeiden.

Fehlende Kontrolle über die Technologiebasis (M): Da der Technologiestandard Matrix unter der Kontrolle einer externen Organisation steht, kann nicht garantiert werden, dass die weitere Entwicklung des Standards den Anforderungen der Zielarchitektur oder allgemein der G2X-Kommunikation entspricht. Es besteht ein Risiko, dass der Matrix-Standard sich in eine Richtung entwickelt, die ihn mit dem Anwendungsbereich der Zielarchitektur inkompatibel macht.

Gefährdungen durch Dritte: Aufgrund der Offenheit des Ökosystems für Drittentwickler und Fremdbetreiber sowie der fehlenden Verifikation beim Beitritt zum Ökosystem ist nicht auszuschließen, dass Implementierungen und Teile der Infrastruktur sich bewusst den Vorgaben der Zielarchitektur widersetzen und somit möglicherweise die Sicherheit der Kommunikation beeinflussen. Die Zielarchitektur trägt dem Rechnung, indem sie eine Zero-Trust-Architektur propagiert (u. a. ADR-0004 und ADR-0013 [102]). Allerdings sind die geplanten Gegenmaßnahmen teilweise noch nicht spezifiziert (ADR-0013) und es ist unklar, ob alle relevanten Angriffsszenarien erkannt und berücksichtigt wurden.

T – Threats (Risiken)

- Mangelnde Nutzerakzeptanz
- Dialektbildung und Inkompatibilität
- Fehlende Governance und Verbindlichkeit
- Eingeschränkte Kontrolle über die Technologiebasis (M)
- Gefährdungen durch Dritte

5.2.6 X-Road

Diese SWOT-Analyse bezieht sich X-Road Version 7.8.0, siehe Abschnitt 4.7.

5.2.6.1 Stärken

Insgesamt liegen die Stärken von X-Road in der Kombination aus technischer Reife, Offenheit, dezentraler Datenhoheit, sicherer Kommunikation und der Fähigkeit zur Integration unterschiedlicher Verwaltungs- und Informationssysteme.

X-Road ist seit 2005 in Estland im produktiven Einsatz und unterstützt dort zentrale Bestandteile der digitalen Verwaltung. Dadurch verfügt X-Road über einen hohen Reifegrad und ist in der Praxis erprobt. Als quelloffenes Protokoll ermöglicht X-Road eine transparente Weiterentwicklung und reduziert die Abhängigkeit von einzelnen Herstellern. X-Road wurde seitdem in weiteren Ländern eingeführt. Das Management der weiteren Entwicklung und Compliance liegt bei dem *Nordic Institute for Interoperability Solutions* (NIIS).

Eine weitere Stärke liegt in der dezentralen Datenhoheit. Die Verantwortung für Daten, Datenschutz und Berechtigungen verbleibt bei den jeweiligen Datenlieferanten und -empfängern. Dadurch können Behörden ihre eigenen Rollen- und Zugriffskonzepte umsetzen und behalten die Kontrolle über ihre Datenbestände. Die Architektur erlaubt zudem, dass ein Security Server mehrere Teilnehmer bedienen kann, wodurch sich der technische Betrieb effizient gestalten lässt.

Durch Modelle wie »Security Server as a Service« kann die Einführung und der Betrieb insbesondere für kleinere Organisationen erleichtert werden.

X-Road fördert die Interoperabilität zwischen heterogenen Informationssystemen durch standardisierte Schnittstellen wie SOAP und REST und ermöglicht damit die Integration bestehender Fachverfahren.

Die verbindliche technische Protokollierung aller Dienstaufrufe stärkt zudem die Nachvollziehbarkeit und Rechtssicherheit der Kommunikation, da dokumentiert

wird, welcher Teilnehmer zu welchem Zeitpunkt welchen Dienst mit welchen Parametern genutzt hat.

X-Road nutzt starke Authentifizierung, gegenseitige Zertifikatsprüfung (mutual TLS), digitale Signaturen und Verschlüsselung, um die Vertraulichkeit der Kommunikation sicherzustellen.

Darüber hinaus ermöglicht X-Road eine flexible Sicherheitsarchitektur, bei der Organisationen beispielsweise den Endpunkt für die Ende-zu-Ende-Verschlüsselung entsprechend ihren Anforderungen festlegen können.

Für die Anbindung auch mehrerer kleinerer Kommunen unterstützt X-Road »Shared« Security Server, also eine logische Multimandantenfähigkeit auf einem gemeinsamen Security Server.

Der Central Server unterstützt Hochverfügbarkeit durch Clustering. Fällt ein Knoten aus, können die Security Server automatisch auf einen anderen verfügbaren Knoten umschalten. So bleibt X-Road bei einem Ausfall des Central Servers weitgehend funktionsfähig. [110]

X-Road basiert auf einer dezentralen Architektur, wodurch ein Single-Point-of-Failure vermieden wird. Die Kommunikationsinfrastruktur verteilt sich auf mehrere unabhängigen Komponenten, sodass Ausfälle einzelner Systeme nicht die gesamte Plattform beeinträchtigt.

S – Strengths (Stärken)

- Zentrale Governance durch NIIS
- Über viele Jahre erprobt und international im Einsatz
- Open-Source
- Datenhoheit bleibt bei den zuständigen Behörden
- Fördert die Interoperabilität zwischen heterogenen Informationssystemen durch standardisierte Schnittstellen
- Rechtssicherheit durch Signierung und Protokollierung von Service-Aufrufen
- Logische Mandantenfähigkeit
- Resilienz durch Clustering des Central Servers
- Dezentrale Architektur

5.2.6.2 Schwächen

Die Anbindung von Teilnehmern in X-Road erfordert die Einrichtung von Security Servern, Zertifikatsmanagement sowie die Konfiguration der Fachverfahren. Diese Verantwortlichkeiten können insbesondere für kleine Kommunen und Organisationen einen zu hohen Aufwand bedeuten.

In X-Road kommuniziert die Fachanwendung des Service Providers ausschließlich mit ihrem lokalen Security Server und muss ansonsten keine direkten externen Verbindungen entgegennehmen. In X-Road erfolgt jedoch der Verbindungsaufbau zum Service-Provider vom zuständigen Security-Server aus. Befindet sich der Security Server nicht in derselben geschützten Zone, stellt dies eine oft unerwünschte Konfiguration dar oder verursacht zusätzlichen Administrationsaufwand.

In der NOOTS-Architekturentscheidung gegen die Verwendung von X-Road als Transporttechnologie und -infrastruktur fand sich als eine Begründung die fehlende Möglichkeit zur »Initiativumkehr« in der Anbindung des Service Providers: Der Service-Provider als anzubindendes Fachverfahren befindet sich generell in einem Firewall-gesicherten Netz. Der Verbindungsaufbau sollte im Idealfall immer vom Fachverfahren zu einem Kommunikationspartner außerhalb des eigenen Netzes erfolgen. Der Aufbau einer Verbindung vom Internet oder der sogenannten *Demilitarisierten Zone* (DMZ) eines Verwaltungsnetzes in das gesicherte Netz hinein ist in vielen Kontexten nicht erwünscht. NOOTS ermöglicht diese Initiativumkehr durch sogenanntes »Long-Polling« von Seiten des Data-Providers (siehe Abschnitt 2.6.6).

Generell erfolgt die Aufrufkette vom Service Consumer über ein oder zwei Security Server zum Service Provider transportverschlüsselt von Station zu Station. Dies bedeutet, dass Request oder Response jeweils bei den Security Servern entschlüsselt vorliegen, sofern Service Consumer und Provider nicht eine separate Verschlüsselung unterlegen. Dies birgt die Gefahr eines unberechtigten Zugriffs auf die Inhaltsdaten bei Kompromittierung des Security Servers.

W – Weaknesses (Schwächen)

- Aufwändiger, Know-How-intensiver Betrieb von Security-Servern inklusive Installation und Konfiguration
- Keine Unterstützung von Ende-zu-Ende-Verschlüsselung zwischen Service Consumer und Provider
- Keine »Initiativumkehr« in der Anbindung von Service-Providern

5.2.6.3 Chancen

X-Road bietet verschiedene Entwicklungspotenziale für den zukünftigen Ausbau digitaler Verwaltungsinfrastrukturen. Durch seine standardisierten Schnittstellen und die Unterstützung offener Standards kann X-Road in übergeordnete Föderationsstrukturen wie NOOTS integriert werden und interoperabel mit anderen nationalen und europäischen Lösungen zusammenarbeiten, ohne selbst als alleiniger Standard etabliert sein zu müssen. Durch die technische Unterstützung von föderalen Strukturen unterstützt X-Road länderübergreifende Vernetzung.

Perspektivisch eröffnet X-Road zudem die Möglichkeit, zentrale Dienste wie »Register-as-a-Service« bereitzustellen, wodurch insbesondere kleinere Kommunen bei der Anbindung und dem Betrieb entlastet werden könnten. Die geplante Bereitstellung einer zentralen Public Key Infrastructure (PKI) bietet darüber hinaus das Potenzial, Sicherheitsanforderungen weiter zu stärken und gleichzeitig den administrativen Betriebsaufwand zu reduzieren.

X-Road ist an andere europäische Technologien anschlussfähig. Durch die Anbindung an eDelivery im Rahmen des Once-Only Technical System (OOTS) kann X-Road grenzüberschreitende Verwaltungsprozesse unterstützen und damit die digitale Zusammenarbeit innerhalb der Europäischen Union fördern. Hierfür steht eine Gateway-Komponente zur Verfügung, die als Brücke zwischen eDelivery und X-Road fungiert. Sie konvertiert Nachrichten automatisch zwischen dem AS4-Protokoll und X-Road-SOAP in beide Richtungen, verbirgt die jeweiligen Kommunikationsprotokolle gegenüber den angebundenen Systemen und ermöglicht so die Nutzung von eDelivery-Diensten über den X-Road Security Server sowie von X-Road-Diensten über einen eDelivery Access Point. [137]

O – Opportunities (Chancen)

- Durch standardisierte Schnittstellen und offenen Standards kann X-Road in übergeordnete Föderationsstrukturen integriert werden
- Anbindung durch Register-as-a-Service wird perspektivisch unterstützt
- Anschlussfähig an andere Technologien der Europäischen Union

5.2.6.4 Risiken

X-Road wird von einer internationalen Community weiterentwickelt. Änderungen an der Roadmap oder den Prioritäten könnten nationale Anforderungen Deutschlands nicht immer vollständig berücksichtigen oder ihnen zuwiderlaufen.

X-Road ist in Deutschland nur in isolierten Szenarien im Einsatz, z. B. in Schleswig-Holstein. Eine Erklärung dafür könnte sein, dass ein Großteil der B2G- und G2G-Kommunikation auf lange etablierten, nachrichtenbasierten Kommunikationsparadigmen basiert. X-Road verfolgt indes einen moderneren serviceorientierten Ansatz, der etabliertem Prozessdenken nicht direkt naheliegt. Daraus ergibt sich unter Umständen eine mangelnde Akzeptanz bei potenziellen Anwendern, da Prozesse neu modelliert werden müssten.

Der Installations- und Betriebsaufwand der Security Server ist als vergleichsweise aufwändig einzuschätzen und stellt damit eine Herausforderung für kleinere Organisationen und Kommunen dar. Die daraus resultierende Anforderung, in vielen Fällen die Security Server in entfernten Rechenzentren zu betreiben, führt netzwerktechnisch zu längeren Anbindungsstrecken, die eigene Herausforderungen bezüglich IT-Sicherheit und Administration mit sich bringen können.

T – Threats (Risiken)

- Weiterentwicklung durch internationale Community ohne Berücksichtigung deutscher Interessen
- Mangelnde Akzeptanz aufgrund eines Wechsels des Kommunikationsparadigmas
- Keine Aufnahme im Deutschland-Stack
- Überforderung der Ressourcen und Kompetenzen kleinerer Organisationen durch den notwendigen Konfigurations- und Wartungsaufwand der Security Server

5.2.7 eDelivery AS4

Die SWOT-Analyse bezieht sich eDelivery AS4 Version 2.0, siehe Abschnitt 4.8.

5.2.7.1 Stärken

Das eDelivery-AS4-Profil ist eine Spezialisierung des AS4-Profils der ebMS 3.0-Spezifikation. Es gewährleistet Einfachheit und eine bessere Konformität mit den zugrundeliegenden und genutzten Webservice-Standards (u. a. SOAP, WSDL, WSS) und ergänzt einen etablierten OASIS- und ISO-Standard (ebMS 3.0).

Datenschutz, Rechtssicherheit, Nachvollziehbarkeit und Nachweisbarkeit von Nachrichten ist durch Authentifizierung, Verschlüsselung sowie die Möglichkeit zum Abrufen von Nachrichten und einen integrierten Empfangsbestätigungsmechanismus gegeben. In einem aktuellen Vergleich der KoSIT von Standards [138]

deckt eDelivery AS4 (Version 1.15) die meisten der betrachteten Anforderungen für einen sicheren Nachrichtentransport ab.

Das eDelivery-AS4-Profil bietet Freiraum für branchen- oder domänenspezifische Anpassungen (Nutzungsprofile), um den dortigen Anforderungen für einen sicheren und nachvollziehbaren Nachrichtenaustausch gerecht zu werden. Ein Best-Practice-Beispiel ist die auf AS4 basierende deutsche Gas- und Strommarktkommunikation. Im Peppol-Netzwerk, in dem AS4 zum Austausch elektronischer Rechnungen zwischen Unternehmen und Behörden (B2G/B2B) genutzt wird, kommunizieren weltweit mehr als 4,5 Millionen registrierte Teilnehmer (Unternehmen und Behörden). Genutzt wird das Netzwerk regelmäßig von rund 3,5 Millionen Unternehmen und Organisationen pro Monat in über 46 Ländern [139]. Dabei werden mehr als 6 Millionen Nachrichten pro Monat ausgetauscht [140].

Es gibt zahlreiche, teilweise quellenoffene oder kostenlos verfügbare Testsysteme und Referenzimplementierungen für den AS4-Standard, z. B. CEF eDelivery Conformance Testing Service der EU-Kommission sowie Domibus.

Es besteht Transparenz über die Entwicklung des Standards (Historie) und seine Mitwirkenden. Das technische eDelivery AS4-Profil entwickelt sich in festen Zyklen, um Sicherheitsmechanismen zu modernisieren. Das AS4-Profil gilt als widerspruchsfrei und ist nutzlast-unabhängig und bereits bei der Entwicklung des Standards wurden Tests durchgeführt, um Interoperabilität sicherzustellen [141].

Für eDelivery AS4 stehen umfassende technische Dokumentationen (Quick Start Guides, Administration Guides, Test Guides), Leitfäden und klar strukturierte Versionshistorien bereit. Diese werden primär über das offizielle eDelivery Portal der Europäischen Kommission [142] sowie über branchenspezifische Plattformen bereitgestellt.

Die im eDelivery-AS4-2.0-Protokoll verwendeten Sicherheitstechnologien (TLS, HTTPS) sind zeitgemäß und zukunftsweisend, so wird z. B. TLS 1.3 unterstützt.

AS4-Netzwerke – wie das Peppol-Netzwerk, welches das AS4-Protokoll als Übertragungsstandard nutzt – sind resilient. Ihre Widerstandsfähigkeit basiert auf mehreren technischen Kernmechanismen: Daten werden über zertifizierte und verteilte Access Points ausgetauscht. Fällt ein solcher Zugangspunkt aus, bleibt das restliche Netzwerk erreichbar. Neben Verschlüsselung, Signierung und rechtlich verbindlichen Empfangsbestätigungen nutzt AS4 dezentrale Verzeichnisse. Des Weiteren leiten dynamische Discovery-Dienste (wie das Peppol SMP/SML) Nachrichten vollautomatisch über die sichersten Routen [143]. Das Peppol-Netzwerk ist ein Paradebeispiel für ein hochverfügbares und sicheres AS4-Netzwerk.

S – Strengths (Stärken)

- Zentrale Governance durch die Europäische Kommission
- Ergänzung eines OASIS-Standards und ISO-Standards (ebMS 3.0).
- Datenschutz, Rechtssicherheit, Nachvollziehbarkeit und Nachweisbarkeit von Nachrichten ist gegeben.
- Das eDelivery-AS4-Profil bietet Freiraum für branchen- oder domänen-spezifische Anpassungen
- Best-Practice-Beispiele zeigen die Skalierbarkeit von AS4-basierenden Anwendungen (z. B. Peppol-Netzwerk).
- Quelloffene Testsysteme und Referenzimplementierungen für den AS4-Standard
- Es besteht Transparenz über die Entwicklung des AS4-Profiles und seiner Implementierung: Versionshistorie, feste Entwicklungszyklen und Roadmap [144]
- Support durch ausführliche Dokumentationen
- Das AS4-Profil gilt als widerspruchsfrei und ist nutzlast-unabhängig.
- Sicherstellung von Interoperabilität durch verfügbare Testsuiten
- Zeitgemäße, zukunftsweisende Sicherheitstechnologien (TLS, HTTPS) im AS4-Profil
- AS4-Netzwerke (wie das Peppol-Netzwerk) sind resilient.

5.2.7.2 Schwächen

In eDelivery AS4-Nachrichten werden die Adressen- und Routing-Informationen (wie Sender- und Empfänger-IDs) nur transportverschlüsselt, da sonst deren Zustellung unmöglich ist [145]. Dies stellt ein potenzielles Datenschutzproblem im Kontext der DSGVO dar, wenn die verwendeten Party-IDs (z. B. Umsatzsteuer-IDs, EIC-Codes oder natürliche Identifikatoren) auf eine bestimmte Person oder ein Unternehmen verweisen.

Das eDelivery-AS4-2.0-Profil unterstützt keine Laufzettel wie in OSCI im Sinne eines abrufbaren, fortlaufend aktualisierten Protokolls, das den gesamten Weg einer Nachricht über mehrere Stationen hinweg dokumentiert. AS4 als reines Punkt-zu-Punkt-Protokoll regelt ausschließlich die sichere Übertragung, Verschlüsselung und Quittierung zwischen zwei direkt miteinander kommunizierenden Instanzen.

Bei eDelivery-AS4-2.0-Profil wird kein Rückkanal für eine fachliche Antwortnachricht offengehalten. Der HTTP-Rückkanal wird ausschließlich für synchrone, rein technische Protokoll-Signale (Quittungen oder Fehlermeldungen) genutzt, danach wird der Kanal unmittelbar geschlossen.

Wie bereits in Abschnitt 4.8.7 erläutert, unterstützt eDelivery AS4 nur die Verschlüsselung der Nachrichten zwischen den Access-Points. Eine weitergehende Ende-zu-Ende-Verschlüsselung zwischen Autor und Leser im 4-Corner-Modell muss, falls gewünscht, auf Anwendungsebene in den Inhaltsdaten erfolgen.

W – Weaknesses (Schwächen)

- Potenzielle Datenschutzprobleme aufgrund unverschlüsselter Adressen und Routing-Informationen
- Keine Unterstützung von E2E-Verschlüsselung
- Keine Unterstützung kompletter Protokollverläufe (»Laufzettel«), die den Weg von Nachrichten dokumentieren

5.2.7.3 Chancen

Das »Ökosystem« von teils quelloffenen oder kostenlos verfügbaren Testsystemen und Referenzimplementierungen sowie der Support durch die Europäische Kommission bei Fragen zum Einsatz von AS4 bieten die Chance für eine Nutzung von AS4 in weiteren national/international verteilten Kommunikationsszenarien. Best-Practice-Beispiele, die zeigen, dass dies auch für viele Teilnehmer und Nachrichten realisierbar ist, sind vorhanden (z. B. das Peppol-Netzwerk oder die Marktkommunikation in deutschen Energiemarkt.)

Der eDelivery-AS4-Standard hat das Potential für einen auch zukünftig sicheren und rechtssicheren, standardisierten Nachrichtenaustausch zwischen Unternehmen und Behörden innerhalb Europas. Dies wurde bereits im europäischen Peppol-Netzwerk praktisch erprobt und zur technischen Sicherheit wird TLS 1.3 eingesetzt.

Da zur Implementierung von EU-OOTS eDelivery AS4 eingesetzt wird, besteht die Chance für eine europaweite einheitliche Lösung statt vieler nationaler Insellösungen [146].

O – Opportunities (Chancen)

- Ein erprobtes »Ökosystem« mit (Open-Source) Software und Support sowie Best-Practice-Beispiele bieten die Chance für den weiteren praktischen Einsatz von AS4 in verteilten Kommunikationsszenarien.
- Der AS4-Standard hat das Potential für einen sicheren, rechtssicheren standardisierten Nachrichtenaustausch zwischen Unternehmen und Behörden innerhalb Europas.
- Zur Implementierung von EU-OOTS wird eDelivery AS4 eingesetzt. Es besteht die Chance für eine europaweite einheitliche Lösung statt vieler nationalen Insellösungen.

5.2.7.4 Risiken

Der Standard eDelivery AS4 basiert wie OSCI und XTA auf Webstandards wie SOAP, WSDL und WSS und damit auf Webtechnologien mit abnehmender Verbreitung. Die eingesetzten Technologien (SOAP, XML, WSDL, WSS) werden immer stärker durch andere Technologien und Prinzipien (JSON, REST) am Markt verdrängt, so dass immer weniger erfahrenes Fachpersonal am Markt verfügbar ist.

eDelivery AS4 hat sich in der Vergangenheit im Bereich der Innenverwaltung als Basis der elektronischen Kommunikation nicht durchsetzen können [147]. Mit der Festlegung bestimmter Kommunikationsszenarien auf Technologien wie NOOTS oder FIT-Connect im Deutschland-Stack sinken die Chancen, dass sich eDelivery AS4 in den Bereichen von B2G- und G2G-Kommunikation weiter etablieren kann.

eDelivery AS4 wird von der Europäischen Kommission weiterentwickelt. Änderungen an der Roadmap oder den Prioritäten könnten zur Folge haben, dass nationale Anforderungen Deutschlands nur ungenügend berücksichtigt werden oder entgegenstehen.

T – Threats (Risiken)

- Basiert auf Technologien mit abnehmender Verbreitung (SOAP etc.)
- Festlegung auf andere Technologien im Deutschland-Stack
- Ungenügende Berücksichtigung nationaler Interessen bei der weiteren Entwicklung

5.3 Szenarienbasierte Technologiebewertung

Die im Folgenden pro Technologie vorgenommenen Einschätzungen beschreiben, wie die jeweilige Technologie in Bezug auf die Anforderungen der vier unterschiedlichen Basis-Kommunikationsszenarien aus Abschnitt 2.6 zu bewerten sind.

5.3.1 OSCI

Die gesamte Kommunikationstransaktion zwischen zwei Teilnehmern (im Sinne der OSCI-Rollen »Sender« und »Empfänger«) wird immer über einen Intermediär abgewickelt. Da der Intermediär auch zentrale Protokollierungsaufgaben über den Laufzettel vornimmt, genießt dieser im Rahmen der Kommunikation ein entsprechendes Vertrauensverhältnis, welches durch technisch-organisatorische Maßnahmen erhalten werden muss.

5.3.1.1 Szenario »Asynchron, mit oder ohne Antwort über separaten Kanal«

Die Kommunikation erfolgt primär über den gleichen Kanal, der maßgeblich durch SOAP und HTTP als Trägermedium bestimmt wird. Eine Nutzung insbesondere asynchroner Callback-Mechanismen mit Kanalwechsel, wie zum Beispiel Webhooks, ist in OSCI nicht vorgesehen.

Das Antwortverhalten (und somit auch die realistische Response-Zeit) wird primär über die Funktion des eingehenden Antrags und die Rolle des Empfängers (aktiv oder passiv) bestimmt und wird somit auch durch dessen Netzwerkerreichbarkeit oder Abrufintervalle beeinflusst.

OSCI unterstützt in Standard und realisierter Infrastruktur alle Anforderungen dieses asynchronen Kommunikationsszenarios mit einer breiten Funktionalität. Aus den Interviews und Recherchen ergaben sich keine Hinweise auf unzureichende Leistungsfähigkeit bezüglich des Durchsatzes oder der Latenzen.

5.3.1.2 Szenario »Asynchron, mit asynchroner Antwort über denselben Kanal«

Etwa im Falle eines Zustellungsauftrags wird dem Absender eine Zustellantwort unmittelbar an den Absender zurück übermittelt. Hierbei sieht die Spezifikation die Erzeugung eines Laufzettels zur Protokollierung des Vorgangs auf der Seite des Intermediär vor.

Der Empfänger übernimmt in diesem Szenario eine aktive Rolle, indem die Nachrichten vom Intermediär über einen Abholauftrag bezogen werden, hier sieht die Spezifikation ebenfalls eine entsprechende Protokollierung vor. Der Absender hat in diesem Szenario lediglich Kenntnis über die Zustellung an den Intermediär als zentrale Zwischenstelle.

Über die implizite oder explizite Erzeugung eines Dialogs lassen sich asynchrone, aber zusammengehörige Nachrichten zwischen zwei OSCI-Teilnehmern gruppieren. Zusammengehörige Nachrichten teilen eine eindeutige *ConversationId*.

Damit unterstützt OSCI auch dieses Szenario vollumfänglich.

5.3.1.3 Szenario »Synchron, Abruf«

Ein synchron ausgeprägter Abruf im Sinne eines Datenbezugs baut auf die gleichen Schritte wie im nachfolgenden Abschnitt 5.3.1.4 vorgestellten Szenario des synchronen Nachrichtenversands auf.

Die OSCI-Spezifikation sieht keinen Opt-Out vor, der die Protokollierung auf Wunsch des Absenders oder durch beinhaltete Daten einschränken könnte. Bei Abruf wird ein Laufzettel zur Protokollierung erzeugt [24, S. 26–27]. Durch die Umsetzung von Kommunikationsabläufen in OSCI besteht das Potential für eine Profilbildung, dass sich durch dessen Anforderungen an die Nachweisbarkeit begründet.

OSCI unterstützt damit zwar grundsätzlich die Anforderungen eines synchronen Abrufs in Bezug auf das Request-/Response-Verhalten (siehe nachfolgenden Abschnitt 5.3.1.4). Eine direkte Unterstützung unterschiedlicher Protokollierungsszenarien ist im Standard jedoch nicht vorgesehen. OSCI setzt voraus, dass für dieses Szenario ein aktiver Empfänger (siehe Abschnitt 2.6.6) existiert und dass dieser durch den Intermediär immer erreichbar ist. Über die konkrete sicherheitstechnische Konfiguration, das heißt Aspekte der »Firewall-Friendliness«, macht die OSCI-Spezifikation keine Aussage. Die Tatsache, dass OSCI-Kommunikation immer über bekannte Intermediäre geleitet wird, schafft diesbezüglich eine Vereinfachung. Es existiert in OSCI jedoch kein Konzept wie die in Abschnitt 2.6.6 beschriebene Initiativumkehr.

5.3.1.4 Szenario »Synchron, Nachrichtenversand mit synchroner Rückmeldung«

Eine Punkt-Zu-Punkt Kommunikation zwischen dem »Sender« und »Empfänger« besteht bei OSCI nicht. Die Abfolge der Kommunikationsschritte wird maßgeblich über die Ausprägung des Antrags definiert, der vom Sender gestellt wird.

Die OSCI-Spezifikation sieht vor, im Falle etwa eines Weiterleitungsauftrags Empfänger mit passiver Rolle zu nutzen, wodurch eine netzseitige Erreichbarkeit zwischen Intermediär und Empfänger gewährleistet sein muss (siehe Abbildung 16).

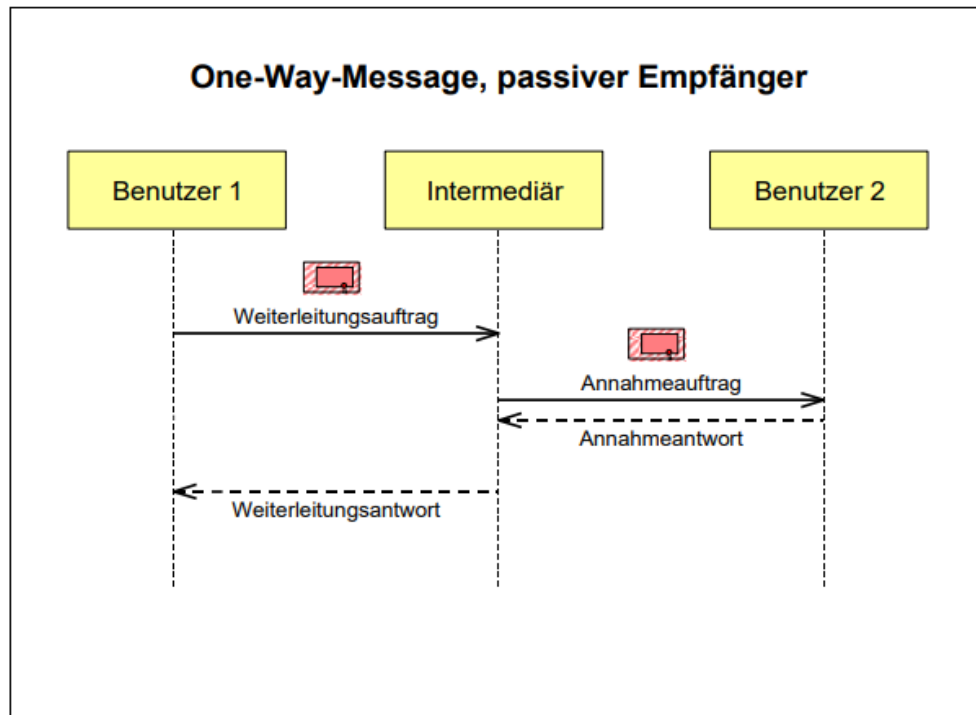


Abbildung 16 Spezifikationsdarstellung »One-Way-Message« [24, S. 26]

Hierbei überträgt der Absender die Nachricht an den Intermediär, welcher diese in Form eines Annahmearauftrags unmittelbar an den Empfänger überträgt. Der Empfänger quittiert diesen Auftrag mit einer Annahmeantwort, die über den Intermediär als Weiterleitungsantwort an den Absender übertragen wird. Der Intermediär protokolliert die Nachrichteneingänge auf dem Laufzettel.

OSCI unterstützt damit sowohl in Standard- wie existierender Infrastruktur die Anforderungen dieses Kommunikationsszenarios.

5.3.2 XTA 2

5.3.2.1 Szenario »Asynchron, mit oder ohne Antwort über separaten Kanal«

Da XTA ein Schnittstellen- und kein Nachrichtenstandard ist, spezifiziert der XTA-Standard nicht, ob der Transportadapter selbst – der XTA-Server – eine eigene Rolle in der Pufferung beim Store-and-Forward oder den Methoden zur Nichtabstreitbarkeit spielt oder dies vollständig der Transportschicht (im überwiegenden Fall OSCI) überlassen ist.

XTA unterstützt jedoch im Standard und in den Implementierungen generell asynchrone Kommunikationsszenarien, bei denen eine Antwort nicht oder separat auf anderem Weg erfolgt, vollumfänglich.

5.3.2.2 Szenario »Asynchron, mit asynchroner Antwort über denselben Kanal«

Im asynchronen Fall fokussiert sich XTA auf den Kommunikationsverlauf einer Nachricht. Es finden sich keine Hinweise auf Mechanismen, die die Identifikation und Protokollierung von ganzen Kommunikationsverläufen oder -dialogen unterstützen, z. B. auf Basis der *ConversationId* von OSCI. Alle Bezüge zu (fachlichen) Antworten in der XTA-Spezifikation betreffen lediglich synchrone Kommunikation. Die Identifikation von Folgekommunikation muss bei XTA folglich auf Anwendungsebene erfolgen, z. B. innerhalb der Nachrichten eines XÖV-Fachstandards oder durch Erweiterung des XTA-Standards.

XTA unterstützt folglich die Anforderungen dieses Kommunikationsszenarios im Standardverhalten nicht direkt. Eine diesbezügliche Erweiterung des Standards erscheint jedoch mit geringem Aufwand möglich. Die in der Praxis über XTA angesprochenen Nachrichtenprotokolle AS4 und OSCI unterstützen die Identifikation asynchroner Folgekommunikation.

5.3.2.3 Szenario »Synchron, Abruf«

XTA unterstützt den synchronen Abruf von Daten durch den Autor beim Leser im 4-Corner-Modell. Der Leser muss dazu für den Aufruf durch den XTA-Server eine XTA-Webservice-Methode *deliverMessage* implementieren und eine Rückmeldung zu der Anfrage des Autors senden.

Hinsichtlich möglicherweise sehr diverser Anforderungen bezüglich der Protokollierung oder Nichtabstreitbarkeit bietet XTA mit den Service-Profilen viele Konfigurationsmöglichkeiten. Wie in Abschnitt 5.2.2 ausgeführt, sind diese jedoch nicht verbindlicher Teil des Standards, das heißt die Umsetzung der jeweiligen Anforderungen ist nicht gewährleistet. Wie mehrfach argumentiert, findet sich in der Praxis eine enge Kopplung von XTA und OSCI. Es ist aufgrund der Unverbindlichkeit der Service-Profile ungewiss, ob die rechtssichere Protokollierung, z. B. zur Vermeidung von Profilbildung in der Infrastruktur, über XTA-Vorgaben deaktiviert werden kann.

In der Evaluation von OSCI / XTA für den Einsatz in NOOTS, also dem Szenario synchronen Registerabrufs, wurde OSCI / XTA mit folgenden Kritikpunkten als Basistechnologie abgelehnt [89]: Die OSCI / XTA-Infrastruktur sei zu heterogen und komplex, die Unterstützung des XTA-Standards unvollständig und die Kommunikationsmuster seien für fachlich synchrone Nachweisabrufe im NOOTS nur eingeschränkt geeignet. Diese Argumentation wird im Anhang B.1 von [89] ausführlicher argumentiert. Auch die zum Teil niedrige Akzeptanz von XTA und

hohe Herausforderungen bei der Umsetzung des Identitätsdatenabrufs (IDA) und die Vermischung von Fach- und Transportlogik in den XTA-Servern wurden erwähnt. In Summe sei aus Sicht der NOOTS-Verantwortlichen der notwendige Zeitbedarf für Ertüchtigungen der OSCI / XTA-Infrastruktur zu hoch. Die vorliegende Studie kann Teile dieser Argumentation bestätigen, siehe Abschnitt 5.2.2.

Zusammenfassend lässt sich sagen, dass XTA synchrone Szenarien und unterschiedliche Protokollierungsvorgaben prinzipiell unterstützt, die Umsetzung auf Transportebene jedoch nicht gesichert ist und in der Praxis weitere Herausforderungen existieren.

5.3.2.4 Szenario »Synchron, Nachrichtenversand mit synchroner Rückmeldung«

Wie im vorangegangenen Abschnitt ausgeführt, wird der synchrone Nachrichtenversand mit Rückmeldung vollständig unterstützt. Obwohl auch hier die Konfiguration der rechtssicheren Protokollierung über Service-Profile nicht gewährleistet ist, ist sie in der praktischen Anwendung bei XTA üblich und wird aus diesem Grund hier als gegeben angesehen.

XTA unterstützt damit die Anforderungen dieses Kommunikationsszenarios in vollem Umfang.

5.3.3 FIT-Connect

5.3.3.1 Szenario »Asynchron, mit oder ohne Antwort über separaten Kanal«

Dieses Szenario wird von FIT-Connect in vollem Umfang unterstützt, siehe Abschnitt 5.2.3.

Wegen des Polling-Intervalls von mindestens 3 bis 5 Sekunden zum Zeitpunkt der Recherche mittels Rate-Limiting am Endpunkt und eines ebenfalls zeitlimitierten Auslösens der Webhooks, die für Fachverfahren eingetragen wurden, ergibt sich bei FIT-Connect automatisch eine Verzögerung in der asynchronen Datenübertragung. Dadurch war die Infrastruktur zum Zeitpunkt der Recherche nicht für Anwendungen geeignet, die eine sehr geringe Latenz benötigen. Laut Auskunft des Produktmanagements wurden seitdem jedoch Latenzzeiten gesenkt und das Rate-Limiting erhöht, was eine schnellere Zustellung ermöglicht.

5.3.3.2 Szenario »Asynchron, mit asynchroner Antwort über denselben Kanal«

Antworten für einen bestimmten Kommunikationsvorgang, der mittels *caseId* identifiziert wird, können über einen eigens dafür implementierten Endpunkt in der Submission-API vom Fachverfahren an die FIT-Connect Plattform übergeben werden. Diese Antworten müssen auch E2E verschlüsselt werden. Wenn das OZG-Portal in der Lage sein soll, Antworten über FIT-Connect zu empfangen,

muss es auch daher seinen öffentlichen Schlüssel im Self-Service-Portal hinterlegen. Die Antworten für einen bestimmten Fall können über einen Endpunkt abgerufen werden, der die Antworten nach ihrem Erzeugungszeitpunkt aufsteigend sortiert. Das abrufende System muss den Abruf jeder Antwort entweder quittieren oder im Fehlerfall die Antwort ablehnen.

FIT-Connect unterstützt mit diesen Mechanismen die Anforderungen dieses Kommunikationsszenarios.

5.3.3.3 Szenario »Synchron, Abruf«

Dieses Szenario wird von FIT-Connect nicht unterstützt. Ein direkter synchroner Datenabruf ist in FIT-Connect derzeit nicht vorgesehen. REST-Schnittstellen, die einen direkten Datenabruf von einem Fachverfahren ermöglichen würden, sind im Moment in der FIT-Connect Plattform nicht verfügbar und müssten erst definiert werden, ebenso wären Anpassungen an den SDKs für die Fachverfahren erforderlich, um einen fachlich synchronen Abruf zu unterstützen. Weiterhin ist nach unserer Kenntnis keine angepasste Protokollierung für unterschiedliche Datenschutzszenarien möglich.

FIT-Connect bietet mit den laut Produktmanagement gesenkten Latenzen und der Option von Webhooks grundsätzliche Bausteine für die Realisierung synchroner Szenarien. Einschränkend ist hier jedoch anzumerken, dass nach unseren Recherchen derzeit kein Konzept für Callback- oder Push-Funktionalität mit Initiativumkehr existiert.

5.3.3.4 Szenario »Synchron, Nachrichtenversand mit synchroner Rückmeldung«

Dieses Szenario wird von FIT-Connect aufgrund der fehlenden Mechanismen in der Plattform und im SDK nicht unterstützt, wie im vorhergehenden Abschnitt 5.3.3.3 erläutert wird.

FIT-Connect bietet jedoch standardmäßig die geforderte rechtssichere Protokollierung. Wie auch im vorhergehenden Abschnitt erläutert, existieren die weiteren Bausteine für die Umsetzung synchroner Kommunikation in der FIT-Connect-Plattform mit der Einschränkung fehlender Initiativumkehr.

5.3.4 NOOTS

5.3.4.1 Szenario »Asynchron, mit oder ohne Antwort über separaten Kanal«

Da die Anschlussknoten des NOOTS die übermittelten Nachrichten nicht zwischenspeichern, ist die Realisierung asynchroner Anfragen mit den bisher vorliegenden Konzepten des NOOTS nicht direkt lösbar.

Wenn zum Beispiel der vorgesehene Empfänger einer Nachricht gerade offline oder aus anderen Gründen nicht empfangsbereit für die Nachricht ist, so würde das NOOTS nach aktuellem Stand dem Autor der Nachricht eine Retry- oder gar eine Fehlermeldung zurücksenden und der Autor müsste die Übermittlung zu einem späteren Zeitpunkt erneut versuchen (siehe Abbildung 12, S. 76).

Zusammenfassend lässt sich feststellen, dass NOOTS derzeit keine asynchronen Kommunikationsszenarien unterstützt.

5.3.4.2 Szenario »Asynchron, mit asynchroner Antwort über denselben Kanal«

Für dieses Szenario gelten die gleichen Vorbehalte wie für das voranstehende asynchrone Szenario. Dieses Szenario passt aber auch deshalb schlecht zur derzeit verfolgten Designphilosophie des NOOTS, da das Konzept einen weitgehend zustandslosen Anschlussknoten vorsieht, der nach Übermittlung einer Registerabfrage die Kommunikationsverbindung sofort wieder abbauen kann, ohne auf weitere Transaktionsschritte zu warten.

Soll jedoch eine fachlich asynchrone Antwort über denselben Rückkanal fließen, so müsste dieser Kanal während der Wartezeit entweder aufrechterhalten oder bei Bedarf wieder in gleicher Form rekonstruiert werden. Zudem müsste gewährleistet sein, dass der Data Consumer zum Antwortzeitpunkt online und empfangsbereit ist – andernfalls müsste der SAK des Data Consumers oder eine weitere, zwischengeschaltete Instanz die eintreffende Antwort zwischenpuffern, oder der Data Provider müsste seine Antwort so oft wiederholen, bis der Data Consumer empfangsbereit ist.

Zu diesen Aspekten finden sich in der vorliegenden öffentlichen Architekturdocumentation des NOOTS keine ausgearbeiteten Konzepte. Nach heutigem Stand ist das NOOTS für diese Form der Kommunikation daher (noch) nicht geeignet.

5.3.4.3 Szenario »Synchron, Abruf«

Das NOOTS wurde spezifisch für synchrone Abrufszszenarien konzipiert. Es realisiert dazu das Kommunikationsmuster »Request-Response/Sync mit erneutem Abruf (Retry)«. Dabei sendet die anfragende Stelle, der Data Consumer, eine XNachweis-Anfrage an die Nachweis-liefernde Stelle, den Data Provider, und erwartet *immer* eine sofortige, fachlich synchrone Antwort.

Der Data Provider wartet entweder per Long Polling oder per Call-back-Adresse auf eingehende Anfragen, ist also – sofern online – sofort bereit zu reagieren. Er beantwortet die Anfrage unverzüglich:

- Im günstigsten Fall liefert der Data Provider in seiner Antwort sofort die gewünschten Registerdaten an den Data Consumer zurück (siehe Abbildung 11, S. 76).
- Sollte der Data Provider nicht in der Lage sein, die Daten sofort bereitzustellen, so kann er den Data Consumer vertrösten und ihm als Antwort einen späteren Zeitpunkt für einen erneuten Abrufversuch vorschlagen (»Retry«). Der Data Consumer kann dann seine XNachweis-Anfrage zu gegebener Zeit erneut senden, wobei der Zeitvorschlag des Data Providers hilft, aussichtsloses Polling des Data Consumers in zu kurzen Zeitintervallen zu vermeiden (siehe Abbildung 12, S. 76).
- Ist der Data Provider offline oder kommt keine durchgehende Kommunikationsverbindung zustande, so sendet der SAK, bei dem der Kommunikationsversuch fehlgeschlagen ist, eine Fehlermeldung an den Data Consumer.

Mit dieser Festlegung vermeidet das NOOTS, in den Anschlussknoten Nachrichten zwischenspeichern, so dass die Anschlussknoten weitgehend zustandslos operieren können. Dies vereinfacht deren Realisierung und erhöht die Resilienz des NOOTS.

Insofern erfüllt NOOTS die grundlegenden Anforderungen eines synchronen Abrufs, bietet jedoch nach unserer Kenntnis der Architekturdokumentation nicht die Aktivierung rechtssicherer Protokollierung von Abrufen für Anwendungsfälle außerhalb des Registerdatenabrufs.

5.3.4.4 Szenario »Synchron, Nachrichtenversand mit synchroner Rückmeldung«

Dieses Kommunikationsmuster wird derzeit im NOOTS-Projekt nicht ausdrücklich verfolgt. Grundsätzlich spricht aber nichts dagegen, beliebige Daten im Request zu übertragen und in der Response – statt wie bei XNachweis-Anfragen direkt mit den gewünschten Daten zu antworten – zunächst nur eine Quittungsmitteilung oder eine Zurückweisung fachlich synchron zurückzumelden. Die aktuell einsehbare Dokumentation zu den NOOTS-APIs von Data Consumer und Data Provider bezieht sich jedoch ausschließlich auf den Registerabruf und berücksichtigt derzeit keine anderen Szenarien.

Wie das NOOTS dieses Szenario in Zukunft unterstützen würde, bedarf erst noch einer genaueren Ausarbeitung seitens des BVA. Dabei wäre insbesondere zu klären, wie ein rechtsverbindlicher Nachweis über die Zustellung oder den Erhalt vom System generiert und bereitgestellt werden kann, um die Nichtabstreitbarkeit von Kommunikationstransaktionen bei Bedarf zu garantieren.

Zusammenfassend lässt sich feststellen, dass NOOTS derzeit zwar die meisten grundlegenden Anforderungen bezüglich der technisch synchronen Kommunikation erfüllt, aber Konzepte fehlen, um generische Daten (z. B. Antragsdaten)

zu übertragen und dabei die rechtssichere und zugleich datenschutzkonforme Protokollierung und Nachweisführung umzusetzen.

5.3.5 ZaPuK

ZaPuK und seine Transportschicht Matrix sind nicht als klassisches Transport- oder Request-Response-Protokoll zu betrachten, sondern bieten eher ein Publish/Subscribe Modell zum persistenten Veröffentlichen und Synchronisieren von JSON-Nachrichten.

5.3.5.1 Szenario »Asynchron, mit oder ohne Antwort über separaten Kanal«

Die Kommunikation in Matrix erfolgt generell asynchron. Der Homeserver speichert die Nachrichten zwischen und liefert sie auf Anfrage an den Leser aus. Anders als bei anderen Technologien kann diese Zwischenspeicherung auch persistent erfolgen, sodass der Empfänger die Nachricht auf verschiedenen Geräten zeitversetzt abrufen kann.

Die Rechtssicherheit der Kommunikation wird durch Matrix aktuell nicht unterstützt. Eine Implementierung der notwendigen Mechanismen ist in ZaPuK geplant. Matrix stellt dafür einige der notwendigen Bausteine wie Abrufbestätigungen mit Zeitstempeln oder signierte Events zur Verfügung, jedoch waren zum Zeitpunkt der Studienrecherche zu diesen Themen noch keine konkreten Konzepte abrufbar.

Bei gleichzeitiger Anwesenheit des Autors und Lesers können Nachrichten durch Long Polling unmittelbar empfangen werden. Die maximale Größe der übertragenen Nachrichten ist prinzipiell nicht begrenzt, wird in der Praxis jedoch durch die Verarbeitung und Verschlüsselung auf den Endgeräten eingeschränkt.

Mit der oben beschriebenen Einschränkung bezüglich der Konzeption rechtssicherer Protokollierung erfüllen die ZaPuK-Konzepte diese asynchronen Szenarien damit im vollen Umfang

5.3.5.2 Szenario »Asynchron, mit asynchroner Antwort über denselben Kanal«

Die Kommunikation in Matrix erfolgt prinzipiell in sogenannten »Räumen«, die Nachrichten innerhalb einer Konversation in Beziehung zueinander setzen. Zur Protokollierung der Kommunikation eines Antrags kann jeweils ein eigener Raum erstellt werden. Es ist möglich, eine Antragsnummer oder dergleichen als den Namen des Raums zu verwenden, um die Konversation einem Fachprozess zuzuordnen. Die Historie des Nachrichtenaustauschs wird dabei durch den Homeserver protokolliert. Aufgrund der Ende-zu-Ende-Verschlüsselung sind in diesen Raumhistorien die Inhalte der Nachrichten nicht enthalten, jedoch sind Metadaten wie die Teilnehmer und Zeitstempel der Kommunikation für den Homeserver

einsehbar. Aus Sicht des Datenschutzes gilt es zu beachten, dass die Historie auf allen Homeservern synchronisiert wird, die an der Konversation teilnehmen. Eine zentrale Löschung der Protokolle ist damit nicht möglich, ist jedoch in diesem Szenario auch nicht gefordert.

Matrix bietet für ZaPuK damit alle notwendigen Bausteine, um dieses Kommunikationsszenario vollumfänglich umzusetzen. Konkrete Konzepte zu allen Aspekten waren jedoch zum Zeitpunkt der Studienrecherche nicht abrufbar.

5.3.5.3 Szenario »Synchron, Abruf«

Matrix ist nicht für klassische Request-Response Kommunikation konzipiert. Die Technologie bietet keine Möglichkeit, eine unmittelbare Antwort auf eine Anfrage zu erzwingen. Aus technischer Sicht ist es möglich, einen »Request« in einen Raum zu senden, die ein Leser durch Long Polling unmittelbar erhalten und beantworten kann.

Die Firewall-Friendliness ist durch Long Polling zum Homeserver gegeben. Jedoch werden typische Request-Response Funktionen wie das Erkennen doppelter Anfragen, Timeouts und dergleichen aktuell weder durch Matrix unterstützt, noch sind sie in ZaPuK vorgesehen. Zudem erfolgt über die Synchronisation der Raumevents bei Matrix immer eine Protokollierung der Kommunikation. Die Vorhaltezeit der Historie kann durch den Homeserver kontrolliert werden, jedoch kann der Homeserver des Anfragestellers die Protokollierung auf dem Homeserver des Daten-Bereitstellers nicht beeinflussen.

In Summe unterstützt ZaPuK in seiner bisherigen Konzeption damit dieses Kommunikationsszenario nicht.

5.3.5.4 Szenario »Synchron, Nachrichtenversand mit synchroner Rückmeldung«

Die Einschränkungen in Bezug auf Request-Response Kommunikation gelten auch für dieses Szenario. Im Vergleich zum Abruf kann eine automatische Formatprüfung einer Nachricht durch einen maschinellen Teilnehmer im Kommunikationsraum innerhalb weniger Sekunden durchgeführt werden. Matrix bietet eine native API für die Umsetzung externer Programme, die auf Nachrichten in einem Raum reagieren können. Diese Bearbeitung wäre jedoch weiterhin asynchron und erhält keine Unterstützung für Timeouts auf Ebene der Transportschicht.

Damit unterstützt ZaPuK auch dieses synchrone Kommunikationsszenario nicht.

5.3.6 X-Road

5.3.6.1 Szenario »Asynchron, mit oder ohne Antwort über separaten Kanal«

X-Road ist nicht für asynchrone Nachrichtenübermittlung im Sinne einer Store-and-Forward-Architektur vorgesehen. X-Road speichert Nachrichten nicht über längere Zeiträume, bis sie vom Empfänger abgerufen werden. Kann eine Nachricht nicht an den Security Server des Empfängers oder von diesem zum Service Provider des Empfängers übermittelt werden, schlägt die gesamte Übertragung fehl. Eine Zwischenspeicherung oder garantierte Zustellung gehört nicht zu den Kernfunktionen von X-Road. Ist der Leser zu einem bestimmten Zeitpunkt nicht erreichbar, dann muss der Autor die Nachricht zu einem späteren Zeitpunkt noch einmal versenden.

X-Road unterstützt damit dieses Kommunikationsszenario grundsätzlich nicht.

5.3.6.2 Szenario »Asynchron, mit asynchroner Antwort über denselben Kanal«

Dieses Szenario setzt voraus, dass Nachrichten in beiden Richtungen zwischengespeichert werden. Wie bereits im vorherigen Szenario beschrieben, ist X-Road nicht für asynchrone Nachrichten vorhergesehen. X-Road besitzt keine Store-and-Forward-Architektur und stellt keine Zwischenspeicherung von Nachrichten bereit. Können Nachrichten nicht unmittelbar an den Security Server des Empfängers oder den dahinterliegenden Dienst übermittelt werden, schlägt die Übertragung fehl und muss von der aufrufenden Anwendung erneut initiiert werden.

X-Road unterstützt damit dieses Kommunikationsszenario grundsätzlich nicht.

5.3.6.3 Szenario »Synchron, Abruf«

X-Road unterstützt synchrone Request-Response-Kommunikation zwischen einem Daten-Abruf und einem Daten-Bereitsteller und ermöglicht den direkten Abruf von Datensätzen aus einem angeschlossenen Informationssystem. Die Anfrage wird unmittelbar verarbeitet und die Antwort innerhalb derselben Kommunikationsverbindung zurückgegeben. Kann die Anfrage nicht verarbeitet werden, wird ein entsprechender Fehler zurückgemeldet.

Eine Eigenschaft von X-Road ist, dass die Anfrage des Daten-Abrufers über den eigenen Security Server zum Security Server des Daten-Bereitstellers geleitet wird. Von dort baut der Security Server aktiv die Verbindung zum Daten-Bereitsteller auf, um den Request weiterzuleiten. Dies entspricht in der Logik einer Callback-Lösung. Wie in Abschnitt 2.6.6 beschrieben, ist ein potenzielles Problem dieser Aufrufform, dass sich der Daten-Bereitsteller im behördlichen Kontext meistens in einem Firewall-geschützten Behördennetz befindet. Liegt der Security Server außerhalb der Firewall-geschützten Zone, muss das Behördennetz eine

entsprechende Freischaltung vorsehen, was oft nicht erwünscht ist. Die fehlende Unterstützung dieser sogenannten »Initiativumkehr«, bei der ein Verbindungsaufbau immer vom Daten-Bereitsteller zu seinem Security Server erfolgt, wurde in den NOOTS-Architekturentscheidungen [89] als einer der Gründe für die Ablehnung von X-Road genannt. Da nur der eigene Security Server freigeschaltet werden muss, sind die erforderlichen administrativen Freigaben jedoch sparsam.

Um unterschiedliche Datenschutzanforderungen umsetzen zu können, z. B. in Hinsicht auf die Verhinderung von Profilbildung über die Protokolle, unterstützt X-Road eine angepasste Protokollierung per Konfiguration.

X-Road unterstützt in Summe die Anforderungen dieses Kommunikationsszenarios. In Bezug auf fehlende Möglichkeiten zur Initiativumkehr existieren jedoch Einschränkungen hinsichtlich Firewall-Friendliness in Konstellationen, in denen der Security Server außerhalb der vertrauenswürdigen Netzwerkzone liegt.

5.3.6.4 Szenario »Synchron, Nachrichtenversand mit synchroner Rückmeldung«

Dieses Szenario wird von X-Road voll unterstützt, da X-Road eine synchrone Request-Response-Kommunikation von einem Service Consumer (z. B. einem Antragsportal) zu einem Service Provider (z. B. einem antragsbearbeitenden Fachverfahren) über die involvierten Security Server ermöglicht. Eine Nachricht kann an ein Fachverfahren übermittelt und dort unmittelbar automatisiert verarbeitet werden. Der empfangende Security Server kann innerhalb derselben Kommunikation eine Antwort zurückgeben.

Die Anforderungen an eine synchrone Request-Response-Kommunikation mit Timeouts und einer zeitnahen Antwort entsprechen dem Kommunikationsmodell von X-Road. Die Kommunikation erfolgt direkt zwischen den Security Servern der beteiligten Organisationen.

X-Road unterstützt zudem die Protokollierung der technischen Kommunikation und macht damit die Bereitstellung signierter Nachweise über Kommunikationsereignisse möglich. Die fachliche Protokollierung und die Speicherung von Geschäftsprozessergebnissen müssen jedoch durch die angeschlossenen Fachverfahren umgesetzt werden.

Bezüglich fehlender Initiativumkehr gelten jedoch die gleichen Einschränkungen wie beim synchronen Datenabruf.

5.3.7 eDelivery AS4

5.3.7.1 Szenario »Asynchron, mit oder ohne Antwort über separaten Kanal«

eDelivery AS4 unterstützt fachlich asynchrone Kommunikation. Der standardisierte asynchrone Dokumentenaustausch (über sogenannte One-Way/Push- oder Push-and-Pull-Muster) ist das primäre und dabei am häufigsten genutzte Kommunikationsmuster. Standardmäßig nutzt das eDelivery-AS4-Profil das One-Way/Push-Muster, bei dem eine Nachricht asynchron an den Access Point des Empfängers gesendet wird. Rechtssichere Empfangsbestätigungen werden bei Bedarf als völlig eigenständige, asynchrone Nachrichten zurückgeschickt. Dabei müssen Sender und Empfänger nicht gleichzeitig online sein. Die Access Points speichern die Nachrichten sicher, bis sie vom Empfänger abgeholt (gepullt) oder zugestellt (gepusht) werden können.

Um eine Fachantwort auf eine Nachricht – auch über einen anderen separaten Kanal – eindeutig der Nachricht zuordnen zu können, werden in eDelivery AS4 vom Nachrichtensender fachlich eindeutige Bezeichner (IDs) verwendet. Diese (Korrelation-)IDs verknüpfen fachlich zusammengehörige, aber technisch komplett unabhängige (asynchrone) Nachrichten.

Die Nachricht wird zusammen mit der ID asynchron an den Access Point des Empfängers übertragen. Die technische Verbindung wird danach sofort geschlossen. Das Empfängersystem verarbeitet dann die Daten, was beliebig lange dauern kann. Danach sendet das Empfängersystem die Antwort mit derselben ID an einen Access Point des ursprünglichen Senders, wo das interne Fachsystem die Antwort mit Hilfe der eindeutigen fachlichen ID der ursprünglichen Nachricht zuordnen kann.

Für generische Kommunikationsszenarien sind keine allgemeinen Einschränkungen bezüglich des Durchsatzes oder der Latenzen bekannt. Dieses Kommunikationsszenario wird damit vollumfänglich durch eDelivery AS4 unterstützt.

5.3.7.2 Szenario »Asynchron, mit asynchroner Antwort über denselben Kanal«

Über den im vorangegangenen Abschnitt beschriebenen Kommunikationsablauf wird die Referenzierbarkeit von Folgekommunikation für dieses Kommunikationsszenario unterstützt.

5.3.7.3 Szenario »Synchron, Abruf«

Das eDelivery-AS4-Profil unterstützt grundsätzlich keine fachlich synchrone Kommunikation, bei der eine Antwort in direkter Fortsetzung derselben Verbindung zurückgegeben wird. Obwohl das zugrundeliegende ebMS3.0-Protokoll

synchrone Antworten zulässt, ist dies im eDelivery-AS4-Profil auf technische Empfangsbestätigungen beschränkt [148].

5.3.7.4 Szenario »Synchron, Nachrichtenversand mit synchroner Rück«

Wie oben beschrieben, unterstützt das e-Delivery-AS4-Profil keine fachlich synchrone Kommunikation, das heißt eine Unterstützung dieses Kommunikationsszenarios ist durch eDelivery AS4 nicht gegeben.

5.4 Zusammenfassende Bewertung für Kommunikationsszenarien

Die folgenden Unterabschnitte fassen die Bewertungen aus Abschnitt 5.3 pro Szenario jeweils in einer Matrix zusammen. Die Zeilen der Matrix repräsentieren dabei die jeweilige Technologie, die Spalten die Anforderungen des jeweiligen Szenarios aus Abschnitt 2.6.

Da die verfügbaren Beschreibungen in der Regel keinen Hinweis darauf geben, dass sich allgemeine Performance-Metriken wie Durchsatz, Latenzzeiten, Nachrichtengröße und dergleichen von Kommunikationsszenario zu Kommunikationsszenario unterscheiden, sind sie lediglich im ersten Szenario als Spalten aufgeführt.

In den Tabellen ist für Technologien, die bezüglich des jeweiligen Kommunikationsszenarios ein kategorisches Ausschlusskriterium aufweisen, die gesamte Zeile rot markiert. In diesen Fällen ist lediglich das Ausschlusskriterium mit »Nein« bewertet, für die restlichen Anforderungen des jeweiligen Szenarios ist keine Einschätzung vorgenommen. Eigenschaften, die aus Sicht des Autorenteam ein-schränkenden Charakter besitzen, sind blassgelb für leichte Einschränkungen, gelb für stärkere Einschränkungen markiert.

Es ist zu beachten, dass die Informationen in diesem Abschnitt zusammenfassenden Charakter haben. Es ist in dieser verkürzten Form nicht möglich, alle rechtlichen, fachlichen und technischen Anforderungen eines speziellen Anwendungsfalls innerhalb eines abstrakten Kommunikationsszenarios zu bewerten. Die Tabellen geben ausschließlich die prinzipielle Erfüllung der Anforderungen für die abstrakten Kommunikationsszenarien aus Abschnitt 2.6 wieder. Ob damit alle speziellen Anforderungen eines bestimmten Anwendungsfalls innerhalb eines Kommunikationsszenarios durch die jeweilige Technologie erfüllt sind, kann daraus nicht geschlossen werden. So ist es beispielsweise möglich, dass eine Technologie im aktuellen Ausbau von Standard, Implementierungen und Infrastruktur die prinzipiellen Anforderungen für das Kommunikationsszenario »Synchroner Abruf« erfüllt, aber nicht die spezifischen Durchsatz- oder Latenzanforderungen eines konkreten Anwendungsfalls.

5.4.1 Szenario »Asynchron, mit oder ohne Antwort über separaten Kanal«

Tabelle 5 Eignung der Technologien für Szenario »Asynchron, mit oder ohne Antwort über separaten Kanal«

Technologie	Nachrichten puffern	Rechtssichere Protokollierung	Durchsatz / Latenz	Maximale Nachrichtengröße
OSCI	Ja	Ja	Nicht spezifiziert	Nicht spezifiziert*
XTA	Ja	Ja	Nicht spezifiziert	Nicht spezifiziert*
FIT-Connect	Ja	Ja	Latenz im Sekundenbereich**	5GB
NOOTS	Nein	–	–	–
ZaPuK	Ja	Teilweise***	Nahe Echtzeit	Unbegrenzt
X-Road	Nein	–	–	–
eDelivery AS4	Ja	Ja	Nicht spezifiziert	Theoretisch unbegrenzt, praktisch 2 GB, Nutzlast zerlegbar

* Die OSCI- und XTA-Spezifikationen wurden für den Transport großer Datenmengen erweitert. Die real angewendeten Größenlimits hängen jedoch von der Implementierung ab.

** Latenz in FIT-Connect: Die Auslieferungslatenz in FIT-Connect ist, wenn Webhooks nicht verwendet werden können, durch das Polling-Intervall beschränkt. Dieser betrug zum Zeitpunkt der Recherche in der Standardeinstellung 3-5 Sekunden. Auch Webhooks werden gegebenenfalls zeitversetzt ausgelöst. Laut FIT-Connect Produktmanagement wurden diese Werte seither gesenkt.

*** Rechtssichere Protokollierung ist in ZaPuK geplant, aber ohne Finalisierung der zugehörigen Konzepte. Matrix stellt die für rechtssichere Protokolle notwendigen Funktionen wie Lesebestätigungen mit Zeitstempeln und signierte Events zur Verfügung.

5.4.2 Szenario »Asynchron, mit asynchroner Nachricht über denselben Kanal«

Tabelle 6 Eignung der Technologien für Szenario »Asynchron, mit asynchroner Nachricht über denselben Kanal«

Technologie	Nachrichten puffern	Rechtssichere Protokollierung	Referenzierbarkeit Folgekommunikation
OSCI	Ja	Ja	Ja
XTA	Ja	Ja	Nein*

Technologie	Nachrichten puffern	Rechtssichere Protokollierung	Referenzierbarkeit Folgekommunikation
FIT-Connect	Ja	Ja	Ja
NOOTS	Nein	–	–
ZaPuK	Ja	Teilweise**	Ja
X-Road	Nein	–	–
eDelivery AS4	Ja	Ja	Ja

* Laut XTA-Standard sind nur für den synchronen Fall Fachantworten vorgesehen. Folgekommunikation ist folglich nur über die Fachstandards oder auf Anwendungsebene möglich, erscheint jedoch mit niedrigem Aufwand nachrüstbar und wird auch von den verwendeten Nachrichtenprotokollen unterstützt.

** Rechtssichere Protokollierung ist in ZaPuK geplant, aber ohne Finalisierung der zugehörigen Konzepte. Matrix stellt die für rechtssichere Protokolle notwendigen Funktionen wie Lesebestätigungen mit Zeitstempeln und signierte Events zur Verfügung.

5.4.3 Szenario »Synchron, Abruf«

Tabelle 7 Eignung der Technologien für Szenario »Synchron, Abruf«

Technologie	Unterstützung sync. Request / Response	Callback-/ Push-Unterstützung	Round-Trip, kurze Latenz	Angepasste Protokollierung
OSCI	Ja	Ja	Nicht spezifiziert	Im Prinzip*
XTA	Ja	Ja	Nicht spezifiziert	Theoretisch**
FIT-Connect	Nein***	Ja*****	Im Sekundenbereich	Nein****
NOOTS	Ja	Ja	Ja	Nein****
ZaPuK	Nein	–	–	–
X-Road	Ja	Ja*****	Ja	Ja
eDelivery AS4	Nein	–	–	–

* OSCI verlangt standardmäßig die Protokollierung für Zwecke der Rechtssicherheit. Die flexible, geschachtelte Nachrichtenstruktur ermöglicht jedoch Einflussnahme auf die protokollierten Inhalte.

** Der XTA-Standard kann die Protokollierung in vielfältiger Weise über Service-Profile vorgeben. Service-Profile sind jedoch optionaler Bestandteil des Standards.

*** FIT-Connect bietet relativ geringe Latenzen, fachliches Request/Response mit Zeitlimits wird jedoch nicht in der API und den SDKs unterstützt.

**** Die Protokollierung in NOOTS und FIT-Connect ist für die speziellen Anforderungen der jeweiligen Kern-Anwendungsfälle konzipiert. Ein generisches Konzept für die Anpassung der Protokollierung existiert nach unserer Kenntnis jeweils nicht.

***** Keine Unterstützung von Initiativumkehr.

5.4.4 Szenario »Synchron, Nachrichtenversand mit synchroner Rückmeldung«

Tabelle 8 Eignung der Technologien für Szenario »Synchron, Nachrichtenversand mit synchroner Rückmeldung«

Technologie	Unterstützung sync. Request / Response	Callback-/ Push-Unterstützung	Round-Trip, kurze Latenz	Rechts-sichere Protokollierung
OSCI	Ja	Ja	Nicht spezifiziert	Ja
XTA	Ja	Ja	Nicht spezifiziert	Ja
FIT-Connect	Nein*	Ja****	Im Sekundenbereich	–
NOOTS	Spezialisiert**	Ja	Ja	Nein***
ZaPuK	Nein	–	–	–
X-Road	Ja	Ja****	Ja	Ja
eDelivery AS4	Nein	–	–	–

* FIT-Connect bietet relativ geringe Latenzen, fachliches Request/Response mit Zeitlimits wird jedoch nicht in der API und den SDKs unterstützt.

** Die synchrone Kommunikation über den SAK ist in NOOTS auf den Registerabruf spezialisiert. Die generische Nachrichtenübertragung im B2G- oder G2G-Kontext, z. B. die synchrone Übermittlung von OZG-Anträgen, ist zwar vorstellbar, aber nicht konzipiert.

*** Die Protokollierung in NOOTS ist für die speziellen Anforderungen des Registerabrufs konzipiert.

**** Keine Unterstützung von Initiativumkehr.

5.4.5 Vergleichender Szenarien Überblick

Die folgende Tabelle stellt die Technologien vergleichend über alle Kommunikationsszenarien dar. In der Farbcodierung sind Zellen wie folgt farblich markiert:

- *Blassgelb*: Die Anforderungen des Szenarios sind mit Einschränkungen erfüllt.
- *Gelb*: Die Anforderungen des Szenarios sind formal nicht erfüllt. Die funktionalen Bausteile existieren jedoch in der Technologie und eine entsprechende Umsetzung erscheint realisierungsnah.

- *Orange*: Die Anforderungen des Szenarios sind formal nicht erfüllt. Es existieren jedoch Bausteine, aber auch weitere Einschränkungen.
- *Rot*: Die Anforderungen sind nicht erfüllt, es liegen keine diesbezüglichen Konzepte vor und eine Umsetzung erscheint nur mit höherem Aufwand möglich.

Die Tabelle stellt lediglich eine verdichtete Bewertung der vorangegangenen Abschnitte für die einzelnen Kommunikationsszenarien dar. Die Begründungen für die einzelnen Bewertungen sind diesen Abschnitten zu entnehmen.

Tabelle 9

Gesamtüberblick über alle Kommunikationsszenarien

Technologie	Asynchron ohne Antwort	Asynchron mit Antwort	Synchroner Abruf	Synchroner Nachrichtenversand
OSCI	Ja	Ja	Ja	Ja
XTA	Ja	Bausteine vorhanden	Einschränkung	Ja
FIT-Connect	Ja	Ja	Bausteine vorhanden	Bausteine vorhanden
NOOTS	Nein	Nein	Einschränkung	Bausteine vorhanden
ZaPuK	Bausteine vorhanden	Bausteine vorhanden	Nein	Nein
X-Road	Nein	Nein	Einschränkung	Einschränkung
eDelivery AS4	Ja	Ja	Nein	Nein

6 Handlungsempfehlungen

6.1 Technische Handlungsempfehlungen

Im Rahmen der Recherchen und Interviews zu den einzelnen Technologien wurden eine Reihe von technologieübergreifenden Erkenntnissen und Best Practices gesammelt, die in den folgenden technischen Handlungsempfehlungen zusammengefasst sind.

6.1.1 Übergreifendes Requirements Engineering und Architekturdesign

Im Verlauf der Studienrecherche ist klar geworden, dass in unterschiedlichen Technologien grundlegende Architekturentscheidungen verschieden getroffen wurden. So werden in verschiedenen Technologien Themen wie Rechtssicherheit oder Nichtabstreitbarkeit, aber auch Ende-zu-Ende-Verschlüsselung unterschiedlich stark gewichtet oder zumindest teilweise in fachlicher Verantwortung außerhalb der Transportschicht gesehen. Die betrachteten Technologien beschreiben jedoch oft nicht nur eine Transportschicht, sondern eine gesamte Kommunikationsinfrastruktur. Dabei arbeiten sie im Schnittstellendesign, in den Datenformaten und teilweise auch im Transport verschiedene fachliche Anforderungen ein (bspw. Asynchronität in FIT-Connect, Persistenz in ZaPuK, Synchronität in NOOTS).

Wir empfehlen, dass ein übergreifendes Requirements Engineering stets mit systematischem Architekturdesign gekoppelt wird, um im Design der Technologie eine klare, sinnvolle Trennung von Transport- und Fachlogik herzustellen. Grundlegend ist hier auch die Beachtung der abzudeckenden Kommunikationsszenarien.

6.1.2 Technische Hilfsmittel für Softwareentwickelnde

Bezüglich der analysierten Technologien bietet sich ein sehr unterschiedliches Bild hinsichtlich der angebotenen Hilfsmittel für Softwarehersteller. Alle eingesetzten Technologien sollten folgende Eigenschaften aufweisen:

- Klare, angemessene Dokumentation inklusive Tutorials
- Effiziente SDKs oder APIs, die eine gute Administrierbarkeit sicherstellen, insbesondere in Hinblick auf IT-Sicherheit
- Ausführliche spezifikationskonforme Beispiel- und Referenzimplementierungen

- Versionskontrolle, Fehlerdokumentation und Behebung nach gängigen IT-Standards
- Semantische Versionierung von Artefakten mit dokumentierten Änderungen

Sofern die Entwickler-Community diese Artefakte nicht eigenständig bereitstellt, so sind die notwendigen Ressourcen für die Erstellung durch öffentliche Stellen zur Verfügung zu stellen, um die Zukunftsfähigkeit der Technologie zu gewährleisten.

6.1.3 Angemessene Entwicklung von IT-Standards

Sofern die Technologien als eigene IT-Standards hauptsächlich von öffentlichen Stellen gepflegt werden, ist in der Spezifizierung eines Standards der Gewinn von Flexibilität und Freiheitsgraden gegen das Risiko von Unterspezifizierung und Dialektbildung abzuwägen. Die Förderung von Interoperabilität durch bedarfsgerechte, auf echten Notwendigkeiten beruhenden Erweiterungen sollte integraler Bestandteil des Entwurfsprozesses sein.

Neben den oben genannten Hilfsmitteln sollte sich die Pflege eines Standards an relevanten Vorbildern in der IT orientieren. Dies beinhaltet beispielsweise auch die Schaffung von Testsuites¹⁴, Zertifizierungsprogrammen für Software mit Konformitätsanspruch oder sogenannten »Logo«-Programmen¹⁵.

6.1.4 Beachtung von Resilienz und Skalierbarkeit

Einige der betrachteten Infrastrukturen sind noch im Aufbau. Es ist nachvollziehbar, dass Anforderungen an Skalierbarkeit und Resilienz gegen technische Störungen oder Angriffe in der Anfangsphase aufgrund niedriger Systemlast zunächst zurückgestellt werden. Dies entbindet jedoch nicht davon, für den Zielausbau geeignete technische Konzepte vorzusehen, um die möglichen Risiken zu adressieren, wie etwa horizontale Skalierbarkeit, Kapazitätsmanagement, redundante Betriebsmodelle, Disaster-Recovery-Konzepte, Abwehr von DDoS-Angriffen (*Distributed Denial of Service*), Schlüsselrotation und *Observability*-Konzepte. Auch der Einsatz geeigneter dezentraler Konzepte in Dienststrukturen kann zu einem resilienten Ökosystem beitragen, um Angriffsvektoren zu entkräften, die auf Single-Points-Of-Failure zielen.

Bei zentralen Lösungen oder Komponenten liegt die Empfehlung klar beim Einsatz Cloud-nativer Software, um Skalierbarkeit und zukunftsfähigen Betrieb sicherzustellen.

¹⁴ Zum Beispiel <https://ttn-3.etsi.org/index.php/downloads/publics/publics-etsi> Abruf 29.07.2026

¹⁵ Zum Beispiel <https://www.ipv6ready.org/> Abruf 29.07.2026

6.1.5 Betriebsmodelle für kleine und mittlere Kommunen

Mehrere der untersuchten Technologien setzen den Betrieb bestimmter Komponenten pro Behörde oder Kommune voraus. Viele kleine oder mittlere Kommunen wären jedoch mit dem Betrieb und der Wartung dieser Komponenten überfordert. Das mit der Governance einer Technologie beauftragte Management muss für tragfähige Konzepte zum Betrieb der erforderlichen Technik auch für kleine und mittlere Kommunen unter Berücksichtigung der IT-Sicherheit Sorge tragen. Beispiele für solche Konzepte sind beispielsweise mandantenfähige Anschlussknoten oder »Register as a Service«.

Auch geben viele Kommunen den Betrieb ihrer IT in die Hände von Dienstleistern. Einige der untersuchten Technologien warten mit Self-Service-Portalen auf, die es Behörden und Kommunen ermöglichen sollen, ihre Anbindungen selbst zu konfigurieren. In Interviews mit kommunalen Dienstleistern wurde bemängelt, dass bei den Self-Service-Angeboten oft komfortable APIs zur Verwaltung einer größeren Anzahl von Kommunen durch die Dienstleister nicht ausreichend berücksichtigt seien. Vor einem Flächen-Rollout einer Technologie sollten diese Convenience-Funktionen berücksichtigt worden sein.

6.1.6 Brücken- und Adapterlösungen

In vielen Fällen müssen Fachverfahren, die an unterschiedliche Netze – z. B. Internet oder behördliches Verbindungsnetz – angeschlossen sind, miteinander kommunizieren. Mit steigender Anzahl von Anbindungen werden effiziente Brückenlösungen zwischen den verschiedenen Netzen benötigt. Dies muss beim weiteren Ausbau der betreffenden Technologien berücksichtigt werden.

Im Kickoff-Workshop zur Studie und in Gesprächen mit Stakeholdern wurde weiterhin der Wunsch ausgedrückt, die diversifizierte »Landschaft« von etablierten und entstehenden Kommunikationstechnologien auf die unbedingt notwendigen zu konsolidieren. Sofern in der nahen Zukunft Entscheidungen zur Obsoleszenz von Technologien in bestimmten Bereichen gefällt werden, ist für eine Übergangszeit, die realistisch mehrere Jahre in Anspruch nehmen kann, die Interoperabilität von Fachverfahren, die mit unterschiedlichen Technologien angebunden sind, sicherzustellen. Dazu sollte die Entwicklung von Brückenlösungen beauftragt werden, sodass die Fachverfahrenshersteller nicht für alle derzeit im Feld befindlichen Technologien individuelle Adapter entwickeln und pflegen müssen.

Beispiele für solche Brückenlösungen könnten beispielsweise sein:

- ein XTA-Server, der neben OSCI auch Matrix oder FIT-Connect als Transportschicht verwenden kann, oder

- ein FIT-Connect-SDK, das auch über die OSCI-Infrastruktur Nachrichten übertragen kann.

Hindernis für solche Entwicklungen ist jedoch die Tatsache, dass alle betrachteten Technologien unterschiedliche und inkompatible Routing- und Verzeichnisdienste einsetzen. Auch ist bezüglich solcher Vorhaben mit Widerständen von Interessenparteien zu rechnen.

In den Recherchen und Interviews zur vorliegenden Studie fiel auf, dass Themen wie PKI, Identity-Management, Berechtigungsverwaltung und Verzeichnisdienste, die in allen Technologien benötigt werden, sehr unterschiedlich behandelt und parallel sehr divers sowie nicht-interoperabel entwickelt werden. Wir empfehlen dringend, in diesem Bereich eine Angleichung vorzunehmen und Interoperabilität herzustellen.

6.2 Handlungsempfehlungen zur Governance

Im Rahmen der Recherchen und Interviews zu den einzelnen Technologien wurden eine Reihe von technologieübergreifenden Erkenntnissen und Best Practices gesammelt, die in den folgenden technischen Handlungsempfehlungen zusammengefasst sind.

6.2.1 Digitale Souveränität in der Technologieentwicklung

Mit einer gewissen Sorge haben wir festgestellt, dass viele der etablierten und auch aktuell in Entwicklung befindlichen Technologien nationale Eigenentwicklungen sind. Dies sichert zwar im ersten Anschein die digitale Souveränität über die Technologie, andererseits führt ein solches Vorgehen oft in die Abhängigkeit von wenigen Anbietern. So existieren im Fall von OSCI / XTA – wie auch in einer früheren Studie [49, S. 18] festgestellt und durch unsere Analyse bestätigt – reale Markthindernisse aufgrund der nur »halboffenen« Entwicklung und Pflege des Standards, charakterisiert durch wenig transparente Beteiligungsprozesse, fehlende offene Referenzimplementierungen sowie rein proprietäre Software für zentrale Komponenten wie OSCI-Intermediäre und XTA-Server. Auch eine Reihe der aktuell in Entwicklung befindlichen Technologien sind derzeit zumindest teilweise »Closed-Code«-Eigenentwicklungen. Für deren Open-Source-Stellung wurden in den Interviews bisher nur vage Absichtserklärungen ohne konkrete Roadmap geäußert.

Dabei ist Quelloffenheit nicht nur ein zentrales Element für Transparenz, digitale Souveränität und ein faires Ökosystem aus Softwareherstellern, sondern explizites Gebot in föderalen IT-Richtlinien, etwa dem Servicestandard für die digitale Verwaltung [128], der föderalen Architekturrichtlinie [130] und den Architekturprinzipien des Deutschland-Stacks [149]. Wir empfehlen – sofern nicht

besondere Gründe dagegensprechen – alle eigenentwickelten Technologien in diesem Kontext quelloffen zu stellen.

Quelloffene Entwicklungen sollten auf geeigneten, zentralen Plattformen erfolgen, insbesondere auf der dafür bereitgestellten Plattform openCode.de¹⁶. Interna wie zum Beispiel konkrete Systemkonfiguration sollten jedoch weiterhin auf privater Infrastruktur abgelegt werden, um sie vor unbefugtem Zugriff zu schützen. Durch die Nutzung von openCode kann eine transparente Entwicklung mit Aspekten aus Sicht der deutschen Verwaltungsdigitalisierung und digitaler Souveränität verknüpft werden.

Etablierte Plattformen wie openCode ermöglichen eine Diskussion und Beteiligung auf Basis einer breiten, dort bereits vorhandenen Nutzerbasis. Eine solche Möglichkeit zur Diskussion ist bei verteilten, projektspezifischen Versionskontrollsystemen so nicht möglich, insbesondere da Akteure zunächst auf diesen Plattformen pro Projekt separat ein Onboarding durchlaufen müssen.

Die Beteiligung an internationalen Entwicklungen von Open-Source-Projekten stellt zwar vordergründig eine Einschränkung der Selbstständigkeit dar, kann jedoch durch eine gemeinsame Entwicklung nicht nur die internationale Anschlussfähigkeit von Technologien verbessern, sondern bietet auch die Chance auf größere Vielfalt und Leistungsfähigkeit des Ökosystems der Entwicklergemeinschaft.

6.2.2 Europäische Interoperabilität

Wie im letzten Abschnitt erwähnt, bietet eine Beteiligung an europäischen Entwicklungsprojekten eine Chance höherer Effektivität. Darüber hinaus besteht mit der europäischen »Verordnung für ein interoperables Europa« die Verpflichtung öffentlicher Stellen, die Interoperabilität innerhalb Europas zu fördern [150]. Es ist eine offensichtliche Beobachtung nicht nur der vorliegenden Studie, dass aktuelle, zentrale Entwicklungsprojekte des Deutschland-Stacks oder anderer Rahmen der Verwaltungsdigitalisierung nationale Eigenentwicklungen sind.

Auch im Interesse der verpflichtenden europäischen Interoperabilität sollte die Nutzung von oder Beteiligung an europäischen Softwareinitiativen ernsthaft geprüft werden.

6.2.3 Identitätsverwaltung und Authentifizierung

Zur sicheren Kommunikation benötigt jede Technologie eine Möglichkeit, die Identität eines Kommunikationsteilnehmers zu bestätigen. Ein Kommunikationsteilnehmer kann hierbei sowohl ein technisches System als auch eine natürliche

¹⁶ <https://opencode.de/>

Person sein. Die Authentifizierung eines Teilnehmers bildet die Grundlage für die Authentizität und Vertraulichkeit der ausgetauschten Nachrichten. Aktuell greifen dabei mehrere der betrachteten Technologien unter anderem auf die Verwaltungs-PKI als verlässliche Informationsquelle zurück, da vor der Ausstellung eines Zertifikats durch die V-PKI eine vertrauenswürdige Instanz eine gründliche Verifikation des Antragstellers durchführt.

Der Identitätsnachweis über ein Zertifikat der V-PKI bringt jedoch verschiedene Probleme mit sich. Der Verifikationsprozess ist zwar ausführlich und vertrauenswürdig, dadurch jedoch auch aufwendig und langwierig. Zertifikate für Zertifikatvergabestellen stellt ausschließlich das BSI aus. Zertifikate für einzelne Dienste kann dann wiederum eine Zertifikatvergabestelle bereitstellen. Die Skalierbarkeit der Prüfprozesse ist jedoch stark begrenzt.

Wegen des hohen Aufwands werden in der Regel möglichst wenige Zertifikate bei der V-PKI beantragt und mit einer langen Gültigkeitsdauer ausgegeben. Eine lange Gültigkeit birgt jedoch zusätzliche Risiken, wie etwa einen längeren Missbrauchszeitraum bei einem unbemerkten Diebstahl eines Zertifikats und eingeschränkte Kryptoagilität. Des Weiteren ist der Nachweis der Identität über ein Zertifikat, insbesondere für kleinere Kommunen, komplex und fehleranfällig. Bei einer falschen Verwendung von Zertifikaten kann der private Schlüssel, der als Nachweis der Identität genutzt wird, versehentlich offengelegt werden. Zudem sind diese Schlüssel möglicherweise für Dritte zugänglich, die Fachverfahren im Auftrag betreiben. Die genannten Probleme bestehen generell auch bei Alternativen wie ELSTER-Zertifikaten, die von einigen der betrachteten Technologien genutzt werden sollen.

Der Baustein »Identität & Vertrauen« ist im Deutschland-Stack bereits vorgesehen, beschreibt jedoch aktuell lediglich die Ist-Landschaft mit Lösungen inklusive der eID und EUDI-Wallet. Die zuvor genannten Problemstellungen übertragen sich jedoch auch auf Lösungen wie etwa dem »Mein Unternehmenskonto«, die auf dem Vertrauen in die V-PKI oder die ELSTER-Zertifikate aufbauen.

Da die Identitätsprüfung bei der Ausstellung von Nachweisen und die Authentifizierung von Kommunikationsteilnehmern für alle betrachteten Technologien eine zentrale Hürde darstellen, halten wir die Bereitstellung eines einheitlichen und verlässlichen Dienstes im Rahmen des Deutschland-Stacks für empfehlenswert. Der Fokus sollte dabei auf einer Verbesserung der Prozesse zur Beantragung, Ausstellung und Erneuerung der Nachweise liegen. Die Verifikation der Identität muss zwingend das aktuelle Vertrauensniveau aufrechterhalten, während die Skalierbarkeit und die Möglichkeiten zur (teilweisen) Automatisierung verbessert werden sollten.

Den modernen Standards zur Identitätsverwaltung entsprechend, sollten die Nachweise feingranular auf einzelne Dienste und Systeme bezogen werden können und eine möglichst kurze Gültigkeitsdauer haben. Der Einsatz und die Verwaltung der Nachweise durch die Kommunen sollte möglichst einfach sein, um Konfigurations- und Bedienfehler zu vermeiden.

Der Nachweis einer Identität oder Organisationszugehörigkeit sollte möglich sein, ohne das zentrale Geheimnis, wie den privaten Schlüssel eines Organisationszertifikats, an Dritte weitergeben oder auf einem risikobehafteten System speichern zu müssen. Die bestehenden Dienste, wie die Bund-ID und das Unternehmenskonto, und die bereits im Deutschland-Stack anerkannten Standards, wie OAuth und OIDC, bieten hier bereits eine solide Grundlage.

Parallel zur Entstehung dieser Studie beschäftigt sich das Projekt »Föderale API-Autorisierungsinfrastruktur« [151] mit der verwandten Frage der Autorisierung von Anfragen an die Basisdienste des Deutschland-Stacks. Die geplante Infrastruktur baut ebenfalls bestehenden Diensten auf, wie »Mein Unternehmenskonto« und der V-PKI, stellt in seiner Betrachtung jedoch ebenfalls die zuvor genannten Modernisierungsbedarfe der V-PKI und Lücken in den bestehenden Identitätsdiensten fest [152]. Das Projekt schlägt die Erstellung einer Föderation aus verschiedenen Identitätsprovidern nach dem Vorbild des DNF-AAI¹⁷ sowie die Modernisierung der V-PKI vor. Wir unterstützen die Bestrebungen und Empfehlungen des Projekts in diesen Bereichen. Dabei gilt es jedoch zu beachten, dass sich der kritische Prozess der Identitätsprüfung und damit das Vertrauen in die Infrastruktur auf die einzelnen Identitätsprovider und die Aufnahme dieser in die Föderation verschiebt. Damit nimmt die vorgeschlagene Federation-Betriebsstelle eine vergleichbare Rolle zum BSI in der bestehenden V-PKI ein und muss entsprechend vertrauenswürdig sein.

6.2.4 Klare Steuerung und Verantwortlichkeiten

Laut Interviews im Rahmen der vorliegenden Studie sind einige der Problemfelder in den etablierten Technologien OSCI und XTA auf die fragmentierte Governance und mangelnde Ressourcenausstattung in steuernden Bereichen zurückzuführen: Weiterentwicklung, Betrieb und Pflege des Standards, der Implementierungen und der Infrastruktur liegen in unterschiedlichen Händen mit teilweise auseinanderstrebenden Interessenstrukturen.

Bei FIT-Connect ist dies nach unserer Beobachtung besser gelöst, indem Schnittstellen, Implementierungen und Infrastrukturen zentral gesteuert werden. Für andere Technologien wie etwa ZaPuK ist es noch zu früh, die entstehenden Governance-Strukturen zu beurteilen.

¹⁷ Infoportal: <https://www.aai.dfn.de/> Abruf: 18.08.2026

Bei der Gestaltung der Governance einer in Entwicklung befindlichen Technologie sollten positive wie negative Erfahrungswerte der existierenden, produktiven Technologien berücksichtigt werden. Dies schließt nicht nur die in diesem Dokument betrachteten Technologien ein, sondern es lassen sich viele wertvolle Erfahrungen aus erfolgreichen internationalen Projekten in der Kommunikationstechnologie ziehen, z. B. IPv6.

Weiterhin empfehlen wir dringend, beim Aufbau neuer Technologiestrukturen eine geeignete Steuerung zu etablieren, mit klaren Verantwortlichkeiten während des gesamten Systemlebenszyklus und effektiven Feedbackstrukturen zur angemessenen Berücksichtigung der Interessen aller Stakeholder. In diesem Zusammenhang ist für eine ausreichende Abdeckung der dazu notwendigen Ressourcen Sorge zu tragen, nicht nur für die Entwicklung und Einführung der Technologie, sondern auch für die Verstetigung des Betriebs und der Instandhaltung.

Das in Abschnitt 6.2.3 angesprochene nicht-interoperable Auseinanderstreben von isolierten Lösungen für PKI, Identity-Management, Berechtigungsverwaltung und Verzeichnisdienste sollte mittels einer übergeordneten Steuerung konsolidiert werden.

In den Interviews zur vorliegenden Studie wurde vielfach berichtet, dass Partikularinteressen Wahrnehmungen und Entscheidungsprozesse in und um die Entwicklung von Technologien beeinflussen. Isolierte, inhaltlich artverwandte und parallel entwickelte Projekte führen jedoch zu redundanten Entwicklungen und erhöhen gesamtgesellschaftliche Kosten. Es werden inkompatible, heterogene Subökosysteme geschaffen, die zu einer Zersplitterung der Kommunikationslandschaft beitragen.

Eine kollaborative, gemeinschaftliche Konzeptionierung und Entwicklung sollte Individualvorgängen vorgezogen werden. Eine kollaborative Herangehensweise kann somit auch als zentrales Werkzeug dienen, zukünftige Ökosysteme homogen zu gestalten. Im Rahmen kollaborativer Entwicklungen besteht außerdem Potenzial für die Verknüpfung mit Open-Source-Ansätze, um auch der Zielsetzung »Public Money, Public Code« gerecht zu werden. Solche Ansätze können helfen, Ökosysteme auch für private Akteure, Unternehmen ebenso wie Privatpersonen, zugänglich zu machen.

Die Etablierung einer geeigneten Steuerung zur Einhegung der berichteten Partikularinteressen wird vom Autorenteam der vorliegenden Studie als eine Aufgabe der obersten föderalen Entscheidungsgremien für die Verwaltungsdigitalisierung betrachtet.

6.2.5 Konsolidierung der Verwaltungsprozesse

Ein wichtiges Motiv für die Beauftragung der vorliegenden Studie ist die angestrebte Konsolidierung der Verwaltungs-IT. Die Erfahrung lehrt jedoch, dass es schwer ist, IT-Systeme zu vereinheitlichen, solange die Prozessstrukturen, die unterstützt werden sollen, uneinheitlich sind. Dies gilt insbesondere für den Zuschnitt von Workflows und Berechtigungen.

Solange verschiedene Behördenstandorte Verwaltungsvorgänge unterschiedlich strukturieren und uneinheitliche Rollen- und Berechtigungskonzepte verwenden, können IT-Systeme eine solch heterogene Prozesslandschaft nicht konsistent unterstützen, weil zum Beispiel für jede Behörde ein individueller Rollenzuschnitt technisch abgebildet werden muss.

Dies trifft vor allem die Fachverfahren, aber in zunehmendem Maße auch fortschrittliche Transporttechnologien wie etwa das NOOTS, dass sich zum Ziel gesetzt hat, für den Registerzugriff maßgeschneiderte, aber dennoch generische Autorisierungskonzepte anzubieten. Dieser im Grundsatz sehr begrüßenswerte Lösungsansatz wird aber auf erhebliche Probleme stoßen, wenn verschiedene Verwaltungsinstanzen allzu unterschiedliche, womöglich inkompatible Auffassungen von Rollen, Berechtigungen oder Verarbeitungszwecken haben.

Daher ist es ein wichtiger vorbereitender Schritt einer Technologiekonsolidierung, zunächst für eine Prozesskonsolidierung zu sorgen. Die erfolgreiche Einführung einer neuen Transporttechnologie mit ausgereiftem Identitäts- und Berechtigungsmanagement setzt ein gemeinsames Verständnis von Vorgängen und Begrifflichkeiten voraus.

6.2.6 Konsolidierung von Technologien

In Abschnitt 6.1.6 wurde der Wunsch von Stakeholdern nach Konsolidierung der im Einsatz befindlichen oder perspektivischen Technologien angesprochen. In die Bewertung der Technologien sollten jedoch nicht nur die in dieser Studie einbezogenen Kriterien herangezogen, sondern der gesamte Technologiekontext betrachtet werden. Die in dieser Studie betrachteten Kriterien richteten sich auftragsgemäß nach B2G- und G2G-Kommunikationsszenarien. Technologien wie Matrix bieten darüber hinaus zusätzliche Funktionalitäten wie G2C-Kommunikation, Chat oder Videostreaming, die andere betrachtete Technologien nicht aufweisen.

Das Ersetzen einer Technologie sollte aus unserer Sicht zunächst domänenbezogen betrachtet werden, da unterschiedliche Domänen verschiedene Anforderungen stellen, die durch die eingesetzte Technologie und deren perspektivische Ablösung in unterschiedlichem Maß abgedeckt werden. So bietet möglicherweise die aktuell eingesetzte Technologie bestimmte Eigenschaften für eine rechts-

sichere Kommunikation, die von der potenziellen Ablösetechnologie noch nicht vollständig abgedeckt sind. Der Abgleich mit einer ersetzenden Technologie *muss* sicherstellen, dass alle fachlichen Anforderungen der Fachdomäne angemessen unterstützt werden. Funktionale Lücken sollten vor der Ersetzung der älteren Technologie geschlossen werden, um eine Störung der Verwaltungsprozesse auszuschließen und die Akzeptanz der ersetzenden Technologie durch die Anwender sicherzustellen.

Sind die fachlichen Anforderungen erfasst und alle funktionalen Lücken erfasst, sollte für das Ersetzen einer Technologie in der betreffenden Domäne eine Kosten-Nutzen-Analyse, gekoppelt mit einer Chancen-Risiko-Abwägung, durchgeführt werden.

6.2.6.1 Kostenbetrachtung des Weiterbetriebs ohne Ersetzen der Bestandstechnologie

Für die Kosten-Nutzen-Analyse wird zunächst eine Aufstellung der perspektivischen Kosten des Weiterbetriebs der aktuell eingesetzten Bestandstechnologie benötigt.

Für die Kommunikationsinfrastruktur, deren Kosten oft übergeordnete Stellen wie Bund oder Länder übernehmen, sind folgende Kosten zu betrachten:

- Betriebskosten
- Personalkosten
- Wartungskosten zur Sicherstellung des reibungslosen Weiterbetriebs (z. B. Security-Updates)
- Lizenzgebühren
- Kosten für die funktionale Weiterentwicklung
- Kosten für technische Erneuerungen, z. B. notwendige Hardware-Aktualisierungen
- Kosten für technische und organisatorische Umstellung inklusive Schulungen

Für die angebundenen Fachverfahren, deren Kosten in der Regel zu Lasten der einsetzenden Behörden anfallen, sind folgende Kosten zu berücksichtigen:

- Wartungskosten für die Anbindungen (z. B. Updates)
- Lizenz- und Nutzungsgebühren der Anbindungen
- Kosten für technische Erneuerungen, z. B. notwendige Hardware-Aktualisierungen

Diese Kosten sollten in realistischer Weise Kostensteigerungen beinhalten, die sich aus dem mittel- oder langfristigen Weiterbetrieb der aktuell eingesetzten

Technologie ergeben, zum Beispiel aufgrund einer geringeren Marktverfügbarkeit, fehlender Herstellerunterstützung, einem möglichen Fachkräftemangel oder aufgrund erforderlicher Maßnahmen gegen zunehmende Sicherheitsrisiken.

6.2.6.2 Kostenbetrachtung für eine Migration

Dieselbe Aufstellung laufender Kosten wird für die ersetzende Technologie benötigt.

Zusätzlich müssen weitere Migrationskosten (gemeinsam für Ebenen Bund / Länder und Behörden) betrachtet werden:

- Kosten für die technische und organisatorische Umstellung inklusive Schulungen, Anpassungen von Betriebsprozessen, Kosten für disruptive Effekte
- Kosten für einen Übergangsbetrieb beider Technologien inklusive gegebenenfalls erforderlicher temporärer Adapter- oder Brückenlösungen
- Kosten für die Änderung der Anbindung von Fachverfahren inklusive Schulung und der Anpassung von Prozessen an die neue Technologie

Für eine optimale Kostenstrukturierung sollten die Kosten für eine eigene Durchführung und ein »Outsourcing« an einen Dienstleister gegenübergestellt werden. Das betrifft sowohl die Investitionskosten (CAPEX) als auch die laufenden Betriebskosten (OPEX). Ebenfalls sollten dabei auch eventuelle Mehrkosten durch Risikofaktoren entsprechend der Eintrittswahrscheinlichkeit einfließen, wie etwa Kosten für Verzögerungen bei Anpassungsarbeiten in Eigenregie oder durch einen Dienstleister, der die Haftung für die Tätigkeiten übernimmt.

6.2.6.3 Betrachtung von mittel- und langfristigen Nutzeneffekten

Um einen fairen Vergleich eines Verbleibs bei der Bestandstechnologie gegen die Migration zu einer alternativen Technologie durchzuführen, müssen ebenfalls mittel- oder langfristige Kosten- und Nutzeneffekte einer Migration eingerechnet werden, die sich ohne sie nicht einstellen, zum Beispiel:

- Niedrigere Personalkosten
- Zeitersparnis
- Effizienzsteigerung durch Digitalisierung weiterer Verwaltungsprozesse
- Weniger Fehler, IT-Sicherheitsgewinn
- Qualitätsverbesserung
- Interoperabilitätsnutzen

6.2.7 Migrationsstrategien

Vor der endgültigen Entscheidung für den Umstieg in einer Domäne auf eine andere Technologie sollte eine Migrationsstrategie entwickelt werden, die nicht nur die organisatorischen Umstände geklärt hat, sondern auch die Maßnahmen, die für die aktuell eingesetzte und die ablösende Technologie getroffen werden müssen:

- Technische Anpassungen der ablösenden Technologie für die Anforderungen in der Fachdomäne
- Technische Anpassungen der abzulösenden Technologie für den »Brückenbetrieb«, in dem beide Technologien interoperabel sein müssen
- Technische Anpassungen der Fachverfahren
- Roadmap für das Rollout unter Beachtung des Aufbaus der neuen Infrastruktur und technischen Anpassungen der ablösenden Technologie
- Einplanung notwendiger Wartungsintervalle der abzulösenden Technologie, z. B. für Sicherheitsupdates
- Gegebenenfalls Rückbau der abzulösenden Infrastruktur
- Technische und organisatorische Maßnahmen zur schnellen Entstörung und Nutzerunterstützung bei unvermeidlichen Disruptionen in der Umstiegsphase

6.2.8 Keine Vermischung von konkreten Technologien und Rechtsbindung

In Interviews und Recherchen zu der vorliegenden Studie wurde mehrfach beobachtet, dass die Referenzierung konkreter Technologien in rechtsverbindlichen Dokumenten zu unerwünschten Effekten führte. Beispiele:

- In der XBasisdaten-Verordnung [46] wurde der Einsatz des konkreten Schnittstellenstandards XTA in Verbindung mit OSCI-Transport vorgeschrieben – aus Sicht mancher Interviewteilnehmer ohne ausreichende Begründung. Laut Interviews mit dem BVA hat diese Vorgabe zu erheblichem Mehraufwand und Verzögerungen ohne klaren Mehrwert geführt.
- OSCI in der eingesetzten Version befindet sich seit 2002 auf dem Versionsstand 1.2. Aus unserer Sicht gab es seitdem eine Reihe von Änderungen und Erweiterungen des Standards, die mit einer entsprechenden Versionsänderung hätten einhergehen müssen, wie dies in der Softwareentwicklung üblich ist. Stattdessen wurde auf das ungewöhnliche Konstrukt sogenannter Korrigenda zurückgegriffen, die im Bundesanzeiger veröffentlicht werden. Diese Vorgehensweise erschwert Entwicklerteams signifikant die Übersicht, welche Funktionalitäten tatsächlich aktueller Teil des Standards und welche bereits veraltet sind. Laut einer von uns nicht überprüften Aussage in einem Interview

wurde die OSCI-Versionsnummer 1.2 trotz relevanter Änderungen nicht angetastet, um keine rechtsverbindlichen Dokumente ändern zu müssen.

Wir empfehlen dringend, in legal bindenden Dokumenten keine konkreten Technologien mit oder ohne konkrete Version zu benennen, sondern stattdessen die Eigenschaften von Übertragung oder Anbindung technologie-neutral anhand qualitativer Merkmale einzufordern.

Liste der Interviews

Termin	Interviewteilnehmer
20.04.2026	Projektleitung NOOTS
28.04.2026	Koordinierungsstelle für IT-Standards (KoSIT)
29.04.2026	Bundesministerium für Digitalisierung und Staatsmodernisierung (BMDS), Referat DS I 1
07.05.2026	Produktmanagement FIT-Connect, Projekt-Team
08.05.2026	ZaPuK, Mitglieder des Steuerungskomitees
12.05.2026	NOOTS Architektur BVA)
13.05.2026	Projektteam NEO (FITKO)
26.06.2026	Bundesverwaltungsamt, Anbindung IDA-Verfahren
27.05.2026	Produktmanagement der FITKO
02.06.2026	ZaPuK Architektur (FITKO)
03.06.2026	Projektteam NEO (FITKO)
10.06.2026	CIO Schleswig-Holstein
18.06.2026	Databund (HSH)
19.06.2026	Governikus
22.06.2026	Governikus / Mitglieder Arbeitsgruppe »IT-Standards in der Justiz« der Bund-Länder-Kommission (BLK)
24.06.2026	NOOTS Architektur (BVA)
25.06.2026	Projektleitung Einführung X-Road, Land Schleswig-Holstein
26.06.2026	Databund (nextgov iT)
30.06.2026	Taskforce Digitalisierung, IT Niedersachsen
01.07.2026	Produktmanagement FIT-Connect, Projekt-Team
03.07.2026	Kommunale Datenverarbeitung Oldenburg (KDO)

Literaturverzeichnis

- [1] IT-Planungsrat: »Einheitliche Webservices im Kontext der elektronischen Rechnung« 21. Februar 2018. [Online] https://www.it-planungsrat.de/fileadmin/beschluesse/2018/Beschluss2018-12_116_1_eRechnung.pdf [Abruf 4. August 2026].
- [2] IT-Planungsrat: »Verwaltungsdigitalisierung: Deutschland-Stack, gemeinsames Portfolio und neue föderale Steuerung beschlossen« 18. März 2026. [Online] <https://www.it-planungsrat.de/aktuelles/details/verwaltungsdigitalisierung-deutschland-stack-gemeinsames-portfolio-und-neue-foederale-steuerung-beschlossen> [Abruf 17. August 2026].
- [3] IT-Planungsrat: »Deutschland-Stack - Anlage Portfolio zum Beschlussvorschlag 49. IT-Planungsrat« März 2026. [Online] https://www.it-planungsrat.de/fileadmin/beschluesse/2026/Beschluss_2026_03_Deutschland-Stack_Portfolio.pdf [Abruf 29. Juli 2026].
- [4] R. T. Fielding: »Architectural styles and the design of network-based software architectures« University of California, Irvine, 2000. [Online] <https://www.proquest.com/openview/fc2d064044b971dda476dfb429a2b344/1?pq-origsite=gscholar&cbl=18750> [Abruf 7. Mai 2026].
- [5] World Wide Web Consortium (W3C): »SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)« 27. April 2007. [Online] <https://www.w3.org/TR/soap12-part1/> [Abruf 29. Juli 2026].
- [6] World Wide Web Consortium: »W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures« 5. April 2012. [Online] <https://www.w3.org/TR/xmlschema11-1/structures.html> [Abruf 17. August 2026].
- [7] T. Garland: »JSON vs XML: Key Differences, Examples, and When to Use Each« JSONLint, updated 14. August 2026. [Online] <https://jsonlint.com/json-vs-xml> [Abruf 17. August 2026].
- [8] S. Kumari und S. K. Rath: »Performance comparison of SOAP and REST based Web Services for Enterprise Application Integration« *International Conference on Advances in Computing, Communications and Informatics*, S. 1656–1660, 2015.
- [9] F. Halili und E. Ramadani: »Web Services: A Comparison of Soap and Rest Services« *Modern Applied Science*, Bd. 12, S. 175, 2018.
- [10] J. Makkonen: »Performance and usage comparison between REST and SOAP web services« Master Thesis, Aalto University, School of Science, 2017.
- [11] S. Devalla: »Performance Benchmarking of RESTful and SOAP APIs in Enterprise IoT Control Systems« *Journal of Scientific and Engineering Research*, Bd. 5, Nr. 11, S. 376–390, 2018.
- [12] Y. J. Ekie, B. Gueye und I. Niang: »A comparative analysis of SOAP and REST web service composition based on performance in local and remote cloud environments« *4th International Conference on Networking, Information Systems & Security, in NISS '21*. New York, NY, USA: Association for Computing Machinery, S. 1–8, 2021.
- [13] D. Rathod: »Performance Evaluation of Restful Web Services and SOAP/ WSDL Web Services« *International Journal of Advanced Research in Computer Science*, Bd. 8, Nr. 7, 2017.

- [14] E. Daka und V. Januzi: »Comparative analysis of SOAP and REST for optimising web services in mobile weather forecast applications: evaluating performance and scalability« *International Journal of Internet Protocol Technology*, Bd. 17, Nr. 2, S. 101–109, 2024.
- [15] D. Davis: »Web services reliable messaging (WS-ReliableMessaging)« OASIS, 2006. [Online] <https://docs.oasis-open.org/ws-rx/wsrn/200510/wsrn-1.1-spec-cd-02.pdf> [Abruf 7. Mai 2026].
- [16] L. Finch und P. Prasad: »Comparative Study: SOAP vs REST for Infra-Centric Data Transfer« 19. Dezember 2025. [Online] https://www.researchgate.net/profile/Prabhu-Prasad/publication/393509718_COMPARATIVE_STUDY_SOAP_VS_REST_FOR_INFRA-CENTRIC_DATA_TRANSFER/links/686d7c3cb991270ef3023fd5/COMPARATIVE-STUDY-SOAP-VS-REST-FOR-INFRA-CENTRIC-DATA-TRANSFER.pdf?tp=eyJlb250ZXh0lp7I [Abruf 3. August 2026].
- [17] International Organization for Standardization (ISO): »ISO/IEC. 7498-1: Information technology - Open Systems Interconnection (OSI) - Basic Reference Model: The basic model 1994.
- [18] Organization for the Advancement of Structured Information Standards: »OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features« 1. Oktober 2007. [Online] https://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.pdf [Abruf 7. August 2026].
- [19] Föderale IT-Kooperation: »OSCI-XTA« 18. April 2024. [Online] <https://docs.fitko.de/kompass/docs/it-landschaft/basisdienste/datenuebermittlung/transportsysteme/osci-xta/> [Abruf 8. Juli 2026].
- [20] Koordinierungsstelle für IT-Standards: »Spezifikation XTA 2 (Version 3.1.1)« 2024. [Online] https://www.xoev.de/sixcms/media.php/13/XTA_2_Version_3.1.1_Spezifikation_11112024.pdf [Abruf 29. Juli 2026].
- [21] Koordinierungsstelle für IT-Standards: »OSCI | XTA« n.d. [Online] <https://www.xoev.de/osci-xta-3355> [Abruf 8. Juli 2026].
- [22] Governikus GmbH & Co. KG: »Sichere Kommunikation über OSCI und XTA« Januar 2025. [Online] https://www.governikus.de/wp-content/uploads/2025/02/Governikus_Broschuere_OSCI.pdf [Abruf 4. August 2026].
- [23] Deutsches Institut für Normung e.V.: »DIN EN ISO/IEC 27001:2024-01 Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme - Anforderungen Berlin /*/b:Locals/b:Local[@LCID=\$_LCID]/b:General/b:EnumSeparator"/> DIN Media GmbH, 2024.
- [24] Governikus GmbH und Co. KG, cit GmbH, Koordinierungsstelle für IT-Standards, PPI Financial Systems AG, SAP AG, Stadtverwaltung Hagen: »OSCI-Transport 1.2 mit integrierten Korrigenda 1-10 und „Effiziente Übertragung großer Datenmengen"« 7. Mai 2026. [Online] https://www.xoev.de/sixcms/media.php/13/OSCI-1.2_mit_Korrigenda_und_Effi.pdf [Abruf 3. August 2026].
- [25] Koordinierungsstelle für IT-Standards: »OSCI | XTA - Einsatzszenarien« Koordinierungsstelle für IT-Standards, [Online] <https://www.xoev.de/sicherertransport/einsatzszenarien> [Abruf 1. Juli 2026].
- [26] Governikus GmbH & Co. KG: »OSCI Bibliothek Java« n.d. [Online] <https://gitlab.opencode.de/governikus/osci/osci-bib-java> [Abruf 7. Juli 2026].
- [27] Governikus GmbH & Co. KG: »OSCI-Bibliothek« n.d. [Online] <https://www.governikus.de/service/osci-bibliothek/> [Abruf 7. Juli 2026].
- [28] Governikus GmbH & Co. KG: »openCode Untergruppe "OSCI"« n.d. [Online] <https://gitlab.opencode.de/governikus/osci> [Abruf 27. Juli 2026].
- [29] Koordinierungsstelle für IT-Standards: »Implementierungen« April 2024. [Online] <https://www.xoev.de/osci-xta/implementierungen-23235> [Abruf 7. Juli 2026].

- [30] InformationsTechnikZentrum Bund: »DVDV – das Diensteverzeichnis der öffentlichen Verwaltung« [Online] <https://www.itzbund.de/DE/itloesungen/standardloesungen/dv dv/dv dv.html> [Abruf 6. Juli 2026].
- [31] Bundesamt für Sicherheit in der Informationstechnik: »BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen« 2026. [Online] <https://www.bsi.bund.de/dok/TR-02102> [Abruf 3. August 2026].
- [32] Bundesamt für Sicherheit in der Informationstechnik: »BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung« 2025. [Online] <https://www.bsi.bund.de/dok/TR-03116> [Abruf 3. August 2026].
- [33] Bundesamt für Sicherheit in der Informationstechnik: »BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen« 2026. [Online] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=15 [Abruf 3. August 2026].
- [34] National Vulnerability Database: »CVE-2016-2183« 31. August 2016. [Online] <https://nvd.nist.gov/vuln/detail/CVE-2016-2183> [Abruf 24. Juli 2026].
- [35] Koordinierungsstelle für IT-Standards: »OSCI Versionsübersicht« [Online] <https://www.xoev.de/osci-xta/standard-osci-transport-1-2/osci-versionsuebersicht-23217> [Abruf 2. Juli 2026].
- [36] Koordinierungsstelle für IT-Standards: »Fragen und Antworten« [Online] <https://www.xoev.de/osci-xta/faq-23062> [Abruf 2. Juli 2026].
- [37] Semantic Versioning: »Semantic Versioning« [Online] <https://semver.org/> [Abruf 2. Juli 2026].
- [38] Föderale IT-Kooperation: »Bekanntmachung der Änderung des Standards OSCI-Transport 1.2 unter Angabe des Herausgabedatums und des Beginns der Anwendung« Bundesanzeiger, 28. Mai 2026. [Online] <https://www.bundesanzeiger.de/pub/publication/tyaePpxap1b1YRe1cOV/content/tyaePpxap1b1YRe1cOV/BAAnz%20AT%2028.05.2026%20B4.pdf> [Abruf 6. Juli 2026].
- [39] Koordinierungsstelle für IT-Standards: »OSCI/XTA Referenzimplementierung« [Online] <https://www.xoev.de/osci-xta/uebergreifende-hilfsmittel/referenzimplementierung-23333> [Abruf 2. Juli 2026].
- [40] Koordinierungsstelle für IT-Standards: »XTA2V3 Referenzimplementierung« Koordinierungsstelle für IT-Standards, 12. September 2025. [Online] <https://projekte.kosit.org/transport-public/Referenzimplementierung> [Abruf 4. August 2026].
- [41] Koordinierungsstelle für IT-Standards: »XTA2V5 Referenzimplementierung« Koordinierungsstelle für IT-Standards, 25. November 2025. [Online] <https://projekte.kosit.org/transport-public/xta2v5-referenzimplementierung> [Abruf 2. Juli 2026].
- [42] Governikus GmbH & Co. KG: »COM Despina Referenzumgebung« Governikus, n.d. [Online] <https://www.governikus.de/produkt/com-despina-referenzumgebung/> [Abruf 2. Juli 2026].
- [43] Koordinierungsstelle für IT-Standards: »Spezifikation XTA 2 (Version 5.1.1)« 26. Juli 2024. [Online] https://www.xrepository.de/api/xrepository/urn:xoev-de:kosit:standard:xta2_5.1.1:dokument:Spezifikation [Abruf 29. Juli 2026].
- [44] Koordinierungsstelle für IT-Standards: »XML-Schema zu OSCI-Transport 1.2 mit eingearbeiteten Korrigenda 1-10 und "Effiziente Übertragung großer Datenmengen"« [Online] <https://www.xoev.de/sixcms/media.php/13/OSCI-Transport%201.2%20XML-Schema%20incl.%20Korrigenda%201-10%20vom%202026-05-07.zip> [Abruf 2. Juli 2026].

- [45] IT-Planungsrat: »Standardisierungsagenda: Einheitliche Anforderungen an Transportverfahren (XTA)« 22. März 2017. [Online] <https://www.it-planungsrat.de/beschluss/beschluss-2017-06> [Abruf 15. Juli 2026].
- [46] Bundesministerium des Innern und für Heimat : »Verordnung zur Einführung eines Datenübermittlungsstandards XBasisdaten (XBasisdaten-Verordnung - XBasisdatenV)« 28. März 2022. [Online] <https://www.gesetze-im-internet.de/xbasisdatenv/BJNR060100022.html> [Abruf 4. August 2026].
- [47] R. Braden: »Requirements for Internet Hosts -- Communication Layers« Internet Engineering Task Force (IETF), Oktober 1989. [Online] <https://datatracker.ietf.org/doc/html/rfc1122> [Abruf 7. Juli 2026].
- [48] Koordinationsstelle für IT-Standards: »XTA Rahmenbedingungen« 18. Februar 2025. [Online] https://www.xoev.de/sixcms/media.php/13/XTA-Rahmenbedingungen_1.0.1.pdf [Abruf 29. Juli 2026].
- [49] Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie NRW: »Bericht Praxistest OSCI in NRW« Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie NRW, Düsseldorf, 2022.
- [50] E. Christensen, C. Francisco, G. Meredith und W. Sanjiva: »Web Services Description Language (WSDL) 1.1« 15. März 2001. [Online] <https://www.w3.org/TR/wsdl.html> [Abruf 17. August 2026].
- [51] Koordinierungsstelle für IT-Standards: »XTA2V3 Konformitätstester« [Online] <https://projekte.kosit.org/transport-public/XTA2V3-KonTest> [Abruf 21. Juli 2026].
- [52] Koordinierungsstelle für IT-Standards: »XTA2V5 Konformitätstester« [Online] <https://projekte.kosit.org/transport-public/XTA2V5-KonTest> [Abruf 21. Juli 2026].
- [53] Bundesverwaltungsamt: »OSCI-Studie: Untersuchung zur Leistungsfähigkeit und Skalierbarkeit von OSCI und XTA« Bundesverwaltungsamt, Köln, 2023.
- [54] Koordinierungsstelle für IT-Standards: »XTA Konformitätstester« n.d. [Online] <https://www.xoev.de/osci-xta/standard-xta-2/xta-hilfsmittel/konformitaetstester-23202> [Abruf 29. Juli 2026].
- [55] Koordinierungsstelle für IT-Standards: »XTA: Hilfsmittel« n.d. [Online] <https://www.xoev.de/osci-xta/standard-xta-2/xta-hilfsmittel-23081> [Abruf 21. Juli 2026].
- [56] Koordinierungsstelle für IT-Standards: »XTA-Konformitätsvorgaben zur Umsetzung von XTA 2 Version 3.x« 2021. [Online] https://www.xoev.de/sixcms/media.php/13/XTA_Konformitaetsvorgaben_Produkt_XTA2V3.pdf [Abruf 4. August 2026].
- [57] Föderale IT-Kooperation: »Rückkanal« n.d. [Online] <https://docs.fitko.de/fit-connect/docs/metadata/ReplyChannel/> [Abruf 17. Juli 2026].
- [58] Föderale IT-Kooperation: »Ereignisprotokoll / Event Log (Überblick)« n.d. [Online] <https://docs.fitko.de/fit-connect/docs/getting-started/event-log/overview/> [Abruf 22. Juli 2026].
- [59] Föderale IT-Kooperation: »Submission API« n.d. [Online] <https://docs.fitko.de/fit-connect/docs/apis/submission-api/#post-/v2/submissions> [Abruf 24. Juli 2026].
- [60] Föderale IT-Kooperation: »FIT-Connect Destination API (Git-Repository)« n.d. [Online] <https://git.fitko.de/fit-connect/destination-api> [Abruf 24. Juli 2026].
- [61] Föderale IT-Kooperation: »FIT-Connect Submission API (Git-Repository)« n.d. [Online] <https://git.fitko.de/fit-connect/submission-api> [Abruf 24. Juli 2026].
- [62] Föderale IT-Kooperation: »FIT-Connect Routing API (Git-Repository)« n.d. [Online] <https://git.fitko.de/fit-connect/routing-api> [Abruf 24. Juli 2026].

- [63] Föderale IT-Kooperation: »Einreichung – Fachdaten« n.d. [Online] <https://docs.fitko.de/fit-connect/docs/getting-started/submission/data/> [Abruf 24. Juli 2026].
- [64] Föderale IT-Kooperation: »Limits bei Einreichungen« n.d. [Online] <https://docs.fitko.de/fit-connect/docs/getting-started/limits/> [Abruf 17. Juli 2026].
- [65] Föderale IT-Kooperation: »Submissions senden (Java SDK) – Übertragung großer Attachments« n.d. [Online] <https://docs.fitko.de/fit-connect/docs/sdks/java-sdk/sender/#%C3%BCbertragung-gr%C3%9Fer-attachments> [Abruf 17. Juli 2026].
- [66] Föderale IT-Kooperation: »FIT-Connect (GitLab Group / Repository-Übersicht)« n.d. [Online] <https://git.fitko.de/fit-connect/> [Abruf 17. Juli 2026].
- [67] Föderale IT-Kooperation: »Work items – Backlog and Planning Board« n.d. [Online] https://git.fitko.de/fit-connect/planning/-/work_items [Abruf 20. Juli 2026].
- [68] FJD Information Technology AG; Föderale IT-Kooperation: »FIT-Connect Support Service Desk (Jira Service Management)« n.d. [Online] <https://fjdag.atlassian.net/servicedesk/customer/portal/8> [Abruf 20. Juli 2026].
- [69] Föderale IT-Kooperation: »FIT-Connect Major Releases – Ein neuer Meilenstein« n.d. [Online] https://docs.fitko.de/fit-connect/docs/major-release/allgemeine_informationen/ [Abruf 23. Juli 2026].
- [70] Föderale IT-Kooperation: »Vorgaben für kryptographische Verfahren« n.d. [Online] <https://docs.fitko.de/fit-connect/docs/details/crypto/> [Abruf 22. Juli 2026].
- [71] Föderale IT-Kooperation: »FAQ« n.d. [Online] <https://docs.fitko.de/fit-connect/docs/fag/#:~:text=das%20Verwaltungssystem%20oder%20der%20Onlinedienst%20die%20Virencans%20durchf%C3%BChren> [Abruf 23. Juli 2026].
- [72] Bundesamt für Sicherheit in der Informationstechnik: »BSI-Richtlinie TR-03172 Portalverbund« 14. November 2024. [Online] <https://www.bsi.bund.de/dok/tr-03172> [Abruf 5. August 2026].
- [73] Föderale IT-Kooperation: »Betriebsumgebungen der FIT-Connect-Infrastruktur« n.d. [Online] <https://docs.fitko.de/fit-connect/docs/getting-started/environments/#ip-adressen> [Abruf 27. Juli 2026].
- [74] Föderale IT-Kooperation: »Föderierungs- und Skalierungskonzept« n.d. [Online] <https://git.fitko.de/fit-connect/konzepte/-/blob/main/Foederierungs-und-Skalierungskonzept.md> [Abruf 27. Juli 2026].
- [75] IT-Planungsrat: »Deutliche Fortschritte in der Verwaltungsdigitalisierung – gemeinsam und konkret« 17. Juli 2026. [Online] <https://www.it-planungsrat.de/aktuelles/details/deutliche-fortschritte-in-der-verwaltungsdigitalisierung-gemeinsam-und-konkret> [Abruf 24. Juli 2026].
- [76] Föderale IT-Kooperation: »Feedback zu FIT-Connect« 7. Juli 2026. [Online] <https://gitlab.opencode.de/fitko/fit-connect/feedback> [Abruf 24. Juli 2026].
- [77] B. f. Justiz: »Vertrag über die Errichtung, den Betrieb und die Weiterentwicklung des Nationalen Once-Only-Technical-Systems (NOOTS) – Vertrag zur Ausführung von Artikel 91c Absatz 1, Absatz 2 GG – NOOTS-Staatsvertrag« 24. März 2025. [Online] https://www.gesetze-im-internet.de/noots_stvtr/BJNR1450B0025.html [Abruf 29. Juli 2026].
- [78] Bundesverwaltungsamt: »AD-NOOTS-06: Grobkonzept Intermediäre Plattform (IP)« 19. Juni 2026. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-06_+Grobkonzept+Intermediaere+Plattform+_IP_.md [Abruf 13. Juli 2026].
- [79] Bundesverwaltungsamt: »AE-NOOTS IP-2025-01: Welche Rolle nimmt die Intermediäre Plattform im Kontext des NOOTS ein?« 28. Februar 2025. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AE-NOOTS-XX/AE-NOOTS_+IP-2025-01.md [Abruf 13. Juli 2026].

- [80] Bundesverwaltungsamt: »AE-NOOTS IP-2025-02: Wie viele Intermediäre Plattformen gibt es in Deutschland? Wie ist ihr Zuschnitt gestaltet?« 28. Februar 2025. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AE-NOOTS-XX/AE-NOOTS_IP-2025-02.md [Abruf 13. Juli 2026].
- [81] Bundesverwaltungsamt: »AD-NOOTS-19: Grobkonzept Transportinfrastruktur« 19. Juni 2026. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-19_Grobkonzept+Transportinfrastruktur.md [Abruf 13. Juli 2026].
- [82] Bundesverwaltungsamt: »Technische Architektur und Anschlussbedingungen an das NOOTS« 2026. [Online] https://www.bva.bund.de/DE/Services/Behoerden/Verwaltungsdienstleistungen/Registernmodernisierung/Informationen-OeffentlicheStellen/Textbaustein_TA_Service-Teaser.html [Abruf 13. Juni 2026].
- [83] Bundesverwaltungsamt: »AD-NOOTS-18: Grobkonzept Sicherer Anschlussknoten« 19. Juni 2026. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-18_Grobkonzept+SichererAnschlussknoten+SAK_.md [Abruf 13. Juli 2026].
- [84] Bundesverwaltungsamt: »AD-NOOTS-08: Grobkonzept Vermittlungsstelle (VS)« 19. Juni 2026. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-08_Grobkonzept+Vermittlungsstelle+VS_.md [Abruf 13. Juli 2026].
- [85] Bundesverwaltungsamt: »AD-NOOTS-07: Grobkonzept Registerdatennavigation (RDN)« 19. Juni 2026. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-07_Grobkonzept+Registerdatennavigation+RDN_.md [Abruf 13. Juli 2026].
- [86] Bundesverwaltungsamt: »AD-NOOTS-05: Grobkonzept IAM für Behörden« 19. Juni 2026. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-05_Grobkonzept+IAM+f%C3%BCr+Beh%C3%B6rden.md [Abruf 13. Juli 2026].
- [87] Bundesverwaltungsamt: »AD-NOOTS-10: Grobkonzept Integration IDM für Personen (IDMP)« 22. Mai 2026. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-10_Grobkonzept+Integration+IDM+Personen+IDMP.md [Abruf 13. Juli 2026].
- [88] Bundesverwaltungsamt: »AE-NOOTS IDMU-2025-01: Wird die Umsetzung des IDM für Unternehmen weiter vorangetrieben?« 3. Januar 2025. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AE-NOOTS-XX/AE-NOOTS_IDMU-2025-01.md [Abruf 13. Juli 2026].
- [89] Bundesverwaltungsamt: »AE-NOOTS TRA-2023-01: Wie kann ein einheitlicher, alle Ebenen und Ressorts überspannender Transportmechanismus für die sichere und verlässliche Nachrichtenkommunikation zwischen Teilnehmern aus unterschiedlichen Verwaltungsebenen geschaffen werden?« Januar 2023. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AE-NOOTS-XX/AE-NOOTS_TRA-2023-01.md [Abruf 13. Juli 2026].
- [90] Bundesverwaltungsamt: »SAK-APIs-Arbeitsstand« 2026. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/tree/main/SAK-APIs-Arbeitsstand?ref_type=heads [Abruf 27. Juli 2026].
- [91] Bundesverwaltungsamt: »XNachweis« 2026. [Online] https://www.xrepository.de/details/urn:xoev-de:bva:standard:xnachweis_0.1 [Abruf 13. Juni 2026].
- [92] Bundesverwaltungsamt: »AE-NOOTS TRA-2024-04: Soll der SAK als eigenständige Komponente, oder als Bibliothek bereitgestellt werden?« 2024. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AE-NOOTS-XX/AE-NOOTS_TRA-2024-04.md [Abruf 13. Juli 2026].

- [93] Föderale IT-Kooperation: »Das NOOTS – Basis der Registermodernisierung« n.d. [Online] <https://noots.gov.de/> [Abruf 27. Juli 2026].
- [94] Bundesamt für Sicherheit in der Informationstechnik: »IT-Sicherheitsanforderungen an die Datenübermittlung in der Registermodernisierung« 25. März 2026. [Online] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03176/BSI-TR-03176.pdf?__blob=publicationFile&v=7 [Abruf 13. Juli 2026].
- [95] Bundesamt für Sicherheit in der Informationstechnik: »BSI TR-03190: IT-Sicherheitsanforderungen für die Anbindung an das NOOTS (V 1.0)« 25. März 2026. [Online] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03190/BSI-TR-03190.pdf?__blob=publicationFile&v=8 [Abruf 13. Juli 2026].
- [96] Bundesverwaltungsamt: »AE-NOOTS TRA-2023-02: An welcher Stelle endet die Ende-zu-Ende-Verschlüsselung in NOOTS?« Mai 2025. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AE-NOOTS-XX/AE-NOOTS_TRA-2023-02.md [Abruf 13. Juli 2026].
- [97] Bundesverwaltungsamt: »Architekturdokumentation des Nationalen Once-Only-Technical-Systems« 2026. [Online] <https://gitlab.opencode.de/noots/public/ad-noots/Architektur> [Abruf 16. Juli 2026].
- [98] Bundesverwaltungsamt: »AD-NOOTS-00: Quellenverzeichnis« 25. Juni 2026. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AD-NOOTS-XX/AD-NOOTS-00_%2BQuellenverzeichnis.md?ref_type=heads#ad-noots-damas-01 [Abruf 16. Juli 2026].
- [99] Föderale IT-Kooperation: »NOOTS Startseite« 2026. [Online] <https://noots.gov.de/> [Abruf 16. Juli 2026].
- [100] Föderales IT-Architekturboard: »Föderale Zielarchitektur für Postfach- und Kommunikationslösungen« 13. Mai 2025. [Online] https://gitlab.opencode.de/it-planungsrat/fit-ab/zapuk/-/raw/main/Zielarchitektur/Architekturkonzept/2025-06-26_Beschluss-2025-28_ZaPuK_Architekturkonzept.pdf?ref_type=heads&inline=false [Abruf 24. Juli 2026].
- [101] Föderale IT-Kooperation: »Matrix-based G2X communication („Neo“)« n.d. [Online] <https://gitlab.opencode.de/fitko/matrix-g2x/> [Abruf 30. Juli 2026].
- [102] Föderales IT-Architekturboard: »Zielarchitektur Postfach- und Kommunikationslösungen -- Architekturentscheidungen« 2026. [Online] https://gitlab.opencode.de/it-planungsrat/fit-ab/zapuk/-/tree/main/Zielarchitektur/Architekturentscheidungen?ref_type=heads [Abruf 23. Juli 2026].
- [103] The Matrix.org Foundation: »About Matrix« n.d. [Online] <https://matrix.org/foundation/about/> [Abruf 30. Juli 2026].
- [104] The Matrix.org Foundation: »The Matrix Ecosystem« n.d. [Online] <https://matrix.org/ecosystem/> [Abruf 30. Juli 2026].
- [105] Föderales IT-Architekturboard: »Die föderale Zielarchitektur für Postfach- und Kommunikationslösungen (ZaPuK) -- Die FITKO stellt vor« 16. Januar 2026. [Online] https://www.fitko.de/fileadmin/fitko/veranstaltungen/die_fitko_stellt_vor/20260116-Handout_FITKO_stellt_vor_ZaPuK.pdf [Abruf 24. Juli 2026].
- [106] IT Planungsrat: »Beschluss B-2026/18-IT« IT Planungsrat, 17. Juni 2026. [Online] <https://www.it-planungsrat.de/beschluss/b-2026-18-it> [Abruf 30. Juli 2026].
- [107] Zentrales IT-Management Schleswig-Holstein: »X-Road im Detail« Staatskanzlei Schleswig-Holstein, 2026. [Online] <https://x-road-sh.de/x-road/> [Abruf 1. Juli 2026].

- [108] Nordic Institute: »X-Road Architecture - Technical Specification« Git Hub, 11. November 2025. [Online] https://github.com/nordic-institute/X-Road/blob/develop/doc/Architecture/arc-g_x-road_architecture.md [Abruf 23. Juni 2026].
- [109] Nordic Institute for Interoperability Solutions (NIIS): »Technical Specification X-Road Architecture« 1. Juni 2023. [Online] https://docs.x-road.global/Architecture/arc-g_x-road_architecture.html [Abruf 1. Juli 2026].
- [110] P. Kivimäki: »Changes in the X-Road Central Server High Availability Support« Nordic Institute for Interoperability Solutions, 23. Januar 2020. [Online] <https://www.niis.org/blog/2020/1/23/changes-in-the-central-server-high-availability-support-in-version-6230> [Abruf 24. Juli 2026].
- [111] Nordic Institute for Interoperability Solutions: »X-Road Repository« n.d. [Online] <https://github.com/nordic-institute/X-Road> [Abruf 29. Juli 2026].
- [112] »X-Road Implementation Models« X-Road, [Online] <https://x-road.global/implementation-models> [Abruf 1. Juli 2026].
- [113] Nordic Institute for Interoperability Solutions: »X-Road Security« [Online] <https://x-road.global/security> [Abruf 24. Juli 2026].
- [114] Europäische Kommission: »AS4 Access Point specifications: eDelivery AS4 - 2.0« 5. Dezember 2024. [Online] <https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/845480153/eDelivery+AS4+-+2.0> [Abruf 20. Juli 2026].
- [115] Organization for the Advancement of Structured Information Standards: »AS4 Profile of ebMS 3.0 Version 1.0« 23. Januar 2013. [Online] <https://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html> [Abruf 20. Juli 2026].
- [116] B. B. d. E. u. W. e.V.: »BDEW AS4-Profil - AS4-Nutzungsprofil zum Datenaustausch für regulierte Prozesse in der Energiewirtschaft« 2. Februar 2026. [Online] https://www.bundesnetzagentur.de/DE/Beschlusskammern/BK06/BK6_83_Zug_Mess/835_mitteilungen_datenformate/Mitteilung_55/Anlagen/Rz%C3%9C_AS4-Profil_1_2_Konsultationsfassung_20260202.pdf?blob=publicationFile&v=1 [Abruf 20. Juli 2026].
- [117] Europäische Kommission: »Domibus – eDelivery AS4 Access Point Reference Implementation« n.d. [Online] <https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467110244/Domibus> [Abruf 20. Juli 2026].
- [118] P. Helger: »Phax - Phase 4 Repository« n.d. [Online] <https://github.com/phax/phase4> [Abruf 20. Juli 2026].
- [119] NorStella Oxalis Community: »oxalis-ng Repository« n.d. [Online] <https://github.com/OxalisCommunity/oxalis-ng> [Abruf 20. Juli 2026].
- [120] NorStella Oxalis Community: »Oxalis Network – The Open Source Peppol Community« n.d. [Online] <https://www.oxalis.network/> [Abruf 20. Juli 2026].
- [121] Holodeck B2B Project: »Holodeck B2B – Open Source AS4 MSH« n.d. [Online] <https://holodeck-b2b.org/> [Abruf 20. Juli 2026].
- [122] Europäische Kommission: »The .Net implementation of AP: eDelivery AS4 1.x profile« n.d. [Online] <https://ec.europa.eu/digital-building-blocks/code/projects/EDELIVERY/repos/eessi-as4.net/browse> [Abruf 20. Juli 2026].
- [123] Europäische Kommission: »eDelivery Conformance Testing Service« n.d. [Online] <https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467118600/eDelivery+conformance+testing> [Abruf 20. Juli 2026].

- [124] National Institute of Standards and Technology: »NIST SP 800-52 Rev. 2« August 2019. [Online] <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf> [Abruf 10. August 2026].
- [125] Föderale IT-Kooperation: »eDelivery« 22. August 2023. [Online] <https://docs.fitko.de/kompass/docs/it-landschaft/basisdienste/datenuebermittlung/transportssysteme/edelivery/> [Abruf 20. Juli 2026].
- [126] Europäische Kommission: »eDelivery AS4 conformant solutions« n.d. [Online] <https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467110150/eDelivery+AS4+conformant+solutions> [Abruf 20. Juli 2026].
- [127] International Organization for Standardization (ISO): »ISO/IEC 25010:2023, Systems and software engineering - Systemsn and software Quality Requirements and Evaluation (SQuaRE) Genf, 2023.
- [128] Bundesministerium für Digitales und Staatsmodernisierung: »Der Servicestandard für die digitale Verwaltung« n.d. [Online] <https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/servicestandard/servicestandard-node.html> [Abruf 17. Juli 2026].
- [129] Föderale IT-Kooperation: »Bewertung von IT-Standards« [Online] <https://docs.fitko.de/fit-standards/konformitaetskriterien/> [Abruf 17. Juli 2026].
- [130] Föderale IT-Kooperation: »Föderale IT-Architekturrichtlinie« 2025. [Online] <https://foederale-it-architekturrichtlinie.gov.de/> [Abruf 10. August 2026].
- [131] E. Matthias: »Architekturprinzipien« Deutschland-Architektur, 13. Mai 2026. [Online] <https://refa-test-3f5b4c.usercontent.opencode.de/docs/framework/core-principles/> [Abruf 17. Juli 2026].
- [132] Bundesverwaltungsamt: »BD-NOOTS-01 White Paper: Zero Trust im NOOTS« 2026. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/BD-NOOTS-XX/BD-NOOTS-01_+White+Paper_+Zero+Trust+im+NOOTS.md [Abruf 13. Juli 2026].
- [133] Bundesverwaltungsamt: »BD-NOOTS-03 White Paper: Mandantenfähigkeit -SAK« 31. Oktober 2025. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/BD-NOOTS-XX/BD-NOOTS-03_+White+Paper_+Mandantenfaehigkeit+_SAK.md [Abruf 13. Juli 2026].
- [134] Bundesverwaltungsamt: »BD-NOOTS-03 Whitepaper Mandantenfähigkeit SAK« 31. Oktober 2025. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/BD-NOOTS-XX/BD-NOOTS-03_%2BWhite%2BPaper_%2BMandantenfaehigkeit%2B_SAK.md?ref_type=heads [Abruf 6. August 2026].
- [135] P. Mennig, B. Rach und M. Berg: »Gemeinsame IT-Architektur für die Registermodernisierung: Herausforderungen und Lösungsansätze« Kompetenznetzwerk Digitale Verwaltung (NEGZ), Fraunhofer IESE, Kaiserslautern, 2026, zur Veröffentlichung angenommen.
- [136] Föderale IT-Kooperation: »Matrix G2X Communication Solution Architecture (NEO) -- Architecture Decisions« 2026. [Online] https://gitlab.opencode.de/fitko/matrix-g2x/solution-architecture/-/tree/develop/architecture_decisions?ref_type=heads [Abruf 23. Juli 2026].
- [137] V. Sirviö und P. Kivimäki: »X-Road as an Interoperability Component in European eDelivery« 3. April 2019. [Online] <https://ec.europa.eu/digital-building-blocks/sites/download/attachments/75668015/2019-04-03-X-Road%20as%20an%20Interoperability%20Component%20in%20European%20eDelivery.pdf?api=v2> [Abruf 3. August 2026].
- [138] Koordinierungsstelle für IT-Standards: »Vergleich der Möglichkeiten von ebMS/AS3-Profilen mit OSCI-Transport 1.2« 22. Januar 2026. [Online] https://www.xoev.de/sixcms/media.php/13/Featurelist_Vergleich_OSCI_ebMS_AS4_0.9.1.pdf [Abruf 20. Juli 2026].
- [139] Peppol: »Peppol Network Statistics« 5. August 2026. [Online] <https://poppe.app/stats> [Abruf 18. August 2026].

- [140] Peppol.nu: »Peppol Statistics« n.d. [Online] <https://www.peppol.nu/knowledge-base/peppol-statistics/> [Abruf 23. Juli 2026].
- [141] Europäische Kommission: »eDelivery AS4 2.0 maturity confirmed through collaborative interoperability testing« 27. Februar 2026. [Online] <https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/blog/2026/02/27/952471325/eDelivery+AS4+2.0+maturity+confirmed+through+collaborative+interoperability+testing> [Abruf 20. Juli 2026].
- [142] Europäische Kommission: »eDelivery« n.d. [Online] <https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467110114/eDelivery> [Abruf 30. Juli 2026].
- [143] OpenPEPPOL AISBL: »Peppol AS4 Profile - Version 2.0.3« n.d. [Online] <https://docs.peppol.eu/edelivery/as4/specification/> [Abruf 23. Juli 2026].
- [144] Europäische Kommission: »eDelivery software roadmap and releases for the second half of 2025« 11. Juni 2025. [Online] <https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/blog/2025/06/11/902432385/eDelivery+software+roadmap+and+releases+for+the+second+half+of+2025> [Abruf 30. Juli 2026].
- [145] Europäische Kommission: »eDelivery AS4 Security Profile - Update Recommendations« 29. Januar 2023. [Online] <https://ec.europa.eu/digital-building-blocks/sites/download/attachments/668554357/%28eDelivery%29.%28eDelivery%20AS4%20Security%20Profile%20-%20Update%20Recommendations%29.%28v1.0%29.pdf?api=v2> [Abruf 22. Juli 2026].
- [146] Europäische Kommission: »Playbook for National Coordinators« n.d. [Online] <https://ec.europa.eu/digital-building-blocks/sites/spaces/OOTS/pages/713524841/steps+National+Coordinators> [Abruf 20. Juli 2026].
- [147] Bundesverwaltungsamt: »AE-NOOTS TRA-2023-01« 2026. [Online] https://gitlab.opencode.de/noots/public/ad-noots/Architektur/-/blob/main/AE-NOOTS-XX/AE-NOOTS_%2BTRA-2023-01.md [Abruf 30. Juli 2026].
- [148] C. Aeby: »eDelivery for connecting synchronous and asynchronous systems« Europäische Kommission, 19. März 2018. [Online] <https://ec.europa.eu/digital-building-blocks/sites/spaces/EDELCOMMUNITY/pages/55876267/eDelivery+for+connecting+synchronous+and+asynchronous+systems> [Abruf 22. Juli 2026].
- [149] Bundesministerium für Digitales und Staatsmodernisierung: »Deutschland-Stack Gesamtbild« 2025. [Online] <https://deutschland-stack.gov.de/gesamtbild/> [Abruf 10. August 2026].
- [150] Europäisches Parlament und Rat der Europäischen Union: »Verordnung (EU) 2024/903 über Maßnahmen für ein hohes Maß an Interoperabilität des öffentlichen Sektors in der Union (Verordnung für ein interoperables Europa)« 22. März 2024. [Online] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202400903 [Abruf 30. Juli 2026].
- [151] Ministerium für Infrastruktur und Digitales Sachsen-Anhalt: »Föderale API-Autorisierungsinfrastruktur« 10. Juli 2026. [Online] https://gitlab.opencode.de/sachsen-anhalt/midfoederale-api-autorisierungsinfrastruktur/-/tree/main?ref_type=heads [Abruf 18. August 2026].
- [152] IT-Planungsrat: »Zielarchitektur föderale API-Autorisierungsinfrastruktur - Langfassung« 29. Mai 2026. [Online] https://www.it-planungsrat.de/fileadmin/beschluesse/2026/Beschluss_2026_16_API-Autorisierungsinfrastruktur_Langfassung_Zielarchitektur.pdf [Abruf 18. August 2026].

Dokumentinformation

Titel: Studie zur Analyse der B2G- und G2G-Kommunikation mit Fokus auf Nachrichten-, Transport- und Verschlüsselungsprotokollen

Datum: 21. August 2026

Report: 011.26/D

Status: final

Klassifikation: Öffentlich

Copyright 2026, Fraunhofer IESE.
Alle Rechte vorbehalten. Diese Veröffentlichung darf für kommerzielle Zwecke ohne vorherige schriftliche Erlaubnis des Herausgebers in keiner Weise, auch nicht auszugsweise, insbesondere elektronisch oder mechanisch, als Fotokopie oder als Aufnahme oder sonst wie vervielfältigt, gespeichert oder übertragen werden. Eine schriftliche Genehmigung ist nicht erforderlich für die Vervielfältigung oder Verteilung der Veröffentlichung von bzw. an Personen zu privaten Zwecken.