



Antragsrouting bei EfA-Online-Diensten in NRW: Anleitung für Umsetzungsprojekte eines EfA-Online-Dienstes

Version 1.0 (Stand: 10.11.2021)

INHALTSVERZEICHNIS

Abbildungsverzeichnis	5
Tabellenverzeichnis	5
Abkürzungsverzeichnis	5
I Allgemeines	8
I.1 Ausgangslage und Rahmenbedingungen	8
I.2 Zielsetzung	9
I.3 Geltungsbereich	10
I.4 Nutzen	10
I.5 Adressatenkreis dieses Dokuments	11
I.6 Abgrenzung und Ausblick	11
II Grundlagen	12
II.1 Fachlich / Organisatorischer Überblick	13
II.1.1 Digitalisierungsprogramm Föederal und EfA-Umsetzungsprojekte	13
II.1.2 Zuständigkeiten OZG-Umsetzung NRW	13
II.1.3 LeiKa-Leistungen und Vollzugskompetenz	13
II.1.4 DVDV-Bundesmaster, DVDV-Server und pflegende Stellen	14
II.1.5 Intermediäre und Intermediär-Betreiber	15
II.1.6 Informationssicherheit, Datenschutz und Auftragsverarbeitung	16
II.2 Technische Komponenten	18
II.2.1 Formularmanagementsysteme	18
II.2.2 Portale	18
II.2.3 Verbindungsnetze	19
II.2.4 Datenaustauschformate	20
II.2.5 Deutsches Verwaltungsdiensteverzeichnis	21
II.2.6 OSCI-Transportstandard und OSCI-Infrastruktur	21
II.2.7 XTA Standard und XTA-Server	25

II.2.8	Public Key Infrastruktur der Verwaltung - Zertifizierungsstelle	27
II.2.9	Zentrale Datenaustausch Infrastruktur	30
II.2.10	Fachverfahren	31
II.2.11	Dokumentenbasierte Sachbearbeitung ohne Fachverfahren	31
II.2.12	Elektronische Verwaltungsarbeit	31
II.2.13	Governikus MultiMessenger	32
II.2.14	E-Mail und De-Mail	33
II.3	Überblick der Transportwege	34
III	Antragsrouting für Verwaltungsleistungen auf Landesebene	35
III.1	Vorgehensweise beim Antragsrouting auf Landesebene	35
III.2	LL - Antragsrouting vom Serviceportal zu einem Landesportal innerhalb des Landes NRW	37
III.3	LX - Antragsrouting vom Land NRW (Serviceportal) zu einem Landesportal außerhalb des Landes NRW	38
III.4	XL - Antragsrouting von einem Landesportal außerhalb des Landes NRW zu einem Landesportal in NRW ³⁹	
III.5	Sonderfall: Antragsrouting bei Sachbearbeitung ohne Fachverfahren	40
IV	Antragsrouting für Verwaltungsleistungen auf Kommunalebene	42
IV.1	Vorgehensweise beim Antragsrouting auf Kommunalebene	42
IV.2	(L)K - Antragsrouting vom Land NRW (Fachportal) zu einer Kommune in NRW	44
IV.3	(L)X - Antragsrouting vom Land NRW (Fachportal) zu einer Kommune außerhalb des Landes NRW	45
IV.4	KK - Antragsrouting vom Land NRW (Kommunalportal) zu einer Kommune in NRW	46
IV.5	KX - Antragsrouting vom Land NRW (Kommunalportal) zur zuständigen Fachbehörde einer Kommune außerhalb des Landes NRW	48
IV.6	XK – Antragsrouting von einem kommunalen Portal außerhalb von NRW zur zuständigen Fachbehörde einer Kommune in NRW	49
IV.7	Sonderfall: Antragsrouting bei Sachbearbeitung ohne Fachverfahren	50
V	Testinfrastruktur	51
VI	Hinweise für die Einrichtung des Antragsroutings	52

VI.1	Hinweise für EfA-Online-Dienst-Umsetzungsprojekte	53
VI.2	Hinweise für anzubindende Fachbehörden	55
VII	Ansprechpartner und weiterführende Informationen	56
VII.1	Ansprechpartner	56
VII.2	Weiterführende Informationen	57
VIII	Anhang - Handreichung Governikus	59
VIII.1	Voraussetzungen	59
VIII.2	Inhalt Transportprofil	59

Abbildungsverzeichnis

Abbildung 1: Routing von Antragsdaten - vereinfachte Darstellung.....	12
Abbildung 2: OSCI-Transport - Ebenen der Kommunikation (Quelle Spezifikation OSCI-Transport Version 1.2).....	23
Abbildung 3: OSCI-Rollenmodell im Kontext der Verschlüsselung.....	24
Abbildung 4: Rollenmodell in der OSCI-Infrastruktur (Quelle: Spezifikation XTA 2 Version 3), ergänzt um den OSCI-Intermediär (Anpassungen sind gelb markiert)	26
Abbildung 5: Eingesetzte Zertifikate im Kontext des Antragsroutings.....	29
Abbildung 6: GMM bei IT.NRW - Einsatzszenario: Weiterleitung von Antragsdaten als E-Mail.....	32
Abbildung 7: Transportwege Antragsrouting in NRW.....	34
Abbildung 8: Transportwege für Antragsrouting mit Vollzug auf Landesebene	35
Abbildung 9: Transportweg LL.....	37
Abbildung 10: Transportweg LX.....	38
Abbildung 11: Transportweg XL.....	39
Abbildung 12: Transportwege für Antragsrouting mit Vollzug auf Kommunalebene	42
Abbildung 13: Transportweg (L)K, Beispiel Sozialplattform (IT.NRW)	44
Abbildung 14: Transportweg (L)X	45
Abbildung 15: Transportweg KK	46
Abbildung 16: Transportweg KX	48
Abbildung 17: Transportweg XK.....	49

Tabellenverzeichnis

Tabelle 1: Typisierung der Regelungs- und Vollzugskompetenz im LeiKa.....	14
Tabelle 2: Eingesetzte Zertifikate im Kontext des Antragsroutings	29
Tabelle 3: Ansprechpartner mit Relevanz für das Antragsrouting	56
Tabelle 4: Für das Antragsrouting relevante Dokumente.....	57

Abkürzungsverzeichnis

Abkürzung	Erklärung
AVV	Auftragsverarbeitungsvertrag
beBPO	besonderes Behördenpostfach
BMI	Bundesministerium des Innern, für Bau und Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
d-NRW	Die d-NRW AöR ist eine rechtsfähige Anstalt des öffentlichen Rechts.

	Die Anstalt unterstützt ihre Träger und, soweit ohne Beeinträchtigung ihrer Aufgaben möglich, andere öffentliche Stellen beim Einsatz von Informationstechnik in der öffentlichen Verwaltung.
DOI	Deutschland-Online-Infrastruktur
DVDV	Deutsches Verwaltungsdiensteverzeichnis
EfA	„Einer für Alle“
EUGH	Europäischer Gerichtshof
EVA	Elektronische Verwaltungsarbeit
FIM	Föderales Informationsmanagement
FITKO	Föderale IT-Kooperation
FMS	Formularmanagementsystem
GMM	Governikus MultiMessenger
HSI	Hohe Sicherheitsinfrastruktur (IT.NRW)
IT-NetzG	Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes
IT.NRW	Information und Technik Nordrhein-Westfalen
KDN	Dachverband kommunaler IT-Dienstleister
KoSIT	Koordinierungsstelle für IT-Standards
KRZN	Kommunales Rechenzentrum Niederrhein
LeiKa	Leistungskatalog
LVN	Landesverwaltungsnetz
MAGS	Ministerium für Arbeit, Gesundheit und Soziales
MKFFI	Ministerium für Kinder, Familie, Flüchtlinge und Integration
MWIDE	Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie
NdB-VN	Netze des Bundes-Verbindungsnetz
OSCI	Online Service Computer Interface

OZG	Onlinezugangsgesetz
PDF	Portable Document Format
PKI	Public-Key-Infrastruktur
RZF	Das Rechenzentrum der Finanzverwaltung des Landes Nordrhein-Westfalen
S/MIME	Secure/Multipurpose Internet Mail Extensions
SIT	Südwestfalen-IT
XML	Extensible Markup Language
XÖV	XML in der öffentlichen Verwaltung
XTA	XÖV Transport Adapter
ZDI	Zentrale Datenaustausch Infrastruktur

I Allgemeines

Dieses Kapitel beschreibt neben der Ausgangslage und den wesentlichen Rahmenbedingungen zum Transport von Antragsdaten bei EfA-Online-Diensten auch den Nutzen des vorliegenden Dokuments. Zum Ende des Kapitels wird ein Ausblick auf mögliche Erweiterungen dieser Anleitung gegeben.

I.1 Ausgangslage und Rahmenbedingungen

Im Rahmen der Umsetzung des Onlinezugangsgesetzes (OZG) müssen die Verwaltungen von Bund, Ländern und Kommunen ihre Verwaltungsleistungen bis zum 31.12.2022 auch elektronisch über ein Verwaltungsportal anbieten und die landesweiten Verwaltungsportale zu einem Portalverbund verknüpfen. Insgesamt müssen dazu 575 gebündelte OZG-Leistungen und im OZG-Umsetzungskatalog ca. 7.500 beschriebene Einzelleistungen digital abgewickelt werden können.

Zur Beschleunigung der flächendeckenden Umsetzung des OZG und zur gezielten Unterstützung der Länder bei dieser herausfordernden Aufgabe hat die Bundesregierung Konjunkturmittel in Höhe von 3 Milliarden Euro zur Verfügung gestellt. 1,4 Milliarden Euro davon fließen in die föderale OZG-Umsetzung. Die Vergabe der Mittel aus dem Konjunkturpaket unterliegt konkreten Umsetzungskriterien¹. Eines davon ist das „Einer für Alle“-Prinzip (EfA-Prinzip). Die Aufgaben zur digitalen Bereitstellung von Verwaltungsleistungen und der Vernetzung der zugehörigen Portale sind vielfältig und umfassen alle Verwaltungsebenen. Deshalb kann die Umsetzung des OZG nur arbeitsteilig gelingen. Als umfassende Form der Arbeitsteilung und Zusammenarbeit wurde hierfür das EfA-Prinzip etabliert. EfA-Services sind flächendeckend einsetzbare Lösungen, die einmal von einem Bundesland oder einer Allianz aus mehreren Ländern konzipiert und entwickelt, fachlich betreut und technisch betrieben werden.

In der Abteilungsleiterrunde am 08.12.2020 haben Bund und Länder Mindestanforderungen² an „Einer für Alle“-Services vereinbart. Ergänzend dazu haben Bund und Länder ein Verwaltungsabkommen zur Umsetzung des Onlinezugangsgesetzes verabschiedet. Das Verwaltungsabkommen ist am 30.01.2021 in Kraft getreten. Die Einhaltung der EfA-Mindestanforderungen sowie des Verwaltungsabkommens sind die Voraussetzung zum Erhalt der für die Länder vorgesehenen Finanzmittel aus dem Konjunkturpaket des Bundes.

Mit Services sind in erster Linie Online-Dienste gemeint. Anhand von Online-Diensten kann der Verwaltungskunde (Bürger oder Unternehmen) Anträge digital einreichen. Der Online-Dienst sorgt für eine Validierung der Antragsdaten und leitet diese an die zuständige Fachbehörde weiter. Für die interne Sachbearbeitung nutzen die Sachbearbeiter Fachverfahren, um den Antrag zu bearbeiten. In einigen Fällen erfolgt die Sachbearbeitung ohne Fachverfahren, d. h. manuell ohne (teil)automatisierte Unterstützung durch Software.

¹ Siehe https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-39_Eckpunkte_Umsetzung_des_OZG.pdf

² Siehe https://leitfaden.ozg-umsetzung.de/download/attachments/4621478/EfA-Mindestanforderungen_Version%201.0.pdf?version=1&modificationDate=1612276616029&api=v2

EfA-Online-Dienste werden zentral und länderübergreifend für alle (möglichst viele) empfangenden Behörden betrieben. Die „zentrale“ Bereitstellung kann in NRW durch einen Online-Dienst des Landes oder einen Online-Dienst einer Kommune erfolgen. Alternativ nutzt NRW EfA-Online-Dienste außerhalb des eigenen Bundeslandes. In solchen Fällen ist ein Datentransport vom Online-Dienst an die jeweiligen Fachverfahren sicherzustellen. Für die dazu benötigte Transportinfrastruktur gibt es derzeit noch keine bundesweit einheitliche Vorgehensweise. Daher befinden sich heute unterschiedlichste Ansätze auf Basis etablierter Technologien in Planung, Umsetzung und im Einsatz. Dazu gehören die im Kapitel II beschriebenen Komponenten, wie z. B. das Deutsche Verwaltungsdienstverzeichnis (DVDV), Übertragungen gemäß XÖV Transport Adapter (XTA) und das Online Services Computer Interface (OSCI) einschließlich des Einsatzes von OSCI-Intermediären und deren Betreiber.

Für eine erfolgreiche Umsetzung des EfA-Prinzips müssen die Antragsdaten vom EfA-Online-Dienst bis hin zur zuständigen Behörde transportiert werden. Der Transport der Antragsdaten bedeutet, dass die Antragsdaten das Rechenzentrum des Online-Dienstes verlassen und beim Rechenzentrum der zuständigen Fachbehörden empfangen werden. Die EfA-Online-Dienste werden in einem Bundesland betrieben und von mehreren Bundesländern genutzt. Der Transport der Antragsdaten muss daher neben dem bundeslandinternen Transport der Antragsdaten auch einen Datenaustausch zwischen mehreren Bundesländern unterstützen.

Für NRW hat das EfA-Prinzip folgende Auswirkungen mit Relevanz für den Transport der Antragsdaten:

- NRW stellt zentral eigene EfA-Online-Dienste zur bundesweiten Nutzung zur Verfügung. Es muss somit möglich sein, Antragsdaten von NRW in andere Bundesländer zu transportieren.
- NRW nutzt EfA-Online-Dienste, die außerhalb des eigenen Bundeslandes betrieben werden. Es muss somit möglich sein, diese Antragsdaten in NRW zu empfangen und zu bearbeiten.

Zusammengefasst gelten folgende wesentliche Rahmenbedingungen:

- Gemäß OZG fristgerechte Umsetzung der EfA-Online-Dienste inkl. Transport der Antragsdaten an die zuständige Fachbehörde bis Ende 2022
- Konformität zu den EfA-Mindestanforderungen und Verwaltungsabkommen, um Mittel aus dem Konjunkturprogramm zu erhalten

1.2 Zielsetzung

Das vorliegende Dokument beschreibt wie das Antragsrouting in NRW für EfA-Online-Dienste umzusetzen ist. Es betrachtet sowohl landes- als auch kommunale Verwaltungsleistungen. Dabei werden sowohl die notwendigen Aktivitäten eines - Anträge sendenden - EfA-Online-Dienstes als auch die Aktivitäten einer - Antragsdaten empfangenden - Fachbehörde dargestellt. Es handelt sich um eine technische Betrachtung, organisatorische Aspekte werden nur sofern für den Kontext notwendig betrachtet. Beschrieben werden sowohl die Architektur für die Unterstützung eines spezifischen Antrags als auch die Architektur der für die Antragstellung notwendigen Parameterpflege im DVDV.

Es handelt sich um ein generisches Anbindungskonzept, d. h. es geht nicht auf einzelne Verwaltungsleistungen ein. Ergänzend dazu wird es verwaltungsleistungsspezifische Anbindungsleitfäden geben. Ziel ist es, dass spezifische Anbindungsleitfäden Bezug auf das vorliegende Dokument nehmen, sodass nur verwaltungsleistungsspezifische Besonderheiten beim Transport der Antragsdaten gesondert aufgeführt werden müssen.

I.3 Geltungsbereich

Die vorliegende Anleitung zur Umsetzung eines Antragsroutings enthält Empfehlungen und keine Vorgaben (insbesondere für bereits in Produktion befindliche Lösungen). Sie umfasst folgenden Geltungsbereich:

- Beschreibung des unidirektionalen Transports von Antragsdaten zwischen EfA-Online-Dienst und empfangender Fachbehörde,
- Grundlage für die Überprüfung bereits identifizierter und umgesetzter Transportwege im Rahmen einer Risikoanalyse; sind die Abweichungen von dieser Anleitung tolerabel, verbleibt der aktuell umgesetzte Transportweg,
- Ausgangspunkt zur Festlegung eines geeigneten Transportwegs für Verwaltungsleistungen, die bisher keinen Transportweg identifiziert und umgesetzt haben.

Da das Dokument lediglich Empfehlungen enthält, beschreibt es keinen Prozess zur Prüfung der Einhaltung der hier dokumentierten Transportwege.

I.4 Nutzen

Das vorliegende Dokument leistet, falls es in NRW Berücksichtigung findet, folgende Mehrwerte:

- Es stellt eine Konformität zu den antragsroutingrelevanten EfA-Mindestanforderungen sicher.
- Es sorgt dafür, dass im Umfeld Antragsrouting bestimmte Mindestanforderungen mit Hinblick auf Informationssicherheit und Datenschutz eingehalten werden.
- Es leistet einen Beitrag zur Reduzierung des Aufwands bei der Wartung von sicheren Transportwegen. Die verfügbaren Experten können sich auf wenige Transportwege fokussieren und müssen nicht eine Vielzahl von unterschiedlichen Varianten auf Eignung prüfen.
- Umsetzungsprojekte zur Bereitstellung von EfA-Online-Diensten können sich auf verwaltungs-spezifische Besonderheiten fokussieren und den Transport der Antragsdaten auf Grundlage der in diesem Dokument beschriebenen Transportwege realisieren. Der initiale Aufwand bei der Gestaltung eines Antragsroutings für eine Verwaltungsleistung kann somit reduziert werden.

I.5 Adressatenkreis dieses Dokuments

Das Dokument setzt ein technisches Grundwissen voraus. Es ist primär an folgende Adressaten (Leser) gerichtet:

- Umsetzungsprojekte für EfA-Online-Dienste: Auf Grundlage dieses Dokuments sollen Online-Dienst-spezifische Leitfäden für das Antragsrouting erstellt werden können. Die Online-Dienst-spezifischen Leitfäden werden dann verwendet, um einen weiteren Teilnehmerkreis, wie etwa Fachverfahrenshersteller zu informieren.
- Rechenzentrumsbetreiber Land und Kommunen: Auf Grundlage dieses Dokuments kann die grundlegende Fähigkeit geschaffen werden, ein zu den EfA-Mindestanforderungen konformes Antragsrouting zu gestalten.

Ziel ist es, das Dokument möglichst praxisnah zu gestalten. Somit ist Feedback explizit gewünscht. Das Dokument soll laufend um neue Erkenntnisse fortgeschrieben werden. Für Ansprechpartner siehe Kapitel VII.1.

I.6 Abgrenzung und Ausblick

Nicht im Umfang dieser Anleitung ist die Umsetzung einer bidirektionalen, synchronen Kommunikation zwischen Online-Dienst und Fachverfahren. Die synchrone Kommunikation ist für eine erfolgreiche OZG-Umsetzung nicht zwingend erforderlich. Ein Online-Antrag kann somit aus Sicht des Kunden nicht vollautomatisch in Realzeit abschließend bearbeitet werden. Als Konsequenz reicht es aus, wenn der Online-Dienst unidirektional die Antragsdaten an die zuständige Fachbehörde sendet. Die Kommunikation mit dem Verwaltungskunden nach erfolgter Sachbearbeitung erfolgt separat über Postfächer der Nutzerkonten und ist nicht Gegenstand dieser Anleitung.

In diesem Dokument wird ausschließlich der Transport des Antrags vom Online-Dienst bis hin zur zuständigen Fachbehörde dargestellt. Sonstige Datentransporte, wie z. B. der Versand des Bescheids an den Antragsteller nach eingereichtem Antrag über das Servicekonto Postkorb, werden nicht betrachtet.

Das Antragsrouting über Sondernetze³, d. h. Netze, die nicht an das LVN angebunden sind, wird in diesem Dokument ebenfalls nicht behandelt.

Die Empfehlungen in dieser Anleitung beziehen sich auf aktuell im Einsatz befindliche, produktiv gesetzte und erfolgreich erprobte Transportinfrastrukturen (vgl. Kapitel II). So ist auch die aktuell von der Föderalen IT-Kooperation (FITKO) zur Vereinfachung des Antragsrouting entwickelte, aber noch nicht produktiv gesetzte FIT-Connect-Lösung nicht Gegenstand dieser Anleitung. Das Dokument wird mit der erfolgreichen Einführung neuer Technologien – wie FIT-Connect – ergänzt, sobald diese sich im Rahmen einer Pilotierung

³ Zu den Sondernetzen zählen z. B. RZF, FIN-Netz, IM₁, CN-Pol.

bewährt haben. Ergänzend dazu soll diese Anleitung aus Erfahrungen in der Praxis kontinuierlich weiterentwickelt werden.

II Grundlagen

In diesem Kapitel werden die fachlich/organisatorischen Anforderungen sowie die für das Antragsrouting relevanten technischen Komponenten beschrieben.

Das vorliegende Dokument befasst sich mit dem Transport der Antragsdaten von einem zentral betriebenen EfA-Online-Dienst bis hin zur zuständigen Fachbehörde (siehe Abbildung 1).

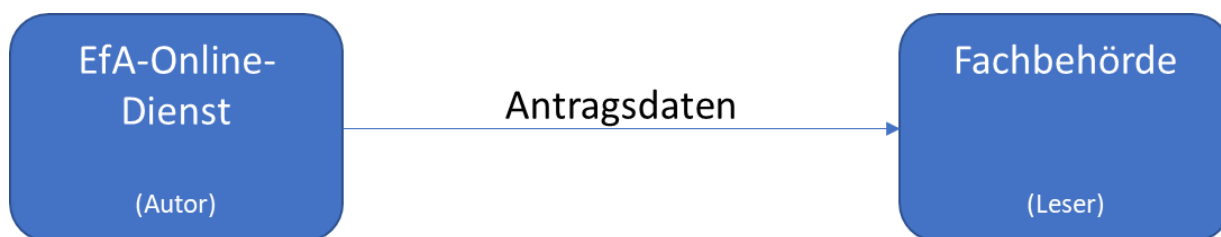


Abbildung 1: Routing von Antragsdaten - vereinfachte Darstellung⁴

Ein EfA-Online-Dienst bietet ein digitales Antragsformular für Verwaltungskunden (Bürger und Unternehmen) an. Er unterstützt den Verwaltungskunden bei der Antragsstellung und validiert die Antragsdaten. Nachdem der Verwaltungskunde den Antrag bestätigt hat, initiiert der EfA-Online-Dienst das Antragsrouting, d. h. der Antrag wird an die zuständige Fachbehörde weitergeleitet. Dazu bereitet der EfA-Online-Dienst die Antragsdaten in das erforderliche Nachrichtenformat auf und fügt alle weiteren Anhänge, wie z. B. Nachweise, hinzu. Dabei wird der Antrag von einigen Online-Diensten optional im Portable Document Format (PDF) versendet, damit die Sachbearbeitung einer Fachbehörde, die kein Fachverfahren hat, den Antrag manuell bearbeiten kann.

Die zuständige Fachbehörde empfängt die Antragsdaten und führt die Sachbearbeitung durch. Nach erfolgter Sachbearbeitung erhält der Antragssteller einen Bescheid. Der Transport von Daten nach erfolgter Sachbearbeitung ist nicht Gegenstand dieser Anleitung.

⁴ Die in der Abbildung aufgeführte Rollen Autor und Leser beziehen sich auf das OSCI-Rollenmodell, siehe Kapitel II.1.6.I.6

II.1 Fachlich / Organisatorischer Überblick

In diesem Abschnitt erfolgt ein fachlich/organisatorischer Überblick mit Relevanz für das Antragsrouting.

II.1.1 Digitalisierungsprogramm Föderal und EfA-Umsetzungsprojekte

Im Rahmen der Umsetzung des OZG werden über 7.500 Einzelleistungen in 575 OZG-Leistungen gebündelt und im OZG-Umsetzungskatalog beschrieben. Zur effizienteren Umsetzung ähnlicher Leistungen wurden die OZG-Leistungsbündel nach thematischem Zusammenhang in Themenfelder aufgeteilt. Im Digitalisierungsprogramm Föderal⁵ werden die 460 der 575 OZG-Leistungsbündel mit Landes- und kommunalem Vollzug gestaltet. Das Digitalisierungsprogramm Föderal verantwortet auch die EfA-Umsetzungsprojekte zur Einführung dieser neuen EfA-Online-Dienste.

Für weitere Informationen siehe OZG-Leitfaden⁶.

II.1.2 Zuständigkeiten OZG-Umsetzung NRW

Die OZG-Koordinatoren der Ministerien sowie die Themenfeldkoordinatoren des Dachverbands kommunaler IT-Dienstleister (KDN) verantworten die Aktivitäten der Themenfelder im Digitalisierungsprogramm Föderal. NRW ist zusammen mit den entsprechenden Bundesressorts Federführer für die Themenfelder Arbeit & Ruhestand sowie Engagement & Hobby. Auf Landesebene koordiniert d-NRW im Auftrag des Ministeriums für Wirtschaft, Innovation, Digitalisierung und Energie (MWIDE) die Umsetzung des OZG. Die Entwicklung von EfA-Online-Diensten erfolgt über d-NRW oder IT.NRW. Auf Kommunalebene ist der KDN⁷ koordinierend tätig.

Das MWIDE verantwortet den Aufbau der themenfeldübergreifenden Infrastruktur für Landesverwaltungsleistungen wie z. B. Serviceportal, Servicekonto und Verwaltungssuchmaschine. Die Entwicklung erfolgt durch d-NRW und KDN. IT.NRW und der KDN sind verantwortlich für die Bereitstellung und den Betrieb der Infrastruktur.

II.1.3 LeiKa-Leistungen und Vollzugskompetenz

Im Leistungskatalog (LeiKa) wird für jede Verwaltungsleistung unterschieden, welche Verwaltungsebene die Regelungs- und Vollzugskompetenz innehat. Hierfür wurde eine Typologie entwickelt, die in Tabelle 1 dargestellt ist.

⁵ Siehe <https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/digitalisierungsprogramme/foederal/foederal-node.html#:~:text=Im%20Digitalisierungsprogramm%20F%C3%B6deral%20%C3%BCbernehmen%20einzelne,Leistungen%2C%20die%20zum%20Themenfeld%20geh%C3%B6ren>

⁶ Siehe <https://leitfaden.ozg-umsetzung.de/display/OZG/OZG-Leitfaden>

⁷ Siehe <https://www.kdn.de/>

Tabelle 1: Typisierung der Regelungs- und Vollzugskompetenz im LeiKa⁸

LeiKa-Typ	Regelungskompetenz	Vollzugskompetenz
1	Bundesebene	Bundesebene
2a	Bundesebene	Landesebene
2b		Ausführungsvorschriften durch Landesebene, Vollzug durch kommunale Ebene
3a	Bundesebene (Abweichungsrecht)	Landesebene
3b		Ausführungsvorschriften durch Landesebene, Vollzug durch kommunale Ebene
4	Landesebene	Kommunale Ebene
5	Kommunale Ebene	Kommunale Ebene

Für NRW sind nur Verwaltungsleistungen von Typ 2-5 von Relevanz. Die Verwaltungsleistungen vom Typ 1 werden ausschließlich auf Bundesebene behandelt.

Für das Antragsrouting ist die Vollzugskompetenz maßgeblich, da sie den Vollzug einer Verwaltungsleistung nach dem EfA-Prinzip ermöglicht.⁹ Für die Verwaltungsleistungen vom Typ 2-5 können zwischen Verwaltungsleistungen im Landesvollzug und in kommunalem Vollzug unterschieden werden:

- Verwaltungsleistungen mit Vollzugskompetenz auf Landesebene sind vom Typ 2a und 3a
- Verwaltungsleistungen mit Vollzugskompetenz auf kommunaler Ebene sind vom Typ 2b, 3b, 4 und 5.

II.1.4 DVDV-Bundesmaster, DVDV-Server¹⁰ und pflegende Stellen

Digitale Verwaltungsdienste setzen eine IT-Infrastruktur voraus, die eine gut geschützte Kommunikation zwischen Behörden garantiert. Das Deutsche Verwaltungsdienstverzeichnis (DVDV) ermöglicht diese sichere elektronische Kommunikation von und mit Behörden über die vorhandenen Fachverfahren, siehe Kapitel II.2.5.

⁸ Siehe <https://www.xrepository.de/details/urn:de:gk-leika:leika:typisierung>

⁹ Die Regelungskompetenz spielt für das Antragsrouting keine Rolle. Maßgeblich ist, ob der Antrag auf Kommunal- oder auf Landesebene behandelt wird.

¹⁰ DVDV-Server sind die vom DVDV-Bundesmaster gespiegelten Server im jeweiligen Bundesland. Der bisher gebräuchliche Begriff „DVDV-Landesserver“ wird inzwischen nicht mehr verwendet.

Der zentrale DVDV-Bundesmaster wird vom ITZBund bereitgestellt. Die Daten des DVDV-Bundesmaster werden über Replikationsmechanismen auf die DVDV-Server der einzelnen Bundesländer automatisiert übertragen. Änderungen können nur im DVDV-Bundesmaster eingepflegt werden. Zur Durchführung dieser Änderungen gibt es pro Bundesland eine „Pflegerische Stelle“¹¹, welche ausschließlich die Daten des DVDV für das jeweilige Bundesland verändern kann. Pro Bundesland wird zurzeit nur eine Pflegerische Stelle zugelassen. Die Pflegerischen Stellen garantieren die Korrektheit der zur Verfügung gestellten Daten.

In NRW wird der DVDV-Server im Auftrag des KDN Dachverbandes durch das KRZN und die Stadt Münster (citeq) betrieben und kann sowohl von Landesdiensten wie auch kommunalen Diensten genutzt werden.

DataClearing NRW ist dabei pflegerische Stelle¹² sowohl für Land als auch Kommune.

II.1.5 Intermediäre und Intermediär-Betreiber

Die Übermittlung der Antragsdaten erfolgt in Form von OSCI-Nachrichten¹³. Sie wird durch einen Intermediär unterstützt. Ein Intermediär transportiert nicht nur Nachrichten, sondern protokolliert zur Nachvollziehbarkeit der Kommunikation auch den Nachrichtenfluss, prüft Zertifikate und kann weitere Mehrwertdienste erbringen. Betreiber von Intermediären übernehmen Dienstleistungen, um eine sichere und rechtsverbindliche Kommunikation zwischen Fachverfahren sowie zwischen EfA Online-Diensten und Fachverfahren zu unterstützen. Dabei geht es maßgeblich um die Einhaltung der Datenschutzgrundverordnung (DSGVO) bei der Weitergabe von personenbezogenen oder anonymisierten Daten an Dritte. Daher sind auch Anforderungen an eine potenzielle Auftragsverarbeitung zu beachten, siehe Kapitel II.1.6.

Intermediär-Betreiber verantworten alle IT-Lösungen, die für diesen Zweck notwendig sind.

II.1.5.1 Intermediäre für die kommunale Verwaltung

Für die kommunale Verwaltung in NRW übernimmt die Betreibergemeinschaft des Zweckverbandes Kommunales Rechenzentrum Niederrhein (KRZN) und der Stadt Münster diese Aufgabe im Auftrag des KDN. Sie sind für den Betrieb verantwortlich und stehen gesamtschuldnerisch für die Rechte und Pflichten gegenüber dem KDN ein.

Sie betreiben den OSCI-Intermediär der Datenaustauschplattform NRW¹⁴ und den DVDV-Server in NRW. Ergänzend dazu aktualisiert die Betreibergemeinschaft als pflegerische Stelle die Eintragungen in das DVDV bei ITZBund. Für weitere Informationen über die eingesetzten technischen Komponenten siehe Kapitel II.2.

¹¹ Siehe <https://www.itzbund.de/DE/itloesungen/standardloesungen/dvdv/dvdv.html;jsessionid=32087692C5DF99EE21AC1A7100E89950.internet351?nn=178690#title2568461>

¹² Siehe <https://www.dataclearing-nrw.de/basis-dienste/pflege-und-betrieb-des-dvdv-und>
<https://www.dataclearing-nrw.de/unsere-dienstleistungen/dvdv-pflege>

¹³ Auf OSCI-Nachrichten wird im Kapitel II.2.6 detailliert eingegangen.

¹⁴ Im Folgenden wird für den OSCI-Intermediär der Datenaustauschplattform NRW auch die Bezeichnung OSCI-Intermediär von DataClearing NRW benutzt, um eine klare Unterscheidung von der Zentralen Datenaustausch Infrastruktur von IT.NRW zu ermöglichen.

Für die Nutzung des OSCI-Intermediärs im Rahmen der Transportwege (L)K und KK (siehe Abschnitte IV.2 und IV.4) gibt eine Basis-Vereinbarung (Vertrag) zwischen dem KDN und den DataClearing NRW-Betreibern KRZN und citeq über die Nutzung der Infrastruktur (Datenaustauschplattform, Intermediärsleistungen) und deren Finanzierung (keine Finanzierung im Vorgriff, sondern jeweils mit „Start eines Dienstes“).

Im Unterschied zu den Transportwegen (L)K und KK ist die Finanzierung des Transportwegs XK (siehe Abschnitt IV.6) zum aktuellen Zeitpunkt noch nicht abschließend geklärt und muss im Rahmen der Projektumsetzung betrachtet werden.

Ergänzend zu diesem KDN Dienst bieten einige kommunale IT-Dienstleister eigene OSCI-Intermediäre an.

II.1.5.2 Intermediäre für die Landesverwaltung

Für die Landesverwaltung betreibt IT.NRW im Auftrag der Justiz und des MWIDE einen OSCI-Intermediär, der zunächst grundsätzlich für den Empfang von Antragsdaten in EfA-Projekten genutzt werden kann. Die Nutzung ist mit dem MWIDE und IT.NRW abzustimmen. Über die Weiterentwicklung der OSCI-Infrastruktur der Landesverwaltung wird abhängig von dem Nutzungsbedarf entschieden.

II.1.6 Informationssicherheit, Datenschutz und Auftragsverarbeitung

Das EfA-Umsetzungsprojekt verantwortet die Feststellung des Schutzbedarfes und die Umsetzung der Anforderungen zur Informationssicherheit und zum Datenschutz. Für das Antragsrouting ist insbesondere das daraus abgeleitete Transportprofil von Relevanz. Sofern der Fachdatenstandard als XÖV-Standard dokumentiert wird, ist das Transportprofil in der XÖV-Spezifikation ebenfalls zu dokumentieren. Das Transportprofil enthält z. B. Anforderungen an zu verwendende Zertifikate, Verschlüsselung und Signatur von Antragsdaten, siehe Anhang Kapitel VIII.2.

Grundsätzlich muss der Datenschutzbeauftragte der ersten verarbeitenden Stelle prüfen ob und wie die Antragsdaten verarbeitet werden dürfen. Der Schutz von personenbezogenen Daten muss auf der gesamten Transportstrecke vom Autor bis zum Leser bei allen verarbeitenden Stellen lückenlos sichergestellt werden. Alle Daten- und Grundschutzanforderungen sowie Verantwortlichkeiten sollten bereits bei der Konzeption des EfA-Online-Dienstes geklärt und im EfA-Umsetzungsprojekt als eigene Arbeitspakete unter Einbeziehung von Fachexperten behandelt werden. Auch im laufenden Betrieb des EfA-Online-Dienstes muss die Einhaltung der Anforderungen sowie die Wirksamkeit der umgesetzten Sicherheitsmaßnahmen fortlaufend überwacht und bei Bedarf angepasst werden.

Ergänzend dazu muss für das Antragsrouting geprüft werden, ob auf der Transportstrecke eine Auftragsverarbeitung vorliegt. Gemäß Artikel 28 der Datenschutzgrundverordnung (DSGVO) liegt eine Auftragsverarbeitung vor, wenn Dritte durch den Verantwortlichen im Sinne des Artikel 4 Nr. 7 DSGVO mit der Verarbeitung personenbezogener Daten beauftragt werden. Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Auftragsverarbeitungsvertrags (AVV). Dabei verpflichtet sich der Auftraggeber wesentliche in der DSGVO festgelegte Anforderungen an die Verarbeitung der Daten zu erfüllen. Dies ist insbesondere für Intermediär-Betreiber von Bedeutung. Ein AVV kann entbehrlich sein, wenn es sich nur um die

Verarbeitung verschlüsselter personenbezogener Daten handelt. Der Europäische Gerichtshof (EUGH) hat in seinem Urteil vom 19.10.2016 (Az.: C-582/14) ausgeführt, dass grundsätzlich dynamische IP-Adressen, die der Anbieter eines Online-Mediendienstes speichert, personenbezogene Daten darstellen. Allerdings finden die Schutzprinzipien der DSGVO - unter Berufung auf den Erwägungsgrund 26 zur EU-Datenschutzrichtlinie - keine Anwendung auf Daten, die derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist. Diese Rechtsprechung dürfte auch beim Transport verschlüsselter Daten im Rahmen von EfA-Online-Diensten anzuwenden sein, wenn z. B. der Intermediär-Betreiber die Daten aufgrund einer vorherigen Verschlüsselung nicht einsehen kann.

Grundlegende Voraussetzung für das Vermeiden einer Auftragsverarbeitung ist daher die Verschlüsselung der personenbezogenen Daten vor einem Wechsel der organisatorischen Zuständigkeit. Für die EfA-Online-Dienste ist somit das im Kapitel II.2.5 detaillierter beschriebene Verschlüsselungskonzept anzustreben:

- Betreiber von EfA-Online-Diensten verschlüsseln personenbezogene Antragsdaten, bevor diese transportiert werden.
- Intermediär-Betreiber sowie Betreiber von XTA-Servern können die personenbezogenen Antragsdaten nicht einsehen.
- Fachbehörden entschlüsseln die personenbezogenen Antragsdaten.

Da die Entschlüsselung der Antragsdaten oft im Rahmen einer Maschine-zu-Maschine-Kommunikation in einem Rechenzentrum erfolgt, ist genau zu spezifizieren welche Auswirkung diese Regelung hat. So kann es z. B. sein, dass nur in einem bestimmten Netzsegment innerhalb des Rechenzentrums entschlüsselt werden darf. Dieses Netzsegment muss in der Zuständigkeit der Fachbehörde liegen.

Ob die im EUGH-Urteil vom 19.10.2016 (Az.: C-582/14) unter Berufung auf den Erwägungsgrund 26 zur EU-Datenschutzrichtlinie beschriebenen Voraussetzungen vorliegen, müssen die beteiligten Stellen jeweils mit ihren Datenschutzbeauftragten beurteilen. Gemäß Artikel 32 Abs 1 lit. c) DSGVO muss dabei auch das neue Schutzziel der Belastbarkeit¹⁵ der Systeme hinsichtlich der schnellen Wiederherstellung personenbezogener Daten durch ein vorliegendes Backup¹⁶ bei einem Ausfall berücksichtigt werden.

Aktuell wird das Thema Datenschutz bei EfA-Online-Diensten von unterschiedlichen Beteiligten auf Bundes-Länder-Ebene intensiv diskutiert. Sollten als Ergebnis der Diskussionen gesetzliche Änderungen vorgenommen oder ein Beschluss des IT-Planungsrats gefasst werden, wird das vorliegende Dokument entsprechend aktualisiert.

¹⁵ Im Schutzziel Belastbarkeit geht es um Robustheit und Resilienz der Systeme. Damit ist sicherzustellen, dass das System seine Leistung trotz einer internen oder externen Störung erbringt und den Systembetrieb aufrechterhält.

¹⁶ Entweder ein (un)verschlüsseltes Backup vor dem Transport zum OSCI-Intermediär oder ein verschlüsseltes Backup beim OSCI-Intermediär

II.2 Technische Komponenten

Hier werden die für das Antragsrouting relevanten technischen Komponenten aufgeführt. Diese technischen Komponenten bieten die Grundlage für die Empfehlungen in Kapitel III und Kapitel IV.

II.2.1 Formularmanagementsysteme

EfA-Online-Dienste werden in der Regel mit Hilfe von Formularmanagementsystemen (FMS) umgesetzt und betrieben. Formularmanagementsysteme initiieren über das zur Antragstellung genutzte Portal (vgl. Kapitel I II.2.2) den Versand der Antragsdaten. Die technischen Adressen inklusive der zur Verschlüsselung notwendigen Zertifikate der empfangenden Fachbehörde erhält das Portal aus dem DVDV, in der Regel indirekt über die ZDI oder einen XTA-Server. Nach erfolgter Verschlüsselung der Antragsdaten initiiert das Formularmanagementsystem bzw. das genutzte Portal den Versand der Antragsdaten.

Für die Kommunikation zwischen FMS/Portal und DVDV kommt ein XTA-Server (Sender) zum Einsatz. Es erfolgt somit kein direkter Dialog zwischen DVDV und Portal. Für weitere Informationen über DVDV, OSCI und XTA siehe Kapitel II.2.5, II.2.6 und II.2.7.

II.2.2 Portale

Portale sind in diesem Kontext der digitale Zugang für die Verwaltungskunden. Die Portale integrieren Basisdienste und FMS. Sie werden zusammen mit dem FMS und den dort konfigurierten Online-Diensten im gleichen Rechenzentrum betrieben. Im Folgenden werden die in dieser Anleitung betrachteten Portale beschrieben.

Serviceportal.NRW

Das Serviceportal.NRW ist das Verwaltungsportal des Landes NRW. Es wird für Verwaltungsleistungen und Online-Dienste auf Landesebene eingesetzt. Es besteht aus einer Frontend- und einer Backendkomponente. Die Frontendkomponente integriert Inhalte und Antragsprozesse. Die Backendkomponente enthält ein Content Management System zur Redaktion der Inhalte und eine Integrationskomponente, die im Rahmen eines Antragsprozesses den Austausch mit dem Servicekonto.NRW, dem Beahldienst (ePayBL) und dem FMS (Lucom) ermöglicht. Zudem sorgt die Integrationskomponente dafür, dass der Transport der Antragsdaten an die zuständige Fachbehörde initiiert wird. Hierfür erfolgt eine Kommunikation mit der Datenaustauschplattform (siehe auch Kapitel II.2.8). Das Serviceportal.NRW wird zusammen mit dem Formularmanagementsystem bei IT.NRW betrieben.

Fachportal (Betrieb: Landesrechenzentrum)

Fachportale bündeln themenbezogen Verwaltungsleistungen mit Vollzug sowohl auf Landes- als auch auf Kommunalebene. IT.NRW führt aktuell folgende Fachportale ein: Familienportal (Auftraggeber: MKFFI), Sozialplattform (Auftraggeber: MAGS) sowie das Portal Anerkennung ausländischer Berufsqualifikationen (Auftraggeber: MAGS). Sie basieren technisch auf dem Serviceportal.NRW und werden als jeweils separate Instanzen betrieben.

Kommunalportal.NRW

Auf dem Kommunalportal.NRW werden Basiskomponenten wie die Authentifizierung über das Servicekonto.NRW, der Beahldienst ePayBL, ein Zuständigkeitsfinder sowie Anbindungen an das Formularmanagementsystem bereitgestellt. Das Kommunalportal.NRW wird für Verwaltungsleistungen mit Vollzug auf kommunaler Ebene eingesetzt.

Fachportale (Betrieb: kommunales Rechenzentrum)

Kommunale IT-Dienstleister betreiben ebenfalls Fachportale, die themenbezogen kommunale Verwaltungsleistungen bündeln. Als Beispiele sind das Bauportal und das Wirtschafts-Service-Portal zu nennen.

Landes- und Kommunalportale außerhalb des Landes NRW

Diese Portale sind von Relevanz, wenn NRW EfA-Online-Dienste nutzt, die außerhalb des Landes NRW betrieben werden.

II.2.3 Verbindungsnetze

Verbindungsnetze verbinden Rechenzentren und Behörden. Im Kontext des Antragsroutings kann zwischen drei Verbindungsnetzen unterschieden werden:

- Landesverwaltungsnetz NRW (LVN)
- Bund-Länder-Kommunen – Verbindungsnetz (NdB-VN), ehemals Deutschland-Online-Infrastruktur (DOI)
- Internet

Landesverwaltungsnetz NRW (LVN)

Das LVN ist eine Infrastrukturleistung von IT.NRW für die Landesverwaltung in NRW. Es ist ein vom Internet unabhängiges Intranet und verbindet die gesamte Landesverwaltung. Das LVN bildet die grundlegende Infrastruktur für den Transport von Daten zwischen Landesrechenzentren und Behörden bis hin zu den Arbeitsplätzen der Sachbearbeitung der Landesverwaltung. Für das LVN wurde vom Referat „E-Government Infrastruktur“ im MWIDE ein hoher Schutzbedarf festgestellt. Die dafür festgelegten Sicherheitsmaßnahmen befinden sich aktuell in der Umsetzung (LVN-Zuständigkeit). Unter der Annahme, dass die Sicherheitsmaßnahmen umgesetzt wurden, kann für den landesinternen Transport von personenbezogenen Daten auf den Einsatz des OSCI-Transportstandards verzichtet werden. Allerdings ist auch hier eine Transportverschlüsselung (TLS/HTTPS) der Daten notwendig, ein unverschlüsselter Transport ist nicht zulässig.

Bund-Länder-Kommunen-Verbindungsnetz (NdB-VN)

Das zur Netzinfrastruktur der Netze des Bundes gehörende NdB-VN¹⁷ wurde für die ebenenübergreifende sichere Kommunikation zwischen Bundes-, Länder- und kommunalen IT-Netzen der Öffentlichen Verwaltung in Deutschland errichtet. Die Netzinfrastruktur ist in Art. 91c (4) Grundgesetz verankert. Gemäß §3 IT-

¹⁷ siehe auch https://www.bdbos.bund.de/DE/NdB/ndb_node.html

NetzG¹⁸ erfolgt die Kommunikation zwischen Bund und den Ländern über das Verbindungsnetz. Es wird aktuell beim Bundesministerium des Innern, für Bau und Heimat (BMI) noch geklärt inwieweit dieses Gesetz auch für eine Kommunikation ohne Beteiligung des Bundes Verwendung finden muss. Gemäß Technische Richtlinie BSI (TR-03107-1) reicht der Einsatz des NdB-VN für eine Kommunikation mit Vertrauensniveau normal aus¹⁹. Um die Anforderungen einer Kommunikation mit hohem Vertrauensniveau sicherzustellen, ist entsprechend der technischen Richtlinie ergänzend zum Transport über das NdB-VN der Einsatz des OSCI-Transportstandards notwendig (vgl. Kapitel II.2.5).

Internet

Das Internet wird als unsicheres Netz betrachtet. Mit dem Einsatz des OSCI-Transportstandards kann dennoch ein sicherer Datentransport mit Vertrauensniveau hoch erreicht werden, siehe Kapitel II.2.5.

II.2.4 Datenaustauschformate

Damit die Fachbehörden die Antragsdaten maschinell und (teil)automatisiert verarbeiten können, müssen die Antragsdaten genau definiert werden. Das EfA-Umsetzungsprojekt trägt hierfür die Verantwortung. Für diesen Zweck werden in erster Linie neue XÖV-Standards²⁰ eingeführt oder bestehende angepasst. XÖV ist ein etablierter Standard, um elektronische Nachrichtenübermittlungen innerhalb oder mit der öffentlichen Verwaltung zu spezifizieren. Ein XÖV-Standard enthält Informationen über Nachrichten sowie deren Datentypen. Ergänzend zu den XÖV-Standards werden im Föderalen Informationsmanagement (FIM²¹) Standard für Verwaltungsleistungen u. a. Datenfelder für FMS standardisiert zur Weiterverwendung bereitgestellt werden. Der Standard XDatenfelder definiert ein Austauschformat für die vom FIM-Baustein „Datenfelder“²² bereitgestellten Inhalte. Das auf diesem Weg erstellte Datenschema kann als Grundlage für die Festlegung eines XÖV-Standards dienen oder unabhängig davon das Datenaustauschformat definieren. Gemäß EfA-Mindestanforderungen sind ergänzend zu XÖV und XDatenfelder weitere Fachstandards denkbar, sofern bestimmte Aspekte wie z. B. Offenheit erfüllt werden. Da einige Fachbehörden kein Fachverfahren einsetzen, sollte ergänzend zum maschinenlesbaren Datenformat ein Antrag als PDF erzeugt und transportiert werden können. Auf Grundlage des PDF kann eine manuelle Antragsbearbeitung durch die Sachbearbeitung ermöglicht werden.

¹⁸ Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes

¹⁹ Siehe Technische Richtlinie BSI (TR-03107-1): „Die Nutzung eines sicheren Transportnetzes (zum Beispiel IVBB/IVBV, Deutschland-Online-Infrastruktur) ist für das Vertrauensniveau normal ausreichend“, Kapitel 8.2.3 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf?__blob=publicationFile&v=1

²⁰ Siehe hier: <https://www.xoev.de/xoev/xoev-produkte/xoev-handbuch-5060>

²¹ Siehe hier: https://www.xrepository.de/details/urn:xoev-de:fim:standard:xdatenfelder_o.5

²² Siehe hier: <https://fimportal.de/>

Damit für die jeweiligen Nachrichten im XÖV-Standard die zuständigen Fachbehörden eindeutig definiert werden können, ist ein Eintragungskonzept in das DVDV²³ erforderlich. Die entsprechenden Schlüsseltabellen mit Identifikationsnummer und Name der zuständigen Fachbehörde werden im XRepository²⁴ veröffentlicht.

II.2.5 Deutsches Verwaltungsdiensteverzeichnis

Das Deutsche Verwaltungsdiensteverzeichnis (DVDV) hat die Funktion einer zentralen Registrierungsstelle für Online-Dienste der öffentlichen Verwaltung und ermöglicht eine rechtsverbindliche elektronische Kommunikation von und mit Behörden über die vorhandenen Fachverfahren. Es enthält Informationen über die technischen Verbindungsparameter aller Dienste der Behörden in Deutschland. Darin enthalten sind auch technische Adressen und Verschlüsselungszertifikate. Dadurch sind Sender und Empfänger von Nachrichten eindeutig identifizierbar. Die Anfragen eines Online-Dienstes bzgl. Adressen und Zertifikate sind an den DVDV-Server des jeweiligen Bundeslandes zu stellen und nicht direkt an den DVDV-Bundesmaster.

II.2.6 OSCI-Transportstandard und OSCI-Infrastruktur

OSCI ist der verbindliche²⁵ Transportstandard für e-Government in der Öffentlichen Verwaltung. Der OSCI-Transportstandard²⁶ ist entwickelt worden, um zwischen Bürgern, Verwaltungen und Unternehmen sichere, vertrauenswürdige und rechtsverbindliche Datenübermittlungen sogar über das grundsätzlich unsichere Internet zu ermöglichen.

Die Nutzung des OSCI-Transportstandards generiert auch in sicheren Netzen Mehrwerte, wie zum Beispiel Ende-zu-Ende Sicherheit und -Adressierung, oder auch Nachweise zur Integrität der Nachrichten, die durch die Netzebene allein nicht abgedeckt werden. Verantwortlich für die Entwicklung und den Betrieb des OSCI-Transportstandards ist die Koordinierungsstelle für IT-Standards (KoSIT). Die aktuelle Version des OSCI-Transportstandards (Version 1.2) wurde 2002 finalisiert. Die Version 2.0 des Standards findet kaum Verwendung und ist auch nicht auf der Internetseite der KoSIT zu finden.

Gemäß der technischen Richtlinie TR-03107-1 („Elektronische Identitäten und Vertrauensdienste im E-Government“)²⁷ kann mit dem Standard OSCI-Transport „eine große Bandbreite an Vertrauensniveaus ab-

²³ Siehe Kapitel II.2.13

²⁴ Siehe <https://www.xrepository.de/>

²⁵ Siehe hier: <https://www.itzbund.de/DE/itloesungen/standardloesungen/osci/osci.html>

²⁶ Siehe hier: <https://www.xoev.de/downloads-2316#Standards>

²⁷ Siehe <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf>

gedeckt werden [...], die vom Vertrauensniveau hoch bis zu einem vollständigen Verzicht auf Sicherheitsmaßnahmen und somit keinem Vertrauensniveau reicht". „Für Vertrauensniveau ist im Kontext von OSCI-Transport die Verwendung von XML-Signatur und XML-Verschlüsselung für die Inhaltsdaten vorgesehen“²⁸.

Aufgrund eines mehrstufigen Verschlüsselungskonzepts erfüllt der OSCI-Transportstandard auch die hohen Sicherheitsanforderungen für elektronische Signaturen²⁹, so dass Behörden sensible Daten rechtsverbindlich abgesichert über das Internet übermitteln können. Die mehrstufige Verschlüsselung ergibt sich aus der Signatur und Verschlüsselung der Inhaltsdaten beim Autor einerseits (innerer Umschlag) und der Signatur und zusätzlichen Verschlüsselung der vom Sender ergänzten Nutzungsdaten andererseits (äußerer Umschlag). Durch die hier beschriebene strikte Trennung von Inhaltsdaten und Nutzungsdaten einer OSCI-Nachricht sind Vertraulichkeit, Integrität, Authentizität, Nichtabstreitbarkeit und Zurechenbarkeit der Nachrichten auf dem kompletten Transportweg gewährleistet. Der Empfänger entschlüsselt für die Zustellung der OSCI-Nachricht zum Leser lediglich die Nutzungsdaten, während die Entschlüsselung der Inhaltsdaten nur durch den berechtigten Leser erfolgen kann.

Beim OSCI-Transportstandard erfolgt die Kommunikation zwischen Autor (Benutzer 1) und Leser (Benutzer 2) wie in Abbildung 2 dargestellt niemals direkt, sondern immer über eine weitere Instanz, den bereits beschriebenen OSCI-Intermediär.

²⁸ Strikt genommen gilt die technische Richtlinie lediglich für den OSCI-Transport zwischen Personen und öffentlichen Stellen (z. B. Notar/Gericht) und nicht für die Kommunikation zwischen Behörden, siehe TR-03107-1, Kapitel 10.8.

²⁹ Siehe auch <https://www.bmwi.de/Redaktion/DE/Artikel/Service/eidas-durchfuehrungsgesetz.html>

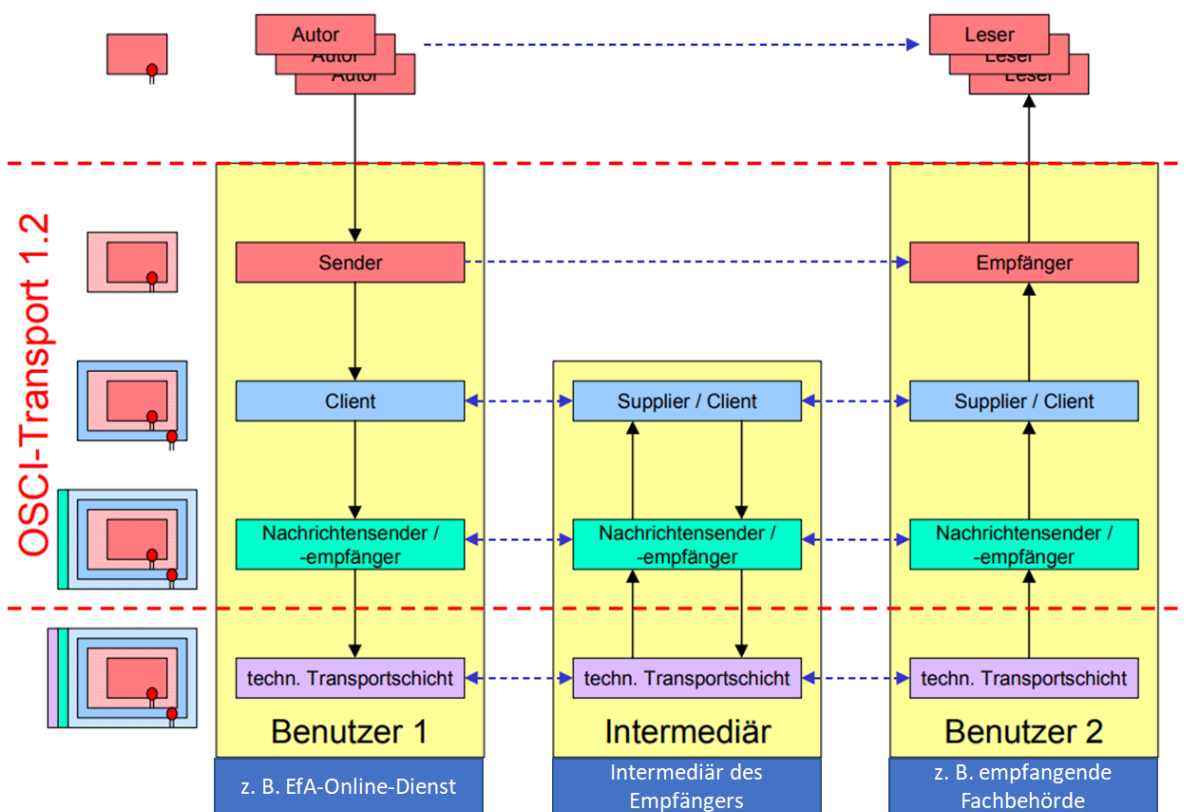


Abbildung 2: OSCI-Transport - Ebenen der Kommunikation (Quelle Spezifikation OSCI-Transport Version 1.2)

Benutzer 1 (z. B. ein EfA Online-Dienst) möchte einen digitalen Antrag an Benutzer 2 (z. B. ein Fachverfahren der zuständigen Fachbehörde) senden. Für die Prüfung der Zertifikate entschlüsselt der OSCI-Intermediär lediglich die Nutzungsdaten und verschlüsselt diese wieder mit dem Transportzertifikat. Der OSCI-Intermediär kann auf die vom Autor verschlüsselten Inhaltsdaten nicht zugreifen.

Das Diagramm zeigt den Prozess der OSCI-Nachricht (Objekt-Signatur-Container-Interaktion) zwischen einem Autor und einem Leser sowie zwischen einem Sender und einem Empfänger.

Legende:

- - - - - : optional
- : zwingend

Prozessfluss (Sender-Seite):

- Der **Sender** generiert **Nutzdaten** und erzeugt eine **Nutzdatensignatur**.
- Die **Nutzdaten** und die **Nutzdatensignatur** werden verschlüsselt in den **(verschlüsselten) Nutzdatencontainer** der **OSCI-Nachricht** gepackt.
- Der **Sender** validiert sein eigenes **Sig.-Zert.** (optional).

Prozessfluss (Empfänger-Seite):

- Der **Empfänger** empfängt die **OSCI-Nachricht**.
- Er kann den **(verschlüsselten) Nutzdatencontainer** entschlüsseln, um die **Nutzdaten** und die **Nutzdatensignatur** zu erhalten.
- Die **Nutzdaten** und die **Nutzdatensignatur** werden validiert (optional).

Prozessfluss (Autor-Seite):

- Der **Autor** erstellt **Inhaltsdaten** und verfasst die **Inhaltsdatensignatur**.
- Die **Inhaltsdaten** und die **Inhaltsdatensignatur** werden verschlüsselt in den **(verschlüsselten) Inhaltsdatencontainer** der **OSCI-Nachricht** gepackt.
- Der **Autor** validiert sein eigenes **Sig.-Zert.** (optional).

Prozessfluss (Leser-Seite):

- Der **Leser** kann den **(verschlüsselten) Inhaltsdatencontainer** entschlüsseln, um die **Inhaltsdaten** und die **Inhaltsdatensignatur** zu erhalten.
- Die **Inhaltsdaten** und die **Inhaltsdatensignatur** werden validiert (optional).

³³ Anstelle von Nutzungsdaten werden auch die Begriffe Nutz- oder Transportdaten verwendet.

Der OSCI-Intermediär des Empfängers öffnet den äußeren Umschlag und führt seine Prüfungen durch. Danach verschlüsselt und signiert er ggf. die OSCI-Nachricht erneut und stellt diese zur Abholung durch den Empfänger³⁴ bereit.

Der Empfänger holt die OSCI verschlüsselten Antragsdaten (OSCI-Nachricht) beim OSCI-Intermediär ab, entschlüsselt die Nutzungsdaten und transportiert die Antragsdaten zum Leser³⁵.

Der Leser entschlüsselt die Inhaltsdaten.

Wichtig: Der Transport der Antragsdaten erfolgt direkt zum OSCI-Intermediär des Ziellandes und nicht indirekt über mehrere OSCI-Intermediäre. Somit wird bei einem Datentransport an ein Bundesland außerhalb von NRW der OSCI-Intermediär des Ziellandes direkt angesprochen. Der OSCI-Intermediär bei DataClearing NRW ist in diesem Fall nicht beteiligt, siehe Kapitel II.1.5.

Unter OSCI-Infrastruktur werden IT-Lösungen verstanden, die einen OSCI-Transport gemäß dem OSCI-Transportstandard unterstützen. OSCI braucht keine eigene Benutzerverwaltung, da sie mit einer offenen Benutzergruppe arbeitet und die Benutzer sich über das Fachverfahren registrieren. Der Zugriff wird über Zertifikate gewährt. Governikus COM Tauri (vormals OSCI-Manager der Governikus Service Components) kann als OSCI-Intermediär eingesetzt werden. Governikus COM Tauri ist Teil der „Anwendung Governikus“, die als Anwendung des IT-Planungsrats geführt wird. Anwendungen des IT-Planungsrats sind IT-Lösungen, die aus Projekten oder projektähnlichen Strukturen hervorgegangen sind und deren Betrieb bzw. Pflege und Fortentwicklung auf Dauer gewährleistet werden soll.

Damit EfA-Online-Dienste Anträge an Governikus COM Tauri senden können, müssen Sender-Accounts eingerichtet werden. Der Sender-Account orientiert sich am Zertifikat des Senders und enthält übergreifende Regeln für den Versand der Nachricht, wie z. B. Löschfristen. EfA-Online-Dienste müssen somit Sender-Accounts bei allen bundesweit beteiligten OSCI-Intermediären einrichten.

II.2.7 XTA Standard und XTA-Server

XTA (XÖV Transport Adapter) ist ein Transportverfahren zur Übermittlung von XÖV-Nachrichten. Er definiert einen Webservice (XTA-WS) als Schnittstelle zur Anbindung von IT-Fachverfahren an eine technische Infrastruktur für die Nachrichtenübermittlung.

Der Bedarf an XTA entstand aus Erkenntnissen bei einer direkten Anbindung der Fachverfahren an einen OSCI-Intermediär. Diese Schnittstellen wurden oft uneinheitlich realisiert und verursachten dadurch Mehraufwände bei den Betreibern von Intermediären³⁶. Dies galt auch für die Anbindung von Standard-Fachverfahren, die in vielen Bundesländern oder auch Kommunen im Einsatz sind, aber jeweils unterschiedlich an die OSCI-Intermediäre angebunden werden mussten.

³⁴ Empfänger der Antragsdaten kann z. B. ein XTA-Server oder auch der Leser selbst sein.

³⁵ Leser der Antragsdaten kann z. B. ein Fachverfahren der zuständigen Fachbehörde sein.

³⁶ Vgl. Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**

Das in Abbildung 4 dargestellte „Rollenmodell in der OSCI-Infrastruktur“ zeigt, wo die XTA-Kommunikation verortet werden kann. Sender und Empfänger sind XTA-Server, die XTA-Webservices für die Fachverfahren anbieten und die OSCI-Kommunikation übernehmen.

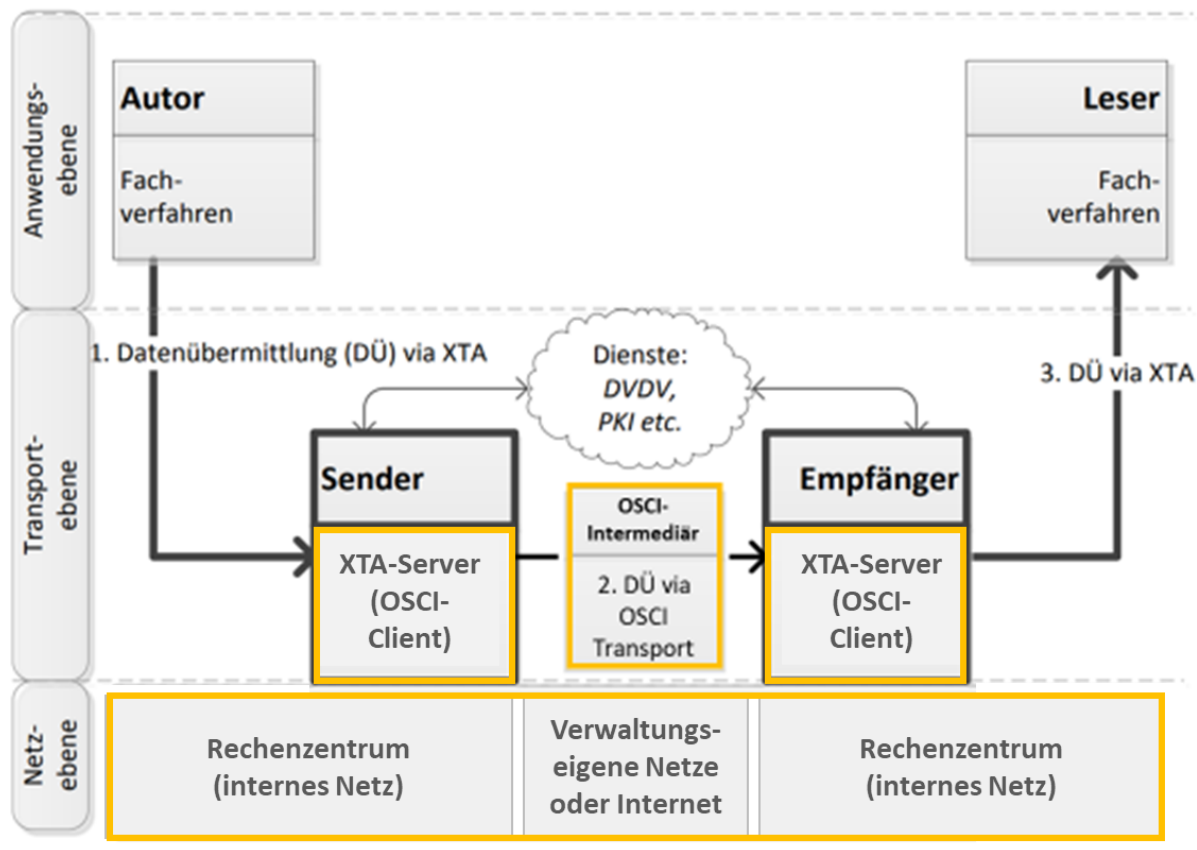


Abbildung 4: Rollenmodell in der OSCI-Infrastruktur (Quelle: Spezifikation XTA 2 Version 3), ergänzt um den OSCI-Intermediär (Anpassungen sind gelb markiert)

OSCI wird für die Kommunikation über verwaltungseigene Netze oder Internet genutzt, um einen Datenaustausch entsprechend Vertrauensniveau hoch zu ermöglichen³⁷. Als Konsequenz müssen für einen OSCI konformen Transport die XTA-Server im gleichen Rechenzentrum wie die angebundenen Fachverfahren betrieben werden. Für die Umsetzung des Transports der EfA-Online-Dienste bedeutet dies, dass ein XTA-Server im Rechenzentrum des Portals/EfA-Online Dienstes und ein XTA-Server in den Rechenzentren der empfangenden Fachbehörden/Fachverfahren betrieben werden müssen. Zur Abholung der Antragsdaten über XTA

³⁷ Siehe Technische Richtlinie TR-03107-1 BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf?__blob=publicationFile&v=1, Kapitel 8.3

wird in der Fachbehörde ein XTA-Client implementiert. Mit diesem kann dann über den XTA-Server der „eigene Postkorb“ zum Abholen der Antragsdaten abgefragt werden. Mit „eigener Postkorb“ ist in diesem Dokument der Zugriffsbereich des Empfängers gemeint.

XTA-Server bieten auch XTA-Webservices an, um Anfragen an das DVDV einzuleiten. Der XTA-Server übernimmt somit die Kommunikation mit dem DVDV und entlastet den EfA-Online-Dienst in dieser Hinsicht.

Ergänzend zu den in der XTA-Spezifikation³⁸ aufgeführten Webservices enthält die Spezifikation eine Beschreibung von Service Profilen. Service Profile enthalten Servicequalitäten der Nachrichtenübermittlung. Die Serviceprofile umfassen Aspekte wie Datenschutz, Datensicherheit, zu verwendende Infrastrukturen, Art der Kommunikation (z. B. synchron vs. asynchron), erforderliches Leistungsniveau wie z. B. Verfügbarkeit sowie Aufbau der Transportnachricht inkl. eingesetzte kryptographische Mittel der Verschlüsselung und Signatur. XTA Service Profile sind XML-Dokumente, die auf einer in XTA standardisierten XML-Schema-Definition basieren. Sie können genutzt werden, um die benötigten Service Qualitäten eindeutig, einheitlich und medienbruchfrei auswertbar zu definieren. Aktuell finden XTA Service Profile kaum Anwendung.

XTA liegt in verschiedenen Versionen vor, wobei diese Unterschiede beim XTA-Webservice aufweisen. Der IT-Planungsrat empfiehlt bereits seit 2017 XTA 2. KoSIT empfiehlt aktuell den Einsatz von XTA 2 Version 3. XTA 2 Version 4 findet keine Verwendung und soll perspektivisch durch eine neue Version ersetzt werden. Zur Version 4 wurden die Service Profile komplettiert und der Aufbau und die Struktur der Spezifikation deutlich verschlankt. Bei Unklarheiten zur Spezifikation XTA 2 Version 3 empfiehlt sich daher ein Blick auf die korrespondierende Stelle in XTA 2 Version 4. KoSIT weist darauf hin, dass die Größenbeschränkung einer Nachricht auf 40 MB, die noch bis XTA 2 Version 3 enthalten war, in Absprache mit den Kommunikationspartnern ignoriert werden kann. Sender- und Empfängerseite können unterschiedliche XTA-Versionen verwenden, eine Kompatibilität zwischen den Versionen ist jedoch nicht gewährleistet. XTA Versionen bis inklusive 1.1.1 sind aus Sicht von KoSIT veraltet und sollten keine Verwendung finden.

XTA-Server sind IT-Lösungen, die in der XTA Spezifikation definierte Webservices anbieten. Governikus bietet als XTA-Server COM Despina an. Er ist Teil der „Anwendung Governikus“, die als Anwendung des IT-Planungsrats geführt wird, siehe auch Kapitel II.2.5. Ergänzend dazu bietet die Zentrale Datenaustausch Infrastruktur (ZDI) XTA-Webservices an, siehe Kapitel II.2.8.

II.2.8 Public Key Infrastruktur der Verwaltung - Zertifizierungsstelle

Für die Sicherstellung von Integrität und Vertraulichkeit bei der elektronischen Kommunikation im Rahmen von Verwaltungsprozessen wird eine Zertifizierungsstelle benötigt, welche digitale Zertifikate vergeben und überprüfen kann. Eine Public-Key-Infrastruktur (PKI) stellt diese Möglichkeiten bereit, indem sie Schlüssel, Zertifikate und Signaturen verwaltet und prüft. Für die eGovernment Anwendungen der Kommunen sowie

³⁸ Siehe <https://www.xoev.de/downloads-2316#XTA>

Bundes- und Landesbehörden stellt die Public-Key-Infrastruktur der Verwaltung (Verwaltungs-PKI³⁹) dazu die Basistechnologie bereit.

Digitale Zertifikate werden zur Sicherstellung der IT-Sicherheit im Umfeld des Antragsroutings vielfältig eingesetzt. Sie dienen z. B. der Verschlüsselung und Signatur von Nachrichten zwischen EfA-Online-Dienst und Fachbehörde. Darüber hinaus werden Zertifikate für den verschlüsselten Transport der Antragsdaten sowie für den Zugriff auf Intermediäre genutzt. Damit Sender und Empfänger sich gegenüber dem OSCI-Intermediär authentifizieren können, müssen sowohl für Sender als auch für Empfänger individuelle Zertifikate ausgestellt werden.

Die Verteilung der Public Key Zertifikate erfolgt durch DVDV.

Da die Zertifikate eine hohe Sicherheitsrelevanz haben, muss sichergestellt werden, dass sie ausschließlich durch autorisierte Stellen ausgestellt werden. Das BSI betreibt mit der „PCA-1-Verwaltung“⁴⁰ eine Wurzelzertifizierungsstelle für die öffentliche Verwaltung. Von ihr können sich interessierte Zertifizierungsstellen von Bund, Ländern und Kommunen CA (Certificate Authority)-Zertifikate ausstellen lassen, wie z. B. Telesec, DOI-CA Deutschland (T-Systems) und Südwestfalen-IT (SIT)⁴¹. Diese wiederum sind dann dazu berechtigt, Zertifikate, z. B. im Kontext der OZG-Umsetzung, auszustellen⁴².

X.509⁴³ Zertifikate sind ein Standard für eine Public Key Infrastruktur zum Erstellen digitaler Zertifikate⁴⁴. Mit dem X.509 Zertifikat kann der Inhaber eines öffentlichen Zertifikats authentifiziert und verifiziert werden.

Anforderungen an Verschlüsselung und Signatur werden je Fachdatenstandard festgelegt und in OSCI-Transportprofilen dokumentiert, siehe Kapitel II.1.6. Abbildung 5 verortet die Zertifikate, die im Kontext des Antragsroutings eingesetzt werden können. Für eine Beschreibung der OSCI- und XTA-Standards siehe Kapitel II.2.6 (OSCI) und II.2.7 (XTA).

³⁹ Siehe https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Verwaltungs-PKI/verwaltungs-pki_node.html

⁴⁰ Siehe https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Verwaltungs-PKI/Wurzelzertifizierungsstelle/wurzelzertifizierungsstelle_node.html

⁴¹ Telesec hat die größte Verbreitung, NRW nutzt auch Zertifikate vom SIT. DOI-CA wird z. B. für Zugriffe auf den DVDV Master verwendet.

⁴² Für eine Liste der Zertifizierungsstellen siehe https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Verwaltungs-PKI/Wurzelzertifizierungsstelle/StrukturundMitglieder/strukturundmitglieder_node.html

⁴³ Siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02103/BSI-TR-02103.pdf;jsessionid=81BA30470406ACE594189D742BE50DA4.inter-net482?__blob=publicationFile&v=2

⁴⁴ <https://de.wikipedia.org/wiki/X.509>

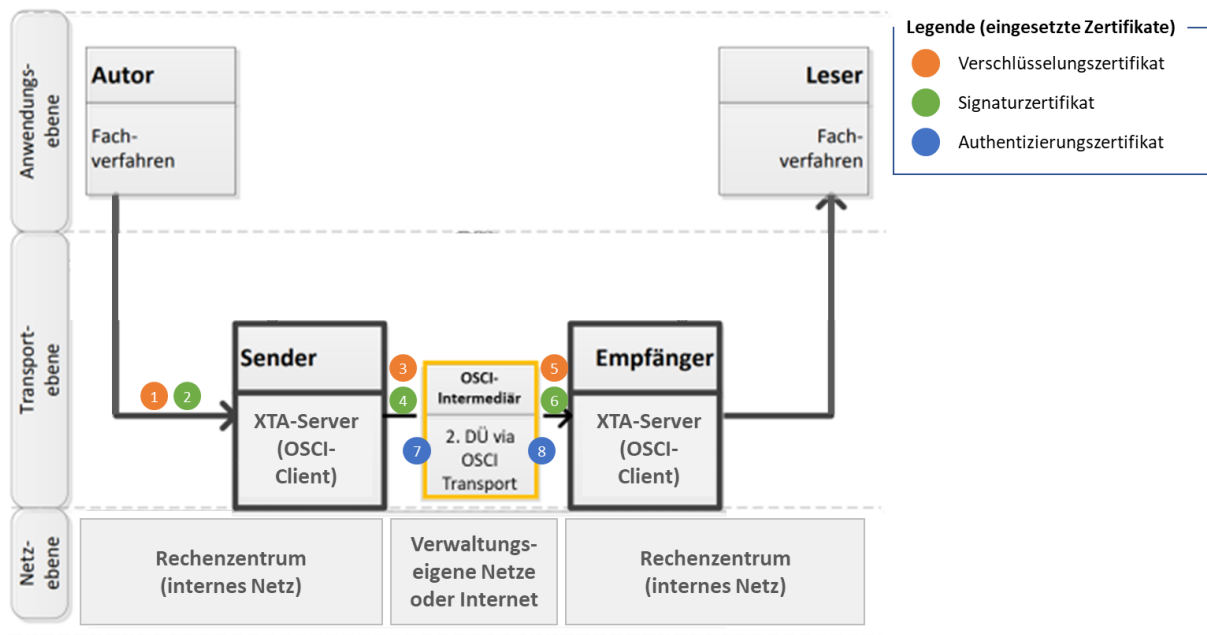


Abbildung 5: Eingesetzte Zertifikate im Kontext des Antragsroutings

Der Zweck der Zertifikate sowie deren Verortung sind in Tabelle 2 aufgeführt. Die ID verweist auf die Ziffer in Abbildung 5.

Tabelle 2: Eingesetzte Zertifikate im Kontext des Antragsroutings

ID	Zweck	Wer führt aus?	Ort Public Key	Ort Private Key
1	Verschlüsselung der Inhaltsdaten ⁴⁵	Autor (z. B. EfA-Online-Dienst)	DVDV	Leser (z. B. Fachverfahren)
2	Signatur der Inhaltsdaten	Autor (z. B. EfA-Online-Dienst)	DVDV	Autor (z. B. EfA-Online-Dienst)
3	Verschlüsselung der Nutzungsdaten zusammen mit den verschlüsselten Inhaltsdaten (äußerer OSCI-Umschlag) – Teilstrecke Sender – OSCI-Intermediär	Sender (z. B. XTA-Server)	DVDV	OSCI-Intermediär
4	Signatur des äußeren OSCI-Umschlags – Teilstrecke Sender - OSCI-Intermediär	Sender (z. B. XTA-Server)	DVDV	Sender (z. B. XTA-Server)

⁴⁵ Anstelle von Inhaltsdaten wird häufig auch von Fachdaten gesprochen. In diesem Dokument sind mit Inhaltsdaten der Antrag inklusive Anhänge gemeint. Unter Antragsdaten ist in diesem Dokument die zu transportierende Nachricht (wie z. B. eine OSCI-Nachricht) verstanden.

5	Verschlüsselung der Nutzungsdaten zusammen mit den verschlüsselten Inhaltsdaten (äußerer OSCI-Umschlag) – Teilstrecke OSCI-Intermediär – Empfänger	OSCI-Intermediär	DVDV	Empfänger (z. B. XTA-Server)
6	Signatur des äußeren OSCI-Umschlags – Teilstrecke OSCI-Intermediär – Fachbehörde	OSCI-Intermediär	DVDV	OSCI-Intermediär
7	Zugriffsrecht auf OSCI-Intermediär	Sender (z. B. XTA-Server)	DVDV	Sender
8	Zugriffsrecht auf OSCI-Intermediär	Empfänger (z. B. XTA-Server)	DVDV	Empfänger

Weitere Zertifikate sind notwendig, um das DVDV zu pflegen und um einen Transport über TLS/HTTPS zu realisieren. Für weitere Informationen, siehe „Beschreibung der Zertifikatsinfrastruktur im Deutschen Verwaltungsdienstverzeichnis (DVDV)“.⁴⁶

II.2.9 Zentrale Datenaustausch Infrastruktur

Die Zentrale Datenaustausch Infrastruktur (ZDI) wird für die sichere Übertragung von Daten und Dateien aus Internet, Landesverwaltungsnetz NRW (LVN) und NdB-VN in die Hochsicherheits-Infrastruktur (HSI) bei IT.NRW (und zurück) genutzt. Sie stellt eine zentrale Infrastruktur für den Datenaustausch zwischen Netzwerkbereichen mit unterschiedlichen Schutzbedarf-Einstufungen bereit.

Die ZDI bietet XTA 2 Version 3 Webservices an. Online-Dienste im Serviceportal.NRW und in den sonstigen Themenportalen (IT.NRW) setzen die ZDI ein, um den Transport der Antragsdaten zu initiieren. Die ZDI übernimmt dabei die Kommunikation mit dem DVDV und holt die technischen Adressen und Zertifikate für eine sichere Übertragung der Antragsdaten an die zuständige Fachbehörde. Die ZDI gewährleistet den Transport der verschlüsselten Daten vom Sender (z. B. Integrationskomponente des Portals) zu den Intermediär-Betreibern der Bundesländer.

Die ZDI wird auch eingesetzt, um Nachrichten von anderen Bundesländern zu empfangen. Die ZDI holt dabei die Nachrichten vom OSCI-Intermediär bei IT.NRW ab und sorgt dafür, dass die zuständige Fachbehörde die Nachricht abholen kann. Die ZDI wird bei IT.NRW betrieben und im OZG-Kontext für Verwaltungsleistungen im Landesvollzug eingesetzt, siehe auch Kapitel II.1.3.

⁴⁶ Siehe https://www.itzbund.de/SharedDocs/Downloads/DE/itloesungen/standardloesungen/dvdv/DVDV_ZertHandout.pdf?__blob=publicationFile&v=3

II.2.10 Fachverfahren

Die zuständige Fachbehörde setzt Fachverfahren ein, um die Sachbearbeitung (teil)automatisiert zu unterstützen. Die Fachverfahren werden, sofern vorhanden, unabhängig von der OZG-Einführung eingesetzt und unterstützen somit auch Anträge, die in papierbasierter Form oder durch Vor-Ort-Besuche bei der Behörde eingereicht werden. Im Rahmen der OZG-Einführung müssen die Fachverfahren angepasst werden, damit sie die Antragsdaten vom Antragsteller digital empfangen können. Dabei müssen sie die Daten in den verschiedenen Fachdatenstandards verarbeiten und Nachrichten direkt oder indirekt vom OSCI-Intermediär/XTA-Server empfangen können. Die Fachverfahren werden oft orientiert an der Zuständigkeit in Landes- oder kommunalen Rechenzentren betrieben. Fachverfahren gibt es sowohl als Individualentwicklungen als auch als Standardlösungen, die bei mehreren Bundesländern/Kommunen im Einsatz sind.

II.2.11 Dokumentenbasierte Sachbearbeitung ohne Fachverfahren

Einige Fachbehörden verfügen nicht über Fachverfahren. Stattdessen erfolgt die Sachbearbeitung dokumentenbasiert. Diese Sachbearbeitung kann vollständig manuell erfolgen oder im Rahmen eines dokumentenbasierten Workflows digital begleitet werden. Ergänzend dazu können Kleinstanwendungen, wie z. B. Excel- oder MS Access-Anwendungen zum Einsatz kommen, die auf dem Arbeitsplatzrechner der Sachbearbeiter installiert sind. Nach Ende der Sachbearbeitung werden die entsprechenden Auswertungen und Bescheide in einer papierbasierten oder elektronischen Akte hinterlegt. Im Rahmen des Antragsroutings muss dafür gesorgt werden, dass der Sachbearbeiter die Antragsdaten und Anhänge empfangen kann. Gemäß EfA-Mindestanforderung⁴⁷ sollten diese bei Bedarf in einem von der Sachbearbeitung lesbaren Format, wie z. B. als PDF, dargestellt werden können.

II.2.12 Elektronische Verwaltungsarbeit

Die Elektronische Verwaltungsarbeit (EVA) umfasst IT-Lösungen, die das Verwaltungshandeln dokumentiert. Es unterstützt zudem die verwaltungsbezogene Zusammenarbeit. Sie ist im Kontext des Antragsroutings von Relevanz, wenn nach Antragsstellung eine dokumentenbasierte Sachbearbeitung erfolgt, siehe Kapitel II.2.11

Die E-Akte ist der zentrale Baustein für die elektronische Aktenführung und unterstützt die rechtskonforme elektronische sowie revisionssichere Ablage von aktenrelevantem Schriftgut.

Die E-Laufmappe unterstützt ad-hoc Verwaltungsprozesse und wird aktuell eingesetzt, um Post- und Laufmappen im Rahmen eines Workflows an die zuständige Sachbearbeitung weiterzuleiten. Anschließend sorgt die E-Laufmappe dafür, dass aktenrelevante Informationen in die E-Akte importiert werden.

⁴⁷ siehe EfA-Mindestanforderung DS1 unter https://ozg.nrw/system/files/media/document/file/EfA-Mindestanforderungen_Version%201.0.pdf, „Sofern es keine Fachverfahren gibt, SOLL der Online-Dienst (zusätzlich) eine lesbare PDF-Datei erzeugen.“

Beide Lösungen werden bei IT.NRW betrieben. Sie sind für alle Landesbehörden und Bezirksregierungen in NRW verfügbar, die EVA eingeführt haben.

II.2.13 Governikus MultiMessenger

Der Governikus MultiMessenger (GMM) fungiert als zentrale Multikanalkommunikationsplattform unter Gewährleistung von Vertraulichkeit und Authentisierung. Er empfängt eingehende Nachrichten in unterschiedlichen Formaten (wie z. B. OSCI-Transportnachrichten) und kann diese über vorkonfigurierte Kanäle weiterleiten (z. B. als E-Mails). Er bietet Funktionen zur Ver- und Entschlüsselung an, prüft Zeitstempel und Zertifikate und protokolliert den Nachrichtenaustausch in einem Laufzettel. GMM wird als Anwendung des IT-Planungsrates weiterentwickelt und gepflegt.

Im Kontext des Antragsroutings wird der GMM vorrangig eingesetzt, wenn bei einer Fachbehörde eine dokumentenbasierte Sachbearbeitung ohne Fachverfahren notwendig ist und wenn der Datentransport als Zwischenlösung per E-Mail erfolgen muss. Für eine schematische Darstellung der Architektur des GMM bei IT.NRW für dieses Einsatzszenario siehe Abbildung 6.

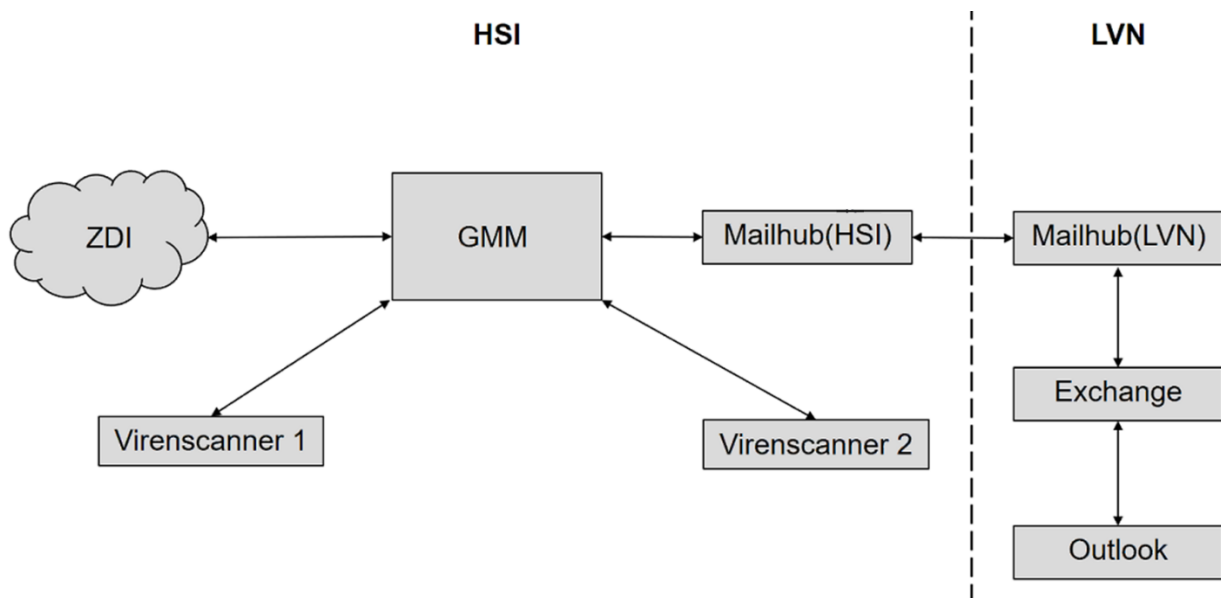


Abbildung 6: GMM bei IT.NRW - Einsatzszenario: Weiterleitung von Antragsdaten als E-Mail⁴⁸

Die ZDI erhält den Antrag inklusive Anhänge direkt vom EfA-Online-Dienst oder holt diese indirekt über einen OSCI-Intermediär ab. Der GMM ruft den XTA 2-Webservice der ZDI auf und holt die Nachricht ab. Er entschlüsselt und prüft den Antrag inklusive Anhänge (Zertifikate, Zeitstempel etc. siehe oben). Anschließend wird der Antrag inklusive Anhänge per E-Mail an das Funktionspostfach der zuständigen Fachbehörde weitergeleitet.

⁴⁸ Quelle IT.NRW - Referat Sicherheitsinfrastrukturen, Trustcenter

IT.NRW und einzelne kommunale Dienstleister betreiben jeweils individuelle Instanzen des GMM.

II.2.14 E-Mail und De-Mail

Der Einsatz von E-Mail und De-Mail ist insbesondere für den Datenaustausch bis hin zum Sachbearbeiter von Relevanz, wenn die empfangende Fachbehörde kein Fachverfahren einsetzt, siehe Kapitel II.2.11. So könnte z. B. Governikus MultiMessenger die Antragsdaten vom OSCI-Intermediär abholen und als E-Mail oder als De-Mail an den Sachbearbeiter weiterleiten.

In TR 03107-1: „Elektronische Identitäten und Vertrauensdienste im E-Government“⁴⁹ wird S/MIME (Secure/Multipurpose Internet Mail Extensions) als kryptographische Absicherung von E-Mails und Dateien erwähnt. Mit S/MIME können Nachrichten kryptographisch signiert bzw. verschlüsselt werden. Die Authentifizierung der Kommunikationspartner erfolgt bei S/MIME über X.509-Zertifikate. Diese müssen von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt werden, um Vertrauen der Kommunikationspartner in die Zertifikate sicherzustellen. Meist werden die gleichen PKI-Strukturen genutzt wie für die Ausstellung von TLS-Zertifikaten. Gemäß TR 03107-1 kann E-Mail mit S/MIME mit dedizierter PKI das Vertrauensniveau Substanziell und E-Mail mit Internet-PKI das Vertrauensniveau Normal erreichen. Das Vertrauensniveau hoch kann nicht erreicht werden.

De-Mail ermöglicht einen authentischen, vertraulichen und verbindlichen Austausch von Nachrichten und Dokumenten über das Internet. Gemäß TR 03107-1: „Elektronische Identitäten und Vertrauensdienste im E-Government“⁵⁰ erreicht De-Mail das Vertrauensniveau hoch, wenn der Nutzer De-Mail mit sicherer Anmeldung und mit Empfangsbestätigung förmliche Zustellung einsetzt.⁵¹ Für die verwaltungsinterne Kommunikation spielt De-Mail keine Rolle.

⁴⁹ Siehe <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf>

⁵⁰ Siehe <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf>

⁵¹ Strikt genommen befasst sich TR 03107-1 mit der Kommunikation zwischen Personen und öffentliche Stellen. Sie gibt dennoch eine Indikation über die Sicherheit des Datenaustausches.

II.3 Überblick der Transportwege

Im Kontext des Antragsroutings bei EfA-Online-Diensten in NRW gibt es die in Abbildung 7 dargestellten Transportwege.

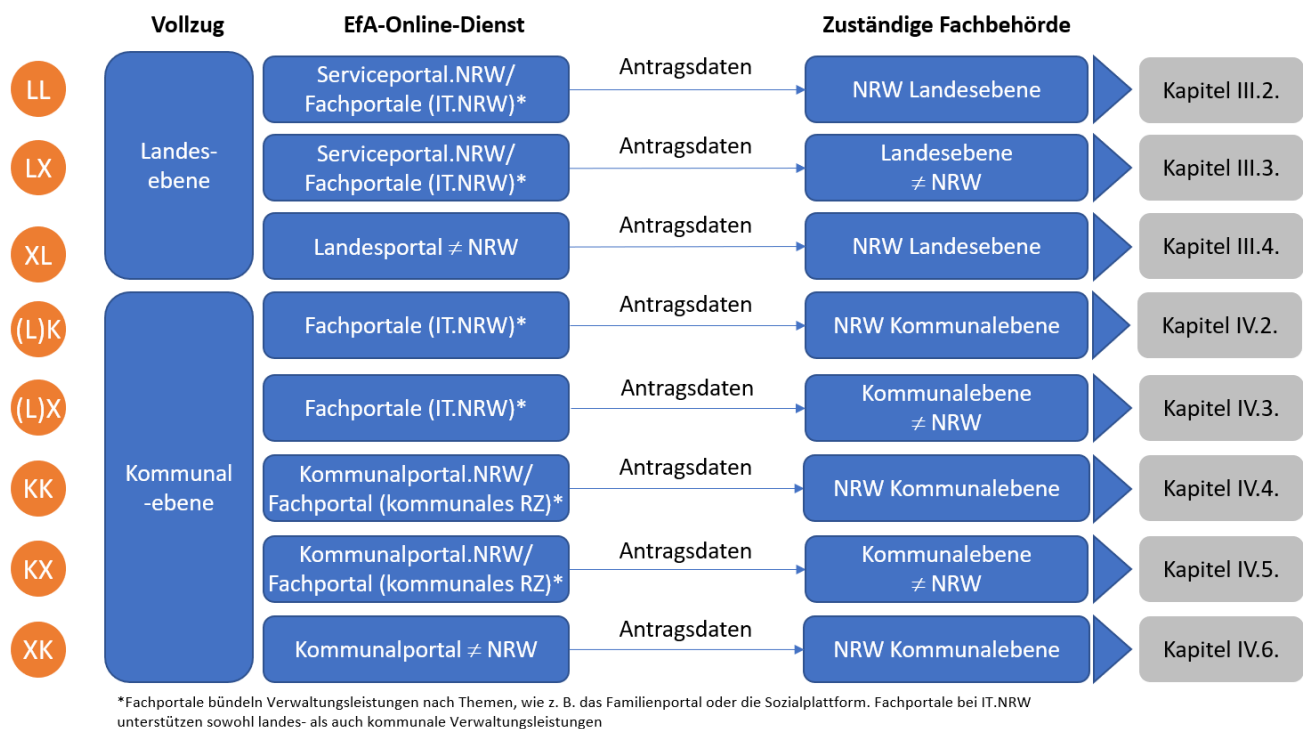


Abbildung 7: Transportwege Antragsrouting in NRW

Das Dokument umfasst eine Beschreibung aller in diesem Dokument empfohlenen Transportwege und verweist jeweils auf die in der Abbildung dargestellten Kürzel. Die Kürzel bestehen aus zwei Großbuchstaben, von denen der erste den Standort (Rechenzentrum) des EfA-Online-Dienstes und der zweite den Standort (Rechenzentrum) der zuständigen Fachbehörde darstellt. Bei den Transportwegen (L)K und (L)X steht das L im Klammern, da der Vollzug auf Kommunalebene ist, das Fachportal jedoch vom einem Landes-IT-Dienstleister betrieben wird. Durch die Klammer kann dieser Transportweg von LX mit Vollzug auf Landesebene unterschieden werden.

Im Folgenden werden diese Kürzel zur Bezugnahme auf den jeweiligen Transportweg weiterverwendet.

III Antragsrouting für Verwaltungsleistungen auf Landesebene

In diesem Kapitel werden die Empfehlungen für die Transportwege auf Landesebene beschrieben. Die Einrichtung eines Transports setzt voraus, dass bereits bestimmte Voraussetzungen geschaffen worden sind. So muss z. B. ein Fachdatenstandard etabliert worden sein, und ein DVDV Eintragungskonzept mit der Logik für die Adressierung der empfangenden Fachbehörden vorhanden sein. Für eine Beschreibung der Voraussetzungen und notwendigen vorbereitenden Aktivitäten, siehe Kapitel VI.

III.1 Vorgehensweise beim Antragsrouting auf Landesebene

Im Kontext des Antragsroutings bei EfA-Online-Diensten für Verwaltungsleistungen mit Vollzug auf Landesebene gilt es die Transportwege LL, LX und XL zu betrachten.

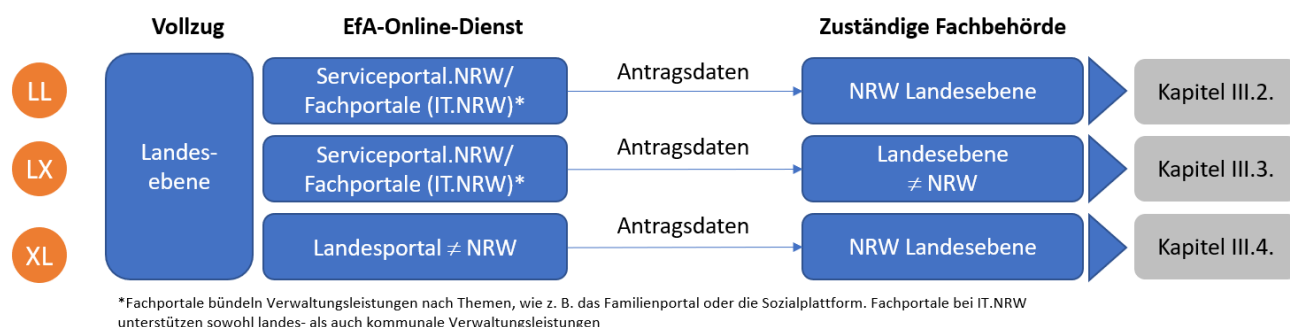


Abbildung 8: Transportwege für Antragsrouting mit Vollzug auf Landesebene

Die Architektur des Antragsroutings auf Landesebene muss sowohl den Transport der Antragsdaten landeseigener EfA-Online-Dienste als auch den Transport von Antragsdaten landesfremder EfA-Online-Dienste unterstützen.

Transport der Antragsdaten landeseigener EfA-Online-Dienste (LL, LX)

Die EfA-Online-Dienste werden im Serviceportal.NRW/Fachportal (IT.NRW) und mit dem dort eingesetzten Formularmanagementsystem (z. B. Lucom FMS) realisiert. Die Integrationskomponente im Backend des Serviceportals.NRW bereitet zusammen mit dem FMS (im Folgenden EfA-Online-Dienst) die Antragsdaten in die erforderliche Struktur des Fachdatenstandards auf. Die Inhaltsverschlüsselung der Antragsdaten erfolgt im EfA-Online-Dienst. Für diesen Zweck wird das Verschlüsselungszertifikat der empfangenden Fachbehörde verwendet. Der EfA-Online-Dienst erhält das Verschlüsselungszertifikat vom DVDV. Er ruft das DVDV nicht direkt auf, sondern initiiert eine XTA 2-Webservice-Anfrage an die ZDI (Methode: lookupService). Die ZDI ruft das DVDV auf, holt das Zertifikat und leitet es an den EfA-Online-Dienst weiter. Nachdem der EfA-

Online-Dienst eine Inhaltsverschlüsselung der Antragsdaten vorgenommen hat, wird der Transport der Antragsdaten zur empfangenden Fachbehörde initiiert. Der EfA-Online-Dienst initiiert eine XTA 2-Webservice-Anfrage an die ZDI (Methoden: createMessageID und sendMessage).

Je nachdem, wohin der Antrag versendet wird, unterscheidet sich das Vorgehen bei der ZDI:

Anträge an landesinterne Behörden (NRW) (LL)

Die ZDI überträgt die Antragsdaten sicher an die zuständige Behörde bzw. den IT-Dienstleister der zuständigen Landesbehörde. Die ZDI sorgt dafür, dass der Antrag entsprechend den Sicherheitsvorgaben vom Bundesamt für Sicherheit in der Informationstechnik (BSI) an das interne Netz des Fachverfahrens transportiert wird. Die empfangende Fachbehörde holt die Antragsdaten über eine XTA 2-Webservice-Anfrage an die ZDI ab (Methode: getMessage). Die Entschlüsselung der Inhaltsdaten erfolgt im zuständigen Fachverfahren (und nicht in der ZDI). Die Antragsdaten werden mit Hilfe von TLS/HTTPS in das interne Netz bei IT.NRW transportiert. Bei Bedarf erfolgt der Transport zu anderen Landesrechenzentren über das LVN. Für das LVN wurde der Schutzbedarf hoch festgestellt. Sind alle Anforderungen des hohen Schutzbedarfs im LVN erfüllt, ist eine OSCI-Kommunikation über OSCI nicht vorgesehen. Sie ist dennoch grundsätzlich möglich, sofern von der empfangenden Landesbehörde gewünscht.

Anträge an Landesbehörden außerhalb NRW (LX)

Befindet sich die empfangende Behörde nicht in NRW, wird der Antrag direkt an einen OSCI-Intermediär des empfangenden Bundeslandes weitergeleitet, d. h. nicht indirekt über einen OSCI-Intermediär in NRW. Hier holt die ZDI die technischen Adressen und Zertifikate für die Transportverschlüsselung vom DVDV-Server des KDN ab.

Transport der Antragsdaten landesfremder EfA-Online-Dienste (XL)

Beim Transport von Antragsdaten landesfremder EfA-Online-Dienste empfängt der OSCI-Intermediär bei IT.NRW die Antragsdaten. Die ZDI agiert als XTA-Server für die empfangende Fachbehörde, die die Antragsdaten mit Hilfe einer XTA 2-Webservice-Anfrage an die ZDI abholt (Methode: getMessage). Die Entschlüsselung der Inhaltsdaten erfolgt im Fachverfahren (und nicht in der ZDI). Die Antragsdaten werden mit Hilfe von TLS/HTTPS in das interne Netz bei IT.NRW und bei Bedarf über das LVN zu anderen Landesrechenzentren transportiert.

III.2 LL - Antragsrouting vom Serviceportal zu einem Landesportal innerhalb des Landes NRW

Beim Transportweg LL werden Antragsdaten landeseigener EfA-Online-Dienste an landeseigene Behörden transportiert, siehe Abbildung 9.

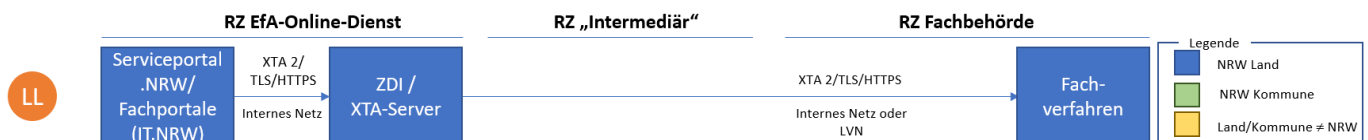


Abbildung 9: Transportweg LL

Zusammengefasst gelten für die Strecke LL folgende Empfehlungen für den Datentransport:

- Teilstrecke EfA-Online-Dienst – ZDI/XTA-Server:
 - EfA-Online-Dienst:
 - Umsetzung des EfA-Online-Dienstes im Serviceportal.NRW oder in einem Fachportal (IT.NRW)
 - Verschlüsselung der Inhaltsdaten direkt beim EfA-Online-Dienst und nicht in der ZDI
 - Nutzung der ZDI für Zertifikatsabfragen (XTA 2 Version 3, Methode: lookupService)
 - Nutzung der ZDI für die Initiierung des Datentransports an die empfangende Fachbehörde (XTA 2 Version 3, Methoden: createMessageID und sendMessage)
 - ZDI/XTA-Server:
 - Abfragen an das DVDV für technische Adressen und Zertifikate
 - Zwischenspeicherung der empfangenen Antragsdaten; ein OSCI-Intermediär wird nicht eingesetzt.
- Teilstrecke ZDI/XTA-Server – Fachbehörde:
 - ZDI/XTA-Server:
 - Ausführung des Datentransports an die empfangende Fachbehörde
 - Fachverfahren:
 - Abholung der Antragsdaten über XTA 2. Implementierung eines XTA-Clients zur Abfrage des eigenen Postkorbs über den XTA 2 Server der ZDI (XTA 2 Version 3, Methode: getMessage)
 - Entschlüsselung von verschlüsselten Inhaltsdaten
- Verwendete Netze: Transport über interne Netze bei IT.NRW oder ggf. LVN (wenn Fachverfahren sich in einem Landesrechenzentrum oder einer Behörde außerhalb von IT.NRW befinden).
- Transportverschlüsselung: TLS/HTTPS
- Alternative: Für Sachbearbeitung ohne Fachverfahren, siehe Kapitel III.5

III.3 LX - Antragsrouting vom Land NRW (Serviceportal) zu einem Landesportal außerhalb des Landes NRW

Beim Transportweg LX werden Antragsdaten landeseigener EfA-Online-Dienste an landesfremde Behörden transportiert, siehe Abbildung 10.

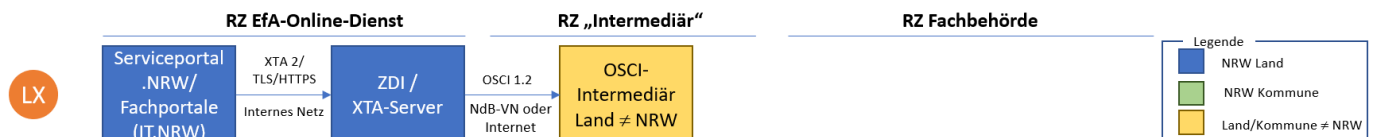


Abbildung 10: Transportweg LX

Zusammengefasst gilt für die Strecke LX folgende Empfehlungen für den Datentransport:

- Teilstrecke EfA-Online-Dienst – Intermediär
 - o EfA-Online-Dienst:
 - Umsetzung des EfA-Online-Dienstes im Serviceportal.NRW oder in einem Fachportal (IT.NRW)
 - Verschlüsselung der Inhaltsdaten direkt beim EfA-Online-Dienst und nicht in der ZDI
 - Nutzung der ZDI für Zertifikatsabfragen (XTA 2 Version 3, Methode: lookupService)
 - Nutzung der ZDI für die Initiierung des Datentransports via OSCI/XTA an den landesfremden OSCI-Intermediär (XTA 2 Version 3, Methoden: createMessageID und sendMessage)
 - o ZDI/XTA-Server:
 - Abfragen an das DVDV für technische Adressen und Zertifikate
 - Ausführung des Datentransports. OSCI-Kommunikation mit dem OSCI-Intermediär des empfangenden Bundeslandes außerhalb NRW.⁵²
 - o OSCI-Intermediär:
 - Empfang der Antragsdaten von der ZDI
 - OSCI-Intermediär des empfangenden Bundeslandes außerhalb NRW
- Teilstrecke Intermediär – Fachbehörde:
 - o Liegt in der Verantwortung des empfangenden Bundeslandes
- Verwendete Netze: Transport an Ziel-Intermediär über NdB-VN oder Internet
- Transportverschlüsselung: TLS/HTTPS im internen Netz, OSCI über Internet/HTTP
- Alternativen: OSCI über Internet/TLS/HTTPS

⁵² Die ZDI kommuniziert direkt mit dem OSCI-Intermediär des Ziellandes und nicht indirekt über einen OSCI-Intermediär im Land NRW.

III.4 XL - Antragsrouting von einem Landesportal außerhalb des Landes NRW zu einem Landesportal in NRW

Beim Transportweg XL werden Antragsdaten landesfremder EfA-Online-Dienste an Behörden in NRW transportiert.

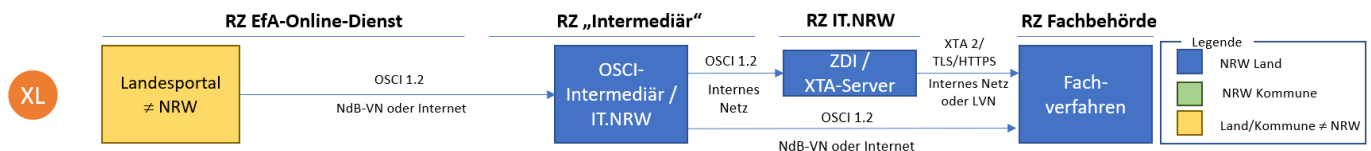


Abbildung 11: Transportweg XL

Zusammengefasst gilt für die Strecke XL folgende Empfehlungen für den Datentransport:

- Teilstrecke EfA-Online-Dienst – Intermediär:
 - OSCI-Intermediär:
 - Empfang der Antragsdaten vom landesfremden EfA-Online-Dienst
 - Verwendung des OSCI-Intermediärs bei IT.NRW
- Teilstrecke Intermediär – Fachbehörde:
 - ZDI/XTA-Server:
 - Abholung der Antragsdaten via OSCI vom OSCI-Intermediär bei IT.NRW
 - Ausführung des Datentransports an die empfangende Fachbehörde
 - Fachverfahren:
 - Abholung der Antragsdaten über XTA 2: Implementierung eines XTA-Clients zur Abfrage des eigenen Postkorbs über den XTA 2 Server der ZDI/XTA-Server (XTA 2 Version 3, Methode: getMessage).
 - Entschlüsselung von verschlüsselten Inhaltsdaten.
- Verwendete Netze: Transport über interne Netze bei IT.NRW oder ggf. LVN (wenn Fachverfahren sich in einem Landesrechenzentrum oder einer Behörde außerhalb von IT.NRW befindet)
- Transportverschlüsselung: über Internet: OSCI, über das interne Netz bei IT.NRW und über LVN: TLS/HTTPS
- Alternativen:
 - Fachverfahren holen Antragsdaten direkt beim OSCI-Intermediär ab. Realisierung eines OSCI-Clients Version 1.2., z. B. durch Nutzung der OSCI-Bibliothek bei Governikus⁵³
 - Für Sachbearbeitung ohne Fachverfahren, siehe Kapitel III.5.

⁵³ Siehe <https://www.governikus.de/osci-bibliothek/>

III.5 Sonderfall: Antragsrouting bei Sachbearbeitung ohne Fachverfahren

Wenn die empfangende Fachbehörde kein Fachverfahren einsetzt, soll der Online-Dienst dafür sorgen, dass die Sachbearbeitung die Antragsdaten inkl. Anhänge als lesbare PDF-Datei empfangen kann, siehe auch Kapitel II.2.11.

Für die Transportstrecke LX hat dies lediglich die Auswirkung, dass der EfA-Online-Dienst die Antragsdaten ergänzend als PDF-Datei bereitstellen muss. Der Datentransport erfolgt unverändert an den OSCI-Intermediär des Zielbundeslandes. Der weitere Datentransport bis zur empfangenden Fachbehörde liegt in der Verantwortung außerhalb von NRW und wird hier nicht betrachtet.

Für die Transportwege LL und XL ist geplant, dass die ZDI die Nachricht entsprechend der Beschreibung in Kapitel III.2 (LL) und Kapitel III.4 (XL) erhält/abholt. Danach transportiert die ZDI die Nachricht an die ebenfalls bei IT.NRW in Betrieb befindliche E-Laufmappe, siehe Kapitel II.2.12. Die E-Laufmappe soll hierfür eine REST-Schnittstelle anbieten. Erst in der E-Laufmappe werden die Antragsdaten entschlüsselt. Anschließend unterstützt die E-Laufmappe die Sachbearbeitung im Rahmen eines dokumentenbasierten Workflows und sorgt nach beendeter Sachbearbeitung dafür, dass die Antragsdaten in die E-Akte importiert werden. Der Datentransport erfolgt ab der ZDI über das interne Netz bei IT.NRW. Die hierfür notwendigen Anpassungen von ZDI und E-Laufmappe sind geplant. Ergänzende Voraussetzung ist, dass die empfangenden Fachbehörden die E-Laufmappe eingeführt haben.

Als Zwischenlösung wird der Einsatz des GMM empfohlen. Die ZDI holt die Antragsdaten direkt (Transportweg LL) oder beim OSCI-Intermediär (Transportweg XL) ab und leitet diese an den ebenfalls bei IT.NRW betriebenen GMM weiter. Dieser führt die Entschlüsselung und ggf. eine erneute Verschlüsselung der Inhaltsdaten (PDF und Anhänge) durch. Die Antragsdaten werden anschließend per E-Mail an das Funktionspostfach der zuständigen Fachbehörde versandt. Die Kommunikation erfolgt über das LVN. Unter der Annahme, dass die für den im LVN festgestellten Schutzbedarf hoch definierten Sicherheitsmaßnahmen umgesetzt wurden, müssen die Inhaltsdaten nicht verschlüsselt werden. Allerdings ist auch hier eine Transportverschlüsselung (TLS/HTTPS) der Nachricht notwendig, ein unverschlüsselter Transport ist nicht zulässig. Da die Antragsdaten im GMM bei IT.NRW entschlüsselt werden, sind mit Hinblick auf Auftragsverarbeitung alle notwendigen Vorkehrungen zu treffen, siehe Kapitel II.1.6.

Zusammengefasst gelten folgende Empfehlungen für den Datentransport in Fachbehörden, die kein Fachverfahren einsetzen:

- Teilstrecke EfA-Online-Dienst – Intermediär:
 - o EfA-Online-Dienst:
 - Antragsdaten in eine lesbare PDF-Datei übertragen (ergänzend zu den maschinenlesbaren Antragsdaten inklusive Anhänge).
 - LL: Transport der Antragsdaten an ZDI

- LX: Transport der Antragsdaten an den OSCI-Intermediär des empfangenden Bundeslandes.⁵⁴
- XL: Transport der Antragsdaten an den OSCI-Intermediär bei IT.NRW
- OSCI-Intermediär:
 - Empfang der Antragsdaten vom EfA-Online-Dienst
 - Verwendung des OSCI-Intermediärs bei IT.NRW
- Teilstrecke Intermediär – Fachbehörde:
 - LL und XL:
 - Abholung der Antragsdaten:
 - Ziellösung (geplant): Empfang der Antragsdaten über E-Laufmappe, siehe oben.
 - Zwischenlösung bis zur Nutzung der E-Laufmappe: Transport der Antragsdaten via ZDI/GMM bei IT.NRW über E-Mail an das Funktionspostfach der zuständigen Fachbehörde
 - LX:
 - Liegt in der Verantwortung des empfangenden Bundeslandes
- Verwendete Netze:
 - LL: Transport über interne Netze bei IT.NRW. Zusätzlich für die Zwischenlösung GMM: Mailversand über das LVN.
 - LX: Transport bis zum OSCI-Intermediär über Internet oder NdB-VN.
 - XL: Transport bis zum OSCI-Intermediär über Internet oder NdB-VN. Danach Transport über interne Netze bei IT.NRW. Zusätzlich für die Zwischenlösung Governikus Multimessenger: Mailversand über das LVN.
- Transportverschlüsselung: über Internet: OSCI, über das interne Netz bei IT.NRW und Mailversand über LVN: TLS
- Alternativen: keine bekannt

⁵⁴ ZDI kommuniziert direkt mit dem OSCI-Intermediär des Ziellandes und nicht indirekt über einen OSCI-Intermediär im Land NRW.

IV Antragsrouting für Verwaltungsleistungen auf Kommunalebene

In diesem Kapitel werden die Empfehlungen für die Transportwege auf Kommunalebene beschrieben. Die Einrichtung eines Transports setzt voraus, dass bereits bestimmte Voraussetzungen geschaffen worden sind. So muss z. B. ein Fachdatenstandard etabliert worden sein, und ein DVDV Eintragungskonzept mit der Logik für die Adressierung der empfangenden Fachbehörden vorhanden sein. Für eine Beschreibung der Voraussetzungen und notwendigen vorbereitenden Aktivitäten, siehe Kapitel VI.

IV.1 Vorgehensweise beim Antragsrouting auf Kommunalebene

Im Kontext des Antragsroutings bei EfA-Online-Diensten für Verwaltungsleistungen mit Vollzug auf Kommunalebene gilt es die Transportwege (L)K, (L)X, KK, KX und XK zu betrachten.

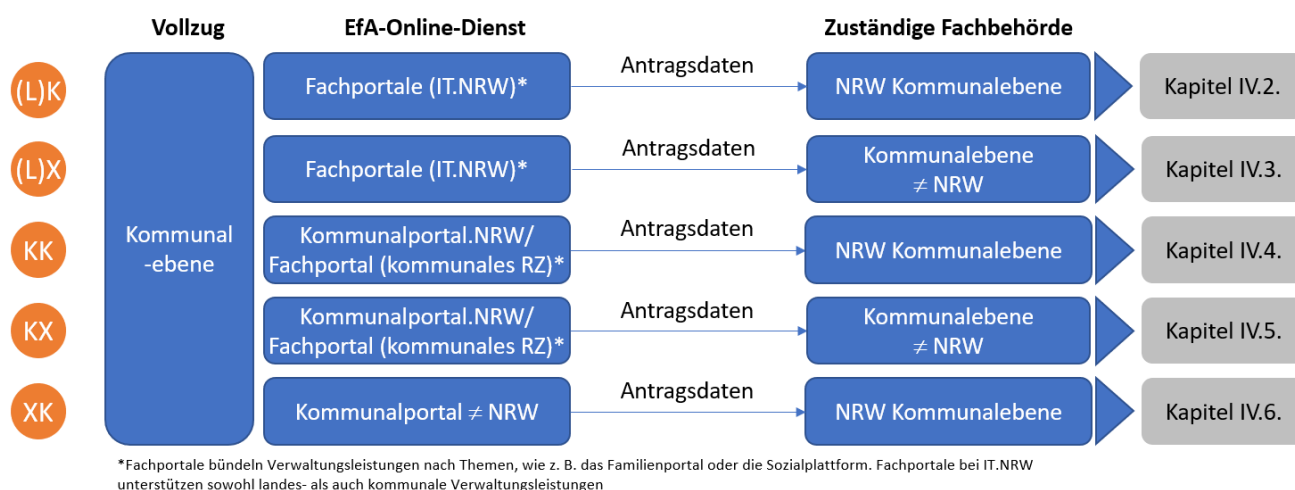


Abbildung 12: Transportwege für Antragsrouting mit Vollzug auf Kommunalebene

Analog zum Antragsrouting auf Landesebene umfasst die Architektur des Antragsroutings auf Kommunalebene zwei Teilaspekte: Zum einen den Transport der Antragsdaten landeseigener EfA-Online-Dienste (Fachportale oder Kommunalportale), zum anderen auch den Transport von Antragsdaten landesfremder EfA-Online-Dienste.

Transport der Antragsdaten landeseigener EfA-Online-Dienste ((L)K, (L)X, KK, KX)

Landeseigene EfA-Online-Dienste finden sich entweder auf einem Fachportal (betrieben bei IT.NRW) oder auf Kommunalportalen (betrieben in einem kommunalen Rechenzentrum).

Fachportal (IT.NRW)

Teilstrecke EfA-Online-Dienst/Portal - Intermediär: Die EfA-Online-Dienste werden im Fachportal (IT.NRW) und mit dem dort eingesetzten Formularmanagementsystem (z. B. Lucom FMS) realisiert. Die Integrationskomponente im Backend des Fachportals (IT.NRW) bereitet zusammen mit dem FMS (im Folgenden EfA-Online-Dienst) die Antragsdaten in die erforderliche Struktur des Fachdatenstandards auf. Die Inhaltsverschlüsselung der Antragsdaten erfolgt im EfA-Online-Dienst. Für diesen Zweck wird das Verschlüsselungszertifikat der empfangenden Fachbehörde verwendet. Der EfA-Online-Dienst erhält das Verschlüsselungszertifikat vom DVDV. Er ruft das DVDV nicht direkt auf, sondern initiiert eine XTA 2-Webservice-Anfrage an die ZDI (Methode: lookupService). Die ZDI ruft das DVDV auf, holt das Zertifikat und leitet es an den EfA-Online-Dienst weiter. Nachdem der EfA-Online-Dienst eine Inhaltsverschlüsselung der Antragsdaten vorgenommen hat, wird der Transport der Antragsdaten zur empfangenden Fachbehörde initiiert. Der EfA-Online-Dienst initiiert eine XTA 2-Webservice-Anfrage an die ZDI (Methoden: createMessageID und sendMessage). Die ZDI leitet den Antrag an den OSCI-Intermediär bei DataClearing NRW oder an den OSCI-Intermediär des empfangenden Bundeslandes außerhalb NRW weiter.

Teilstrecke Intermediär - Fachverfahren: Mit den kommunalen IT-Dienstleistern (inkl. Betreiber behördeneigener Rechenzentren) ist vereinbart, dass sie XTA-Server betreiben (werden), um die Antragsdaten beim OSCI-Intermediär abzuholen⁵⁵. Fachverfahren implementieren XTA-Clients, um die Antragsdaten über den XTA-Server zu empfangen (Nutzung der XTA 2 Methode getMessage). Die Entschlüsselung der Inhaltsdaten erfolgt beim XTA-Server und nicht beim Fachverfahren. Evtl. Vorkehrungen bzgl. Auftragsverarbeitung sind daher einzuplanen, siehe Kapitel II.1.6.

Kommunalportal.NRW/Fachportal (kommunales RZ)

Das Vorgehen ist vergleichbar mit dem Vorgehen für das Fachportal (IT.NRW). Es gibt Unterschiede bei der ersten Transportteilstrecke zwischen EfA-Online-Dienst/Portal und OSCI-Intermediär: Statt der ZDI werden jeweils separate XTA-Server in den Rechenzentren des Kommunalportals und des Fachportals eingesetzt. Die Verschlüsselung der Inhaltsdaten erfolgt beim XTA-Server und nicht beim EfA-Online-Dienst. Evtl. Vorkehrungen bzgl. Auftragsverarbeitung sind daher zu einzuplanen, siehe Kapitel II.1.6.

Transport der Antragsdaten landesfremder EfA-Online-Dienste (XK)

Beim Transport von Antragsdaten landesfremder EfA-Online-Dienste empfängt der OSCI-Intermediär bei DataClearing NRW die Anträge. Der Transport der Antragsdaten erfolgt über XTA-Server der IT-Dienstleister der zuständigen Fachbehörden, siehe Erläuterung zum Fachportal (IT.NRW) oben, Teilstrecke OSCI-Intermediär - Fachverfahren.

⁵⁵ Ein entsprechender Beschluss ist im KDN-Verbandsausschuss geplant.

IV.2 (L)K - Antragsrouting vom Land NRW (Fachportal) zu einer Kommune in NRW

Beim Transportweg (L)K werden Antragsdaten landeseigener EfA-Online-Dienste (Fachportal IT.NRW) an landeseigene Kommunen transportiert.

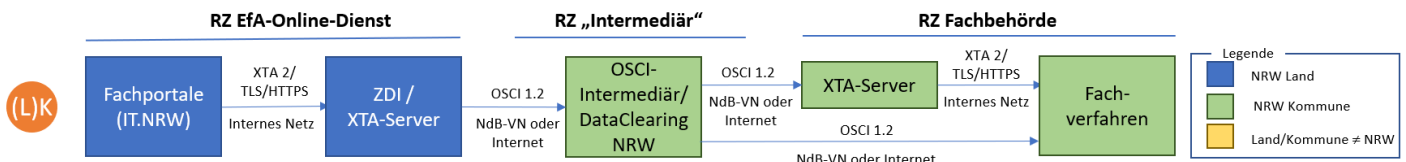


Abbildung 13: Transportweg (L)K, Beispiel Sozialplattform (IT.NRW)

Zusammengefasst gelten für die Strecke (L)K folgende Empfehlungen für den Datentransport:

- Teilstrecke EfA-Online-Dienst – Intermediär:
 - EfA-Online-Dienst
 - Umsetzung des EfA-Online-Dienstes im Fachportal (IT.NRW)
 - Verschlüsselung der Inhaltsdaten direkt beim EfA-Online-Dienst und nicht in der ZDI
 - Nutzung der ZDI für Zertifikatsabfragen (XTA 2 Version 3, Methode: lookupService)
 - Nutzung der ZDI für die Initiierung des Datentransports an den OSCI-Intermediär bei DataClearing NRW (XTA 2 Version 3, Methoden: createMessageID und sendMessage)
 - ZDI/XTA-Server:
 - Abfragen an das DVDV für technische Adressen und Zertifikate
 - Ausführung des Datentransports. OSCI-Kommunikation mit dem OSCI-Intermediär bei Dataclearing NRW
 - OSCI-Intermediär:
 - Empfang der Antragsdaten von der ZDI/XTA-Server
 - Verwendung des OSCI-Intermediärs bei DataClearing NRW
- Teilstrecke Intermediär – Fachbehörde:
 - XTA-Server:
 - Abholung der Antragsdaten:
 - Der XTA-Server der empfangenden Fachbehörde holt die Antragsdaten vom OSCI-Intermediär bei DataClearing NRW ab.
 - Der XTA-Server wird innerhalb des Rechenzentrums der zuständigen Fachbehörde betrieben.
 - Entschlüsselung der Antragsdaten beim XTA-Server. Evtl. Vorkehrungen bzgl. Auftragsverarbeitung einplanen, siehe Kapitel II.1.6.

- Fachverfahren:
 - Abholung der Antragsdaten über XTA 2. Implementierung eines XTA-Clients zur Abfrage des eigenen Postkorbs über den XTA-Server
- Verwendete Netze: Transport über interne Netze bei IT.NRW. Transport über das NdB-VN oder über das Internet
- Transportverschlüsselung: TLS/HTTPS für das interne Netz. OSCI-Transport über HTTP oder über TLS/HTTPS⁵⁶.
- Alternativen:
 - Fachverfahren holen Antragsdaten direkt beim OSCI-Intermediär ab. Realisierung eines OSCI-Clients Version 1.2., z. B. durch Nutzung der OSCI-Bibliothek bei Governikus⁵⁷.
 - Für Sachbearbeitung ohne Fachverfahren, siehe Kapitel IV.7.

IV.3 (L)X - Antragsrouting vom Land NRW (Fachportal) zu einer Kommune außerhalb des Landes NRW

Beim Transportweg (L)X werden Antragsdaten landeseigener EfA-Online-Dienste (Fachportal IT.NRW) an landesfremde Kommunen transportiert.

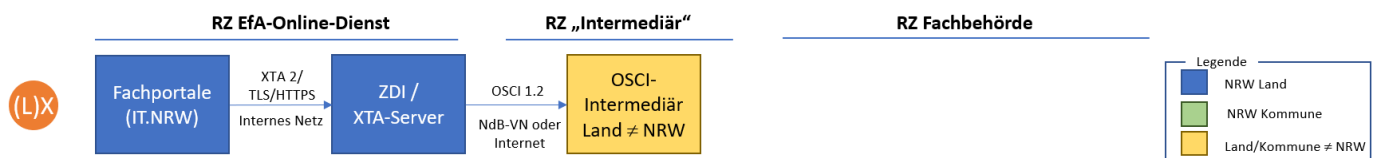


Abbildung 14: Transportweg (L)X

Zusammengefasst gilt für die Strecke (L)X folgende Empfehlungen für den Datentransport:

- Teilstrecke EfA-Online-Dienst – Intermediär:
 - EfA-Online-Dienst:
 - Umsetzung des EfA-Online-Dienstes im Fachportal (IT.NRW)
 - Verschlüsselung der Inhaltsdaten direkt beim EfA-Online-Dienst und nicht in der ZDI
 - Nutzung der ZDI für Zertifikatsabfragen (XTA 2 Version 3, Methode: lookupService)
 - Nutzung der ZDI für die Initiierung des Datentransports via OSCI/XTA an den landesfremden OSCI-Intermediär (XTA 2 Version 3, Methoden: createMessageID und sendMessage)

⁵⁶ Sofern TLS/HTTPS gemäß fachspezifischer Vorgabe eingesetzt werden muss.

⁵⁷ Siehe <https://www.governikus.de/osci-bibliothek/>

- ZDI/XTA-Server:
 - Abfragen an das DVDV für technische Adressen und Zertifikate
 - Ausführung des Datentransports. OSCI-Kommunikation mit dem OSCI-Intermediär des empfangenden Bundeslandes außerhalb NRW.⁵⁸
- OSCI-Intermediär:
 - Empfang der Antragsdaten von der ZDI/XTA-Server
 - Verwendung des landesspezifischen OSCI-Intermediärs
- Teilstrecke Intermediär – Fachbehörde:
 - Liegt in der Verantwortung des empfangenden Bundeslandes
- Verwendete Netze: Transport über interne Netze bei IT.NRW. Transport über das NdB-VN oder über das Internet
- Transportverschlüsselung: TLS/HTTPS für das interne Netz. OSCI-Transport Transport über HTTP oder über TLS/HTTPS⁵⁹.
- Alternativen: keine bekannt

IV.4 KK - Antragsrouting vom Land NRW (Kommunalportal) zu einer Kommune in NRW

Beim Transportweg KK werden Antragsdaten innerhalb NRW vom EfA-Online-Dienst (Kommunalportal) an Kommunen transportiert.

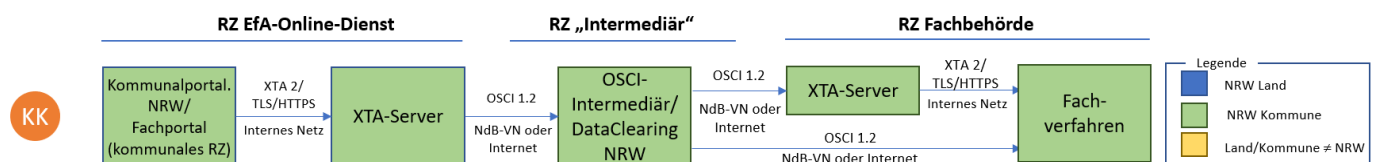


Abbildung 15: Transportweg KK

Zusammengefasst gilt für die Strecke KK folgende Empfehlungen für den Datentransport:

- Teilstrecke EfA-Online-Dienst – Intermediär:
 - EfA-Online-Dienst:
 - Umsetzung des EfA-Online-Dienstes im Kommunalportal.NRW oder in einem Fachportal (kommunales RZ)
 - Die XTA-Server befinden sich in den gleichen Rechenzentren wie das Kommunalportal.NRW oder das Fachportal

⁵⁸ ZDI kommuniziert direkt mit dem OSCI-Intermediär des Ziellandes und nicht indirekt über einen OSCI-Intermediär im Land NRW.

⁵⁹ Sofern TLS/HTTPS gemäß fachspezifischer Vorgabe eingesetzt werden muss.

- Verschlüsselung der Inhaltsdaten im XTA-Server oder (besser) direkt im EfA-Online-Dienst. Falls keine Verschlüsselung im EfA-Online-Dienst durchgeführt wird, sind erforderliche Maßnahmen im Umfeld der Auftragsverarbeitung zu treffen, siehe Kapitel II.1.6.
- Nutzung XTA-Server für Zertifikatsabfragen (XTA 2 Methode lookupService)
- Nutzung XTA-Server für die Initiierung des Datentransports (XTA 2 Methoden createMessageID und sendMessage)
- XTA-Server:
 - Abfragen an das DVDV für technische Adressen und Zertifikate
 - Ausführung des Datentransports. OSCI-Kommunikation mit dem OSCI-Intermediär bei DataClearing NRW.
- OSCI-Intermediär:
 - Empfang der Antragsdaten vom XTA-Server
 - Verwendung des OSCI-Intermediär bei DataClearing NRW, da für den EfA-Einsatz zweck eine Finanzierung durch den KDN erfolgt ist.
- Teilstrecke Intermediär – Fachbehörde:
 - XTA-Server:
 - Abholung der Antragsdaten: Der XTA-Server der empfangenden Fachbehörde holt die Antragsdaten vom OSCI-Intermediär bei DataClearing NRW ab.
 - Der XTA-Server wird innerhalb des Rechenzentrums der zuständigen Fachbehörde betrieben.
 - Entschlüsselung der Antragsdaten beim XTA-Server. Evtl. Vorkehrungen bzgl. Auftragsverarbeitung einplanen, siehe Kapitel II.1.6.
 - Fachverfahren:
 - Abholung der Antragsdaten über XTA 2. Implementierung eines XTA-Clients zur Abfrage des eigenen Postkorbs beim XTA-Server (XTA 2 Methode getMessage)
- Verwendete Netze: Transport über interne Netze. Transport über das NdB-VN oder über das Internet
- Transportverschlüsselung: TLS/HTTPS für das interne Netz. OSCI-Transport mit oder ohne TLS/HTTPS über Internet und NdB-VN.
- Alternativen:
 - Fachverfahren holen Antragsdaten direkt beim OSCI-Intermediär. Realisierung eines OSCI-Clients Version 1.2., z. B. durch Nutzung der OSCI-Bibliothek bei Governikus⁶⁰
 - Für Sachbearbeitung ohne Fachverfahren, siehe Kapitel IV.7.

⁶⁰ Siehe <https://www.governikus.de/osci-bibliothek/>

IV.5 KX - Antragsrouting vom Land NRW (Kommunalportal) zur zuständigen Fachbehörde einer Kommune außerhalb des Landes NRW

Beim Transportweg KX werden Antragsdaten landeseigener EfA-Online-Dienste (Kommunalportal) an landesfremde Kommunen transportiert.

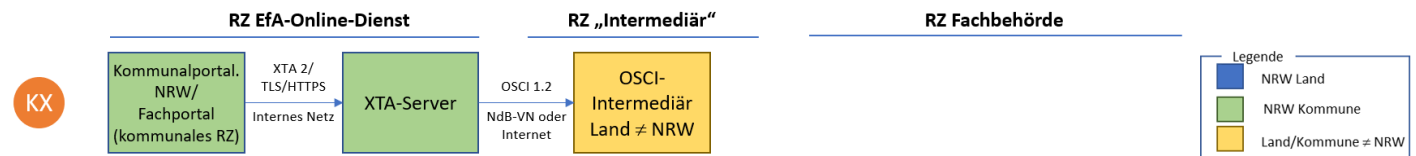


Abbildung 16: Transportweg KX

Zusammengefasst gelten für die Strecke KX folgende Empfehlungen für den Datentransport:

- Teilstrecke EfA-Online-Dienst – Intermediär:
 - EfA-Online-Dienst:
 - Umsetzung des EfA-Online-Dienstes im Kommunalportal.NRW oder in einem Fachportal (kommunales RZ)
 - Die XTA-Server befinden sich in den gleichen Rechenzentren wie das Kommunalportal.NRW oder das Fachportal
 - Verschlüsselung der Inhaltsdaten im XTA-Server oder (besser) direkt im EfA-Online-Dienst. Falls keine Verschlüsselung im EfA-Onlinedienst durchgeführt wird, sind erforderliche Maßnahmen im Umfeld der Auftragsverarbeitung zu treffen, siehe Kapitel II.1.6.
 - Nutzung XTA-Server für Zertifikatsabfragen (XTA 2 Methode lookupService)
 - Nutzung XTA-Server für die Initiierung des Datentransports (XTA 2 Methoden createMessageID und sendMessage)
 - XTA-Server:
 - Abfragen an das DVDV für technische Adressen und Zertifikate
 - Ausführung des Datentransports. OSCI-Kommunikation mit dem OSCI-Intermediär des empfangenden Bundeslandes außerhalb NRW.⁶¹
- Teilstrecke Intermediär – Fachbehörde:
 - Liegt in der Verantwortung des empfangenden Bundeslandes
- Verwendete Netze: Transport über interne Netze. Transport über das NdB-VN oder über das Internet
- Transportverschlüsselung: TLS/HTTPS für das interne Netz. OSCI-Transport mit oder ohne TLS/HTTPS über Internet und NdB-VN.
- Alternativen: Keine

⁶¹ ZDI kommuniziert direkt mit dem OSCI-Intermediär des Ziellandes und nicht indirekt über einen OSCI-Intermediär im Land NRW.

IV.6 XK - Antragsrouting von einem kommunalen Portal außerhalb von NRW zur zuständigen Fachbehörde einer Kommune in NRW

Beim Transportweg XK werden Antragsdaten landesfremder EfA-Online-Dienste an Kommunen in NRW transportiert.

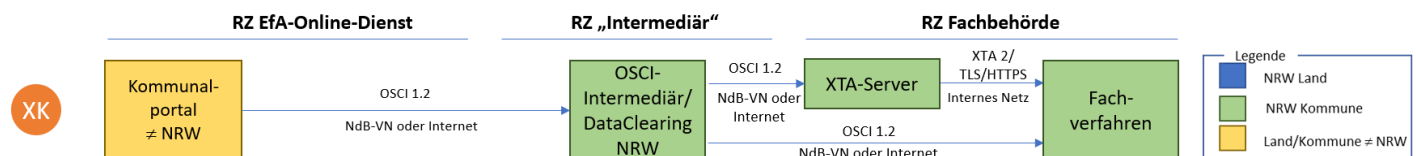


Abbildung 17: Transportweg XK

Zusammengefasst gelten für die Strecke XK folgende Empfehlungen für den Datentransport:

- Teilstrecke EfA-Online-Dienst – Intermediär:
 - OSCI-Intermediär:
 - Empfang der Antragsdaten vom landesfremden EfA-Online-Dienst
 - Verwendung des OSCI-Intermediär bei DataClearing NRW
- Teilstrecke Intermediär – Fachbehörde:
 - XTA-Server:
 - Abholung der Antragsdaten via OSCI vom OSCI-Intermediär bei DataClearing NRW
 - Der XTA-Server wird innerhalb des Rechenzentrums der zuständigen Fachbehörde betrieben.
 - Ausführung des Datentransports an die empfangende Fachbehörde
 - Entschlüsselung der Antragsdaten. Evtl. Vorkehrungen bzgl. Auftragsverarbeitung einplanen, siehe Kapitel II.1.6.
 - Fachverfahren:
 - Abholung der Antragsdaten über XTA 2. Implementierung eines XTA-Clients zur Abfrage des eigenen Postkorbs beim XTA-Server (XTA 2 Methode getMessage)
- Verwendete Netze: Transport über interne Netze. Transport über das NdB-VN oder über das Internet
- Transportverschlüsselung: TLS/HTTPS für das interne Netz. OSCI-Transport mit oder ohne TLS/HTTPS über das Internet und das NdB-VN.
- Alternativen:
 - Fachverfahren holen Antragsdaten direkt beim OSCI-Intermediär ab. Realisierung eines OSCI-Clients Version 1.2., z. B. durch Nutzung der OSCI-Bibliothek bei Governikus⁶².
 - Für Sachbearbeitung ohne Fachverfahren, siehe Kapitel IV.7.

⁶² Siehe <https://www.governikus.de/osci-bibliothek/>

IV.7 Sonderfall: Antragsrouting bei Sachbearbeitung ohne Fachverfahren

Wenn die empfangende Fachbehörde kein Fachverfahren einsetzt, soll der Online-Dienst dafür sorgen, dass die Sachbearbeitung die Antragsdaten inkl. Anhänge (zusätzlich) als lesbare PDF-Datei empfangen kann, siehe auch Kapitel II.2.11.

Für die Transportstrecken (L)X und KX hat dies lediglich die Auswirkung, dass der EfA-Online-Dienst die Antragsdaten ergänzend als PDF-Datei bereitstellen muss. Der Datentransport erfolgt unverändert an den OSCI-Intermediär des Zielbundeslandes, der eine entsprechende Lösung für den Empfang der Daten und den Transport bis hin zur Fachbehörde finden muss.

Für die sonstigen Strecken (L)K, KK und XK holt der IT-Dienstleister der empfangenden Fachbehörde die Antragsdaten bei DataClearing NRW über OSCI ab. Dabei wird der im eigenen Rechenzentrum betriebene XTA-Server eingesetzt. Anschließend holt eine „E-Mail-Routing-Komponente“ die Antragsdaten vom XTA-Server über die XTA 2 Methode getMessage. Die E-Mail-Routing-Komponente transportiert die Antragsdaten an den eigenen Mail-Server über das interne Netz. Die E-Mail wird an das Funktionspostfach der zuständigen Sachbearbeitungsgruppe adressiert. Je nachdem wann die Antragsdaten entschlüsselt werden, sind ggf. Vorkehrungen bzgl. Auftragsverarbeitung einzuplanen, siehe Kapitel II.1.6.

Zusammengefasst gelten folgende Empfehlungen für den Datentransport in Fachbehörden, die kein Fachverfahren einsetzen:

- Teilstrecke EfA-Online-Dienst – Intermediär:
 - EfA-Online-Dienst:
 - Antragsdaten in eine lesbare PDF-Datei übertragen (ergänzend zu den maschinenlesbaren Antragsdaten inklusive Anhänge).
 - (L)K, KK, XK: Transport der Antragsdaten an den OSCI-Intermediär bei DataClearing NRW
 - (L)X, KX: Transport der Antragsdaten an den OSCI-Intermediär des empfangenden Bundeslandes außerhalb NRW.⁶³
 - OSCI-Intermediär:
 - Empfang der Antragsdaten vom EfA-Online-Dienst
 - (L)K, KK, XK: Verwendung des OSCI-Intermediärs bei DataClearing NRW
 - (L)X, KX: OSCI-Intermediär des empfangenden Bundeslandes außerhalb NRW

⁶³ ZDI kommuniziert direkt mit dem OSCI-Intermediär des Ziellandes und nicht indirekt über den OSCI-Intermediär bei Dataclearing NRW

- Teilstrecke Intermediär – Fachbehörde:
 - (L)K, KK, XK:
 - Abholung der Antragsdaten:
 - Der XTA-Server des IT-Dienstleisters der empfangenden Fachbehörde holt die Antragsdaten vom OSCI-Intermediär bei DataClearing NRW ab.
 - Der IT-Dienstleister der empfangenden Fachbehörde nutzt eine „E-Mail-Routing-Komponente“, um die letzte Strecke XTA-Server – E-Mail-Server – Sachbearbeiter zu realisieren.
 - Die „E-Mail-Routing-Komponente“ wird im gleichen Rechenzentrum wie der XTA-Server des IT-Dienstleisters und wie der E-Mail-Server betrieben.
 - In Abhängigkeit vom Zeitpunkt der Entschlüsselung sind bei Bedarf erforderliche Maßnahmen im Umfeld Auftragsverarbeitung zu treffen, siehe Kapitel II.1.6.
 - L(X), KX:
 - Liegt in der Verantwortung des empfangenden Bundeslandes
- Verwendete Netze: Transport über interne Netze. Transport über das NdB-VN oder über das Internet, Datentransport „E-Mail-Routing-Komponente“ – E-Mail-Server über interne Netze des IT-Dienstleisters
- Transportverschlüsselung: Über das Internet: OSCI, Über das interne Netz bei IT.NRW und über LVN: TLS
- Alternativen: keine bekannt

V Testinfrastruktur

Damit Entwickler von EfA-Online-Diensten frühzeitig erste Erfahrungen mit dem Transport von Antragsdaten über die in diesem Dokument beschriebenen Transportwege gewinnen können, ist eine Testinfrastruktur notwendig.

Es ist angedacht eine Testinfrastruktur aufzubauen und ein Testkonzept für deren Verwendung zu erarbeiten. Im ersten Schritt sollen die Anforderungen an die Testinfrastruktur festgehalten werden. Wegen der teilweise gemeinsamen Infrastruktur für das Antragsrouting auf Ebene Land und Kommune wäre eine gemeinsame Testumgebung und/oder ein gemeinsames Testkonzept für Land und Kommune denkbar. Einige Tests sollten übergreifend durchgeführt und nicht im Rahmen der einzelnen Tests der EfA-Online-Dienste vorgenommen werden. Dazu gehört z. B. die Durchführung von Lasttests der OSCI-Intermediäre. Im Testkonzept sollten genaue Regeln definiert werden, welche Tests im Rahmen der EfA-Online-Dienst-Umsetzungsprojekte durchzuführen sind und welche nicht.

Folgende Testumgebungen bzw. Testmöglichkeiten sind bereits etabliert:

- Governikus hat einen Test-OSCI-Intermediär eingerichtet, über den OSCI-Tests durchgeführt werden können. Dort können auch die zur Kommunikation mit dem OSCI-Intermediär erforderlichen OSCI-Bibliotheken für JAVA und .NET Anwendungen herunter geladen werden⁶⁴.
- Die produktive DVDV-Umgebung kann auch für Testzwecke eingesetzt werden. Dazu muss im DVDV Eintragungskonzept eine Schlüsselsystematik für eine Abgrenzung zwischen „fiktiven“ Fachbehörden (für Testzwecke) und „produktiven“ Fachbehörden erarbeitet werden. Für weitere Informationen siehe „Leitfaden für die Erstellung eines DVDV Eintragungskonzepts in NRW“⁶⁵. Ergänzend dazu ist geplant, ein DVDV-Testsystem im ITZBund aufzubauen.
- Bei Dataclearing NRW steht für Tests ein XTA-Server zur Verfügung, z. B. um die Anbindung von Fachverfahren mittels XTA 2 durch die Hersteller zu testen.
- Für Tests des OSCI-Intermediärs bei IT.NRW durch OZG-Dienste steht keine explizite Testumgebung zur Verfügung. Ggf. kann aber ein produktiver OSCI-Intermediär nach Absprache für Tests genutzt werden (Einzelfallentscheidung).

Das vorliegende Dokument wird um weitere Details bzgl. Testumgebung und Testkonzept ergänzt, sobald diese vorliegen.

VI Hinweise für die Einrichtung des Antragsroutings

Die Umsetzung von EfA-Online-Diensten ist eine Aufgabe, die eine Vielzahl von organisatorischen und technischen Aktivitäten umfasst. Diese sind bereits an anderer Stelle dokumentiert. So enthält z. B. der OZG-Leitfaden⁶⁶ ein Vorgehensmodell zur Planung, Konzeption und Umsetzung von Online-Diensten. Ergänzend dazu enthält der EfA-Wegweiser⁶⁷ Hinweise bei der Umsetzung von EfA-Online-Diensten. Darüber hinaus hat NRW landesspezifische Unterlagen erarbeitet, wie z. B. einen Leitfaden für die Erstellung eines DVDV Eintragungskonzeptes in NRW⁶⁸. Eine Auflistung der Dokumente befindet sich in Kapitel VII.2.

⁶⁴ Siehe hier: <https://www.governikus.de/osci-bibliothek/#toggle-id-7>

⁶⁵ Siehe hier: https://ozg.nrw/system/files/media/document/file/leitfaden_dvdv_ek_v1.0_o.pdf

⁶⁶ Siehe <https://leitfaden.ozg-umsetzung.de/display/OZG/OZG-Leitfaden>

⁶⁷ Siehe https://www.onlinezugangsgesetz.de/SharedDocs/downloads/Webs/OZG/DE/wegweiser-efa.pdf?__blob=publicationFile&v=3

⁶⁸ Siehe <https://ozg.nrw/service/dokumente>

Dieses Kapitel enthält somit nur ausgewählte Hinweise mit einer besonderen Relevanz für das Antragsrouting. Die Hinweise richten sich sowohl an EfA-Online-Dienst-Umsetzungsprojekte als auch an die empfangenden Fachbehörden. Sie umfassen u. a. die von der Fa. Governikus KG erarbeitete Handreichung für den Einrichtung eines Datentransports, siehe Anhang – Kapitel VIII.

VI.1 Hinweise für EfA-Online-Dienst-Umsetzungsprojekte

Das EfA-Online-Dienst-Umsetzungsprojekt muss folgende Aktivitäten durchführen, um die Voraussetzungen für einen produktiven Transport von Antragsdaten zu schaffen.

- Einen Standard für den Datenaustausch festlegen: Auswahl und Berücksichtigung oder Anpassung des Datenaustauschstandards (vgl. XÖV-Standards, ggf. Einsatz von FIM-Baustein „Datenfelder“). Bei Bedarf Erarbeitung eines neuen Standards für den Datenaustausch.
- Regeln für den Umgang mit Versionswechseln des Datenaustauschstandards erarbeiten (d. h. bei neuen oder angepassten Nachrichten und Austauschformaten).
- Ein DVDV Eintragungskonzept erstellen, siehe Leitfaden für die Erstellung eines DVDV Eintragungskonzeptes in NRW.⁶⁹
- Die Transportinfrastruktur bis zum Intermediär entsprechend gewähltem Transportweg aufbauen, sofern nicht lückenlos vorhanden, siehe Kapitel III und Kapitel IV. (Die empfangende Fachbehörde sorgt dafür, dass der Transportweg ab dem Intermediär aufgebaut wird, siehe Kapitel VI.2.)
- Ein Transportprofil, d. h. Regeln für einen sicheren Datentransport, festlegen. Für den Inhalt eines Transportprofils siehe Anhang, Kapitel VIII.2.
- Die Dateigrößenbeschränkung der Nachrichten festlegen und mit allen Beteiligten entlang des Transportwegs abstimmen. Dabei ist zu berücksichtigen, dass die Dateigröße der XTA-Nachricht um den Faktor 1,3-1,4 und OSCI-Nachricht um den Faktor 2,2 – 2,7 größer sein wird als die Inhaltsdaten (Antrag inklusive Anhänge).⁷⁰ Sollte die Nachrichtengröße größer als 40 MB sein, wird die in XTA 2 Version 3 (noch) vorhandene Größenbeschränkung überschritten⁷¹. Eine Überschreitung der Nachrichtengröße ist aus Sicht von KoSIT zulässig. Allerdings ist dazu eine Absprache mit den Kommunikationspartnern notwendig, siehe auch Kapitel II.2.7.
- Die Antragsdaten als PDF senden können. Sofern es eine oder mehrere Fachbehörden gibt, die kein Fachverfahren einsetzen, sollte der EfA-Online-Dienst die Antragsdaten ergänzend zum maschinenlesbaren Datenformat als lesbare PDF-Datei bereitstellen. Es wird empfohlen, dass der EfA-Online-Dienst immer die gleichen Daten versendet, unabhängig davon, ob die empfangene Fachbehörde ein Fachverfahren hat oder nicht. Somit muss der EfA-Online-Dienst diesbezüglich keine Logik enthalten. Als Konsequenz wird:

⁶⁹ Siehe <https://ozg.nrw/service/dokumente>

⁷⁰ Hintergrund: Die Anhänge der XTA-Nachrichten werden base64-codiert. Bei der Weiterleitung über OSCI wird die gesamte, nun angewachsene Nachricht nochmals base64 codiert und dann verschlüsselt. (Erfahrungen aus dem Bauportalprojekt)

⁷¹ Diese Größenbeschränkung ist in XTA 2 Version 4 nicht mehr vorhanden.

- das empfangende Fachverfahren den PDF-Antrag empfangen und ignorieren (Variante Sachbearbeitung mit Fachverfahren)
- die Fachbehörde maschinenlesbare Anträge empfangen und ignorieren (Variante Sachbearbeitung ohne Fachverfahren). Dabei muss darauf geachtet werden, dass der PDF-Antrag und die strukturierte Datei im maschinenlesbaren Format nicht voneinander abweichen dürfen, da sonst die Angaben aus der strukturierten Datei gelten⁷².
- Umgang mit Quittierung von empfangenen Nachrichten festlegen. I. d. R. soll der Intermediär die Quittierung senden (und nicht das Fachverfahren). Eventuelle Fehler bei der Validierung der Fachdaten müssen somit im Nachgang erfolgen.
- Einen EfA-Online-Dienst-spezifischen Anbindungsleitfaden erstellen. Der Anbindungsleitfaden kann auf das vorliegende Dokument (inkl. Versionsangabe) Bezug nehmen.
- Fachverfahrenshersteller einbinden⁷³:
 - Information über Ansprechpartner
 - Information über den geplanten Transportweg und über mögliche Alternativen
 - Information über den geplanten Fachdatenstandard
 - Information über den Umgang mit Versionswechseln des Fachdatenstandards
 - Information über Testsysteme und Testvorgehen
 - Bereitstellung von Beispieldatensätzen (Testdateien), damit Fachverfahrenshersteller prüfen können, ob sie die Antragsdaten verarbeiten und evtl. Anpassungen frühzeitig vornehmen können. Fachverfahrenshersteller sollten auch die Möglichkeit haben Änderungsanforderungen an den Fachstandard einzureichen, sofern fachverfahrensübergreifend sinnvoll.
 - Regelmäßiger Austausch mit den Fachbehörden und Fachverfahrensherstellern organisieren, um Fragen zu beantworten und eventuelle Hürden zu identifizieren.
- EfA-Online-Dienst befähigen, Fachdaten entsprechend Transportweg zu erzeugen und die Antragsdaten mit XTA 2 an einen XTA-Server zu senden.
- Transport einrichten:
 - Beschaffung der notwendigen Zertifikate für Signatur, Verschlüsselung und Authentifizierung, siehe Kapitel II.2.8 (Tabelle 2).
 - Entsprechend gewähltem Transportweg: Zugang zu der Transportinfrastruktur für Versand und Empfang der Antragsdaten schaffen. Sofern der Transportweg einen OSCI-Intermediär vorsieht, müssen z. B. Sender-Accounts bei den beteiligten OSCI-Intermediären eingerichtet

⁷² Siehe Serviceportal.NRW Verordnung § 7 Abs. 2 Ziffer 2:

https://recht.nrw.de/lmi/owa/br_vbl_detail_text?anw_nr=6&vd_id=19000&vd_back=N1212&sg=o&menu=1

⁷³ Eine frühzeitige Einbindung der Fachverfahrenshersteller ist sinnvoll, um das Fachverfahren zu ertüchtigen und frühzeitig evtl. Änderungsanforderungen an den Fachdatenstandard zu bekommen.

werden, siehe Kapitel II.2.6. Wichtig: Sender-Accounts sind für alle beteiligten OSCI-Intermediäre notwendig, d. h. auch für OSCI-Intermediäre aus anderen Bundesländern.⁷⁴

- Durchführung von Tests des Datentransports, siehe auch Kapitel V.
- Schließen von AVVs zwischen dem Verantwortlichen gem. Art. 24 DSGVO und den Auftragsverarbeitern gem. Art. 28 DSGVO. Die AVVs müssen, sofern erforderlich, entlang der gesamten Transportstrecke lückenlos vorhanden sein, siehe Kapitel II.1.6.
- Besetzen von Rollen und Verantwortlichkeiten (z. B. Verantwortlicher gemäß DSGVO und Betreiber von Fachverfahren).
- Vertragliche Vereinbarungen treffen, Klärung von Themen wie z. B. Betriebs- und Supportzeiten.
- Hinweise an die Verfasser des vorliegenden Dokuments geben. Somit können zukünftige Versionen des Dokuments entsprechend der gewonnenen Praxiserfahrung angepasst und ergänzt werden. Die Ansprechpartner sind im Kapitel VII.1 dokumentiert.

Die hier beschriebenen Punkte mit Relevanz für die anzubindenden Fachbehörden sollten in einem EfA-Online-Dienst-spezifischen Anbindungsleitfaden festgehalten werden, siehe Kapitel VI.1

VI.2 Hinweise für anzubindende Fachbehörden

Anzubindende Fachbehörden müssen folgende Aktivitäten durchführen, um die Voraussetzungen für einen produktiven Transport von Antragsdaten zu schaffen:

- Fachbehörden im DVDV gemäß Eintragungskonzept eintragen.
- Die Transportinfrastruktur ab dem Intermediär entsprechend gewähltem Transportweg aufbauen, sofern nicht lückenlos vorhanden, siehe Kapitel III und Kapitel IV. (Das EfA-Online-Dienst-Umsetzungsprojekt sorgt dafür, dass der Transportweg bis hin zum Intermediär aufgebaut wird, siehe Kapitel VI.1.)
- Eine der in diesem Dokument aufgeführten Transportalternativen auswählen, siehe Kapitel III und Kapitel IV.
- Sicherstellen, dass die Transportinfrastruktur ab dem Intermediär die Nachrichten entsprechend vereinbarter Dateigröße verarbeiten kann.
- Das Fachverfahren ertüchtigen (sofern vorhanden):
 - o Fähigkeit, Antragsdaten entsprechend des Fachdatenstandards zu verarbeiten. Bei Bedarf und sofern fachverfahrensübergreifend sinnvoll Änderungsanforderungen am Fachdatenstandard vorschlagen.

⁷⁴ Die Aussage bezieht sich in erster Linie auf die Nutzung von Governikus COM Tauri als OSCI-Intermediär. Es wäre zu prüfen, ob für andere Intermediärsprodukte ebenfalls Sender-Accounts o. ä. eingerichtet werden müssen.

- Fähigkeit, entsprechend gewähltem Transportweg Antragsdaten zu holen und ggf. (in Abhängigkeit des gewählten Transportwegs) zu entschlüsseln:
 - XTA 2 Nachrichten vom XTA-Server abholen (Nutzung der XTA-Webservices). Implementierung eines XTA-Clients zur Abfrage des XTA-Servers oder alternativ
 - Antragsdaten direkt beim OSCI-Intermediär abholen. Realisierung eines OSCI-Clients Version 1.2., z. B. durch Nutzung der OSCI-Bibliothek bei Governikus.
 - Nachrichten entsprechend vereinbarter Nachrichtengröße empfangen
- Sicherstellen, dass die innerbehördliche Organisation und technische Ausstattung der empfangenden Fachbehörde:
 - die Integrität der erhaltenen Daten gewährleisten können.
 - die Sachbearbeitung des Antrags vollständig elektronisch durchführen können. Papierfassungen der Unterlagen werden grundsätzlich nicht benötigt oder sind ansonsten von der Behörde selbst auszudrucken.
- Besetzen von Rollen und Verantwortlichkeiten (z. B. Verantwortlicher gemäß DSGVO und Betreiber von Fachverfahren).
- Beteiligen des örtlichen Datenschutzbeauftragten zur Begutachtung der datenschutzrechtlich relevanten Bereiche.
- Vertragsvereinbarungen mit EfA-Online-Dienst-Anbieter treffen, Klärung von Themen wie z. B. Betriebs- und Supportzeiten.

VII Ansprechpartner und weiterführende Informationen

VII.1 Ansprechpartner

Ansprechpartner mit Relevanz für das Antragsrouting sind in Tabelle 3 aufgeführt:

Tabelle 3: Ansprechpartner mit Relevanz für das Antragsrouting

Thema	Organisation - (Name)	Kontaktinformationen
Feedback zu dieser Anleitung	d-NRW	ozg@d-nrw.de
Antragsrouting (Land)	d-NRW	ozg@d-nrw.de
Antragsrouting (Kommune)	KDN	servicekonto@kdn.de

OZG-Koordination (Land)	d-NRW	ozg@d-nrw.de
OZG-Koordination (Kommune)	KDN	
Serviceportal.NRW / Fachportale (IT.NRW)	d-NRW	serviceportal@d-nrw.de
Kommunalportal.NRW	KDN	kommunalportal@kdn.de
OSCI-Intermediär (NRW Kommune)	Dataclearing NRW	info@krzn.de
OSCI-Intermediär (NRW Land)	IT.NRW – Referat 424 „eGovernment Infrastrukturdienste“	virtuelle-poststelle@it.nrw.de
DVDV (Land und Kommune)	Dataclearing NRW	
ZDI	IT.NRW	zdi-cc@it.nrw.de
Governikus MultiMessenger (Land)	IT.NRW	virtuelle-poststelle@it.nrw.de

VII.2 Weiterführende Informationen

Für das Antragsrouting relevante Dokumente sind in Tabelle 4 aufgeführt.

Tabelle 4: Für das Antragsrouting relevante Dokumente

Name des Dokuments	Quelle
EfA-Mindestanforderungen	https://ozg.nrw/system/files/media/document/file/EfA-Mindestanforderungen_Version%201.0.pdf
Spezifikation OSCI Version 1.2	http://www.osci.eu/ws/2014/10/transport/OSCIV2.02_WS-ProfilingAndExtensionSpecification.pdf
Spezifikation XTA 2 Version 3	https://www.xrepository.de/api/xrepository/urn:xoev-de:ko-sit:standard:xta2_3:dokument:Spezifikation_XTA_2_Version_3
Spezifikation XTA (allgemein)	https://www.xoev.de/downloads-2316#XTA

Leitfaden für die Erstellung eines DVDV Eintragungskonzeptes in NRW	https://ozg.nrw/service/dokumente
Governikus Handreichung (Voraussetzungen für einen Transport der Antragsdaten und Inhalt Transportprofil)	Anhang dieses Dokuments, siehe Kapitel VIII

Ergänzend dazu enthält die Ablage <https://ozg.nrw/service/dokumente> weitere OZG-relevante Dokumente.

VIII Anhang - Handreichung Governikus

Die unten aufgeführte Handreichung umfasst grundsätzliche Voraussetzungen für einen Transport von Antragsdaten über einen OSCI-Intermediär sowie den Inhalt eines Transportprofils. Sie wurde von der Fa. Governikus KG erstellt und begrifflich auf die vorliegende Anleitung ausgerichtet.

VIII.1 Voraussetzungen

Folgende Punkte gelten als grundsätzliche Voraussetzungen für einen Transport von Antragsdaten über einen OSCI-Intermediär:

- Autor und Leser haben sich auf ein Transportprofil geeinigt.
- Das Transportprofil verwenden Sender und Empfänger im Auftrag von Autor und Leser.
- Das Transportprofil sollte als Teil des Fachstandards der zu übertragenen Daten definiert werden, weil der Schutzbedarf von der Sicherheitseinstufung der zu übertragenden Daten abhängt.
- Die OSCI-Spezifikation kann nur einen Rahmen und Mindestanforderungen an die kryptographischen Algorithmen festlegen. Aus dem Schutzbedarf der zu übertragenden Daten resultiert die Vorgabe, ob die Nachrichten signiert (Integritätssicherung oder Authentizität oder Nicht-Abstreitbarkeit) oder verschlüsselt (Vertraulichkeit) werden müssen.
- Eine Fachnachricht liegt vor (ggf. ist diese mehrteilig und vorzugsweise im XML-Format aufgebaut).
- Zertifikate für Verschlüsselung und ggf. Signatur liegen dem Autor vor (sie können z. B. aus dem DVDV abgerufen werden), d. h. das Zertifikat mit dem öffentlichen Schlüssel des Lesers für die Inhaltsdaten.
- Zertifikate für Verschlüsselung und ggf. Signatur liegen dem Sender vor (sie können z. B. aus dem DVDV abgerufen werden), d. h.:
 - Das Zertifikat mit dem öffentlichen Schlüssel des Empfängers
 - Das Zertifikat mit dem öffentlichen Schlüssel des Intermediärs für die Verschlüsselung der OSCI-Auftragsdaten.

VIII.2 Inhalt Transportprofil

Ein Transportprofil muss folgendes festlegen:

- die Nutzung von Zertifikaten
- die Quelle der für die Datenübermittlung benötigten, technischen Kommunikationsparameter
- die Signatur von Inhaltsdaten
- die Verschlüsselung von Inhaltsdaten
- die Signatur von Nutzungsdaten

- die Verschlüsselung von Nutzungsdaten
- das Kommunikationsszenario
- die technischen Eigenschaften der Dienste (bspw. verwendetes Transportprotokoll HTTP)
- die Struktur der Inhaltsdaten (welche Content Container mit welchen Contents müssen / dürfen verwendet werden)
- die zu verwendenden kryptographischen Algorithmen