
Konzeption Datenaustauschplattform auf Basis kommunaler Lösung

Version 1.0 (Stand: 13.02.2020)

DETECON
CONSULTING



INHALT

1.	Ausgangssituation	5
2.	Vorgehen	5
2.1	Aufgabenbeschreibung	5
2.2	Methodik	5
2.3	Nutzen	6
3.	Beschreibung Ist-Stand Datenaustauschplattform	7
3.1	Datenaustauschplattform im Kontext der OZG IT-Architektur	7
3.2	DataClearing NRW	8
3.2.1	Deutsches Verwaltungsdienstverzeichnis (DVDV)	10
3.2.2	Governikus Anwendung	11
3.2.3	OSCI (Online Services Computer Interface)*	12
3.2.4	XTA/XTA2*	13
3.2.5	XöV	13
3.3	Schnittstellen zwischen den Komponenten	14
4.	Bewertung Datenaustauschplattform hinsichtlich der Befähigung zur zentralen Landeslösung	15
4.1	Governance / Architektur	15
4.2	Verfügbarkeit	16
4.3	Erweiterbarkeit / Skalierung	17
4.4	Technologische Rahmenbedingungen	17
4.5	Sicherheit	18
5.	Empfehlungen und nächste Schritte	18
5.1	Klärung der Anforderung Empfangsbestätigung/Push-Nachricht	18
5.2	Planung der Erweiterungen der Infrastruktur für die Datenaustauschplattform	19
5.3	Organisatorische Aspekte	19

5.4	Anbindung von Empfängern	21
6.	Zusammenfassung	21
7.	Glossar/Abkürzungsverzeichnis	22
8.	Quellen	24
9.	Kontakt	24
10.	Anlagen	24
10.1	Interviewleitfaden und -ergebnisse	24
10.2	DVDV Deutsches Verwaltungsdiensteverzeichnis	25
10.3	OSCI-Transport_Spezifikation-Version_1.2	25
10.4	Umsetzung OZG IT-Architektur für AG-Technik	25

Abbildungsverzeichnis

Abbildung 1:Zielbild der benötigten Schnittstellen im Dokument OZG - IT Architektur für AG Technik V1.3	7
Abbildung 2: Exemplarisches Beispiel für die Kommunikation über OSCI	9
Abbildung 3:DVDV Architektur	10
Abbildung 4: Aufgabenspektrum des IT Planungsrats	12
Abbildung 5:DataClearing NRW als Standard auf Basis der Beschlüsse und Produkte de IT-Planungsrats	16

1. Ausgangssituation

Im Rahmen der Umsetzung des Onlinezugangsgesetzes (OZG) müssen die Verwaltungen von Bund, Ländern und Kommunen ihre Verwaltungsleistungen auch online anbieten. Als Ergebnis einer umfassenden Betrachtung der deutschen Verwaltungsleistungen wurden 575 gemäß OZG zu digitalisierende Leistungen identifiziert, in 35 Lebens- und 17 Unternehmenslagen gebündelt und im so genannten OZG-Umsetzungskatalog beschrieben (Quelle: IT-Planungsrat).

Die Umsetzung des OZG in NRW wird in 2020 durch die Weiterentwicklung der Standard Portalplattform des Landes NRW „nrwGOV OZG“ begonnen. Für die angestrebte Gesamtarchitektur liegt eine funktionale Beschreibung der Basiskomponenten erstellt von IT.NRW mit dem Stand vom 31.10.2019 vor. Basis für den sicheren Austausch von Datennachrichten (Formularen) ist eine leistungsfähige Integrationsplattform. Die Architektur sieht eine asynchrone Datenvermittlung auf Landesebene und kommunaler Ebene vor.

Bereits heute ist hierzu die Lösung **DataClearing NRW** des KRZN Kamp-Lintfort und der citeq Münster für einzelne Verfahren (XMeld, XhD, XAusländer, XPersonenstand, XGewerbeanzeige, XBau) in Betrieb oder geplant und wird für o.a. Verfahren zwischen den Behörden auf Landesebene und kommunaler Ebene eingesetzt.

2. Vorgehen

2.1 Aufgabenbeschreibung

Die angestrebte Gesamtarchitektur zur Umsetzung des OZG in NRW setzt zwingend eine Datenaustauschplattform zwischen Portalen (mit Anträgen) und den Fachverfahren (in den bearbeitenden Behörden auf kommunaler Ebene und Landesebene) voraus.

Eine solche Lösung existiert bereits im kommunalen Kontext (DataClearing NRW, ein Angebot des KRZN Kamp-Lintfort und der citeq Münster).

Aufgabe ist es diese Lösung hinsichtlich der Nutzbarkeit für die angestrebte Gesamtarchitektur zu analysieren. Insbesondere soll herausgearbeitet werden inwieweit die bisherige Lösung zu einer zumindest temporären Lösung für Landesdienste befähigt werden kann und ob diese Lösungsarchitektur auch als Plattform für Landes- und kommunale Dienste Verwendung finden kann.

2.2 Methodik

Für die Analyse wurden vorhandene Konzepte und Dokumente sowie allgemein zugängliche Informationen aus dem Internet recherchiert und analysiert.

Für die Analyse standen die folgenden Dokumente bzw. Informationen aus dem Internet zur Verfügung:

- > OZG - IT Architektur für AG Technik V1.0
- > OZG - IT Architektur für AG Technik V1.3
- > Konzept zur Umsetzung des Bauportal.NRW Version 0.99 (Stand: 05.08.2019)
- > Infobroschüre: https://www.dataclearing-nrw.de/fileadmin/pdf/broschuere_dataclearing.pdf
- > Informationen des IT-Planungsrats: www.it-planungsrat.de
- > Informationen zum IT-Dienstleister des Bundes: www.itzbund.de
- > Deutsches Verwaltungsdienstverzeichnis (DVDV): www.itzbund.de/DE/Produkte/DVDV/DVDV_Uebersicht/DVDV_Uebersicht_node.html
- > Infos zu DataClearing NRW: www.dataclearing-nrw.de/basis-dienste.html
- > Informationen zu Governikus KG: www.governikus.de
- > Informationen der IT-Dienstleister des Bundes: www.itzbund.de
- > Koordinierungsstelle für IT-Standards (KoSIT): www.xoev.de
- > Informationen zu XÖV-Standards und Codelisten: www.xrepository.de und www.xoev.de

Darüber hinaus wurde ein strukturiertes Interview mit dem heutigen Betreiber der Lösung DataClearing NRW geführt welches wesentlichen Input zu der vorliegenden Analyse geliefert hat.

Für das Experteninterview zu der bereits im Einsatz befindlichen Lösung „DataClearing NRW“ wurde als Ansprechpartner benannt:

Dr. Lars van der Grinten

Kommunales Rechenzentrum Niederrhein

Der Interviewleitfaden sowie die Ergebnisse dieses Interviews finden sich in den Anlagen dieses Dokuments.

2.3 Nutzen

Durch die in diesem Dokument beschriebene Analyse wird ein mögliches Anwendungsszenario für die Datenaustauschplattform als wesentliche Komponente der OZG Architektur untersucht. Es werden auf Basis der vorliegenden Dokumente sowie des durchgeführten Interviews folgende Fragestellungen beantwortet:

- Analyse der durch IT.NRW bereitgestellten funktionalen Beschreibung der Basiskomponenten, inwieweit die kommunale Lösung zu einer, zumindest temporären Lösung für Landesdienste befähigt werden kann.
 - Bewertung, ob diese Lösung auch dauerhaft als einzige Plattform für Landes- und kommunale Dienste Verwendung finden kann.
-

3. Beschreibung Ist-Stand Datenaustauschplattform

3.1 Datenaustauschplattform im Kontext der OZG IT-Architektur

Auf Basis des Anwendungsfalls „elektronischen Antrag einreichen“ sind die entsprechenden technischen Komponenten sowie ihre Funktionalitäten und Schnittstellen für die IT-Architektur OZG beschrieben. Der aktuelle Arbeitsstand des Dokuments OZG Architektur AG-Technik findet sich in den Anlagen dieses Dokuments.

Aus der angestrebten Architektur und dem Prozess zur Abwicklung der Verfahren ergibt sich die Notwendigkeit einer Integrationsplattform zur Abwicklung des Datenaustauschs zwischen den Serviceportalen und den Fachanwendungen auf Landesebene und kommunaler Ebene.

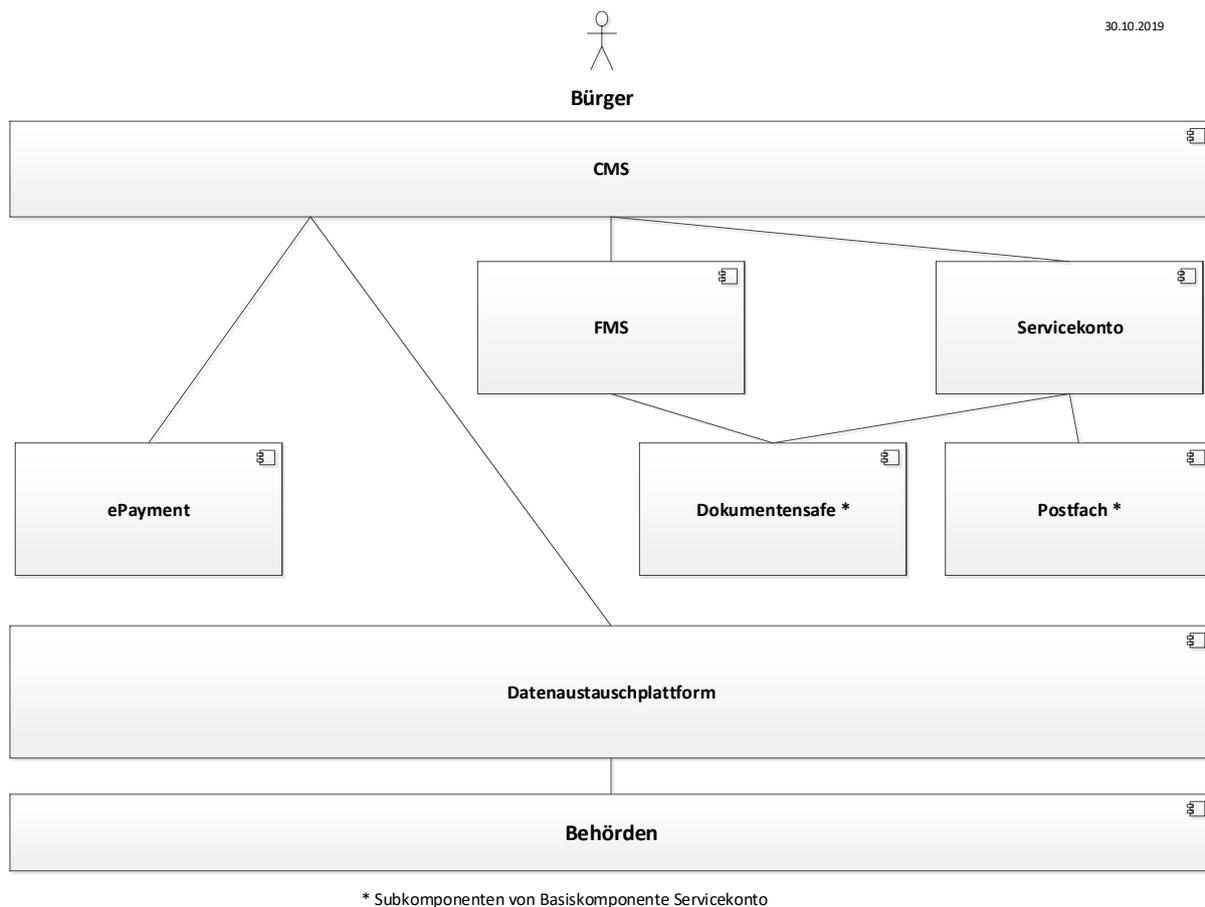


Abbildung 1: Zielbild der benötigten Schnittstellen im Dokument OZG - IT Architektur für AG Technik V1.3

Die Anforderungen an die Datenaustauschplattform sind in der OZG Architektur AG-Technik wie folgt dokumentiert:

Die Datenaustauschplattform dient der Bereitstellung/der Übergabe von Anträgen an die Behörden und Fachverfahren. Hierfür werden alle relevanten Daten eines Antrags bereits im richtigen Format (XÖV-gemäß) vom CMS an sie übermittelt. Der Empfang wird durch den Versand einer Bestätigungsmail an das im Servicekonto vorhandene Postfach des Bürgers / der Bürgerin quittiert.

Anmerkung: Der Versand der Empfangsbestätigung kann nicht durch die Datenaustauschplattform erfolgen, da diese verschlüsselte Dateninhalte zwischen Systemen transferiert. Die Ermittlung der Absenderadresse aus den Dateninhalt ist somit nicht möglich. Es wird angenommen, dass die Zustellung einer Empfangsbestätigung nur durch das entsprechende Fachverfahren und die zuständige Behörde direkt an den Bürger oder über das Serviceportal gesendet werden soll. Die Datenaustauschplattform quittiert nur gegenüber dem Portal den Empfang einer Datei.

3.2 DataClearing NRW

Unter dem Namen DataClearing NRW steht den Kommunen in NRW ein zentraler Dienst des KDN zur Verfügung. Betrieben wird diese zentrale Clearingstelle durch die beiden kommunalen Rechenzentren citeq Münster und Kommunales Rechenzentrum Niederrhein (KRZN) Moers.

Drei zentrale IT-Dienste bilden die Voraussetzung, um einen sicheren und vollautomatisierten Datenaustausch auf der Basis von OSCI zu realisieren:

- > Deutsches Verwaltungsdienstverzeichnis (DVDV)
- > eine OSCI-Vermittlungsstelle (Intermediär) - Produkt Governikus der Fa. Governikus - und damit die gleiche Lösung wie die Landesverwaltung NRW, die Bundesebene und insgesamt 12 weitere Bundesländer
- > OSCI-Schnittstellen bzw. Schnittstellensoftware zu den Fachanwendungen der Behörden auf Landes und kommunaler Ebene

In den folgenden Unterkapiteln 3.2.1 DVDV, 3.2.2 Governikus Anwendung, 3.2.3 OSCI, 3.2.4 XTA2/XTA und 3.2.5 XöV werden die eingesetzten Dienste und Standards kurz beschrieben.

Die folgenden Übermittlungsstandards: XMeld, XhD, XAusländer, XPersonenstand, XGewerbeanzeige, XBau sind bereits heute in Betrieb oder in Planung.

DataClearing NRW:

- > stellt auf einer zukunftssicheren technologischen Basis und aus einer Hand alle erforderlichen zentralen Dienste für eine sichere Datenübermittlung im öffentlichen Bereich bereit.
 - > betreibt hierzu den NRW-Server für das Deutsche Verwaltungsdienstverzeichnis (DVDV), einen Intermediär für NRW sowie Schnittstellenlösungen für den Anschluss der Fachverfahren.
-

- > nutzt als OSCI-Intermediär das Produkt Governikus der Governikus KG und damit die gleiche Lösung wie die Landesverwaltung NRW, die Bundesebene und insgesamt 12 weitere Bundesländer
- > erfüllt mit der aufgebauten Infrastruktur bereits heute die Anforderungen an zukünftige Datenübermittlungen.
- > unterstützt durch die gewählten Standardkomponenten die reibungslose Kommunikation zwischen den Kommunen untereinander und mit der Landesverwaltung NRW

(Quelle: dataclearing-nrw.de , Stand Dezember 2019)

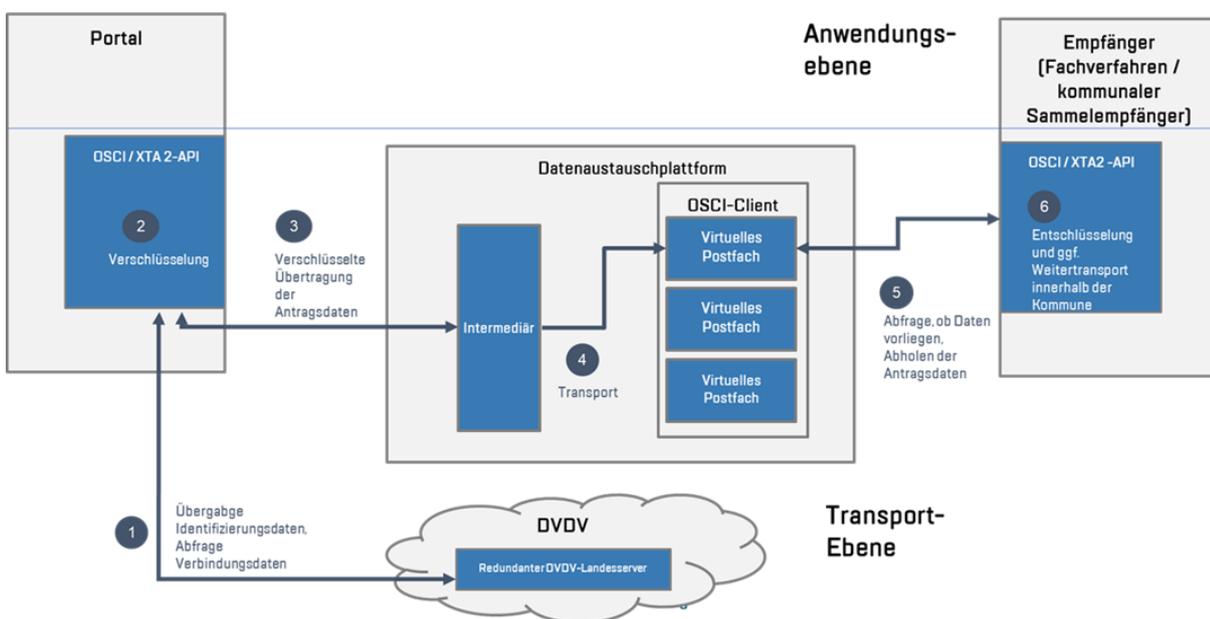


Abbildung 2: Exemplarisches Beispiel für die Kommunikation über die Datenaustauschplattform

In Abbildung 2 wird der Prozess des Versands der Antragsdaten über die Datenaustauschplattform dargestellt. Das Portal erfragt beim DVDV mithilfe einer Dienstziffer (8-12 Ziffern) und dem Schlüssel der Behörde (3-stellig) die Verbindungsdaten (Schritt 1). Die Antragsdaten werden verschlüsselt und anschließend an die Datenaustauschplattform übergeben (Schritt 2/3). Die Plattform legt die Antragsdaten in das virtuelle Postfach der Empfängerbehörde ab (Schritt 4). Auf der Plattform liegen die Daten verschlüsselt, der Plattform sind nur die Adressdaten bekannt. Die Empfängerbehörde fragt periodisch ab, ob Daten im virtuellen Postfach vorliegen und holt diese ab (Schritt 5). Nach Abholung werden sie auf der Plattform mit einem Flag versehen und nach Ablauf einer Frist gelöscht. Die empfangende Behörde entschlüsselt die Antragsdaten und leitet sie ggf. innerhalb der Behörde weiter (Schritt 6).

3.2.1 Deutsches Verwaltungsdienstverzeichnis (DVDV)

Das Deutsche Verwaltungsdienstverzeichnis (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. Das DVDV wird in einem kooperativen Betreibermodell durch Bund, Länder und Kommunen bereitgestellt und in gemeinsamer Verantwortung im IT-Planungsrat durch das Hersteller- und Pflegekonsortium von Governikus und Dataport fortentwickelt.

Das DVDV ist die fach- und verwaltungsübergreifende Infrastrukturkomponente für die sichere und verlässliche Adressierung von automatisierten Diensten und Fachverfahren zur Kommunikation zwischen und mit Behörden der öffentlichen Verwaltung in Deutschland.

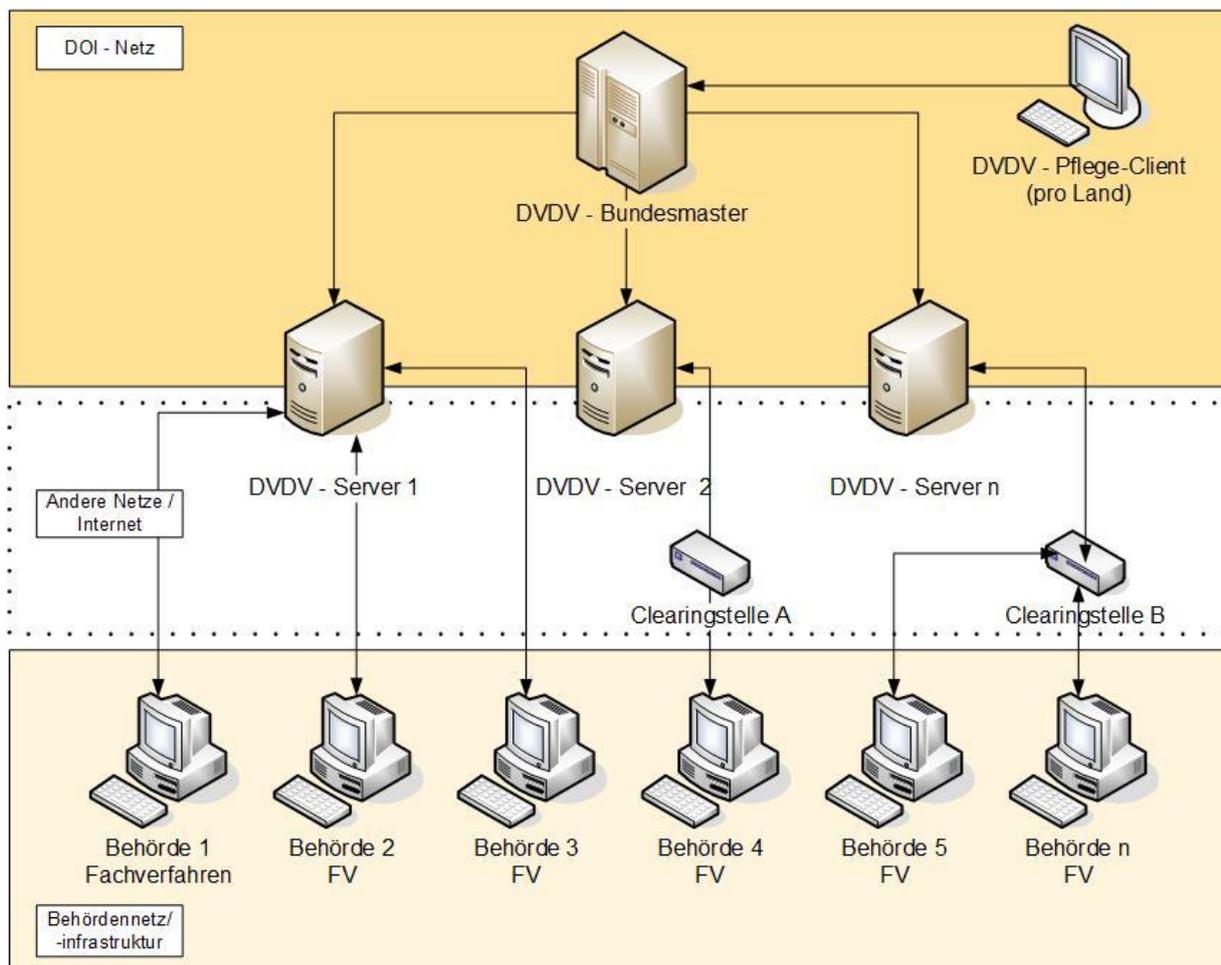


Abbildung 3: DVDV Architektur

Es eröffnet damit die Möglichkeit, E-Government-Transaktionen auf der Basis Service-orientierter Architekturen in sicherer und rechtsverbindlicher Weise anzubieten.

(Quelle: itzbund.de, Stand: Dezember 2019)

3.2.2 Governikus Anwendung

Mit der Anwendung Governikus des IT-Planungsrates stehen Bund, Ländern und Kommunen wichtige Bausteine/Basiskomponenten für Digitalisierungsvorhaben im gesamten Lebenszyklus elektronischer Kommunikation, Dokumente und Daten zur Verfügung.

Das Leistungsspektrum der Anwendung wurde im Laufe der Jahre erheblich erweitert. Ursprünglich als Middleware für die Datenübermittlung auf Basis des OSCI-Transportprotokolls konzipiert, bei dem bereits Signaturen und Kryptografie sowie die Authentisierung eine große Rolle spielten, enthält die Anwendung inzwischen Produkte und Funktionsmodule für die Handlungsfelder eID, sichere Datenübermittlung, Ver- und Entschlüsselung, elektronische Signaturen/Siegel und ihre Verifikation sowie TRESOR-konforme Beweiswerterhaltung.

Die Anwendung Governikus ermöglicht eine gesetzeskonforme Verarbeitung und vertrauliche Ende-zu-Ende-verschlüsselte Übertragung von Daten und Dokumenten. Governikus steht flächendeckend Bund, Ländern und Kommunen zur Verfügung. Die Pflege der Anwendung wird über den Pflegevertrag Governikus, dem alle Bundesländer beigetreten sind, sowie dem Pflegevertrag zur VPS des Bundes finanziert. Der Vertrag mit den Ländern beinhaltet auch die kontinuierliche Weiterentwicklung. Die Kosten werden gemäß Königssteiner Schlüssel anteilmäßig von den Ländern getragen. Über den Vertrag zur VPS des Bundes können separat bedarfsorientiert vom Bund zusätzliche Weiterentwicklungen beauftragt werden.

Die Anwendung Governikus wird kontinuierlich bedarfsorientiert und in Abstimmung mit unseren Kunden weiterentwickelt. Im regelmäßigen Erfahrungs- und Abstimmungsaustausch werden mit Vertretern aus Bund und Ländern in den Gremien "Betreiberausschuss" und "Technikausschuss" über gesetzliche und technische Neuerungen und Herausforderungen diskutiert und sodann dem Gremium "Lenkungsausschuss" vorgelegt. Dieser Ausschuss entscheidet zweimal jährlich über die vorhandene Mittelverwendung für Pflege und Support.

Die Nutzung der Weiterentwicklungen von Bund und den Ländern stehen allen Beteiligten zur Verfügung.

(Quelle: governikus.de, Stand Dezember 2019)

Der IT-Planungsrat koordiniert die Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik, beschließt IT-Interoperabilitäts- und IT-Sicherheitsstandards, steuert E-Government-Projekte und plant bzw. entwickelt das Verbindungsnetz weiter.

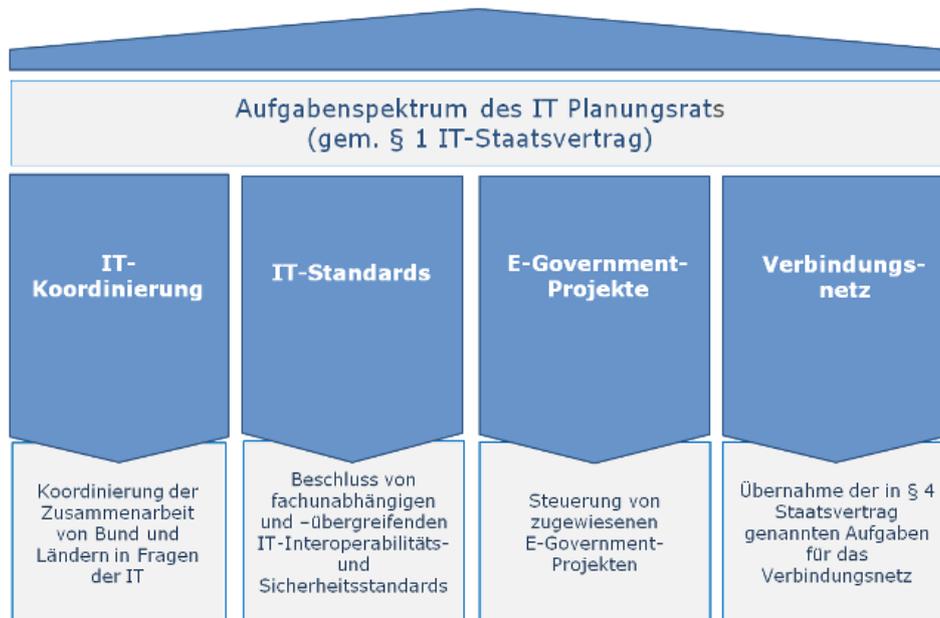


Abbildung 4: Aufgabenspektrum des IT Planungsrats

In diesem Kontext entscheidet der IT-Planungsrat (neben vielen weiteren Themen) über Ausprägung und Weiterentwicklung der zugrundeliegenden Produkte, Protokolle und Komponenten der DataClearing NRW Plattform.

(Quelle: it-planungsrat.de, Stand Dezember 2019)

3.2.3 OSCI (Online Services Computer Interface)*

OSCI (Online Services Computer Interface) basiert auf den vom W3C koordinierten, weltweit anerkannten Standards XML und SOAP. Die Empfehlungen des W3C zur digital signature werden in geeigneter Weise konkretisiert, um die rechtlichen Anforderungen zu erfüllen. Dabei unterstützt OSCI von der fortgeschrittenen bis hin zur akkreditierten elektronischen Signatur alle Qualitätsniveaus. Zudem werden für die Verschlüsselungsverfahren ebenfalls genaue Vorgaben gemacht, um auch auf dieser Ebene die Interoperabilität und Herstellerunabhängigkeit sicherzustellen.

Der Name OSCI (Online Services Computer Interface) steht für mehrere Protokolle, deren gemeinsames Merkmal die besondere Eignung für das E-Government sind:

- > Die sichere und vertrauliche Übertragung digital signierter Dokumente über das Internet. Dies ist beschrieben in OSCI-Transport.

- > Die Standardisierung von Inhaltsdaten, damit strukturierte Dokumente medienbruchfrei und effizient verarbeitet werden können. Hier gibt es mehrere Projekte, z. B. das Datenaustauschformat XMeld für Geschäftsvorfälle des Meldewesens.
- > Außerdem definiert OSCI die notwendigen Datenstrukturen für Quittungsmechanismen mit Zeitstempeln. Ähnlich dem "Einschreiben mit Rückschein" ist beweisbar, dass eine Nachricht den Empfänger erreicht hat, und wann dies geschehen ist.

Zuständig für die Entwicklung der fachlichen Standards, sowie deren Pflege und Weiterentwicklung ist die Koordinierungsstelle für IT-Standards (KoSIT).

Die Eignung von OSCI für die Anforderungen des E-Government sowie die Erfüllung der einschlägigen europäischen Sicherheitsanforderungen wird durch ein Gutachten des BSI bestätigt. Für die einschlägigen DV-Anwendungen des Bundes wird OSCI durch das SAGA 5.0 Modul Technische Spezifikationen empfohlen.

(Quelle: itzbund.de, Stand: Dezember 2019)

3.2.4 XTA/XTA2*

XTA/XTA2 ist ein vom IT-Planungsrat empfohlener Interoperabilitätsstandard zur Einbindung von IT-Fachapplikationen in eine Infrastruktur für Nachrichtenübermittlung.

XTA (XÖV Transport Adapter) definiert einen Webservice für die Anbindung von IT-Fachapplikationen an eine technische Infrastruktur für Nachrichtenübermittlung (Transportverfahren). Diese Webservice-Definition (genannt XTA-Webservice) ist für alle Fachlichkeiten einsetzbar. Außerdem bietet XTA Definitionen für Struktur und Semantik von "Service Profilen" an. Mittels eines instanziierten "XTA Service Profils" formuliert eine Fachlichkeit die durch sie geforderten Service Qualitäten für die Nachrichten- und Datenübermittlung dieser Fachlichkeit.

(Quelle: xrepository.de und xoev.de, Stand: Dezember 2019)

*** Zur Beschreibung der Anforderungen an einen Parallelbetrieb von XTA2 und OSCI in einer Datenaustauschplattform wird ein Workshop durchgeführt, zu dem Vertreter von Dataclearing und Governikus eingeladen werden.**

3.2.5 XöV

Mit dem XÖV-Standardisierungsrahmen wird der öffentlichen Verwaltung eine gemeinsam abgestimmte und einheitliche Vorgehensweise zur Entwicklung von IT-Standards geboten. Das Regelwerk des Standardisierungsrahmens stellt sicher, dass die Entwicklung neuer Standards auf der Basis gemeinsamer Methoden, Konzepte und Gestaltungsrichtlinien erfolgt. Durch diese Festlegung ist es möglich, die Qualität der Standards im Rahmen der IT-Zertifizierung anhand der im Rahmenwerk definierten Konformitätskriterien objektiv festzustellen und so die notwendige Investitionssicherheit zu gewährleisten.

Das dem Rahmenwerk zugrundeliegende Prinzip der Wiederverwendung von Komponenten und Methoden stellt sicher, dass bei der Entwicklung neuer Standards die Ergebnisse und Erfahrungen bereits bestehender Standards genutzt werden. So wird nicht nur die Effizienz und Qualität bei der Entwicklung neuer Standards gesteigert sondern auch die Interoperabilität über die Grenzen von Fachverfahren gesteigert.

Der XÖV-Standardisierungsrahmen wurde mit der Absicht entworfen, die systematische Entwicklung und Bereitstellung von IT-Standards für den elektronischen Datenaustausch im E-Government zu fördern, sodass elektronische Prozesse für die Verwaltung kostengünstig, schnell und mit hoher Qualität umgesetzt werden können.

Basierend auf einer Reihe von abgestimmten Regeln soll der im XÖV-Handbuch dokumentierte XÖV-Standardisierungsrahmen einen effizienten Ansatz bieten, Standards zur Datenübermittlung zu entwickeln, zu betreiben und aufeinander abzustimmen.

(Quelle: xoev.de, Stand: Dezember 2019)

3.3 Schnittstellen zwischen den Komponenten

An dieser Stelle wird der Prozess des Zusammenspiels der Komponenten beschrieben. Für eine detaillierte Schnittstellenbeschreibung aller Schnittstellen zwischen den Komponenten müssen weitere Interviews mit technischen Experten geführt werden. Ein Dokument zur Beschreibung der Schnittstelle für den Austausch von XÖV Daten über OSCI ist hier einsehbar: https://www.itzbund.de/static/download/Produkte/XOeV/OSCI-Transport/OSCI-Transport_Spezifikation-Version_1.2-2002-06-02.pdf Zur Vollständigkeit ist diese auch im Anhang 10.3 dieses Dokuments verfügbar.

Für den Transport der Antragsdaten über die Plattform wird der folgende generische Prozess angenommen:

- > Das Portal möchte Behörde A (bearbeitende Zielbehörde) einen Antrag eines Bürgers übermitteln.
 - > Behörde A stellt eine Anfrage an den zuständigen DVDV-Landesserver. Zur eindeutigen Identifizierung übermittelt das Portal Informationen an den DVDV-Landesserver (z.B. Identifikationsmerkmal der bearbeitenden Behörde und des Services).
 - > Der DVDV-Landesserver sucht mit den Informationen im eigenen Verzeichnis die Daten der Zielbehörde. Der DVDV-Landesserver findet die Daten der Zielbehörde und gibt dem Portal die Kommunikationsdaten (z.B. Adressdaten) als Antwort.
 - > Das Portal bereitet die XöV Datei für das entsprechende Verfahren mit den Antragsdaten des Bürgers auf, verschlüsselt diese und übergibt diese mit den Daten der Zielbehörde an den Intermediär.
 - > Der Intermediär quittiert dem Portal den Empfang der Nachricht, die Existenz des angeforderten Dienstes und die Existenz der gewünschten Zielbehörde.
 - > Der Intermediär nimmt die Daten entgegen und legt diese für die Abholung durch die bearbeitende Behörde ab.
-

- > Die bearbeitende Behörde fragt regelmäßig bei dem Intermediär an, ob Nachrichten zur Bearbeitung vorliegen und holt diese Nachrichten ab.
- > Der Intermediär protokolliert den Prozess und die entsprechenden Zeitstempel. Abgeholte Nachrichten löscht der Intermediär von der Datenaustauschplattform.
- > Das Fachverfahren in der Zielbehörde entschlüsselt die Datennachricht und verarbeitet die XöV Datei.

4. Bewertung Datenaustauschplattform hinsichtlich der Befähigung zur zentralen Landeslösung

Die Bewertung der Datenaustauschplattform erfolgt im Wesentlichen auf Basis der Ergebnisse des Interviews vom 09.12.2019.

Die Bewertung erfolgt nach den Kriterien:

- > Governance / Architektur
- > Verfügbarkeit
- > Erweiterbarkeit / Skalierung
- > Technologische Rahmenbedingungen
- > Sicherheit

4.1 Governance / Architektur

Die Lösung DataClearing NRW wird durch das KRZN Kamp-Lintfort und der citeq Münster betrieben und bietet auf Basis der Produkte der Governikus KG eine Plattform für den Datenaustausch (Intermediär) zwischen Kommunikationspartnern über die im öffentlichen Bereich gebräuchlichen Verfahren an. Die Lösung besteht im Wesentlichen aus dem Betrieb des DVDV (Deutsches Verwaltungsdienstverzeichnis) für Nordrhein-Westfalen und dem Governikus-Intermediär für die sichere Datenübermittlung zwischen Anwendungen. Die Nutzung der Plattform durch die Kommunen des Landes NRW erfolgt durch den Beitritt zum Governikus Pflegevertrag. Aktuell sind 396 Kommunen in NRW an der Plattform angeschlossen und tauschen ca. 10-15 Mio. Nachrichten pro Jahr über die Intermediärplattform aus.

Die Weiterentwicklung und die Umsetzung von Change Requests wird durch die Einflussnahme des IT-Planungsrats auf das Produkt gewährleistet und durch die Governikus KG umgesetzt.

Der Betreiber DataClearing NRW betreibt die Datenaustauschplattform als Software as a Service und muss entsprechend dem Datenaufkommen, welches durch die OZG-Umsetzung entsteht, weitere Ressourcen zur Verfügung stellen. Dies muss in Absprache mit den beteiligten Stakeholdern erfolgen. Siehe zur Skalierbarkeit Kapitel 4.3.

DataClearing NRW setzt dabei auf den durch den IT-Planungsrat und der KoSIT beschlossenen Standards OSCI, XTA/XTA2 und XöV auf und setzt die empfohlenen Produkte des Deutschen Verwaltungsdienstverzeichnis (DVDV) und der Governikus KG für den Betrieb der Infrastruktur zum sicheren Austausch von Daten zwischen den Behörden ein.



Abbildung 5: DataClearing NRW als Standard auf Basis der Beschlüsse und Produkte de IT-Planungsrats

Grundsätzlich ist auf Basis der o.a. Standards ein sicherer und verschlüsselter Datenaustausch auf Landesebene, auf kommunaler Ebene und zwischen Landesebene und kommunaler Ebene möglich. Dabei hat der Betreiber des „Transportsystems“ keinen Zugang zu den verschlüsselten Daten der Kommunikationspartner.

Es ist unter Datenschutzaspekten umstritten, ob es sich bei dem Transport verschlüsselter Nachrichten um Auftragsdatenverarbeitung handelt. Dies ist im Einzelfall durch Datenschutzbeauftragte zu überprüfen. Durch technisch-organisatorische Maßnahmen wie den Abschluss einer Auftragsdatenverarbeitungserklärung ist eine, die datenschutzrechtlichen Vorgaben einhaltende Umsetzung möglich.

Derzeit finanziert sich der Service DataClearing NRW durch die teilnehmenden Kommunen. Über einen Umlageschlüssel, der von der Bevölkerungszahl abhängig ist wird ein Gesamtpreis je Kommune errechnet. Es ist zu erwarten, dass die Anforderungen des OZG an die Leistung der Datenaustauschplattform, Investitionen in Infrastruktur aber auch Personal erforderlich machen. Weiterhin kommen auch Nutzer auf Landesebene hinzu. Abhängig von den zukünftigen Mengengerüsten und Datenvolumen muss das Verrechnungsmodell angepasst werden und die Investitionsrisiken durch die Stakeholder übernommen werden.

Als Finanzierungsmodell ist zwischen nutzungsabhängigen Modellen (Pay per Use) oder pauschalen Festbeträgen abzuwägen.

4.2 Verfügbarkeit

Um eine hohe Verfügbarkeit der Lösung zu erreichen, ist die Infrastruktur für die Datenaustauschplattform derzeit redundant ausgelegt. Aktuell sind keine Aufzeichnungen/Statistiken über auftretende Störungen bei dem Betreiber DataClearing NRW verfügbar. Die auftretenden Störungen sind nach Einschätzung des Betreibers zu über 90% inhaltliche Datenfehler und nicht in der Datenaustauschplattform selbst begründet. Der Datenaustausch wird kontinuierlich durch den Betreiber überwacht und Störungen aktiv mit den Kommunikationspartnern (Sender/Empfänger) behoben. Hinsichtlich der Infrastruktur entspricht die Lösung bereits den Anforderungen zur Nutzung als zentrale Lösung. Hinsichtlich der Verfügbarkeit empfehlen wir für eine vollumfängliche Befähigung zur zentralen Lösung die Etablierung von IT Service Management nach ITIL. Siehe dazu Kapitel 5.3.

4.3 Erweiterbarkeit / Skalierung

Eine Erweiterung der heute zur Verfügung stehenden Ressourcen ist durch einen Ausbau der technischen Infrastruktur (Netze, Loadbalancer, Server, usw.) möglich. Der DVDV auf Landesebene NRW wird derzeit auf zwei Servern an unterschiedlichen Standorten betrieben. Es erfolgt eine automatische Lastverteilung zwischen den beiden Servern. Der Intermediär wird über Cluster mit 6 Servern betrieben. Die Anzahl der Server ist dynamisch erweiterbar. Grenzen sind derzeit nicht bekannt. Für große Lasten eines bestimmten Services ist bedarfsweise auch eine eigene dedizierte Infrastruktur implementierbar. Aktuell besteht auf Seiten der Governikus-Komponente eine Größenbeschränkung auf Nachrichtenebene von je 60 MB je Nachricht. Voraussichtlich werden einzelne OZG-Leistungen größere Nachrichtenvolumina benötigen.

Für diesen Fall sind unterschiedliche Lösungsszenarien machbar. Eine Erweiterung der maximalen Nachrichtengröße für die Governikus-Komponenten wird aktuell laut Interview mit DataClearing bei Governikus bereits angestrebt.

Alternativ ist der Transport über die Datenaustauschplattform nur möglich, wenn Nachrichten in einzelne kleinere Blöcke aufgeteilt werden. Das ist jedoch mit Anforderungen an Fachverfahrenshersteller verbunden, die diese Blöcke im Fachverfahren wieder zusammensetzen müssten.

Abseits der Datenaustauschplattform ist es möglich, große Dateianhänge auf Contentmanagementsystemen vorzuhalten und über die Datenaustauschplattform nur den Verweis auf die Downloadmöglichkeit an den Empfänger zu versenden.

Einer Erweiterbarkeit der existierenden Lösung ist möglich. Dazu sind voraussichtlich Infrastrukturmaßnahmen wie z.B. eine Erhöhung der Netzwerkbandbreite erforderlich. Zu Empfehlungen bezüglich der Erweiterung der Infrastruktur siehe Kapitel 5.2.

Bezüglich der Größenbeschränkung auf Nachrichtenebene wird empfohlen, über den IT Planungsrat/Governikus eine Erweiterung über 60 MB hinaus zu veranlassen.

4.4 Technologische Rahmenbedingungen

Die OSCI Dienste sind in der Regel asynchron. Die Netzwerktechnische Anbindung erfolgt über Internet oder die Netze des Bundes. Die Server stehen jeweils in einer DMZ (im Falle des Intermediärs mit vorgeschaltetem Loadbalancer). Die Weiterentwicklung der eingesetzten Produkte, Protokolle und API's wie z.B. OSCI-2 und XTA2 wird durch die Gremien des IT-Planungsrats gesteuert und vorangetrieben.

Auf Empfängerseite (beispielsweise einer kommunalen Behörde) sind die Voraussetzungen für Anbindung an die Datenaustauschplattform zu schaffen.

Das Empfänger-Fachverfahren muss über eine OSCI/XTA-Schnittstelle oder eine vorgeschaltete zentrale Komponente der Behörde verfügen, die eine entsprechende Schnittstelle enthält und die Entgegennahme der Daten von der Datenaustauschplattform sicherstellt. Tiefergehende Beschreibungen zu Nutzung der Schnittstellen sind auf der Homepage von Governikus verfügbar.

Für die verschlüsselte Kommunikation mit dem DVDV ist auf Empfängerseite ein Zertifikat (Kosten 80 EUR für drei Jahre) zu beschaffen. Zudem ist je Empfänger ein Eintrag ins DVDV vorzunehmen, bei dem u.a. die Zertifikatsdaten anzugeben sind. Die Eintragung neuer Empfänger-Einträge ins DVDV ist laufend möglich.

Darüber hinaus ist für jeden Dienst einmalig durch das Land eine Eintragung ins DVDV vorzunehmen. Die Eintragung neuer Dienste ist jeweils zum 1.5. und 1.11. eines jeden Jahres möglich.

Zu Empfehlungen hinsichtlich der Anbindung von Empfängern an die Datenaustauschplattform siehe Kapitel 5.4.

4.5 Sicherheit

Der Datenaustausch erfolgt über den Protokollstandard OSCI (Online Services Computer Interface) für die sichere, vertrauliche und rechtsverbindliche Übertragung elektronischer Daten im e-Government. OSCI wurde vom Bundesministerium des Inneren im Rahmen von SAGA als obligatorischer Standard für elektronische Transaktionen mit der Bundesverwaltung gesetzt.

Im Rahmen dieser Analyse wurden keine weiteren IT-Sicherheitsthemen bzgl. der eingesetzten technischen Infrastruktur (Netzwerke, Firewalls, Server, usw.) behandelt, da davon ausgegangen wird, dass der bereits bestehende Betrieb der Lösung DataClearing NRW durch KRZN Kamp-Lintfort und der citeq Münster die entsprechenden geltenden Regelungen des Landes NRW einhält und periodisch überprüft.

5. Empfehlungen und nächste Schritte

5.1 Klärung der Anforderung Empfangsbestätigung/ Push-Nachricht

Die Anforderungen an die Datenaustauschplattform sind in dem Dokument: OZG - IT Architektur für AG Technik V1.3 wie folgt formuliert:

Die Datenaustauschplattform dient der Bereitstellung/der Übergabe von Anträgen an die Behörden und Fachverfahren. Hierfür werden alle relevanten Daten eines Antrags bereits im richtigen Format (XÖV-gemäß) vom CMS an sie übermittelt. Der Empfang wird durch den Versand einer Bestätigungsmail an das im Servicekonto vorhandene Postfach des Bürgers quittiert.

Der Versand der Empfangsbestätigung kann nicht durch die Datenaustauschplattform erfolgen, da diese verschlüsselte Dateninhalte zwischen Systemen transferiert. Die Ermittlung der Absenderadresse aus den Dateninhalt ist somit nicht möglich. Es wird angenommen, dass die Zustellung einer Empfangsbestätigung nur durch das entsprechende Fachverfahren und die zuständige Behörde direkt an den Bürger oder über das Serviceportal gesendet werden soll.

Im oben genannten Dokument ist zudem festgehalten, dass die Datenaustauschplattform eine Nachricht für die Abholung des bereitgestellten Antrags an den Empfänger sendet. Die aktuell verwendete Lösung basiert auf einem Pull-Verfahren, bei dem der Empfänger periodisch überprüft, ob neue Nachrichten in seinem Postfach vorliegen. Eine Nachricht zur Abholung wird daher nicht benötigt. Der entsprechende Satz im Kapitel 5.7 „Senden einer Nachricht für die Abholung des bereitgestellten Antrags“ im Dokument OZG - IT Architektur für AG Technik V1.3 ist zu streichen.

5.2 Planung der Erweiterungen der Infrastruktur für die Datenaustauschplattform

Für die Umsetzung des OZG muss die Infrastruktur für die Datenaustauschplattform sowohl aus technischer als auch aus organisatorischer Sicht stark ausgebaut werden, da mit einer wesentlich höheren Nutzungsintensität des Services zu rechnen ist.

Es wird die Durchführung einer Ist-Analyse der heute genutzten Ressourcen hinsichtlich Netzwerke, Bandbreiten, Server, Mengengerüste, personelle Ressourcen empfohlen.

Zudem ist die Abschätzung der zukünftig benötigten Ressourcen vorzunehmen. Als Grundlage der Abschätzung dient eine von der Landesregierung durchzuführende Schätzung der zu erwartenden Mengengerüste bei der OZG-Umsetzung.

Auf Basis der Abschätzung der benötigten Ressourcen können ein Zeit- und Maßnahmenplan für die Erweiterung der Infrastruktur entwickelt und die Kosten dafür bewertet werden.

5.3 Organisatorische Aspekte

Neben der technischen Funktionalität der betrachteten Lösung ist auch der organisatorische Rahmen zu betrachten. Bei der Recherche zum vorliegenden Dokument wurde vor allem die technische Funktionalität betrachtet. Wenn die vorhandene Lösung als zentrale OZG-Komponente befähigt wird, steigen die Anforderungen an das Rechenzentrum hinsichtlich strukturierter organisatorischer Prozesse. Die Anzahl der Stakeholder, die Menge der potentiellen Incidents und die potentielle Schadenshöhe bei Ausfall des Rechenzentrums steigt.

Die organisatorischen Aspekte der eingesetzten Lösung sind daher ebenfalls im Detail zu betrachten, dies ist für das vorliegende Konzept nur rudimentär geschehen. Aktuell ist es beispielsweise über die Web-Seite dataclearing-nrw.de nicht möglich sich über Störungen der Services zu informieren oder über einen geschützten Bereich Störungen zu melden. Im Rahmen des Interviews konnten keine Aussagen zu Aufzeichnungen oder Statistiken über auftretende Störungen gemacht werden.

Es wird empfohlen, die Servicemanagementprozesse nach vorhandenen Standards wie z.B. ITIL auszurichten. Dies beinhaltet u.a. die Einführung und das Monitoring von Service Level Agreements nach üblichen Standards, sowie das Einrichten eines Incident Managements mit Help Desk, Ticketing und Incident-Monitoring.

Wir empfehlen, einschlägige Standards für den sicheren Betrieb der Netze und Rechenzentren zu erfüllen. Dazu zählen IT Service Management nach ISO/IEC 20000-1, IT-Grundschutz nach ISO/IEC 27001, Informationssicherheitsmaßnahmen für Cloud-Dienste nach ISO/IEC 27017 und Business Continuity Management nach ISO 22301.

Da die Lösung für den Transport der Nachrichten sowohl den Zugang über Internet- als auch über das Netz des Bundes anbietet, empfehlen wir die Durchführung von Penetrationstest zur Schwachstellenanalyse der Zugangspunkte durchzuführen, wenn dies nicht bereits turnusmäßig durchgeführt wird.

5.4 Anbindung von Empfängern

Bei der Etablierung der Datenaustauschplattform entstehen Aufwände auf Seiten der Empfänger. Daher wird empfohlen, den Empfängern, beispielsweise Kommunen, eine Unterstützung in Form eines Blueprints bereitzustellen, in dem die erforderlichen Maßnahmen zur Anbindung an die Datenaustauschplattform deutlich gemacht werden.

Die Registrierung eines Dienstes (Fachverfahren) erfordert einen Eintrag im DVDV und erfolgt über einen Antrag. Es sind pro Jahr zwei Pflegezeitpunkte am 01.05. und 01.11. für DVDV Einträge vorgesehen. Dies könnte sich bei zeitkritischer Implementierung nachteilig auswirken und macht eine verlässliche Planung erforderlich.

Um diesen Risiken zu begegnen und eine stärkere Kontrolle der Umsetzungsplanung für die einzelnen Fachverfahren zu haben, wird empfohlen, eine zentrale Stelle zu benennen, die für das Land die Eintragung neuer Dienste ins DVDV beantragt.

6. Zusammenfassung

Folgende Fragestellungen sollen beantwortet werden:

1. Analyse der durch IT.NRW bereitgestellten funktionalen Beschreibung der Basiskomponenten, inwieweit die kommunale Lösung zu einer, zumindest temporären Lösung für Landesdienste befähigt werden kann.
2. Bewertung, ob diese Lösungsarchitektur auch dauerhaft als Plattform für Landes- und kommunale Dienste Verwendung finden kann.

Zusammenfassend kann festgehalten werden, dass die bestehende Lösung von DataClearing NRW kurz- bis mittelfristig zu einer temporären Lösung für Landesdienste befähigt werden kann. Die DataClearing NRW Plattform nutzt die durch den IT-Planungsrat vorgegebenen Standards und wird im Bereich Meldewesen bereits eingesetzt. Abweichend von der im Dokument *OZG - IT Architektur für AG Technik V1.3* benannten Funktionalität, ist durch die aktuelle Lösung keine Funktionalität für das Versenden einer Empfangsbestätigung an das E-Mail-Postfach des Antragstellers möglich.

Die Nutzung als dauerhafte einzige Plattform für Landes- und kommunale Dienste ist ebenfalls möglich. Durch die Nutzung der durch den IT-Planungsrat vorgegebenen Standards und Produkte und dem verschlüsselten Datenaustausch zwischen den Kommunikationspartnern, ist ein Datenaustausch auf Landesebene, auf kommunaler Ebene und zwischen Landesebene und kommunaler Ebene möglich. Dabei hat der Betreiber des „Transportsystems“ keinen Zugang zu den verschlüsselten Daten der Kommunikationspartner.

Für die Nutzung durch das Land ist ein Finanzierungsmodell zu wählen, dabei ist zwischen nutzungsabhängigen Modellen (Pay per Use) oder pauschalen Festbeträgen abzuwägen.

Mit der schrittweisen Umsetzung des OZG ist eine massiv steigende Anzahl von angeschlossenen Fachverfahren zu erwarten. Damit einhergehend erhöht sich auch die Anzahl der zu übertragenden Nachrichten und das damit verbundene Datenvolumen. Diese Anforderungen des OZG und der zugehörigen Fachverfahren erfordern einen sukzessiven Ausbau der DataClearing NRW Plattform sowohl in technischer als auch in organisatorischer Hinsicht. Die Nutzung als einzige Plattform für Landes- und kommunale Dienste mit dem zu erwartenden hohen Datenaufkommen setzt die in Kapitel 5 gegebenen Empfehlungen voraus.

7. Glossar / Abkürzungsverzeichnis

Begriff	Beschreibung
API	Application Programming Interface (Programmierschnittstelle). Sie dient zum Austausch und der Weiterverarbeitung von Daten und Inhalten zwischen verschiedenen Websites, Programmen und Anbietern.
DVDV	Das Deutsche Verwaltungsdienstverzeichnis (DVDV). Siehe Kapitel: 3.2.1
Intermediär	Der Intermediär ist die Plattform für den OSCI-konformen Transport und Übermittlung der Daten. Eingehende Nachrichten werden geprüft und weiterleitet oder dem Empfänger zur Abholung bereitgestellt. Der Intermediär kann bei vertraulichen, verschlüsselten Daten lediglich die Transportinformationen lesen bzw. interpretieren und hat keinen Zugang auf die Inhalte der Nachrichten.
KoSIT	Koordinierungsstelle für IT-Standards. Die KoSIT hat die Aufgabe, die Entwicklung und den Betrieb von IT-Standards für den Datenaustausch in der öffentlichen Verwaltung zu koordinieren. Das Aufgabenspektrum umfasst unter anderem auch den Betrieb der Standardisierungsagenda und des XÖV-Rahmenwerks.
NRW Connect	Digitale Kollaborationsplattform des Landes NRW, die alle Voraussetzungen für eine produktive Kollaboration im Arbeitsalltag bedient und den Informationsfluss fördert
nwrGOV	nwrGOV ist das gemeinsame Landes-Design und ein einheitliches Landes-CMS (Content Management System) für Internetauftritte und Portale aller Landesbehörden und Einrichtungen des Landes NRW.

OSCI	Online Services Computer Interfaces ist eine Sammlung verschiedener Netzwerkprotokolle für die öffentliche Verwaltung, mit welcher sich Nachrichten sicher und vertraulich übermitteln lassen.
OZG	Onlinezugangsgesetz (Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen) von 2017
Serviceportal.NRW	Einstiegspunkt zu den E-Government Diensten der Landesverwaltung NRW.
SOAP	Simple Object Access Protocol ist ein Netzwerkprotokoll, mit dessen Hilfe Daten zwischen Systemen ausgetauscht und Remote Procedure Calls durchgeführt werden können.
XTA/XTA2 Standard	Fachunabhängiger Standard für Transportverfahren. XTA/XTA2 standardisiert die elektronische Übermittlung von Daten im E-Government.

8. Quellen

- > OZG - IT Architektur für AG Technik V1.0
- > OZG - IT Architektur für AG Technik V1.3
- > Konzept zur Umsetzung des Bauportal.NRW Version 0.99 (Stand: 05.08.2019)
- > Infobroschüre: https://www.dataclearing-nrw.de/fileadmin/pdf/broschuere_dataclearing.pdf
- > Informationen des IT-Planungsrats: www.it-planungsrat.de
- > Informationen zum IT-Dienstleister des Bundes: www.itzbund.de
- > Deutsches Verwaltungsdienstverzeichnis (DVDV): www.itzbund.de/DE/Produkte/DVDV/DVDV_Uebersicht/DVDV_Uebersicht_node.html
- > Infos zu DataClearing NRW: www.dataclearing-nrw.de/basis-dienste.html
- > Informationen zu Governikus KG: www.governikus.de
- > Informationen der IT-Dienstleister des Bundes: www.itzbund.de
- > Koordinierungsstelle für IT-Standards (KoSIT): www.xoev.de
- > Informationen zu XÖV-Standards und Codelisten: www.xrepository.de und www.xoev.de

9. Kontakt

Christian Neumann

d-NRW AöR

Telefon: 0231 222 438-23

Mobil: 0151 / 42435959

neumann@d-nrw.de

10. Anlagen

10.1 Interviewleitfaden und -ergebnisse

Interviewleitfaden und -ergebnisse des Interviews am Montag 09.12.2019 mit Herrn:

Dr. Lars van der Grinten

Kommunales Rechenzentrum Niederrhein



20191209

d-NRW_Fragebogen I

10.2 DVDV Deutsches Verwaltungsdiensteverzeichnis



DVDV_Infoheft.pdf

10.3 OSCI-Transport_Spezifikation-Version_1.2



OSCI-Transport_Spe
zifikation-Version_1

10.4 Umsetzung OZG IT-Architektur für AG-Technik



201910 OZG - IT
Architektur für AG T
