Eckpunktepapier zum Einsatz eines verfahrensübergreifenden Identifiers - „4-Corner Modell“

Fassung vom 10.01.2020

Frank Steimke, KoSIT

1 Motivation und Begründung

2 Eigenschaften der Infrastruktur

2.1 Die sektorübergreifende Datenübermittlung erfolgt nicht direkt zwischen den beiden Behörden, sondern immer über Dritte Stellen

2.2 Die bei der sektorübergreifenden Datenübermittlung zu beteiligenden Dritten müssen öffentliche Stellen im Sinne des § 2 BDSG sein

2.3 Die an der Datenübermittlung zu beteiligenden Dritten haben die Aufgabe, die sektorübergreifenden Datenübermittlungen zu kontrollieren und zu protokollieren

2.4 Die Dritten Stellen kennen die Metadaten der Datenübermittlung, insbesondere kennen sie die Identität der Kommunikationspartner

2.5 Der Identifier ist nicht Bestandteil der Metadaten der Datenübermittlung

2.6 Die Dritten Stellen müssen ihre Aufgaben ohne Kenntnis des Nachrichteninhalts erbringen können

2.7 Die Vertraulichkeit der Datenübermittlung muss mindestens auf der Strecke zwischen den Transporteuren sichergestellt sein

2.8 Jede sektorübergreifende Datenübermittlung muss durch eine Dritte Stelle unter Angabe der Kommunikationspartner und dem Zweck hergestellt (vermittelt) werden

2.9 Einträge in den Verzeichnis- bzw. Vermittlungsdienst können nur durch öffentliche Stellen in einem offengelegten (transparenten) Prozess erfolgen

2.10 Alle zur Infrastruktur gehörenden Komponenten werden in einem offenen, von der öffentlichen Verwaltung kontrollierten Prozess betrieben und weiterentwickelt

3 Konkretisierung für die Innenverwaltung

1 Motivation und Begründung

Verlässliche Angaben zur Identität der betroffenen Person sind die Grundlage aller personenbezogenen Verwaltungsleistungen. Die öffentliche Verwaltung speichert Daten zu Personen auf der Basis entsprechender Befugnisse in elektronisch geführten Registern, die nach dem Prinzip der behördlichen Zuständigkeit fachlich und häufig auch geografisch dezentral organisiert sind. Bei der elektronischen Abwicklung von Verwaltungsverfahren muss die eindeutige Zuordnung von Datensätzen in Registern zur jeweils betroffenen Person gewährleistet werden. Die irrtümliche Zuordnung von Datensätzen zur falschen Person muss ebenso ausgeschlossen werden, wie die ergebnislose Suche trotz vorhandener Datensätze.

Für eine verlässliche Zuordnung von Datensätzen in Registern zur betroffenen Person dürfen in Teilbereichen der öffentlichen Verwaltung eindeutige Identifikatoren genutzt werden. Beispiele hierfür sind die Steuer-ID (§ 139 AO) und die AZR Nummer (§ 3 AZRG). Ihre Verwendung ist jeweils nur für bestimmte Geschäftsvorfälle zulässig.

Verfahrensübergreifend wird derzeit häufig eine Kombination von Stamm- bzw. Basisdaten der betroffenen Person für eine Identifikation herangezogen (Name, Angaben zur Geburt, aktuelle Anschrift). Dieser faktisch vorhandene „sprechende Identifikator“ weist sowohl funktionale als auch datenschutzrechtliche Mängel auf.

Vor diesem Hintergrund hat die IMK die Einführung eines registerübergreifenden Identitätsmanagements beschlossen (210. Sitzung im Juni 2019, TOP 12). Es soll ein Identitätsregister eingerichtet werden, in dem die Grunddaten aller Personen mit Verwaltungskontakt in Deutschland gepflegt werden. BMI schlägt vor, das Identitätsregister unter Nutzung der Steuer-ID-Datenbank des BZSt einzurichten. Eine eindeutige Zuordnung der Personalienidentität über alle Register der öffentlichen Verwaltung hinweg soll mithilfe eines Identifiers sichergestellt werden. BMI schlägt vor, hierfür die Steuer-ID oder einen davon abgeleiteten Identifikator zu verwenden. Dieser Identifier ist eine Kennziffer im Sinne des Artikel 87 DSGVO.

Im Zuge der Einführung eines Identifiers müssen aus verfassungsrechtlichen Gründen Maßnahmen ergriffen werden die verhindern, dass es durch eine unzulässige Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von umfassenden Persönlichkeitsprofilen kommen kann. Zugleich muss sichergestellt sein, dass rechtmäßige Datenübermittlungen uneingeschränkt möglich sind und zuverlässig funktionieren. Für jede Datenübermittlung bedarf es zunächst einer entsprechenden Rechtsgrundlage. In der nach dem Prinzip der behördlichen Zuständigkeit dezentral organisierten Registerlandschaft der öffentlichen Verwaltung ist die *Zusammenführung* von Daten gleichbedeutend mit der *Übermittlung* von Daten. Daher soll die unzulässige Zusammenführung einzelner Lebens- und Personaldaten, die zur Erstellung von Persönlichkeitsprofilen führen könnte, dadurch ausgeschlossen werden, dass Kontrolle über Datenübermittlungen zwischen Behörden ausgeübt wird.

Zu diesem Zweck sollen innerhalb der Behörden- bzw. Registerlandschaft der öffentlichen Verwaltung *Sektoren* anhand fachlicher Kriterien definiert werden, beispielsweise *Finanzen / Gesundheit / Arbeit und Soziales / Innenverwaltung*. Sektor-übergreifenden Datenübermittlungen, die den Identifier enthalten, dürfen nur über eine technische Infrastruktur erfolgen, die die erforderlichen Kontrollmöglichkeiten des Staates gewährleistet.

Auf diese Weise wird mittels rechtlicher und technischer Maßnahmen sichergestellt, dass Datenübermittlungen zwischen Sektoren stets nur in einem kontrollierten und überwachten Umfeld stattfinden können. Die unkontrollierte Zusammenführung von Daten aus unterschiedlichen Sektoren ist nicht möglich, so dass die Erstellung von Persönlichkeitsprofilen durch „den Staat“ bzw. eine Behörde wirksam verhindert wird.

2 Eigenschaften der Infrastruktur

Nachfolgend werden Eigenschaften einer Infrastruktur für Datenübermittlungen zwischen Behörden genannt, die erforderlich sind, um die notwendigen Kontrollfunktionen bei Datenübermittlungen zwischen Sektoren ausüben zu können.

Die Eigenschaften werden abstrakt und technikneutral beschrieben. Zur Erläuterung der Eigenschaften wird die konkrete Umsetzung in der Innenverwaltung herangezogen. Die dabei genannten, konkreten Standards bzw. Komponenten dienen nur der Illustration.

Sektor-übergreifende Datenübermittlungen zwischen Behörden, die den Identifier enthalten, sind nur zulässig, wenn sie über eine technische Infrastruktur mit den nachfolgend genannten Eigenschaften erfolgt:

2.1 Die Datenübermittlung erfolgt nicht direkt zwischen den beiden Behörden, sondern immer über Dritte Stellen

*Die beiden Stellen, zwischen denen auf der Basis bestehender Rechtsgrundlagen übermittelt werden, werden als **Autor** bzw. **Leser** bezeichnet. Die Daten dürfen nicht direkt zwischen diesen beiden Stellen ausgetauscht werden, sondern es müssen Dritte Stellen beteiligt sein, bei denen die nachfolgend dargestellten Kontrollfunktionen wahrgenommen werden können.*

In der Innenverwaltung ist dieses Prinzip durch den Im Auftrag des IT-Planungsrats von der KoSIT herausgegebene OSCI Transport Standard und die vom IT-Planungsrat bereitgestellte Anwendung „Governikus“ realisiert. Für die Herstellung einer Verbindung (Vermittlungsdienst) wird das vom Bund und den Ländern gemeinsam betriebene „Deutsche Verwaltungsdiensteverzeichnis DVDV 2“ genutzt. Die Infrastruktur der Innenverwaltung wird gebildet durch die abgestimmte Nutzung technischer Standards und geeigneter, von der öffentlichen Verwaltung betriebener Anwendungen.

Die rechtliche Verpflichtung zur Anwendung dieser Infrastruktur ist u. a. in §§ 2, 3 der 1. BMeldDÜV für die Übermittlung von Meldedaten festgelegt.

2.2 Die bei der Datenübermittlung zu beteiligenden Dritten müssen öffentliche Stellen im Sinne des § 2 BDSG sein

Der Betreiber des Vermittlungsdienstes und die für den Transport zuständigen Stellen müssen selbst der staatlichen Kontrolle unterliegen.

In der Innenverwaltung ist diese Bedingung nach unserem Kenntnisstand für alle Betreiber der OSCI-Intermediäre (Anwendung Governikus des IT-Planungsrats) und alle als Clearing- bzw. Vermittlungsstellen agierenden Organisationseinheiten ebenso gewährleistet, wie für alle Betreiber des Deutschen Verwaltungsdiensteverzeichnisses DVDV auf Bundes- und Landesebene.

2.3 Die an der Datenübermittlung zu beteiligenden Dritten haben die Aufgabe, die sektorübergreifenden Datenübermittlungen zu kontrollieren und zu protokollieren

*Es muss mindestens protokolliert werden: **Wer** übermittelt Daten **an Wen** aus welchem **Anlass** zu welchem **Zeitpunkt**.*

In der Innenverwaltung führen die am Transport beteiligten Stellen entsprechende Protokolle auf Basis des OSCI Laufzettels. Die konkreten Inhalte der Protokollangaben und die Aufbewahrungsfristen sind innerhalb der Innenverwaltung abgestimmt.

In der Innenverwaltung nehmen die Betreiber der OSCI Intermediäre eine zusätzliche, ursprünglich nicht vorgesehene Kontrollfunktion wahr: nach dem Erhalt einer Nachricht prüfen sie im Zusammenspiel mit dem Vermittlungsdienst DVDV, ob die Behördenkategorie des Absenders und der Anlass der Datenübermittlung zusammenpassen. Beispiel: wenn eine Nachricht aus Anlass einer Fortschreibung von Meldedaten gemäß § 23 BMG übermittelt wird, dann muss der Absender der Nachricht eine Behörde der Kategorie „Meldebehörde" sein. Andernfalls wird ein Fehler gemeldet, auf den entsprechend reagiert werden kann.

2.4 Die Dritten Stellen müssen ihre Aufgaben ohne Kenntnis des Nachrichteninhalts erbringen können

Sowohl die originären Aufgaben des sicheren Transports bzw. der Herstellung (Vermittlung) einer Verbindung, als auch die hier beschriebenen Kontroll- und Überwachungsfunktionen müssen die Dritten Stellen auch dann in vollem Umfang wahrnehmen können, wenn sie keine Kenntnis vom eigentlichen Nachrichteninhalt haben.

*Eine andere Formulierung dieser Eigenschaft lautet: Die Infrastruktur muss die Möglichkeit einer **Ende-zu-Ende Verschlüsselung** zwischen den beiden behördlichen Kommunikationspartnern (Autor und Leser) unterstützen.*

In der Innenverwaltung wird dieses Prinzip zunächst durch die Verwendung des OSCI Transport Standards realisiert. Dieser unterstützt die kryptografisch unterschiedliche Behandlung der Metadaten und der eigentlichen Inhaltsdaten, so dass der sichere Transport auch dann gewährleistet wird, wenn die Betreiber der OSCI Intermediäre keinerlei Kenntnis vom Nachrichteninhalt erlangen können.

Angesichts wachsender Anforderungen an die Infrastrukturen der öffentlichen Verwaltung wird dieses Prinzip durch den ebenfalls im Auftrag des IT-Planungsrats von der KoSIT herausgegebenen Standard XTA erweitert, und noch stärker auf die Anforderungen der als Transporteur agierenden Stellen angepasst.

2.5 Die Dritten Stellen kennen die Metadaten der Datenübermittlung, insbesondere kennen sie die Identität der Kommunikationspartner

*Die Identität der behördlichen Kommunikationspartner (**Autor** und **Leser**) soll durch Zertifikate nachgewiesen werden, die einer von der öffentlichen Verwaltung kontrollierten Publik Key Infrastructure (PKI) entstammen.*

2.6 Der Identifier ist nicht Bestandteil der Metadaten der Datenübermittlung

Durch diese Festlegung soll ausgeschlossen werden, dass Transporteure eine personenbezogene Profilbildung betreiben können, die über alle innerbehördlichen Datenübermittlungen zu einer bestimmten Person Auskunft geben könnte

2.7 Die Vertraulichkeit der Datenübermittlung wird mindestens auf der Strecke zwischen den Transporteuren durch eine hinreichende Verschlüsselung sichergestellt.

2.8 Jede sektorübergreifende Datenübermittlung muss durch eine Dritte Stelle unter Angabe der Kommunikationspartner und dem Zweck hergestellt (vermittelt) werden

Diese Dritte Stelle wird Vermittlungsdienst oder Verzeichnisdienst genannt. Sie versorgt die Transporteure mit den für den Transport erforderlichen Angaben (z. B. öffentlichen

Schlüsseln des Empfängers zwecks Gewährleistung der Vertraulichkeit durch Verschlüsselung).

Die Herstellung einer Verbindung ist nur dann möglich, wenn es für den angegebenen Zweck und die angegebenen Kommunikationspartner einen entsprechenden Eintrag im Vermittlungs- bzw. Verzeichnisdienst gibt. Anders ausgedrückt: Datenübermittlungen, für die keine Rechtsgrundlage angegeben werden kann, oder bei denen die Angaben zu Sender, Empfänger und Zweck nicht zueinander passen, können nicht vermittelt werden.

In der Innenverwaltung kommt für diese Zwecke das DVDV 2 zum Einsatz.

2.9 Einträge in den Verzeichnis- bzw. Vermittlungsdienst können nur durch öffentliche Stellen in einem offengelegten (transparenten) Prozess erfolgen

Die Tatsache, dass nur solche Datenübermittlungen vermittelt werden können, für die es einen hinsichtlich der Kommunikationspartner und dem Zweck passenden Eintrag gibt, ist für die Kontrollfunktionen entscheidend. Daher dürfen Eintragungen nur in einem kontrollierten Verfahren vorgenommen werden.

Nur die durch den Bund bzw. die Länder bestimmten „pflegenden Stellen" sind befugt, Einträge in das DVDV 2 vorzunehmen, welches in der Innenverwaltung als Vermittlungsdienst agiert. Dafür erforderliche Datenübermittlungen zwischen „pflegenden Stellen" und dem DVDV 2 sind ebenfalls durch OSCI-Transport gesichert. Dadurch werden unbefugte Manipulationen verhindert, gleichzeitig wird Nachvollziehbarkeit sichergestellt.

2.10 Alle zur Infrastruktur gehörenden Komponenten werden in einem offenen, von der öffentlichen Verwaltung kontrollierten Prozess betrieben und weiterentwickelt

Entsprechend der bisherigen Ausführungen gehören zur Infrastruktur folgende Anwendungen und Interoperabilitätsstandards:

- *Der Vermittlungs- bzw. Verzeichnisdienst. In der Innenverwaltung: DVDV 2*
- *Der oder die Transporteure. In der Innenverwaltung: die Betreiber der OSCI Intermediäre.*
- *Eine Public Key Infrastrukture (PKI) für den Nachweis der Identität der Kommunikationspartner*
- *Ein oder mehrere Standards für die Interoperabilität zwischen allen an der Datenübermittlung beteiligten Stellen der Infrastruktur. Diese müssen als offene Standards im Sinne der Free Software Foundation Europe e.V. (FSFE) betrieben werden.*

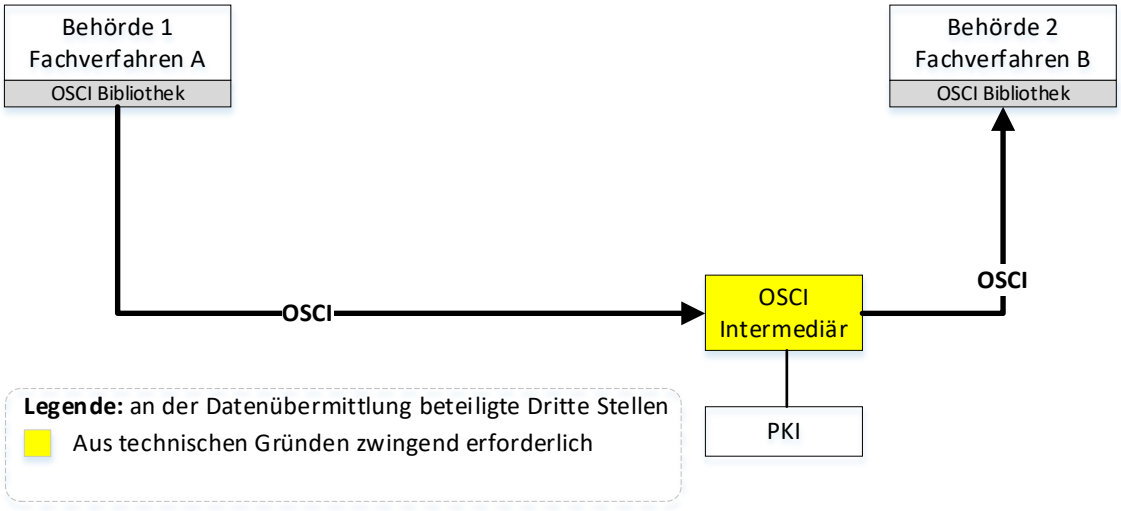
  In der Innenverwaltung sind dies die beiden im Auftrag des IT-Planungsrats herausgegebenen Standards OSCI-Transport und XTA.

Durch die Verpflichtung zur (Weiter-) Entwicklung aller zur Infrastruktur gehörenden Komponenten (Anwendungen und Standards) wird die notwendige Transparenz gewährleistet, die wiederum den Aufsichtsbehörden die Wahrnehmung ihrer Kontrollaufgaben ermöglicht.

3 Konkretisierung für die Innenverwaltung

Nachfolgend werden die allgemein gehaltenen, technikneutralen Anforderungen des Abschnitt 2 für die in der Innenverwaltung vorhandene Infrastruktur konkretisiert und erläutert. Sie basiert auf Standard OSCI Transport. Er wurde durch die OSCI-Leitstelle (Vorläufer der KoSIT) gemeinsam mit dem BSI entwickelt und im Jahr 2002 erstmalig veröffentlicht. Er ist fachunabhängig, das heißt, für die Datenübermittlung zwischen beliebigen Kommunikationspartnern innerhalb und außerhalb der öffentlichen Verwaltung geeignet. Er erfordert zwingend eine Infrastrukturkomponente, bei der kryptografische Funktionen gebündelt und Nachrichten aufbewahrt werden können (Intermediär). Betreiber der Intermediäre können ihre Aufgaben ohne Kenntnis der Inhaltsdaten wahrnehmen (Ende-zu-Ende Verschlüsselung). Dies ermöglicht den Betrieb von Intermediären durch zentrale Stellen. Das ursprüngliche Konzept (ca. 2005) ist in Abbildung 1 dargestellt.

Abbildung 1: Ursprüngliches Konzept für OSCI



Dieses Konzept erwies sich jedoch als nicht ausreichend, weil die Komplexität der Organisation der sicheren Datenübermittlung mit tausenden von Kommunikationspartnern auf der Ebene des Bundes, der Länder und vor allem aller Kommunen unterschätzt worden ist.

Die inzwischen tatsächlich vorhandene, in der Praxis bewährte Infrastruktur der Innenverwaltung ist dementsprechend komplexer. Sie ist Abbildung 4 in dargestellt. Sie wird in identischer bzw. sehr ähnlicher Form auch im Bereich der Übermittlung elektronischer Gewerbeanzeigen gemäß § 14 Absatz 8 GewO und im elektronischen Rechtsverkehr genutzt.

Verzeichnisdienst DVDV 2

Bei einer Vielzahl von Kommunikationspartnern ist eine zentrale Stelle erforderlich, die eine Übersicht über alle insgesamt angebotenen elektronischen Dienste führt. Hierfür wurde das Deutsche Verwaltungsdiensteverzeichnis DVDV eingeführt. Darin ist beispielsweise verzeichnet, welche technischen Kommunikationsparametern für die Behörde erforderlich sind, die den Dienst der Abruf von Meldedaten gemäß § 38 BMG für die Kommune Bremerhaven anbietet.

Nähere Informationen zum DVDV 2 und den aktuell eingetragenen Diensten sind auf der Webseite des ITZ Bund erhältlich [1, 2].

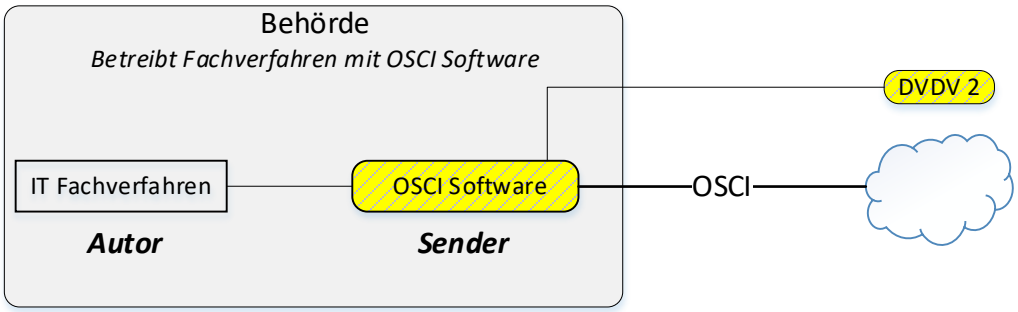
Organisation des sicheren Transports als eigenständige Aufgabe

Bei einer Vielzahl von Kommunikationsbeziehungen ist die Organisation des Nachrichtentransports eine komplexe Aufgabe. Sie beinhaltet den Umgang mit elektronischen Zertifikaten, die Identifikation und Behebung technischer Fehler, die Protokollierung etc.

Transportaufgaben wurden daher ausgelagert und eigenen Rollen zugewiesen. Diese werden als **Sender** bzw. **Empfänger** und zusammenfassend als **Transporteure** bezeichnet. Es gibt unterschiedliche Ausprägungen, die in Abbildung 2 und Abbildung 3 jeweils für die Rolle Sender dargestellt werden.

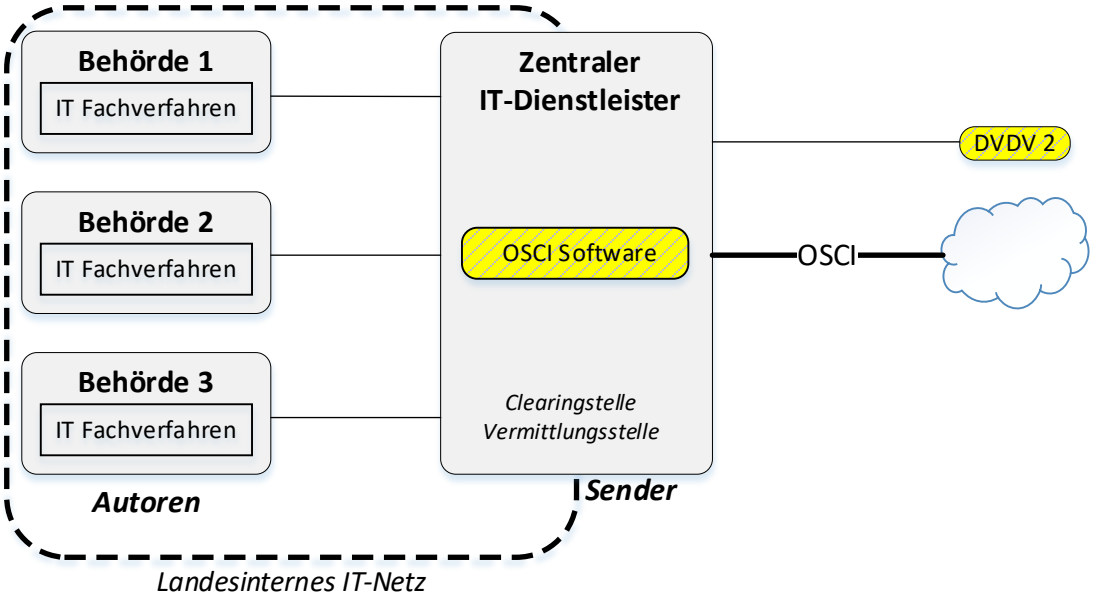
Es kann sich um eine spezielle Software handeln, die als Ergänzung eines IT-Fachverfahrens bereitgestellt wird, um die Datenübermittlung mit OSCI zu organisieren (teilweise als Kommunikationsserver bezeichnet). In diesem Fall agiert die Behörde, bei der das Fachverfahren betrieben wird, gleichzeitig als Transporteur (siehe Abbildung 2).

Abbildung 2: Anbindung mit OSCI Software (Kommunikationsserver)



Häufiger ist jedoch die Errichtung einer für ein Bundesland zentralen Clearing- oder Vermittlungsstelle (siehe § 2 Abs. 3 der 1. BMeldDÜV), bei der die Rolle des Transporteurs im Wege der Datenverarbeitung im Auftrag der angeschlossenen Fachbehörden wahrgenommen wird.

Abbildung 3: Clearing- bzw. Vermittlungsstellen



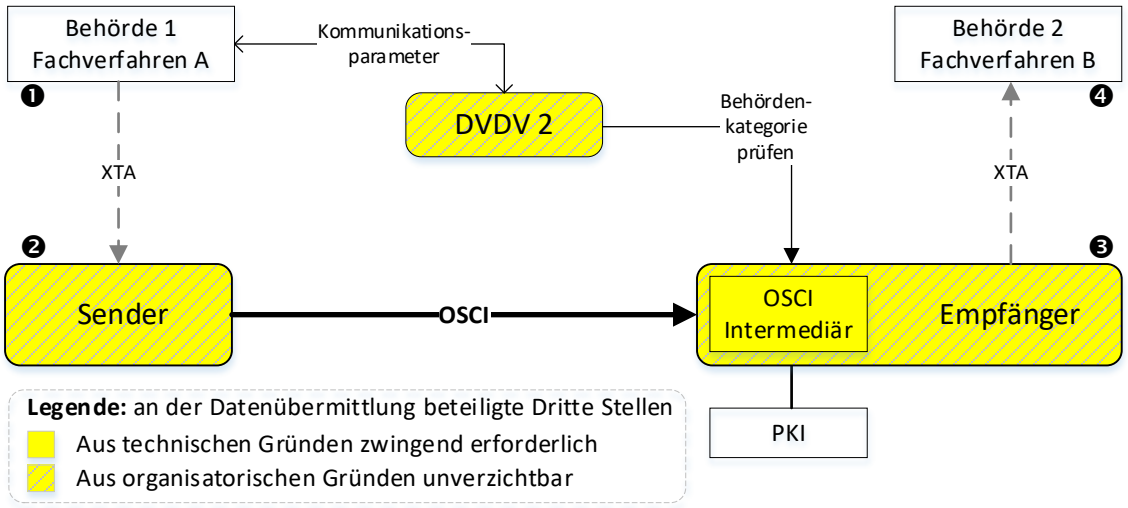
Die Betreiber der für die OSCI Infrastruktur zuständigen Clearingstellen haben sich selbstorganisiert zusammengeschlossen und tagen regelmäßig.

Unabhängig von der Art der Anbindung ergibt sich aufgrund der konzeptionellen Trennung der Aufgaben einer Fachbehörde, die als Autor bzw. Leser einer Fachnachricht agiert, und der

Organisation des sicheren Transport die in Abbildung 4 schematisch dargestellte Infrastruktur der Innenverwaltung. Sie ist seit 2007 ohne nennenswerte Störungen in Betrieb. Jährlich werden mehrere 100 Millionen Nachrichten übermittelt.

Solche Infrastrukturen werden als *4-Corner Modell* bezeichnet (die vier Ecken sind in Abbildung 4 gekennzeichnet). Nach unserem Kenntnisstand ist die Tatsache, dass die beim Transport zu beteiligenden Dritten Stellen ihre Aufgabe auch ohne Kenntnis des Nachrichteninhalts erbringen können, zumindest nicht selbstverständlich (ggfs. ein Alleinstellungsmerkmal).

Abbildung 4: Infrastruktur der Innenverwaltung (schematisch)



Dritte Stellen im Sinne des Eckpunktepapiers

Hinsichtlich der Aussagen des Eckpunktepapiers bedeutet das insbesondere, dass die als Transporteure agierenden Stellen (*„Sender“* und *„Empfänger“* in Abbildung 4 nicht aus technischen Gründen zwangsläufig mit dem Einsatz von OSCI verbunden sind. Dies wäre lediglich der OSCI Intermediär. In der Praxis ist aber deutlich geworden, dass die Organisation des sicheren Nachrichtenversands in einer flächendeckenden Infrastruktur der öffentlichen Verwaltung so komplex ist, dass er spezialisierten Rollen übertragen werden muss.

Dies sind meistens rechtlich eigenständige Organisationseinheiten, deren originäre Aufgabe darin besteht, im Auftrag angeschlossener IT-Fachverfahren die effiziente und verlässliche Datenübermittlung gemäß einschlägigen Rechtsgrundlagen sicherzustellen. Sofern ihnen im Rahmen der Einführung eines verfahrensübergreifenden Identifiers zusätzliche Kontrollaufgaben bei Sektor-übergreifenden Datenübermittlungen zugewiesen werden, sollte ggfs. ihre rechtliche Einordnung neu bestimmt werden.

Neben den Transporteuren kommt auch der Verzeichnisdienst DVDV 2 als *Dritte Stelle* zur Wahrnehmung von Kontrollfunktionen im Sinne des Eckpunktepapiers in Betracht.

Welche Lösung am besten geeignet ist, wird noch zu bestimmen sein, wenn

a) Klarheit über die „Sektoren“ hergestellt worden ist, an deren Grenzen Kontrollfunktionen eine Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen verhindern; und
b) Die dort erforderlichen Kontrollfunktionen näher bestimmt worden sind.

Weblinks

[1] DVDV bei ITZ Bund

[2] Übersicht der Dienste im DVDV