Leitfaden zur elektronischen Kommunikation mit XPersonenstand in Standesämtern

Herausgeber: AG Start XPersonenstand

Inhaltsverzeichnis

1. Einleitung

Nahezu jede Beurkundung eines Personenstandsfalles löst Mitteilungspflichten zu anderen Standesämtern, weiteren Behörden, Gerichten oder sonstigen öffentlichen Stellen aus. Jede dieser Mitteilungen verursacht auf Absender- und Empfängerseite Personal- und Sachaufwand. Bei bundesweit etwa 10 Millionen Mitteilungen pro Jahr summiert sich allein die durch eine elektronische Kommunikation mögliche Einsparung von Portokosten auf erhebliche Beträge. Darüber hinaus steigt die Effizienz in den Standesämtern, wenn Nachrichten in Fachverfahren automatisch erzeugt, elektronisch versandt und in das Fachverfahren des Empfängerstandesamtes zur weiteren Bearbeitung übernommen werden können.

Die Arbeitsgemeinschaft (AG) Start XPersonenstand als Herausgeber dieses Leitfadens hat sich unter anderem zum Ziel gesetzt, die Standesämter dabei zu unterstützen, die erforderliche Infrastruktur zur elektronischen Kommunikation im Personenstandswesen aufzubauen und einzusetzen. An der AG und an der Entwicklung dieses Leitfadens haben mitgewirkt:

- Betrieb des Standards XPersonenstand
    - Stadt Dortmund
    - Koordinierungsstelle für IT-Standards KoSIT
- Bundesstelle für Informationstechnik im Bundesverwaltungsamt (DVDV)
- AG der Clearingstellenbetreiber
    - Thüringer Landesrechenzentrum
    - Dataport AöR
- PG Standard
    - citeq, Stadt Münster
- Personenstandsreferenten der Länder
    - Niedersächsisches Ministerium für Inneres und Sport
    - Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen
    - Thüringer Innenministerium
- Standesämter
    - Stadt Wuppertal
    - Stadt Löhne
    - Stadt Dortmund

1.1. Zielsetzung des Leitfadens

Mit der Novellierung des Personenstandsrechts zum 01.01.2009 wurden die rechtlichen Grundlagen für die elektronische Kommunikation im Personenstandswesen geschaffen. In der Praxis sollen die Standesämter über den Standard XPersonenstand in einem ersten Schritt untereinander und in einem zweiten Schritt mit anderen Behörden, Gerichten und sonstigen öffentlichen Stellen elektronisch kommunizieren können.

Dieser Leitfaden soll dazu beitragen, dass die Standesämter möglichst schnell zur elektronischen Kommunikation über den Standard XPersonenstand in der Lage sind. Hierzu zeigt er die für den elektronischen Mitteilungsverkehr erforderliche Organisation und Technik auf. Im Wesentlichen geht es um die Frage, was Standesämter und deren IT-Dienstleister tun müssen, um Mitteilungen elektronisch auch außerhalb gesicherter Behördennetze versenden und empfangen zu können. Besonderheiten beim Empfang von Geburts- und Sterbeanzeigen sowie gegebenenfalls erforderliche zusätzliche Maßnahmen zur Kommunikation mit Meldebehörden bleiben einer späteren Version dieses Leitfadens vorbehalten.

Der Einsatz von XPersonenstand ist unabhängig vom elektronischen Personenstandsregister (ePR): man braucht kein ePR, um XPersonenstand nutzen zu können. Insofern wird in diesem Leitfaden auf das ePR auch kein Bezug genommen.

1.2. Die Standards XPersonenstand und OSCI-Transport

1.2.1. XPersonenstand

XPersonenstand ist Teil des E-Government-Aktionsplans Deutschland Online, der alle Verwaltungsbereiche umfasst.
So kommt die elektronische Kommunikation bereits im Meldewesen sowie im Pass- und Ausweisbereich zum Einsatz. Die hierfür geschaffenen technischen Infrastrukturen können auch im Personenstandswesen genutzt werden.
Zur Realisierung der elektronischen Übermittlung im Personenstandswesen wurde das standardisierte Datenaustauschformat XPersonenstand unter der Projektleitung der Stadt Dortmund in Zusammenarbeit mit Vertretern des Bundesministerium des Innern, von Standesämtern, Rechenzentren, Verbänden und Verfahrensherstellern entwickelt. Die Definition eines Standards bietet die Gewähr, dass unterschiedliche Systeme verschiedener Anbieter zusammen arbeiten und Informationen auf effiziente Art und Weise austauschen können, ohne dass jeweils gesonderte Absprachen zwischen den einzelnen Systemen notwendig werden. Zugleich wird dadurch eine teil- oder voll automatisierte Verarbeitung der Daten erreicht; z.B. können so Nachrichten auch dann im Fachverfahren des Empfängerstandesamtes weiterverarbeitet werden, wenn sie vom Absender in einem anderen Fachverfahren erzeugt wurden.

Hierzu wurden folgende Nachrichten-Module entwickelt:

- Modul 1 – Kommunikation der Standesämter untereinander
- Modul 2 – Kommunikation der Standesämter zu den Meldebehörden
- Modul 3 – Kommunikation der Standesämter zur Finanzverwaltung
- Modul 4 – Kommunikation der Standesämter zur Statistik
- Modul 5 – Kommunikation der Standesämter zu anderen (z.B. Zentrales Testamentsregister)

Nähere Informationen über die Entwicklungen in den einzelnen Modulen und der Download des aktuellen Standards können den Veröffentlichungen zu XPersonenstand auf den folgenden Internet-Seiten entnommen werden:

http://xpsw.domap.de/ (z.B. Spezifikation, Schemadateien, WSDL-Dateien, Zeitplanung)
https://www.xrepository.deutschland-online.de/xrepository/ (z.B. Schlüsseltabellen)

1.2.2. OSCI-Transport

Für die elektronische Übermittlung personenbezogener Daten bedarf es entsprechender Sicherheitsmechanismen. Genau hier setzt der Datentransportstandard OSCI-Transport an (OSCI=OnlineServicesComputerInterface, das bedeutet: Schnittstelle zur automatisierten elektronischen Datenübertragung). Auch dieser Standard wurde im Rahmen des Aktionsplans Deutschland Online entwickelt. Seit dem 01.01.2007 wird er bundesweit produktiv in der Datenübermittlung des Einwohnermeldewesens eingesetzt. Insbesondere durch Verschlüsselungsalgorithmen und Signaturen werden Authentizität, Integrität und Vertraulichkeit der übertragenen fachlichen Nachrichten sichergestellt. Bildhaft lässt sich OSCI-Transport als Datenübertragung in einem doppelten und versiegelten Umschlag beschreiben.

1.3. Erste Ansprechpartner

Im Regelfall wird der IT-Dienstleister des Standesamtes (sei es ein Rechenzentrum oder die IT-Abteilung der Kommunalverwaltung) neben der Einrichtung der elektronischen Personenstandsregister auch für die Einrichtung und den Betrieb der elektronischen Kommunikation sorgen. Er plant gemeinsam mit dem Standesamt die technische und organisatorische Umsetzung. Später steht er für technische Fragen zur Verfügung (z.B. über eine Hotline). Bei Bedarf spricht er dann die zuständigen Stellen oder Softwareanbieter an. Insbesondere erscheint es sinnvoll, sich mit dem Melde-, Pass- und Ausweisbereich über deren Anbindung an die technische Kommunikationsinfrastruktur abzugleichen. Dies bietet die Möglichkeit, bereits vorhandene Erfahrungen und Kommunikationsinfrastrukturen nutzen zu können und keine unnötigen parallelen Lösungen aufzubauen. In einzelnen Ländern haben sich für OSCI-Transport auch zentrale Infrastrukturen (sogenannte Clearing- oder Vermittlungsstellen) etabliert.

2. Technische Komponenten

Im Folgenden werden die einzelnen erforderlichen Komponenten kurz dargestellt und Hinweise für die konkrete Umsetzung gegeben.

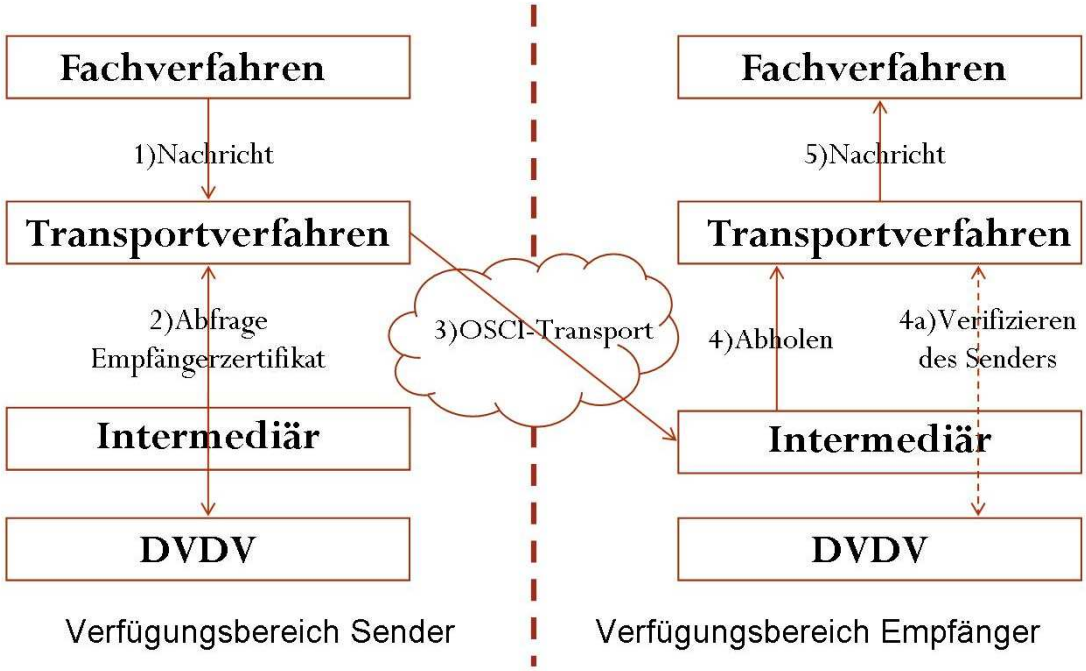

Abbildung: schematische Darstellung der beteiligten Komponenten in XPersonenstand

2.1. Fachverfahren – die Schreibmaschine

Verfahrenshersteller im Personenstandswesen binden die elektronische Kommunikation in ihre Fachanwendung mit ein, sodass sich an den bisherigen Ansprechpartnern nichts ändert.

Das Fachverfahren erzeugt aus den eingegebenen Personenstandsdaten elektronische Nachrichten und leitet diese an ein Transportverfahren weiter. Umgekehrt nimmt das Fachverfahren die Nachrichten vom Transportverfahren entgegen und stellt sie zur Weiterbearbeitung zur Verfügung. Wichtig im Zusammenhang mit der elektronischen Kommunikation ist die Nutzung einer Version des Fachverfahrens, die die jeweils aktuelle Version von XPersonenstand unterstützt. Je nach dem, ob das Fachverfahren in einem Rechenzentrum oder durch die örtliche IT-Abteilung betrieben (neudeutsch „gehostet“) wird, ist dort dafür Sorge zu tragen.

2.2. Transportverfahren – die Poststelle

Ein Transportverfahren kümmert sich um den Versand und Empfang von elektronischen Nachrichten. Wie bei der hausinternen Poststelle muss also auch hier innerhalb eines gesicherten Netzes eine Software zum Einsatz kommen, mit deren Hilfe die Nachrichten in die richtige Form („Briefumschlag“) gebracht und versandt werden. Solche Transportverfahren sind für die elektronische Kommunikation im Melde-, Pass-, und Personalausweisbereich bereits etabliert und können ggf. auch für XPersonenstandsnachrichten mit genutzt werden. Eine besondere Ausprägung erfahren diese Transportverfahren in einzelnen Bundesländern durch die Einrichtung so genannter Clearing- oder Vermittlungsstellen, in denen sich Dienstleister zentral um die Beschaffung und den Betrieb des Transportverfahrens sowie die Anbindung und alle mit der elektronischen Kommunikation im Zusammenhang stehenden Fragen kümmern.

Das Transportverfahren wird im Regelfall automatisiert durch das Fachverfahren aufgerufen und ist während der täglichen Arbeit im Standesamt nicht sichtbar. Es ermittelt die elektronische Erreichbarkeit des Empfängers, verschlüsselt und signiert die Nachricht („Verpackung“)“ und sendet sie an das Postfach des Empfängers. Die Art und Weise des Transportes wird durch bundesrechtliche Vorgabe unter dem Sammelbegriff OSCI-Transport beschrieben (§ 63 Abs. 2 PStV).

2.3. Zertifikate – die elektronische Identifikation

Zertifikate und Signaturen sind wichtige Grundlagen für die elektronische Kommunikation. Sie sind erforderlich, um die Authentizität, die Vertraulichkeit und die Integrität von Daten sicherzustellen.
Beantragt werden sie durch das Standesamt (ggf. mit Unterstützung des jeweiligen IT-Dienstleisters) bei einer Registrierungsstelle. Im Personenstandswesen wie auch im Meldewesen kommen nur Zertifikate der DeutschlandOnlineInfrastruktur (DOI) zum Einsatz. Daher kann auf die im Meldewesen genutzte Registrierungsstelle zugegriffen werden.

Im Gegensatz zur elektronischen Registerführung – ePR -, bei der es der qualifizierten elektronischen Signatur bedarf, werden für die elektronische Kommunikation mit XPersonenstand sogenannte „fortgeschrittene Zertifikate“ benutzt; diese sind auch zur automatisierten Nutzung (z.B. durch ein Transportverfahren) freigegeben und werden entsprechend automatisiert verarbeitet. Dem Standesamt entsteht kein zusätzlicher Aufwand.

2.4. Intermediär – der elektronische Briefkasten

Intermediäre stellen im Rahmen der Kommunikation über OSCI-Transport Postfächer für Standesämter bereit. Damit die anderen Kommunikationspartner aus dem gesamten Bundesgebiet sie regelmäßig erreichen können, müssen die Intermediäre mit hoher Verfügbarkeit ausgestattet sein. Das bedeutet im Regelfall einen Rund-um-die-Uhr-Betrieb an 7 Tagen in der Woche.

Für die Umsetzung der elektronischen Kommunikation im Meldewesen haben sich einige Intermediärsbetreiber etabliert, eine Liste mit Ansprechpartnern findet sich im Anhang.

2.5. DVDV – das Telefonbuch

Für einen elektronischen Mitteilungsverkehr zwischen den Standesämtern, zwischen Standesämtern und anderen Behörden, Gerichten und sonstigen öffentlichen Stellen müssen analog zum Meldewesen auch im Personenstandswesen die Kommunikationspartner eindeutig adressierbar sein.
Zu diesem Zweck werden für die Standesämter die von den Statistischen Landesämtern bundesweit eindeutig vergebenen Standesamtsnummern im Rahmen des Standards XPersonenstand genutzt.
Um elektronische Mitteilungen versenden und empfangen zu können, müssen die Standesämter sowie deren Kommunikationspartner in das Deutsche Verwaltungsdiensteverzeichnis (DVDV) eingetragen werden. Das DVDV wurde im Rahmen der Novellierung des Melderechtsrahmengesetzes (MRRG) ins Leben gerufen und stellt ein Verzeichnis aller Kommunikationspartner dar, die über OSCI-Transport elektronisch erreichbar sind. Hier werden u. a. die Zertifikatsinformationen und Intermediärspostfächer der Standesämter verzeichnet. Für den Abruf der Informationen gibt es einzelne Landesserver, die eine Kopie des „Telefonbuchs“ vorhalten.

Beim DVDV wird automatisiert ermittelt, ob ein anderes Standesamt den elektronischen Dienst (z.B. „Mitteilung X aus dem Modul 1 Standesamt zu Standesamt“) nutzen kann. Wenn dem so ist, schickt das DVDV die Kommunikationsdaten der zu adressierenden Behörde zurück. So kann ein gesicherter Datenaustausch erfolgen. Darüber hinaus dient das DVDV auf der Empfängerseite dazu, die Identität der absendenden Stelle zu überprüfen. Näheres kann unter der Internetadresse http://www.dvdv.de/ eingesehen werden.

Die Allgemeine Verwaltungsvorschrift zum Personenstandsgesetz (PStG-VwV) vom 29. März 2010 sieht bereits unter Punkt 3.1. zu § 16 PStV vor, dass die Standesämter ihre - von den Statistischen Landesämtern vergebene - Standesamtsnummer der im Land zuständigen Stelle für die Pflege des DVDV mitteilen. Die in den Ländern zuständigen Pflegenden Stellen können der Liste im Anhang entnommen werden. Jedes Standesamt oder das ggf. von ihm beauftragte Rechenzentrum hat dafür Sorge zu tragen, dass an die für sein Bundesland zuständige Pflegende Stelle des DVDV stets die aktualisierten Daten (wie z.B. Standesamtsnummer, aktuelle Zertifikate, aktuelle Signaturen etc.) übermittelt werden. In einigen Ländern wird diese Aufgabe zentral von Clearing- oder Vermittlungsstellen wahrgenommen.

3. Maßnahmen zur Inbetriebnahme

Zur Vorbereitung des Betriebs von XPersonenstand müssen in Abstimmung mit Ihrem IT-Verantwortlichen folgende Aktionen durchgeführt werden:

- Einsatz einer XPersonenstand-konformen Fachverfahrensversion
- Nutzung eines Transportverfahrens
- Beschaffung des Kombizertifikats (OSCI-Zertifikat)
- Abstimmung mit Ihrem Intermediärsbetreiber (Erfragen der Kommunikationsdaten)
- Eintrag in das DVDV über die Pflegende Stelle des Landes
- Abstimmung mit dem DVDV-Landesserverbetreiber

Generell gilt für die folgenden Maßnahmen: Soweit Ihre Kommune / Ihr Standesamt von einem Rechenzentrum betreut wird, wird dieses in der Regel die erforderlichen Schritte zur Inbetriebnahme von XPersonenstand einleiten. Bitte stellen Sie Ihrem Rechenzentrum diesen Leitfaden für seine Umsetzung zur Verfügung.
Soweit Ihre Kommune die IT eigenverantwortlich betreibt, muss Ihr Standesamt oder die IT-Abteilung Ihrer Verwaltung die in den folgenden Kapiteln dargestellten Maßnahmen selbst erledigen.

Wenn alle Maßnahmen durchgeführt wurden, müssen folgende Daten und Informationen vorliegen:

- Technische Informationen zur Anbindung des Fachverfahrens
- Technische Informationen zur Anbindung des Transportverfahrens
- OSCI-Zertifikat
- WSDL-Datei zum Zugriff auf das DVDV
- URL und Zertifikat Ihres Intermediärs

Eine detaillierte Checkliste finden Sie im Anhang.

3.1. Einsatz einer XPersonenstand-konformen Fachverfahrensversion

Stellen Sie sicher, dass die von Ihnen genutzte Version Ihres Fachverfahrens XPersonenstand in der jeweils gültigen Fassung unterstützt.
Die Information über die jeweils gültige Fassung von XPersonenstand finden Sie unter http://xpsw.domap.de.

3.2. Nutzung eines Transportverfahrens

Das Transportverfahren stellt die Schnittstelle zwischen Ihrem Fachverfahren und der OSCI-Kommunikation dar. Insofern muss das Transportverfahren zwei Dinge sicherstellen:

- die Kommunikation (Empfang und Versand) mit dem Fachverfahren und
- die Kommunikation (Empfang und Versand) mit dem Intermediär

Erkundigen Sie sich bitte bei Ihrem Rechenzentrum oder bei Ihrer IT-Abteilung, welche OSCI-Transportinfrastruktur im Meldewesen genutzt wird und ob diese zusammen mit Ihrem Fachverfahren genutzt werden kann. Anderenfalls fragen Sie bitte Ihren Fachverfahrenshersteller, welche Transportverfahren von seiner Software unterstützt werden. Alternativ erkundigen Sie sich bei einem Transportverfahrenshersteller, ob Ihr Fachverfahren von seiner Software angebunden werden kann.
Nach entsprechender Beauftragung eines Transportverfahrensherstellers erhalten Sie die Software mit der Dokumentation, wie Sie die Software einrichten und für den OSCI-Transport vorbereiten.

3.3. Beschaffung des notwendigen Zertifikats

Für die Kommunikation im Rahmen des Standards XPersonenstand werden Zertifikatsfunktionen zur Inhaltsdatenverschlüsselung und zum OSCI-Transport benötigt. Beide Funktionen werden über das OSCI-Zertifikat in Form eines Kombizertifikats abgebildet.

Die OSCI-Verschlüsselungszertifikate für XMeld, XhD oder XAusländer sind nur insoweit nicht zu verwenden, als die heute in Betrieb befindlichen Transportverfahren in der Regel nicht in der Lage sind, Nachrichten unterschiedlicher Fachanwendungen inhaltlich zu unterscheiden und entsprechend zuzuordnen.

Das OSCI-Zertifikat muss an die Pflegende Stelle Ihres Landes zur Eintragung in das DVDV weitergeleitet und ggf. dem Intermediärsbetreiber[1] mitgeteilt werden.

Für die Beantragung des ggf. kostenpflichtigen OSCI-Zertifikats gibt es zwei Varianten:

- Behörden aus den nachfolgend aufgeführten Ländern nutzen bitte die etablierten Registrierungsstellen der DOI-CA des jeweiligen Landes:
    - Berlin
    - Brandenburg
    - Mecklenburg-Vorpommern
    - Niedersachsen
    - Rheinland-Pfalz
    - Sachsen-Anhalt
    - Thüringen

[1] Die Notwendigkeit der Zulieferung ist von den Nutzungsbedingungen (Policy) des jeweiligen Intermediärsbetreibers abhängig.

Diese Registrierungsstellen unterstützen Sie auch bei Fragen zum Zertifikatsmanagement und stellen teilweise eigene Anleitungen für die Antragstellung zur Verfügung. Darüber hinaus unterstützen Sie diese Registrierungsstellen bei der Einstellung der Zertifikate in das DVDV (Deutsches Verwaltungsdiensteverzeichnis).
Die näheren Angaben zu den einzelnen Registrierungsstellen finden Sie im Anhang dieses Leitfadens.

- Behörden aus allen anderen Bundesländern nutzen bitte die zentrale Registrierungsstelle des Trust Centers der Fa. T-Systems.
  Die Internetseite der Zertifizierungsstelle zur Beantragung und Abholung des Kombizertifikats (DOI-CA) ist erreichbar unter https://doi.telesec.de/doi/ee.
  Zur späteren Zuordnung Ihres Antrags/Zertifikats müssen Sie beim Aufruf der Internetseite eine Kennung des Zuständigkeitsbereichs (Master-Domäne) angeben, für XPersonenstand sind folgende Daten zu verwenden:

  LOGIN: XPersonenstand
  PASSWORT: holemawa38

  Hinweis: Mit dieser Kennung erfolgt nur die Zuordnung zur Master-Domäne „Oeffentliche Verwaltung“, d. h. es handelt sich nicht um ein individuelles Login, mit dem weitere (Sicherheits-)Merkmale verknüpft sind. Zur Beantragung, Abholung oder Sperrung von Zertifikaten werden Ihnen im Laufe des Antragsprozesses weitere individuelle Passwörter mitgeteilt.

  Unter der Rubrik „Softwarezertifikat beantragen“ kann dort das hier benötigte Zertifikat beantragt und abgeholt werden. Bei der Beantragung ist als Subdomäne „DOI-OSCI“ auszuwählen.

  Eine entsprechende Beschreibung des Beantragungsverfahrens finden Sie unter der Rubrik „Handbücher“ und dort unter dem Titel „Handbuch Teilnehmer öffentliche Verwaltung“ im PDF-Format.

  Nach der Beantragung erhält der Antragsteller eine Referenznummer und ein Download-Passwort, mit denen das Zertifikat auf derselben Internetseite abgeholt werden kann.

3.4. Abstimmung mit Ihrem Intermediärsbetreiber

Der Intermediär hält Ihren elektronischen Briefkasten vor. Im Melde-, Pass- und Personalausweis- sowie im Ausländerwesen haben sich in allen Bundesländern bereits solche Intermediärsbetreiber etabliert. Erkundigen Sie sich bitte bei Ihrem Rechenzentrum oder bei Ihrer IT-Abteilung, welcher Intermediär im Meldewesen genutzt wird und ob dieser auch hier genutzt werden kann. Ergänzend finden Sie im Anhang eine Liste dieser Betreiber inklusive Kontaktinformationen.

Mit dem Betreiber sind entsprechende vertragliche Regelungen über den Betrieb des Postfachs und das damit zusammenhängende Nachrichtenaufkommen zu vereinbaren.
Der von Ihnen gewählte Intermediärsbetreiber wird Ihnen im Zuge des Vertragsabschlusses mitteilen, ob er Ihr OSCI-Zertifikat benötigt. Des Weiteren werden Sie von Ihrem Intermediärsbetreiber dessen URL (entspricht der Postfachadresse) und dessen öffentliches Zertifikat erhalten. Diese Informationen benötigen Sie zur Weiterleitung an die Pflegende Stelle sowie zur Eintragung in Ihr Transportverfahren.

3.5. Eintrag in das DVDV über die Pflegende Stelle des Landes

Folgende Daten sind bei der Kontaktaufnahme mit der Pflegenden Stelle zu benennen:

- Art bzw. Kategorie der Behörde (Standesamt)
- Standesamtsnummer als Behördenschlüssel
- Name/Adressdaten der Behörde
- OSCI-Zertifikat (Kombizertifikat, gleichzeitig Funktion der Inhaltsdatenverschlüsselung)
- Informationen zum verwendeten Intermediär (Zertifikat des Intermediärs, URL des Intermediärs)

Die bei der Verzeichnung der Behörde im DVDV ablaufenden Prozesse zwischen Behörden und Pflegenden Stellen differieren ggf. in den einzelnen Ländern und sind nach den individuellen Vorgaben in den Ländern durchzuführen. Eine Liste mit den Pflegenden Stellen in Deutschland inklusive Kontaktinformationen erhalten Sie im Anhang.

3.6. Abstimmung mit dem DVDV-Landesserverbetreiber

Erkundigen Sie sich bitte bei Ihrem Rechenzentrum oder bei Ihrer IT-Abteilung, welcher DVDV-Landesserver im Meldewesen genutzt wird. Die Kontaktdaten Ihres Landesserverbetreibers finden Sie im Anhang.
Von Ihrem DVDV-Landesserverbetreiber erhalten Sie die Zugriffsdatei auf das DVDV – eine so genannte WSDL-Datei. Diese müssen Sie nach Vorgabe des Transportverfahrens dort eintragen (siehe auch Kapitel 3.2)

Anhang 1: Checkliste

Diese Checkliste zeigt die einzelnen Schritte des Kapitels 3 auf. Wenn Sie die einzelnen Schritte der Checkliste abgehakt haben, steht einer Produktivsetzung von XPersonenstand in Ihrem Umfeld technisch nichts mehr im Wege.

Nr.	Thema	Aufgabe	Erledigt?	Termin
1	OSCI-Zertifikat	Beantragt?	❑	
		Erhalten?	❑	
		abgeholt?	❑	
2	Intermediärsbetreiber	Beauftragt?	❑	
		ggf. Mitteilung des OSCI-Zertifikats	❑	
		Einrichtung des Postfachs	❑	
		Bekanntgabe der URL und des Intermediärszertifikats?	❑	
3	Behörden-ID und Behördenschlüssel	Bildung der Behörden-ID und des Behördenschlüssels abgeschlossen?	❑	
4	Pflegende Stelle DVDV	Beauftragung mit dem Eintrag ins DVDV (inkl. Benennung und Lieferung der erforderlichen Daten) erfolgt?	❑	
5	DVDV-Eintrag durch die Pflegende Stelle	Eintrag in das DVDV ist laut Pflegender Stelle DVDV erfolgt und Quittierung wurde erhalten	❑	
		Haben Sie die WSDL-Datei zur Adressierung des DVDV erhalten?	❑	
6	Transportclient	Liefert das Fachverfahren einen Transportclient mit oder ist ein solcher beschafft worden?	❑	
7	Fachverfahren	Spricht das Fachverfahren XPersonenstand in der aktuellen Version?	❑	
8	Eintrag der Kommunikationsdaten	Sind alle notwendigen Daten vorhanden und an den entsprechenden Stellen eingetragen?	❑	

Anhang 2: Liste der Pflegenden Stellen DVDV

Bundesland	**Pflegende Stelle**	**Ansprechpartner**
Baden-Württemberg	Zweckverband Kommunale Datenverarbeitung Region Stuttgart Krailenshaldenstraße 44 70469 Stuttgart	Herr Rauser Tel.: 0711/810811609 Fax: 0711/810813609 eMail: r.rauser@kdrs.de Herr Kurkowski Tel.: 0711/810811608 Fax: 0711/810813608 eMail: m.kurkowski@kdrs.de
Bayern	Landesamt für Statistik und Datenverarbeitung Neuhauser Straße 8 80331 München	Herr Jürgen Naser Tel.: 089/2119-246 eMail: Juergen.Naser@lfstad.bayern.de Herr Michel Faulian Tel.: 089/2119-976 eMail: michel.faulian@lfstad.bayern.de
Berlin	Landesamt für Bürger- und Ordnungsangelegenheiten Friedrichstraße 219 10958 Berlin	Herr Andreas Reich Herr Jürgen Korn Herr Frank Krüger eMail: DVDV@labo.berlin.de
Brandenburg	Zentraler IT-Dienstleister des Landes Brandenburg(ZIT-BB) Dortustrasse 46 14467 Potsdam	Herr Armin Lamla Tel.: 0331/39707 Fax: 0331/27548 1028 eMail: armin.lamla@zit-bb.brandenburg.de Frau Karin Noack Tel.: 0331/39608 Fax: 0331/27548 1148 eMail: karin.noack@zit-bb.brandenburg.de eMail : zertifikate.mw@zit-bb.brandenburg.de
Bremen	bos | bremen online services GmbH & Co. KG Am Fallturm 9 28359 Bremen	Herr Oliver Mania Tel.: 0421/20495944 Fax: 0421/2049511 eMail: om@bos-bremen.de eMail: info@bos-bremen.de
Hamburg	Dataport AöR PF 1780 24016 Kiel	Herr Dieter Schlüter Tel.: 0431/3295-6260 eMail: dieter.schlueter@dataport.de Frau Anja Clasen Tel.: 0431/3295-6648 eMail: anja.clasen@dataport.de
Hessen	ekom21 – KGRZ Hessen Bartningstr. 51 64289 Darmstadt	Herr Uwe Geerk Tel.: 06151/704-1360 Fax: 06151/704-2030 eMail: uwe.geerk@ekom21.de
Mecklenburg-Vorpommern	ZV EGO-MV Eckdrift 97 19061 Schwerin	Herr Dirk Gros Tel.: 0385/77334717 Fax: 0385/77334728 eMail: dirk.gros@ego-mv.de

Bundesland	Pflegende Stelle	Ansprechpartner
Niedersachsen	Landesbetrieb für Statistik und Kommunikationstechnologie Niedersachsen (LSKN) Göttinger Chaussee 259 30459 Hannover	Frau Astrid Buchmann-Cattau Tel.: 0511/120-27089 Fax: 0511/120-99-27089 eMail: meldewesen@lskn.niedersachsen.de eMail: astrid.buchmann-cattau@lskn.niedersachsen.de
Nordrhein-Westfalen	DataClearing NRW hier: KRZN (Kommunales Rechenzentrum Niederrhein) Friedrich-Heinrich-Allee 130 47475 Kamp-Lintfort	Herr Dr. Lars van der Grinten Tel.: 02842/9070-321 eMail: Lars.van.der.Grinten@krzn.de
Rheinland-Pfalz	Gesellschaft für Kommunikation und Wissenstransfer mbH Hindenburgplatz 3 55118 Mainz	Herr Peter Hempel Tel.: 06131/6277-200 Fax: 06131/6277-100 eMail: support@kommwis.de
Saarland	Zweckverband eGo-Saar Talstraße 9 66119 Saarbrücken	Herr Thomas Schulz Tel.: 0681/9264341 Fax: 0681/9264315 eMail: thomas.schulz@ego-saar.de
Sachsen	Staatsbetrieb Sächsische Informatik Dienste Garnisonsplatz 11 01917 Kamenz	Herr Maik Ohle Tel.: 03578/334438 Fax: 03578/33554438 eMail: maik.ohle@sid.sachsen.de
Sachsen-Anhalt	Oberfinanzdirektion Magdeburg, Landesrechenzentrum Barbarastraße 2 06110 Halle (Saale)	Herr Robert Hannemann Tel.: 0345/1304 823 Frau Constanze Kirbs Tel.: 0345/1304 852 Frau Jeanette Pfordte Tel.: 0345/1304 862 Fax: 0345/1304 899 eMail: dvdv@liz.sachsen-anhalt.de
Schleswig-Holstein	Dataport AöR PF 1780 24016 Kiel	Herr Dieter Schlüter Tel.: 0431/3295-6260 eMail: dieter.schlueter@dataport.de Frau Anja Clasen Tel.: 0431/3295-6648 eMail: anja.clasen@dataport.de
Thüringen	Thüringer Landesrechenzentrum Warsbergstraße 3 99092 Erfurt	Herr Stefan Schwarz Tel.: 0361/37 84 879 eMail: stefan.schwarz@tlrz.thueringen.de Herr Sascha Kubusch Tel.: 0361/37 84 907 eMail: sascha.kubusch@tlrz.thueringen.de Fax: eMail: dvdv@tlrz.thueringen.de

Anhang 3: Liste der DVDV-Landesserverbetreiber

Bundesland	**Landesserver-Betreiber**	**Ansprechpartner**
Baden-Württemberg	Zweckverband Kommunale Datenverarbeitung Region Stuttgart Krailenshaldenstraße 44 70469 Stuttgart	**Verantwortlicher u. adminstrativer AP:** Herr Rauser Tel.: 0711/8108609 Fax: 0711/8108607 eMail: r.rauser@kdrs.de
Bayern	Landesamt für Statistik und Datenverarbeitung (LfStaD) Neuhauser Straße 8 80331 München	**Verantwortlicher AP:** Herr Dr. Wagner Tel.: 089/2119-735 Fax: 089/2119-1-735 eMail: markus.wagner@lfstad.bayern.de **Administrativer AP:** Herr Hohmuth Tel.: 089/2119-877 Fax: 089/2119-1-877 eMail: jan.hohmuth@lfstad.bayern.de **Zentrale eMail-Adresse:** pki-support@lfstad.bayern.de
Berlin	Landesamt für Bürger- und Ordnungsangelegenheiten Friedrichstraße 219 10958 Berlin bzw. IT-Dienstleistungszentrum Berlin Anstalt des öffentlichen Rechts Berliner Straße 112-115 10713 Berlin	**Verantwortlicher AP:** Herr Peters Tel.: 030/90267-225 Fax: 030/90269-2097 eMail: christian.peters@labo.berlin.de **Administrativer AP :** Herr Reich Tel.: 030/90267-2257 Fax: 030/90269-2097 eMail: andreas.reich@labo.berlin.de
Brandenburg	Zentraler IT-Dienstleister des Landes Brandenburg(ZIT-BB) Dortustraße 46 14467 Potsdam	**Verantwortlicher AP:** Herr Falk Tel.: 0331/39-527 Fax: 0331/39-10-527 eMail: thomas.falk@zit-bb.brandenburg.de **Administrativer AP:** Herr Hein Tel.: 0331/39-724 Fax: 0331/39-10-724 eMail: thomas.hein@zit-bb.brandenburg.de **Zentrale eMail-Adresse:** Info@zit-bb.brandenburg.de
Bremen	Dataport Altenholzer Straße 10-14 24161 Altenholz	**Verantwortlicher AP:** Herr Christiansen Tel.: 0431/3295-6601 eMail: dirk.christiansen@dataport.de **Administrativer AP :** Frau Mumm Tel.: 040/428 46-2598 eMail: sabine.mumm@dataport.de

Bundesland	Landesserver-Betreiber	Ansprechpartner
Hamburg	Dataport Altenholzer Straße 10-14 24161 Altenholz	**Verantwortlicher AP:** Herr Christiansen Tel.: 0431/3295-6601 eMail: dirk.christiansen@dataport.de **Administrativer AP :** Frau Mumm Tel.: 040/428 46-2598 eMail: sabine.mumm@dataport.de
Hessen	ekom21 – KGRZ Hessen Carlo-Mierendorff-Straße 11 35398 Gießen	**Verantwortlicher AP:** Herr Engelhardt Tel.: 0641/9830-1-238 Fax: 0641/9830-2-238 eMail: klaus.engelhardt@ekom21.de **Administrativer AP:** Herr Kirchner Tel.: 0641/9830-1-540 Fax: 0641/9830-2-540 eMail: christoph.kirchner@ekom21.de **Zentrale eMail-Adresse:** systembetrieb@ekom21.de
Mecklenburg-Vorpommern	Dataport Altenholzer Straße 10-14 24161 Altenholz	**Verantwortlicher AP:** Herr Christiansen Tel.: 0431/3295-6601 eMail: dirk.christiansen@dataport.de **Administrativer AP:** Frau Mumm Tel.: 040/428 46-2598 eMail: sabine.mumm@dataport.de
Niedersachsen	Zweckverband Kommunale Datenverarbeitung Oldenburg (KDO) Elsässer Straße 66 26121 Oldenburg	**Verantwortlicher AP:** Herr Luers Tel.: 0441/9714-157 Fax: 0441/9714-148 eMail: luers@kdo.de **Administrativer AP:** Herr Slotta Tel.: 0441/9714-209 Fax: 0441/9714-17-209 eMail: slotta@kdo.de **Zentrale eMail-Adresse:** lin@kdo.de
Nordrhein-Westfalen	DataClearing NRW hier: citeq, Stadt Münster Scheibenstraße 109 48153 Münster	**Verantwortlicher AP:** Herr Helmer Tel.: 0251/492-1826 Fax: 0251/492-7710 eMail: helmer@citeq.de **Adminstrativer AP:** Herr König Tel.: 0251/492-1936 Fax: 0251/492-7710 eMail: koenig@citeq.de **Zentrale eMail-Adresse:** sysunix@citeq.de

Bundesland	Landesserver-Betreiber	Ansprechpartner
Rheinland-Pfalz	Landesbetrieb Daten und Information Valenciaplatz 6 55118 Mainz	**Verantwortlicher AP:** Herr Depta Tel.: 06131/605-259 Fax: 06131/605-144 eMail: andreas.depta@ldi.rlp.de **Administrativer AP:** Herr Salzer Tel.: 06131/605-242 Fax: 06131/605-144 eMail: sven.salzer@ldi.rlp.de **Zentrale eMail-Adresse:** info@ldi.rlp.de
Saarland	DataClearing NRW hier: citeq, Stadt Münster Scheibenstraße 109 48153 Münster	**Verantwortlicher AP:** Herr Helmer Tel.: 0251/492-1826 Fax: 0251/492-7710 eMail: helmer@citeq.de **Adminstrativer AP:** Herr König Tel.: 0251/492-1936 Fax: 0251/492-7710 eMail: koenig@citeq.de **Zentrale eMail-Adresse:** sysunix@citeq.de
Sachsen	Staatsbetrieb Sächsische Informatik Dienste (SID) Niederlassung Kamenz Garnisonsplatz 10 01917 Kamenz	**Verantwortlicher AP:** Herr Söhnel Tel.: 03578/33-4710 Fax: 03578/33-55-4710 eMail: andreas.soehnel@sid.sachsen.de **Administrativer AP:** Herr Ohle Tel.: 03578/33-4722 Fax: 03578/33-55-4722 eMail: maik.ohle@sid.sachsen.de **Zentrale eMail-Adresse:** eMail: saxdvdv@sid.sachsen.de
Sachsen-Anhalt	Thüringer LandesRechenZentrum (TLRZ) Warsbergstraße 3 99092 Erfurt	Herr Homann Tel.: 0361/3784-856 Fax: 0361/3784-848 eMail: joerg.homann@tlrz.thueringen.de eMail: dvdv@tlrz.thueringen.de
Schleswig-Holstein	Dataport Altenholzer Straße 10-14 24161 Altenholz	**Verantwortlicher AP:** Herr Christiansen Tel.: 0431/3295-6601 eMail: dirk.christiansen@dataport.de **Administrativer AP:** Frau Mumm Tel.: 040/428 46-2598 eMail: sabine.mumm@dataport.de
Thüringen	Thüringer LandesRechenZentrum (TLRZ) Warsbergstraße 3 99092 Erfurt	Herr Jörg Homann Tel.: 0361/3784-856 eMail: joerg.homann@tlrz.thueringen.de eMail: dvdv@tlrz.thueringen.de

Anhang 4: Liste der Intermediärsbetreiber

Bundesland	**Name und Anschrift**	**Kontakt**
Baden-Württemberg	Kommunale Datenverarbeitung Region Stuttgart (KDRS) Krailenshaldenstr. 44 70469 Stuttgart	Rainer Rauser Tel.: 0711/8108-11609 Fax: 0711/8108-13609 eMail: r.rauser@kdrs.de
Bayern	Bayerisches Landesamt für Statistik und Datenverarbeitung Nehauser Str. 8 80331 München	Dr. Markus Wagner Tel.: 089/2119-735 Fax: 089/2119-1735 eMail: markus.wagner@lfstad.bayern.de
Berlin	rechtlich / fachlich: Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) Friedrichstr. 219 10958 Berlin technisch: IT-Dienstleistungszentrum Berlin (ITDZ Berlin) Berliner Str. 112-115 10713 Berlin	rechtlich / fachlich: Peter Fröhlich Tel.: 030/90269 2241 Fax: 030/90269 2097 eMail: Peter.Froehlich@labo.berlin.de eMail CC: christian.peters@labo.berlin.de technisch: Matthias Teubner Tel.: 030/90222 6629 eMail: Matthias.Teubner@itdz-berlin.de eMail CC: christian.peters@labo.berlin.de
Brandenburg	Brandenburgischer IT-Dienstleister (ZITBB) Dortustrasse 46 14467 Potsdam	Herr Thomas Hein Tel.: 0331/39 724 Fax: 0331/39 10724 eMail: thomas.hein@zit-bb.brandenburg.de
Bremen	bremen online services Am Fallturm 9 28359 Bremen	Herr Oliver Mania Tel.: 0421/204 95 944 Fax: 0421/204 95 11 eMail: om@bos-bremen.de
Hamburg	Dataport Altenholzer Str. 10-14 24161 Altenholz	Kirsten Groneberg-Voigt Tel.: 0431/3295-6634 eMail: Kirsten.Groneberg-Voigt@dataport.de eMail: DataportGovernikus-Support@dataport.de
Hessen	ekom21 KGRZ Hessen Carlo-Mierendorff-Str. 11 35398 Gießen	Christoph Kirchner Tel: 0641/9830-1540 eMail: christoph.kirchner@ekom21.de
Mecklenburg-Vorpommern	DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH Lübecker Straße 283 19059 Schwerin	Mathias Dinkatt Tel.: 0385/48 00 773 Fax: 0385/48 00 98 773 eMail: m.dinkatt@dvz-mv.de

Bundesland	Name und Anschrift	Kontakt
Niedersachsen	HannIT Hildesheimer Str. 20 30169 Hannover	Beate Bartels Mark Seils Tel.: 0511/616-11333 Fax: 0511/616-11081 eMail: meso@hannit.de Ulrich Jestrzembski Tel.: 0511/616-11112 Fax: 0511/616-11081 eMail: Ulrich.Jestrzembski@hannit.de
	ITEBO Dielingerstraße 39/40 49074 Osnabrück	Bernd Jarvers Tel.: 0541/9631-260 Fax: 0541/9631-196 eMail: jarvers@itebo.de Herr Hoffmann Tel.: 0541/9631-814 Fax: 0541/9631-196 eMail: hoffmann@itebo.de
	KDO Elsässer Str. 66 26121 Oldenburg	Marc Langnickel Tel.: 0441/9714-288 Fax: 0441/9714-17288 eMail: langnickel@kdo.de Frank Slotta Tel.: 0441/9714-209 Fax: 0441/9714-17209 eMail: slotta@kdo.de
	KDS Paulinerstr. 14 37073 Göttingen	Simon Hartmann Tel.: 0551/400-4133 Fax: 0551/400- 4101 eMail: hartmann@kds.de
	KOSYNUS Carl-Miele-Str. 4 38112 Braunschweig	Gereon Gieseler Tel.: 0531/48005-30 eMail: g.gieseler@kosynus.de Andreas Jenter Tel.: Service Desk: 0531/48005-55 Fax: Service Desk: 0531/48005-66 eMail: a.jenter@kosynus.de
	LK SFA Vogteistraße 19 29683 Bad Fallingbostel	Herr Patzlee Tel.: 05162/970-285 Fax: 05162/970-900285 eMail: F01401@Heidekreis.de
	Stadt Wolfsburg Porschestraße 49 38440 Wolfsburg	Wolfgang Beuermann Tel.: 05361-28-2702 Fax: 05361-28-2972 eMail: wolfgang.beuermann@stadt.wolfsburg.de Hubert Lux Tel.: 05361/281982 Fax: 05361/28-2550 eMail: Hubert.Lux@stadt.wolfsburg.de Mirko Kratzer Tel.: 05361/281763 Fax: 05361/28-2550 eMail: Mirko.Kratzer@stadt.wolfsburg.de

Bundesland	Name und Anschrift	Kontakt
	adKOMM GmbH Stadtweg 14 85134 Stammham	DV-Analyse Tel.: 01805/235666 Fax: 08405/9286 – 666 eMail: DV-Analyse@adKOMM.de
	citeq, Münster Scheibenstraße 109 48153 Münster	Frank Helmer Tel.: 0251/492-1826 Fax: 0251/492-7710 eMail: helmer@citeq.de
Nordrhein-Westfalen	citeq - Stadt Münster Scheibenstr. 109 48153 Münster DataClearing NRW	Frank Helmer Tel.: 0251/492-1826 Fax: 0251/492-7710 eMail: helmer@citeq.de
	KRZ Niederrhein Friedrich-Heinrich-Allee 130 47475 Kamp-Lintfort DataClearing NRW	Dr. Lars van der Grinten Tel.: 02842/9070-321 eMail: lars.van.der.grinten@krzn.de
	KDVZ Citkomm Griesenbraucker Str. 4 58640 Iserlohn	Michael Kampmann Tel.: 02371/439-228 eMail: kampmann.m@kdvz.de Elmar Brandt Tel.: 02371/439-126 eMail: brandt@kdvz.de
	KRZ Minden/Ravensberg Am Lindenhaus 21 32657 Lemgo	Werner Rabe Tel.: 05261/252-145 eMail: w.rabe@krz.de
Rheinland-Pfalz	LDI Valenciaplatz 6 55118 Mainz	Helpdesk Tel.: 06131/605-360 eMail: helpdesk@ldi.rlp.de
Saarland	Zweckverband eGo-Saar Talstraße 9 66119 Saarbrücken	Thomas Schulz Tel.: 0681/9264341 Fax: 0681/9264349 eMail: thomas.schulz@ego-saar.de
Sachsen	Staatsbetrieb Sächsische Informatik Dienste Niederlassung Kamenz Garnisonsplatz 10 01917 Kamenz	Robert Schenkel Tel.: 03578/33 4732 Fax: 03578/3355 4732 eMail: esv@sid.sachsen.de
Sachsen-Anhalt	Landesrechenzentrum Sachsen-Anhalt (LRZ) Barbarastr. 2 06110 Halle (Saale)	Sebastian Klugmann Tel.: 0345/1304 813 Fax: 0345/1304 899 eMail: sebastian.klugmann@sachsen-anhalt.de
	KID Magdeburg GmbH (KID) Alter Markt 15 39104 Magdeburg	Marco Hauffe Tel.: 0391/24464-120 Fax: 0391/24464-400 eMail: marco.hauffe@kid-magdeburg.de

Bundesland	Name und Anschrift	Kontakt
	adKOMM GmbH Stadtweg 14 85134 Stammham	DV-Analyse Tel.: 01805/235666 Fax: 08405/9286-666 eMail: DV-Analyse@adKOMM.de
	Kosynus GmbH Carl-Miele-Str. 4 38112 Braunschweig	
	KDRS Baden-Württemberg Krailenshaldenstr. 44 70469 Stuttgart	Rainer Rauser Tel.: 0711/8108-11609 Fax: 0711/8108-13609 eMail: r.rauser@kdrs.de
Schleswig-Holstein	Dataport Altenholzer Str. 10-14 24161 Altenholz	Kirsten Groneberg-Voigt Tel.: 0431/3295-6634 eMail: Kirsten.Groneberg-Voigt@dataport.de eMail: DataportGovernikus-Support@dataport.de
Thüringen	Thüringer Landesrechenzentrum Warsbergstraße 3 99092 Erfurt	Stefan Schwarz Tel.: 0361 37 84879 eMail: stefan.schwarz@tlrz.thueringen.de eMail: vms@tlrz.thueringen.de

Anhang 5: Liste der Registrierungsstellen der DOI-CA (Stand: 11 / 2011)

Bundesland	**Kontakt der zuständigen Registrierungsstelle**	**Login für die Web-Seiten der DOI-CA**
Baden-Württemberg	T-Systems International GmbH Trust Center Untere Industriestrasse 20 57250 Netphen Supporthotline des Telekom Trust Centers: Tel.: 0180 5/ 26 82 04 eMail: telesec_support@t-systems.com	Login: XPersonenstand Passwort: holemawa38
Bayern		
Bremen		
Hamburg		
Hessen		
Nordrhein-Westfalen		
Rheinland-Pfalz		
Saarland		
Sachsen		
Schleswig-Holstein		
Berlin	Landesamt für Bürger und Ordnungsangelegenheiten Friedrichstr. 219 10958 Berlin eMail: DOI-XhD@labo.berlin.de	Die Zugangsdaten erfragen Sie bitte bei Ihrer zuständigen Registrierungsstelle
Brandenburg	Brandenburgischer IT-Dienstleister Dezernat Infrastrukturservice Dortusstr. 46 14467 Potsdam	
Mecklenburg-Vorpommern	DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH Lübecker Str. 283 19059 Schwerin	
Niedersachsen	Landesbetrieb für Statistik und Kommunikationstechnologie Niedersachsen - SignaturCard Service - Göttinger Chaussee 259 30459 Hannover Tel.: 0511/120 3990 eMail: SignaturCard-Service@lskn.niedersachsen.de	
Sachsen-Anhalt	Oberfinanzdirektion Magdeburg, Landesrechenzentrum, PKI - Zentrale Stelle Barbarastraße 2 06110 Halle (Saale) Tel: 0345/13043852/3862 eMail: PKILSA-ZRA@liz.sachsen-anhalt.de	
Thüringen	Thüringer LandesRechenZentrum Bereich Vermittlungsstelle Warsbergstraße 3 99092 Erfurt	

Anhang 6: Glossar

Vorbemerkungen

Der AG Start XPersonenstand ist bewusst, dass dieser Leitfaden auf einige technisch geprägte Bezeichnungen und Abkürzungen nicht verzichten kann. Das bringt die bundesweite Einführung eines technischen Standards mit sich.

Um den Umgang mit den IT-Begriffen zu vereinfachen, ist dieses Glossar beigefügt worden, in dem IT-lastige Begriffe erläutert werden. Für IT-Dienstleister bzw. diejenigen Stellen, die sich bereits länger mit OSCI und XöV-Standards beschäftigen, wird das Glossar wohl keine neuen Erkenntnisse bringen.

Ergänzend zu den folgenden Ausführungen wird auf das Glossar im XöV-Handbuch (herausgegeben von der Koordinierungsstelle für IT-Standards – KoSIT – verwiesen (frei verfügbar auf www.xoev.de)

Clearing- und Vermittlungsstelle

Clearing- oder Vermittlungsstellen, zum Teil auch Nachrichtenbroker genannt, sind spezielle Ausprägungen von Transportverfahren. In der Regel kommen solche Transportverfahren in Rechenzentren für eine Vielzahl von Behörden und unterschiedliche Fachverfahren zum Einsatz. Eine Vermittlungsstelle kann auch bei einem anderen Betreiber als dem des Fachverfahrens genutzt werden. Der Betreiber der Vermittlungsstelle kümmert sich mit seinem Expertenwissen darum, dass die XPersonenstandsnachrichten ihr Ziel erreichen. Insbesondere im Fehlerfall bedeutet dies, die Ursachenforschung und -beseitigung durchzuführen.

Deutschland-Online Infrastruktur

Mit dem Vorhaben Deutschland-Online Infrastruktur (DOI) wird eine deutschlandweite Kommunikationsinfrastruktur für alle Behörden der Deutschen Verwaltung bereitgestellt, die eine übergreifende sichere Kommunikation zwischen Bundesnetzen, den Ländernetzen und Netzen der Kommunen ermöglicht. Grundlage von DOI ist die nationale E-Government-Strategie Deutschland-Online von Bund, Ländern und Kommunen aus 2006 mit dem fortgeschriebenen Aktionsplan aus 2009. Das DOI-Netz hat die bisherige föderale Netzinfrastruktur TESTA (Trans-European Services for Telematics between Administrations) zum 05.10.2009 abgelöst.

DOI-CA

Mit der DOI-CA (Deutschland-Online Infrastruktur - Certification Authority) bei der Deutschen Telekom AG wurde eine Zertifizierungsstelle für die Bundesverwaltung beauftragt, bei der u.a. Zertifikate beantragt werden können. Die "DOI-CA" stellt Zertifikate für Teilnehmer von Bund, Ländern und Kommunen aus und ist in die Verwaltungs-PKI integriert (Die Public-Key-Infrastruktur - PKI ist ein

System, das digitale Zertifikate ausstellen, verteilen und prüfen kann.). Sie wird auf der Plattform des Trust Centers der Deutschen Telekom betrieben. Verwaltungseinrichtungen und auch externe Partner von Verwaltungen, z.B. für zentrale Anwendungen wie Meldewesen, OSCI-Kommunikation oder den Bereich der hoheitlichen Dokumente, können Zertifikate der DOI-CA einzeln über eine Web-Seite beim Trust Center beantragen. Die von der DOI-CA ausgestellten Zertifikate und Sperrlisten werden im zentralen Verzeichnisdienst der Verwaltungen veröffentlicht.

DVDV

Das Deutsche Verwaltungsdiensteverzeichnis (DVDV) ist eine fach- und ebenenübergreifende Infrastrukturkomponente des E-Government in Deutschland. In diesem Verzeichnisdienst werden technische Verbindungsdaten von Online-Diensten der öffentlichen Verwaltung hinterlegt. Grundlage ist ein Verzeichnisdienst, in den Behörden und andere Betreiber mit ihren Diensten aufgenommen werden können. Auskunftssuchende und Nutzer des DVDV sind Applikationen (Fachverfahren), nicht (direkt) die Anwenderinnen und Anwender in den Verwaltungen.
Das DVDV, welches durch die Bundesstelle für Informationstechnik (BIT) im Bundesverwaltungsamt betrieben wird, hat damit die Funktion einer zentralen Registrierungsstelle für Online-Dienste der öffentlichen Verwaltung in Deutschland. Zugleich ermöglicht es eine rechtsverbindliche elektronische Kommunikation von und mit Behörden über die vorhandenen Fachverfahren auf höchstem Sicherheitsniveau.

DVDV-Bundesmaster und DVDV-Landesserver

Der Kern des DVDV ist der zentrale Bundesmaster, der durch die Bundesstelle für Informationstechnik (BIT) im Bundesverwaltungsamt (BVA) bereitgestellt wird. Er ist die einzige Stelle, bei der ein schreibender Zugriff auf die Datenbestände erfolgen kann. Der Bundesmaster spiegelt seinen Datenbestand kontinuierlich auf die dezentral in den Ländern verteilten DVDV-Landesserver.

Suchanfragen der Kommunen werden nicht an den DVDV-Bundesmaster gestellt sondern ausschließlich an die dezentralen DVDV-Landesserver. Diese teilen sich somit die Anfragelast und springen bei einem Ausfall gegenseitig ein.

DVDV - Pflegende Stelle

Pflegende Stellen werden von den Ländern zur Pflege der Daten im Deutschen Verwaltungsdiensteverzeichnis eingerichtet. Pro Land wird zurzeit nur genau eine Pflegende Stelle zugelassen. Diese Stellen tragen landesbezogen im Auftrag der Verwaltungen deren Daten in den Bundesmaster des DVDV ein.

Hosting (gehostet)

Das Wort Hosting leitet sich aus dem Englischen für "Gastgeber" ab. Unter Hosting versteht man in diesem Kontext das Bereitstellen, Betreiben und Überwachen einer Anwendung, insbesondere eines Fachverfahrens. Das Hosting wird regelmäßig von einem Rechenzentrum auf dessen Servern durchgeführt(das Fachverfahren wird "gehostet").

Intermediär

Der Intermediär ist die Stelle, über die in OSCI-Transport zwei Kommunikationspartner (wobei hier Computersysteme bzw. Softwarekomponenten und nicht menschliche Benutzer gemeint sind) miteinander kommunizieren.

Der Sender erzeugt eine OSCI-Nachricht und verschlüsselt diese mit dem öffentlichen Schlüssel des Empfängers. Diese verschlüsselte Nachricht wird dann noch einmal mit dem öffentlichen Schlüssel des Intermediärs des Empfängers verschlüsselt (Prinzip des doppelten Umschlags). Der Intermediär des Empfängers kann nun den äußeren Umschlag öffnen und die – immer noch verschlüsselte – eigentliche OSCI-Nachricht in das Postfach des Empfängers ablegen. Geht eine Nachricht beim Intermediär ein, so gilt sie als rechtsverbindlich zugestellt.
Datenschutzrechtlich wichtig ist, dass der Intermediär niemals auf die Inhaltsdaten einer OSCI-Nachricht zugreifen kann.
Der Empfänger wiederum kann die Nachrichten aus seinem Postfach abholen (hierzu benötigt er den öffentlichen Schlüssel des Intermediärs) und verarbeiten.

Zu den Aufgaben des Intermediärs gehören neben der Postfachverwaltung die Zertifikatsprüfung sowie Protokollierungen und zahlreiche andere Prüfungen, die die korrekte Durchführung des Nachrichtentransports sichern.

OSCI

Technische Grundlage der Datenübermittlung mit XPersonenstand ist die Spezifikation OSCI (Online Services Computer Interface), zu der unter http://www.osci.de/materialien/summary.pdf eine Beschreibung zu finden ist.

Registrierungsstelle

Organisation, bei der Zertifikate beantragt werden können. Diese prüft die Richtigkeit der Daten im gewünschten Zertifikat und genehmigt den Zertifikatsantrag, der dann durch die Zertifizierungsstelle signiert wird.

Signatur

Im Rahmen von E-Business werden an die übertragenen Informationen zwei wesentliche Anforderungen gestellt: Erstens muss der Empfänger der Daten zweifelsfrei feststellen können, wer der Absender ist (Authentizität und Nichtabstreitbarkeit) und zweitens muss ausgeschlossen werden, dass die Daten durch die Beteiligten, oder durch Dritte unbemerkt manipuliert oder verfälscht werden können (Integrität).

Beide Anforderungen können durch den Einsatz der elektronischen Signatur erfüllt werden: Mit Hilfe von kryptographischen Verfahren macht die elektronische Signatur jede Manipulation oder Verfälschung an den Originaldaten für den Empfänger sofort erkennbar. (So kann z.B. aus einem Text ein Schlüsselwert berechnet und ebenfalls übermittelt werden. Sollte der Text auf dem Weg zum Empfänger manipuliert worden sein, würde sich aus dem Text beim Empfänger ein anderer Schlüsselwert berechnen lassen und der Empfänger die Manipulation durch den Vergleich der Schlüsselwerte erkennen.) Durch die Zuordnung der kryptographischen Schlüssel zum Kommunikationspartner lässt sich außerdem der Urheber einer signierten Nachricht zweifelsfrei feststellen.

Elektronische Signaturen schützen nicht davor, dass Unbefugte Einblick in Daten erhalten. Bei vertraulichen Daten ist deshalb zusätzlich zur elektronischen Signatur eine Verschlüsselung erforderlich.

Einfache elektronische Signaturen dienen nur dazu, den Urheber einer Nachricht zu kennzeichnen. Für sie sind keine Richtlinien definiert. Es kann sich auch um eine gescannte Unterschrift handeln, die abgespeichert wird. Dieser Signaturtyp hat nur geringen Beweiswert. Einfache Signaturen weisen damit keine Sicherheit gegen Fälschung auf.

Fortgeschrittene Signaturen sind Signaturen, die es ermöglichen, die Authentizität und Unverfälschtheit der durch sie signierten Daten zu prüfen.

Die qualifizierte elektronische Signatur ist die Entsprechung zur herkömmlichen Unterschrift in der elektronischen Welt. Sie ermöglicht die langfristige Überprüfbarkeit der Urheberschaft einer Erklärung im elektronischen Datenverkehr.

TrustCenter

Ein TrustCenter ist eine vertrauenswürdige Stelle, die in elektronischen Kommunikationsprozessen die jeweilige Identität des Kommunikationspartners bescheinigt. Beispielsweise übernehmen TrustCenter die Überprüfung der Gültigkeiten von Zertifikaten sowie die Ausstellung von Zertifikaten, anhand derer die Identität von Kommunikationspartnern ermittelt werden kann.

URL

Eine URL (Uniform Resource Locator) identifiziert und lokalisiert eine Ressource über die zu verwendende Zugriffsmethode (z. B. über ein Netzwerkprotokoll) und den Ort der Ressource in Computernetzwerken. Im allgemeinen Sprachgebrauch wird sie auch als Internetadresse oder Webadresse bezeichnet.

Verschlüsselungsalgorithmus

Der Verschlüsselungsalgorithmus ist eine Verfahrensvorschrift zur Ver- oder Entschlüsselung von Informationen. Mit Hilfe eines oder mehrerer Schlüssel kann eine Information verschlüsselt und wieder entschlüsselt werden. Zum Beispiel könnte man jeden Buchstaben durch seinen Nachfolgebuchstaben und jede Ziffer durch ihre Folgeziffer verschlüsseln: anstelle "Hallo5" würde dann "Ibmmp6" übermittelt.

Das Verschlüsselungsverfahren (kryptographisches System) wird auch dazu genutzt, um Kontrolldaten aus der zu versendenden Information zu erzeugen, die dann zusammen mit der ursprünglichen Information dem Empfänger übermittelt werden. Der Empfänger kann durch Anwendung desselben Verschlüsselungsverfahrens und Vergleich der dadurch erzeugten Kontrolldaten mit den übermittelten Kontrolldaten überprüfen, ob die gesendete Information manipuliert wurde oder nicht.

WSDL

Die Web Service Description Language (WSDL) ist eine plattform-, programmiersprachen- und protokollunabhängige Beschreibungssprache für Netzwerkdienste (Web Services) zum Austausch von Nachrichten auf Basis von XML. WSDL ist eine Metasprache, mit deren Hilfe Funktionen, Daten, Datentypen und Datenaustauschprotokolle eines Netzwerkdienstes beschrieben werden können.

Zertifikat (Kombizertifikat)

Zusammen mit einem signierten Dokument wird ein weiteres, ebenfalls elektronisch signiertes Dokument vorgelegt, das die Signatur des Ersteren beglaubigt. Weil eine solche Beglaubigung auf Englisch "certificate" heißt, wird sie auch im Deutschen meist als Zertifikat bezeichnet.

Ein digitales Zertifikat ist ein Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann.

Für die Ende-zu-Ende-Verschlüsselung des Transportweges ist ein Zertifikat erforderlich. Mit diesem Zertifikat werden die Nachrichten (für den Anwender unbemerkt) ver- und entschlüsselt.

Will man zudem die Nachricht auch noch signieren, benötigt man eine Signatur, mit der man den Unterzeichner bzw. Signaturersteller identifizieren und die Integrität der signierten elektronischen Informationen prüfen kann. Die elektronische Signatur erfüllt somit technisch gesehen den gleichen

Zweck wie eine eigenhändige Unterschrift auf Papierdokumenten. Welche Varianten von Signaturen es gibt, ist im Glossareintrag „Signatur“ erläutert.

Die Signaturen können einen kryptografischen Schlüssel enthalten, mit dem man sowohl ver- und entschlüsseln als auch signieren kann. Das bedeutet, die Funktionen Ver-/Entschlüsselung und Authentisierung können mit einem Zertifikat bereitgestellt werden ("Kombizertifikat").

Änderungsverzeichnis

Version	Zustand	Datum	Autor	Änderungen
1.0	final	09.12.2011	AG Start XPersonenstand	
1.0.1	final	26.03.2012	Adalbert Marienfeld	Pflege DVDV in Rheinland-Pfalz
1.0.2	final	07.09.2012	AG Start XPersonenstand	Präzisierung OSCI-Zertifikat (Punkt 3.3, 2.Absatz)
1.1	final	22.04.2015	AG Start XPersonenstand	Beantragung des OSCI-Zertifikats bei der Fa. T-Systems unter Angabe einer Kennung zur Zuordnung zur Master-Domäne „Oeffentliche Verwaltung“
1.2	final	07.07.2015	Adalbert Marienfeld	Beantragung des OSCI-Zertifikats bei der Fa. T-Systems: Änderung der Beantragungs-Rubrik sowie des Handbuch-Titels