Schleswig-Holstein
Der echte Norden

Schleswig-Holstein
Ministerium für Inneres und Bundesangelegenheiten

Leitfaden zur elektronischen Kommunikation zwischen Standesämtern und Gesundheitsbehörden mit XPersonenstand

(StA2GB)

Herausgeber: AG Sterbefallmitteilungen

Inhaltsverzeichnis

An der AG und an der Entwicklung dieses Leitfadens haben mitgewirkt:

- PG Standard
    - citeq, Stadt Münster
- Innenministerien der Länder
    - Ministerium für Inneres und Bundesangelegenheiten des Landes Schleswig-Holstein
- Gesundheitsministerien der Länder
    - Ministerium für Soziales, Gesundheit, Wissenschaft und Gleichstellung des Landes Schleswig-Holstein
    - Senatsverwaltung für Gesundheit und Soziales des Landes Berlin
    - Sächsisches Staatsministerium für Soziales und Verbraucherschutz
- Standesämter
    - Stadt Kiel
    - Stadt Mönchengladbach
- Gesundheitsbehörden
    - Kreis Plön
    - Landkreis Vorpommern-Rügen
    - Kreis Mettmann
    - Rheinkreis Neuss
    - Stadt Bremerhaven
    - Landesgesundheitsamt Baden-Württemberg
- Kommunales Forum für Informationstechnik e.V. Schleswig-Holstein
- Bayerisches Landesamt für Statistik
- Betrieb des Standards XPersonenstand
    - Stadt Dortmund

Änderungsverzeichnis

Version	Zustand	Datum	Autor	Änderungen
1.0	final	xx.xx.2015	AG Sterbefallmitteilungen	

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,da grundlegende Daten wie z. B. Name, Anschrift und Todeszeitpunkt mehrfach erfasst werden. Bei bundesweit im Jahr 2013 etwa 900.000 Sterbefällen und den dadurch erforderlichen Mitteilungen summiert sich allein die durch eine elektronische Kommunikation mögliche Einsparung von Erfassungskosten bei den Gesundheitsbehörden auf erhebliche Beträge. Nach Schätzungen der Kommunalen Landesverbände Schleswig-Holsteins könnten in den Gesundheitsbehörden Schleswig-Holsteins durch die Einführung der elektronischen Übermittlung durchschnittlich ca. 0,5 Stellen pro Gesundheitsbehörde für die Erfassung eingespart werden. Vergleichbare Schätzungen aus anderen Bundesländern sind nicht bekannt. Die Effizienz bei den Gesundheitsbehörden steigt, wenn Daten beim Empfänger zur weiteren Bearbeitung automatisiert in Fachverfahren übernommen werden können.

Von Seiten der Gesundheitsbehörden wird allerdings darauf aufmerksam gemacht, dass die Erfassung von Sterbefalldaten in den Fachverfahren der Gesundheitsbehörden nicht in allen Bundesländern landesrechtlich den Gesundheitsbehörden als Aufgabe übertragen ist. Hier gilt es dann, landesrechtliche Besonderheiten zu berücksichtigen.

Für eine elektronische Übermittlung der Daten unabhängig von den vor Ort jeweils eingesetzten Fachverfahren setzen die Standesämter den bundesweit einheitlichen Standard XPersonenstand ein. Dieser wurde in der Version 1.7.0 entsprechend erweitert und kann mit deren Wirksamkeit ab 01.05.2016 für die Übermittlung der Sterbefallmitteilungen an die Gesundheitsbehörden genutzt werden. Voraussetzung dafür ist eine landesrechtliche Regelung, die eine Teilnahme an der in diesem Leitfaden beschriebenen elektronischen Kommunikation (XPersonenstand über OSCI-Transport) ausdrücklich zulässt. Die Arbeitsgruppe hat einen Vorschlag für eine solche landesrechtliche Regelung entwickelt (Anhang 8).

1.1. Einordnung der Kommunikation

Das nachstehende Schaubild stellt die Datenflüsse der Gesundheitsbehörde des Sterbeortes bei der Erstellung, Übermittlung und Verwendung der Todesbescheinigungen und der darin enthaltenen Daten dar.

Der Gesamtprozess umfasst eine Vielzahl an beteiligten Kommunikationspartnern. Der Standard XPersonenstand beschreibt mit den Sterbefallmitteilungen der Standesämter an die Gesundheitsbehörden des Sterbeortes den Teilprozess 3 dieses Kommunikationsprozesses. Andere Kommunikationsbeziehungen der Gesundheitsbehörden sind nicht Bestandteil von XPersonenstand. Daher bezieht sich dieser Leitfaden nur auf den Teilprozess 3 im Schaubild.

In diesem Leitfaden wird von der Verwendung von OSCI-Transport für den Teilprozess 3 ausgegangen. Die damit geschaffenen Voraussetzungen für eine elektronische Datenübermittlung eröffnen die

Möglichkeit einer zukünftigen Weiterverwendung in anderen Teilprozessen der dargestellten Prozessübersicht. Dabei wird auf Standards gesetzt, die in den elektronischen Kommunikationsprozessen im Bereich der Innenverwaltung etabliert sind.

Teilprozess 3 stellt eine landesinterne Kommunikation dar, die in geschlossenen Verwaltungsnetzen ablaufen könnte. Für alle weiteren Teilprozesse können länderübergreifende Kommunikationen erforderlich werden, die eine standardisierte Kommunikation mit OSCI-Transport und der Nutzung des DVDV erfordern. Hierzu sind einheitliche Behördennummern sowie eine Adressierung über das Deutsche Verwaltungsdienste-Verzeichnis (DVDV) und ein gesicherter Versand über OSCI-Transport notwendig.

Die in diesem Leitfaden beschriebenen Standardisierungen wären damit als Grundlage für die Implementierung weiterer elektronischer Kommunikationsprozesse in der Gesundheitsverwaltung nutzbar.

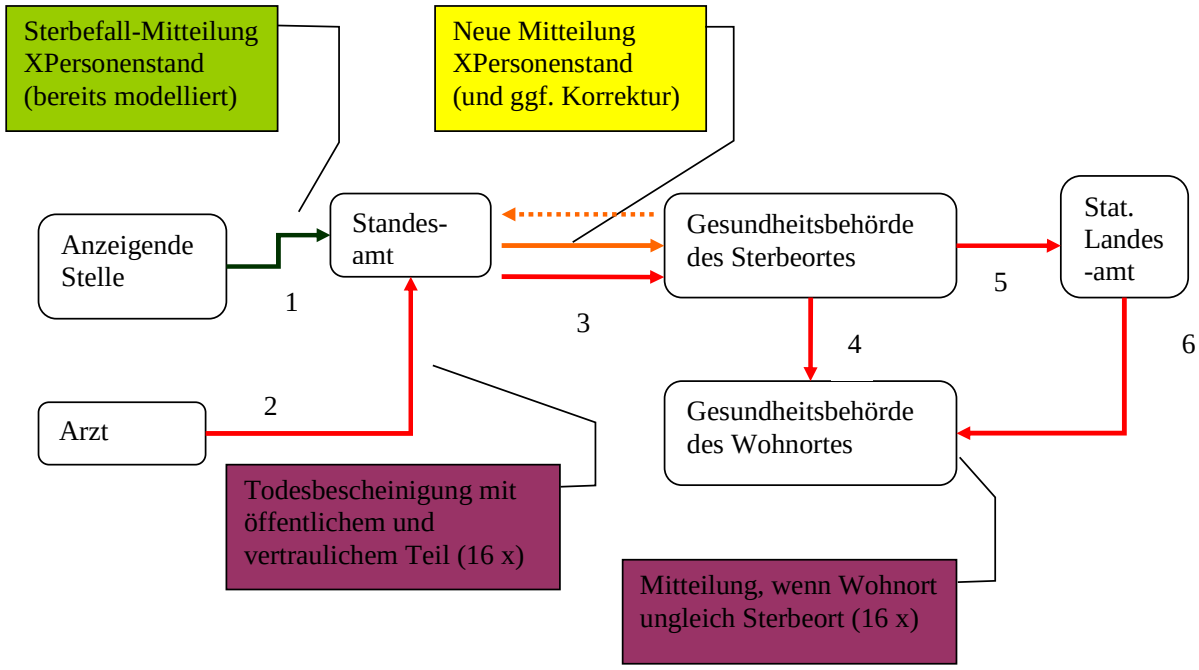

Abbildung 1: Schaubild des Gesamtprozesses einer möglichen elektronischen Kommunikation der Gesundheitsbehörden. Die Erläuterungen finden sich im Anhang 1

1.2. Zielsetzung des Leitfadens

Die Arbeitsgruppe Sterbefallmitteilungen[1] unterstützt mit diesem Leitfaden die Gesundheitsbehörden dabei, die erforderliche Infrastruktur zur elektronischen Kommunikation mit den Standesämtern über den Datenaustauschstandard XPersonenstand aufzubauen und einzusetzen. Hierzu zeigt der Leitfaden die erforderliche Organisation und Technik auf, wie Sterbefallmitteilungen der Standesämter über die in der Innenverwaltung etablierte OSCI-Infrastruktur auch außerhalb gesicherter Behördennetze an die Gesundheitsbehörden übermittelt werden können.

[1] Die Arbeitsgruppe wurde im Jahre 2013 durch die Projektgruppe Standard des Arbeitskreises I der Innenministerkonferenz mit dem Auftrag eingerichtet, unter Einbeziehung der Gesundheitsämter eine umfassende Betrachtung und Bewertung des Datenübermittlungsprozesses zwischen den Standes- und den Gesundheitsämtern bei der Mitteilung von Sterbefällen vorzunehmen. Außerdem soll die AG ermitteln, welche Regelungen und Technik bei den Gesundheitsbehörden implementiert werden muss, um XPersonenstand nutzen zu können.

Dieses Verfahren gilt für die Bundesländer, in denen die Erfassung der Sterbefalldaten durch die Gesundheitsämter landesrechtlich geregelt und etabliert ist. Für andere Bundesländer bietet das Konzept einen sachgerechten technischen Standard für die Entwicklung landesspezifischer Verfahren.

1.3. Die Standards XPersonenstand und OSCI-Transport

1.3.1. XPersonenstand

XPersonenstand ist Teil des E-Government-Aktionsplans Deutschland Online, der alle Verwaltungsbereiche umfasst.
So kommt die elektronische Kommunikation bereits im Melde- und Personenstandswesen sowie im Pass- und Ausweisbereich zum Einsatz. Die hierfür geschaffenen technischen Infrastrukturen können auch von den Gesundheitsbehörden 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 Empfängers weiterverarbeitet werden, wenn sie vom Absender in einem anderen Fachverfahren erzeugt wurden. Von dieser Standardisierung der elektronischen Kommunikation sollen auch die Gesundheitsbehörden profitieren. Daher wurde in der Spezifikation von XPersonenstand mit der Version 1.7.0 das Kapitel 13 für die Kommunikation zwischen Standesämtern und Gesundheitsbehörden eingefügt.
Nähere Informationen hierüber 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)

1.3.2. 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.

1.4. Erste Ansprechpartner

Im Regelfall wird der IT-Dienstleister der Gesundheitsbehörde (sei es ein Rechenzentrum oder die IT-Abteilung der zuständigen Verwaltung) für die Einrichtung und den Betrieb der elektronischen Kommunikation der Gesundheitsbehörde mit seinen Kommunikationspartnern sorgen. Er plant gemeinsam mit der Gesundheitsbehörde 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-, Personenstands-, Ausländer- oder Pass- und Personalausweisbereich 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 verschiedenen Ländern (z.B. Schleswig-Holstein, Thüringen) 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.

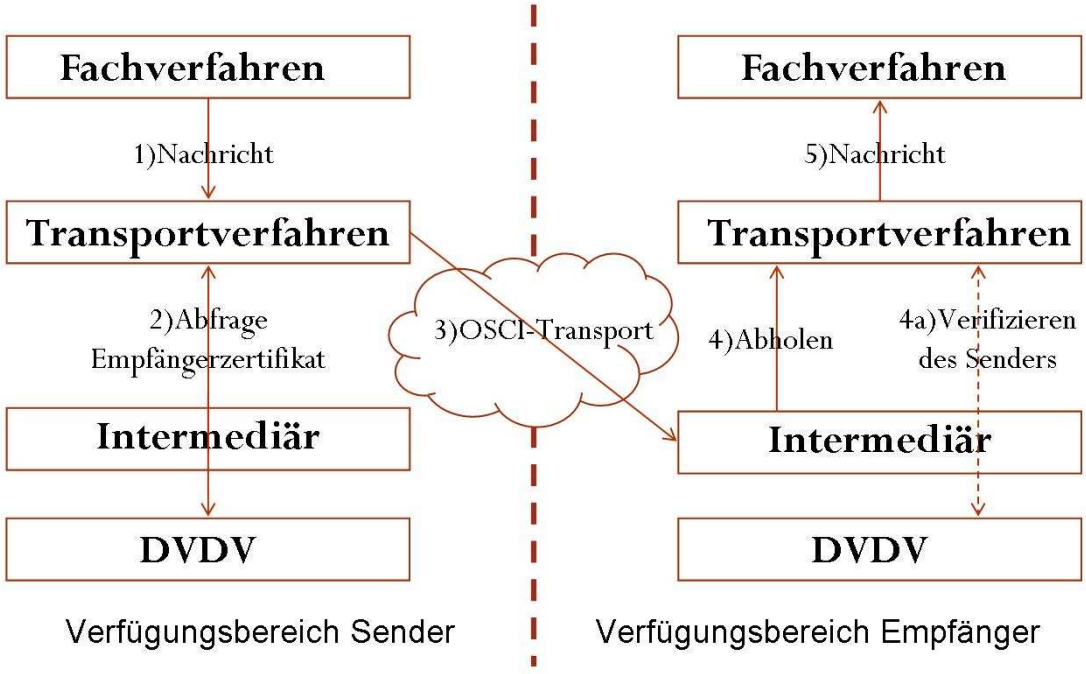

Abbildung 2: schematische Darstellung der beteiligten Komponenten in XPersonenstand

2.1. Fachverfahren – die Anwendungs-Software?

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

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

2.2. Transportverfahren – die elektronische Poststelle

Ein Transportverfahren versendet und empfängt elektronische Nachrichten. Wie bei der hausinternen Poststelle muss also auch hier innerhalb eines gesicherten Netzes ein Verfahren zum Einsatz kommen, mit dessen Hilfe die Nachrichten in die richtige Form („Briefumschlag“) gebracht und versandt werden. Solche Transportverfahren sind für die elektronische Kommunikation im Melde-, Personenstands-, Ausländer-, Pass- und Personalausweisbereich bereits etabliert und sollen auch für XPersonenstandsnachrichten an die Gesundheitsbehörden genutzt werden. Eine besondere Ausprägung erfahren diese Transportverfahren in den Bundesländern, in denen Clearing- oder Vermittlungsstellen eingerichtet sind und sich IT-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 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 sollte durch eine landesrechtliche Vorgabe in den bestattungsrechtlichen Regelungen unter dem Sammelbegriff OSCI-Transport beschrieben werden (vgl. hierzu die Formulierung im Regelungsvorschlag in Anhang 8).

2.3. Zertifikate – die elektronische Identifikation

Zertifikate und die darin enthaltenen Signaturen sind wichtige Grundlagen für die elektronische Kommunikation. Sie sind erforderlich, um die Authentizität, die Vertraulichkeit und die Integrität von Daten sicherzustellen.
In der Datenübermittlung des Personenstandswesens kommen nur „fortgeschrittene Zertifikate“ der DeutschlandOnlineInfrastruktur (DOI) zum Einsatz, die auch zur automatisierten Nutzung (z.B. durch ein Transportverfahren) freigegeben sind. Die Gesundheitsbehörden beantragen ggf. mit Unterstützung des jeweiligen IT-Dienstleisters bei einer Registrierungsstelle (vgl. Anhang 6) ein ebensolches Zertifikat.

2.4. Intermediär – der elektronische Briefkasten

Intermediäre stellen im Rahmen der Kommunikation über OSCI-Transport Postfächer für Gesundheitsbehörden bereit. Damit die anderen Kommunikationspartner aus dem gesamten Bundesgebiet sie regelmäßig erreichen können, müssen Intermediäre mit weitgehender 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 Melde- und Personenstandswesen haben sich einige Intermediärsbetreiber etabliert. Als Intermediärsbetreiber kommen auch die Betreiber der zentralen Infrastrukturen der Clearing- und Vermittlungsstellen in Frage. Eine nicht abschließende Liste mit Ansprechpartnern findet sich im Anhang 5.

2.5. DVDV – das Telefonbuch

Für einen elektronischen Mitteilungsverkehr zwischen den Standesämtern und den Gesundheitsbehörden müssen die Kommunikationspartner eindeutig adressierbar sein. Dazu müssen die Gesundheitsbehörden 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 und der Gesundheitsbehörden verzeichnet.

Für die Aufnahme in das DVDV sind ein Präfix für Behördenkennung und eine eindeutige Behördennummer erforderlich. Das Präfix ist bundesweit für die Gesundheitsbehörden mit „ghb“ festgelegt. Zur Festlegung der Behördennummern sind die Gesundheitsministerien der Länder mit Schreiben vom 8. Dezember 2014 gebeten worden, diese nach einheitlicher Struktur landesspezifisch zu vergeben und

zu pflegen. Im Folgenden ist unter dem Begriff „Behördennummer“ Präfix und Behördennummer zu verstehen.

Beim DVDV wird automatisiert ermittelt, ob ein Standesamt den elektronischen Dienst der Übermittlung von Sterbefalldaten nutzen kann. Wenn dem so ist, schickt das DVDV die Kommunikationsdaten der zu adressierenden Gesundheitsbehörde 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 Gesundheitsbehörden müssen ihre Behördennummer 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. Jede Gesundheitsbehörde 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. Behördennummer, aktuelle Zertifikate, aktuelle Signaturen etc.) übermittelt werden. In einigen Ländern wird diese Aufgabe zentral von Clearing- oder Vermittlungsstellen wahrgenommen.

3. Maßnahmen zur Inbetriebnahme

Vor Aufnahme der elektronischen Kommunikation mit dem Standesamt muss die entsprechende landesrechtliche Regelung im Bestattungsrecht geschaffen sein, die diese Art der Kommunikation zulässt.

Zur technischen Vorbereitung des Betriebs von XPersonenstand in den Gesundheitsbehörden müssen in Abstimmung mit dem IT-Verantwortlichen der Behörde oder dem jeweiligen IT-Dienstleister folgende Aktionen durchgeführt werden:

- Einsatz einer XPersonenstand-konformen Fachverfahrensversion
- Nutzung eines Transportverfahrens
- Beschaffung des Kombizertifikats (OSCI-Zertifikat)
- Abstimmung mit dem Intermediärsbetreiber für das Land (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 die Gesundheitsbehörde von einem Rechenzentrum betreut wird, wird dieses in der Regel die erforderlichen Schritte einleiten. Das zuständige Rechenzentrum sollte diesen Leitfaden zur Umsetzung zur Verfügung haben.
Soweit die IT eigenverantwortlich betrieben wird, muss die Behörde oder die IT-Abteilung der 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 ist im Anhang 2 zur Orientierung hinterlegt.

3.1. Einsatz einer XPersonenstand-konformen Fachverfahrensversion

Die in der Gesundheitsbehörde genutzte Version des Fachverfahrens muss XPersonenstand in der jeweils gültigen Fassung unterstützen.
Die Information über die jeweils gültige Fassung von XPersonenstand sind unter http://xpsw.domap.de nachzulesen.

3.2. Nutzung eines Transportverfahrens

Das Transportverfahren stellt die Schnittstelle zwischen dem gesundheitsbehördlichen 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

Das zuständige Rechenzentrum oder die IT-Abteilung der Gesundheitsbehörde muss klären, ob bereits eine OSCI-Transportinfrastruktur vorhanden ist, damit diese ggf. auch für die Übermittlung an die Gesundheitsbehörden genutzt werden kann. Anderenfalls kann der Fachverfahrenshersteller gefragt werden, welche Transportverfahren von seiner Software unterstützt werden. Alternativ kann der Transportverfahrenshersteller mitteilen, ob das in der Gesundheitsbehörde eingesetzte Fachverfahren von seiner Software angebunden werden kann.

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.

Bereits eingesetzte OSCI-Verschlüsselungszertifikate 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[2] 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

  Diese Registrierungsstellen unterstützen auch bei Fragen zum Zertifikatsmanagement und stellen teilweise eigene Anleitungen für die Antragstellung zur Verfügung. Darüber hinaus unterstützen diese Registrierungsstellen bei der Einstellung der Zertifikate in das DVDV (Deutsches Verwaltungsdiensteverzeichnis).
  Die näheren Angaben zu den einzelnen Registrierungsstellen sind im Anhang 6 dieses Leitfadens zu finden.

- Gesundheitsbehörden aus allen anderen Bundesländern nutzen 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 Anmeldung auf der Internetseite sind folgende Daten zu verwenden:

  LOGIN: XPersonenstand
  PASSWORT: holemawa38

  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 Beantragungsverfahren ist unter der Rubrik „Handbücher“ und dort unter dem Titel „Handbuch Teilnehmer öffentliche Verwaltung“ im PDF-Format zu finden.

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

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 den elektronischen Briefkasten der Gesundheitsbehörde vor. In den Verfahren der Innenverwaltung haben sich in allen Bundesländern bereits Intermediärsbetreiber etabliert. Das zuständige Rechenzentrum oder bei die IT-Abteilung der Behörde können mitteilen, ob ein vorhandener Intermediär genutzt werden kann. Ergänzend ist im Anhang 5 eine Liste dieser Betreiber inklusive Kontaktinformationen zu finden.

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

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 (Gesundheitsbehörde)
- Behördennummer der Gesundheitsbehörde als elektronischer Schlüssel
- Name/Adressdaten der Gesundheitsbehörde
- OSCI-Zertifikat (Kombizertifikat, gleichzeitig Funktion der Inhaltsdatenverschlüsselung)
- Informationen zum verwendeten Intermediär (Zertifikat des Intermediärs, URL des Intermediärs)

Die bei der Eintragung 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 ist im Anhang 3 wiedergegeben.

3.6. Abstimmung mit dem DVDV-Landesserverbetreiber

Der Abruf der Kommunikationsdaten erfolgt über Landesserver, die eine Kopie des bundesweit einheitlichen „Telefonbuchs“ (DVDV) vorhalten.

Das zuständige Rechenzentrum oder die IT-Abteilung der Gesundheitsbehörde haben Informationen, welcher DVDV-Landesserver in den Verfahren der Innenverwaltung genutzt wird. Die Kontaktdaten Ihres Landesserverbetreibers finden Sie im Anhang 4.

Vom zuständigen DVDV-Landesserverbetreiber erhält die Gesundheitsbehörde die Zugriffsdatei auf das DVDV – eine so genannte WSDL-Datei. Diese muss nach Vorgabe des Transportverfahrens dort eintragen (siehe auch Kapitel 3.2) werden.

Anhang 1: Erläuterung der Datenflüsse

Die in Kapitel 1 dargestellte Grafik dient der Veranschaulichung der Datenflüsse zwischen den Beteiligten:

1. Anzeigende Stelle an Standesamt

In der Regel teilt die anzeigende Stelle einem Standesamt einen Sterbefall schriftlich mit. Anzeigende Stelle können Kliniken, Reha-Einrichtungen, Alten- und Pflegeheime oder auch natürliche Personen sein.

2. Arzt über den Bestatter oder der beauftragte Person an das Standesamt

Der Arzt, der die Leichenschau vornimmt, trägt die Daten in den vertraulichen und nichtvertraulichen Teil der Sterbefallmitteilung ein und verschließt den vertraulichen Teil in einem Umschlag. Beide Teile werden an den Bestatter oder deren beauftragte Person weitergegeben.

Der Bestatter oder deren beauftragte Person wenden sich mit vertraulichem und nichtvertraulichem Teil der Sterbefallmitteilung an das Standesamt. Das Standesamt vervollständigt die Daten, beurkundet den Todesfall und vergibt eine Personenstandsregisternummer (Sterberegister).

Hier wäre eine elektronische Mitteilung mit XPersonenstand möglich. Die Mitteilung ist spezifiziert. Die Umsetzung erfolgt nicht, da die Fachverfahren der Bestatter die Daten nicht übermitteln können, weder Bestatter noch Verfahrenshersteller die Kosten für eine Anpassung der Verfahren tragen wollen und es keine rechtliche Verpflichtung zur elektronischen Datenübermittlung gibt.

3. Standesamt an Gesundheitsbehörde Sterbeort

Bisher: Das Standesamt leitet den vertraulichen und nichtvertraulichen Teil der Sterbefallmitteilung in Papierform an die Gesundheitsbehörde weiter (roter Pfeil). Die Gesundheitsbehörde trägt die Daten ggf. von Hand in ihr Fachverfahren[3] ein.

Zukünftig: Das Standesamt versendet eine Mitteilung mit allen im Fachverfahren des Standesamts verfügbaren Daten aus dem nichtvertraulichen Teil der Sterbefallmitteilung an die Gesundheitsbehörde (orangefarbener Pfeil; siehe Kapitel 13 der Spezifikation XPersonenstand 1.7.0); nichtvertraulicher und vertraulicher Teil der Sterbefallmitteilung werden an die Gesundheitsbehörde in Papierform weitergeleitet. Die Gesundheitsbehörde trägt den vertraulichen Teil sowie die Daten, die nicht in der elektronischen Mitteilung enthalten waren, ggf. von Hand in ihr Fachverfahren ein[3]. Der gestrichelte orangefarbene Pfeil deutet die mögliche elektronische Fehlermeldung (RTS-Nachricht) für die elektronische Sterbefallmitteilung an. Die RTS-Nachricht (rts = return to sender) ist ebenfalls in XPersonenstand 1.7.0 modelliert (Kapitel 15 „Administrative Nachrichten“)[4].

4. Gesundheitsbehörde Sterbeort an Gesundheitsbehörde Wohnort

Die Gesundheitsbehörde des Sterbeortes übermittelt den vertraulichen und nichtvertraulichen Teil der Sterbefallmitteilung an die Gesundheitsbehörde des Wohnortes. Grundsätzlich könnte man auch eine elektronische Mitteilung mit XPersonenstand an die Gesundheitsbehörden des Wohnortes senden.

[3] Dies gilt für diejenigen Bundesländer, in denen eine entsprechende Datenerfassung landesrechtlich den Gesundheitsbehörden als Aufgabe zugewiesen worden ist; insoweit besteht keine bundeseinheitliche Verfahrensvorgabe.

[4] Ab Version 1.7.1 von XPersonenstand wird die RTS-Nachricht aus dem gemeinsamen Standard der Innenverwaltung XInneres (Kapitel 4 „Administrative Nachrichten“) verwendet.

Dann fehlten aber die vertraulichen Teile. Bisher ist dieser Schritt in der Prozessbeschreibung nicht vorgesehen.

5. Gesundheitsbehörde Sterbeort an Statistik

Die Gesundheitsbehörde des Sterbeortes übermittelt die Daten an die Statistik. Diese Daten müssen bereits in vielen Fällen elektronisch übermittelt werden (z.B. § 2 Abs. 7 BevStatG).

6. Statistik an Gesundheitsbehörde des Wohnortes

In einigen Ländern findet aufgrund landesrechtlicher Reglungen eine Rückübermittlung von Daten (ärztliche Diagnosen auf den Todesbescheinigungen angereichert um die ICD-Codes) an die Gesundheitsbehörden stattestellt.

Anhang 2: Checkliste

Diese Checkliste zeigt die einzelnen Schritte des Kapitels 4 auf. Wenn Sie die einzelnen Schritte der Checkliste abgehakt haben, steht einer Produktivsetzung von XPersonenstand im Umfeld der Gesundheitsbehörden technisch nichts mehr im Wege.

Nr.	Thema	Aufgabe	Zuständigkeit	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	Behördennummer inkl. Präfix für die Behördenkennung	Bildung der Behördennummer 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 3: Liste der Pflegenden Stellen DVDV

Stand: Mai 2015

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 St.-Martin-Straße 47 81541 München	Herr Klaus Engelhardt Tel.: 089/2119-3257 eMail: klaus.engelhardt@lfstad.bayern.de eMail: vps-serviceline@lfstad.bayern.de
Berlin	Landesamt für Bürger- und Ordnungsangelegenheiten Friedrichstraße 219 10958 Berlin	Herr Christian Peters Frau Heike Finger 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	Governikus 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 Altenholzer Straße 10-14 24161 Altenholz	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 Knorrstraße 30 34134 Kassel	Herr Uwe Geerk Tel.: 06151/704-1360 Fax: 06151/704-2030 eMail: uwe.geerk@ekom21.de
Mecklenburg-Vorpommern	Zweckverband Elektronische Verwaltung in 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	IT.Niedersachsen Göttinger Chaussee 259 30459 Hannover	Frau Astrid Buchmann-Cattau Tel.: 0511/9898-1235 Fax: 0511/120-99-27116 eMail: dvdv@it.niedersachsen.de eMail: astrid.buchmann-cattau@it.niedersachsen.de
Nordrhein-Westfalen	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 Landesbetrieb Daten und Informationen (KommWis) Hindenburgplatz 3 55118 Mainz	Herr Peter Hempel Tel.: 06131/6277-270 Fax: 06131/6277-288 eMail: phempel@kommwis.de eMail: dvdv@nic.rlp.de
Saarland	Zweckverband eGo-Saar Talstraße 9 66119 Saarbrücken	Herr Thomas Schulz Tel.: 0681/9264341 Fax: 0681/9264349 eMail: thomas.schulz@ego-saar.de eMail : vermittlungsstelle@ego-saar.de
Sachsen	Staatsbetrieb Sächsische Informatik Dienste Garnisonsplatz 11 01917 Kamenz	Herr Maik Ohle Tel.: 0351/32647364 eMail: saxdvdv@sid.sachsen.de
Sachsen-Anhalt	Oberfinanzdirektion Magdeburg, Landesrechenzentrum Dataport Standort Halle 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: datatportdvdvst@liz.sachsen-anhalt.de
Schleswig-Holstein	Dataport AöR Altenholzer Straße 10-14 24161 Altenholz	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 4: Liste der DVDV-Landesserverbetreiber

Stand: Juni 2015

Bundesland	**Landesserver-Betreiber**	**Ansprechpartner**
Baden-Württemberg	Zweckverband Kommunale Datenverarbeitung Region Stuttgart Krailenshaldenstraße 44 70469 Stuttgart	Herr Rainer Rauser Tel.: 0711/8108609 Fax: 0711/8108607 eMail: r.rauser@kdrs.de
Bayern	Landesamt für Digitalisierung, Breitband und Vermessung IT-Dienstleistungszentrum Bayern St.-Martin-Straße 47 81541 München	Herr Jan Hohmuth Tel.: 089/2119-2877 Fax: 089/2119-14924 eMail: jan.hohmuth@ldbv.bayern.de pki-support@ldbv.bayern.de
	Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) Hansastraße 16 80686 München	Herr Konrad Baschenegger Tel.: 089/5903-1307 Fax: 089/5482291307 eMail: konrad.baschenegger@akdb.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	Herr Christian Peters Tel.: 030/90267-225 Fax: 030/90269-2097 eMail: christian.peters@labo.berlin.de Herr Andreas Reich Tel.: 030/90267-2257 Fax: 030/90269-2097 eMail: andreas.reich@labo.berlin.de Herr Matthias Teubner Tel.:030/90222-6629 eMail: matthias.teubner@itdz-berlin.de eMail: vps@itdz-berlin.de
Brandenburg	Zentraler IT-Dienstleister des Landes Brandenburg(ZIT-BB) Dortustraße 46 14467 Potsdam	Herr Dr. Reinhard Verch Tel.: 0331/39-826 Fax: 0331/39-10-826 eMail: reinhard.verch@zit-bb.brandenburg.de Herr Thomas Hein Tel.: 0331/39-724 Fax: 0331/39-10-724 eMail: thomas.hein@zit-bb.brandenburg.de eMail: Info@zit-bb.brandenburg.de
Bremen	Dataport Anstalt des öffentlichen Rechts Altenholzer Straße 10-14 24161 Altenholz	Herr Florian Muhlack Tel.: 0431/3295-6474 eMail: florian.muhlack@dataport.de eMail: nachrichtenbrooker@dataport.de
Hamburg	Dataport Anstalt des öffentlichen Rechts Altenholzer Straße 10-14 24161 Altenholz	Herr Florian Muhlack Tel.: 0431/3295-6474 eMail: florian.muhlack@dataport.de eMail: nachrichtenbrooker@dataport.de

Bundesland	Landesserver-Betreiber	Ansprechpartner
Hessen	ekom21 – KGRZ Hessen Carlo-Mierendorff-Straße 11 35398 Gießen	Herr Klaus Engelhardt Tel.: 0641/9830-1-238 Fax: 0641/9830-2-238 eMail: klaus.engelhardt@ekom21.de Herr Christoph Kirchner Tel.: 0641/9830-1-540 Fax: 0641/9830-2-540 eMail: christoph.kirchner@ekom21.de eMail:systembetrieb@ekom21.de
Mecklenburg-Vorpommern	Dataport Anstalt des öffentlichen Rechts Altenholzer Straße 10-14 24161 Altenholz	Herr Florian Muhlack Tel.: 0431/3295-6474 eMail: florian.muhlack@dataport.de eMail: nachrichtenbrooker@dataport.de
Niedersachsen	Zweckverband Kommunale Datenverarbeitung Oldenburg (KDO) Elsässer Straße 66 26121 Oldenburg	Herr Ingo Luers Tel.: 0441/9714-157 Fax: 0441/9714-17-157 eMail: luers@kdo.de Herr Frank Slotta Tel.: 0441/9714-209 Fax: 0441/9714-17-209 eMail: slotta@kdo.de eMail: dvdv@kdo.de
Nordrhein-Westfalen	DataClearing NRW hier: citeq, Stadt Münster Scheibenstraße 109 48153 Münster	Herr Frank Helmer Tel.: 0251/492-1826 Fax: 0251/492-7710 eMail: helmer@citeq.de Herr Felix König Tel.: 0251/492-1936 Fax: 0251/492-7710 eMail: koenig@citeq.de eMail : sysunix@citeq.de
	DataClearing NRW hier: Kommunales Rechenzentrum Niederrhein (KRZN) 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	Landesbetrieb Daten und Information Valenciaplatz 6 55118 Mainz	Herr Andreas Depta Tel.: 06131/605-259 Fax: 06131/605-144 eMail: andreas.depta@ldi.rlp.de Herr Sven Salzer Tel.: 06131/605-242 Fax: 06131/605-144 eMail: sven.salzer@ldi.rlp.de eMail: info@ldi.rlp.de

Bundesland	Landesserver-Betreiber	Ansprechpartner
Saarland	DataClearing NRW hier: citeq, Stadt Münster Scheibenstraße 109 48153 Münster	Herr Frank Helmer Tel.: 0251/492-1826 Fax: 0251/492-7710 eMail: helmer@citeq.de Herr Felix König Tel.: 0251/492-1936 Fax: 0251/492-7710 eMail: koenig@citeq.de eMail : sysunix@citeq.de
Sachsen	Staatsbetrieb Sächsische Informatik Dienste (SID) Niederlassung Kamenz Garnisonsplatz 10 01917 Kamenz	Herr Andreas Söhnel Tel.: 0351/20545180 Herr Maik Ohle Tel.: 0351/32647364 eMail: saxdvdv@sid.sachsen.de
Sachsen-Anhalt	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
Schleswig-Holstein	Dataport Anstalt des öffentlichen Rechts Altenholzer Straße 10-14 24161 Altenholz	Herr Florian Muhlack Tel.: 0431/3295-6474 eMail: florian.muhlack@dataport.de eMail: nachrichtenbrooker@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 5: Liste der Intermediärsbetreiber

Stand: Juni 2015

Bundesland	**Name und Anschrift**	**Kontakt**
Baden-Württemberg	Kommunale Datenverarbeitung Region Stuttgart (KDRS) Krailenshaldenstr. 44 70469 Stuttgart	Herr Rainer Rauser Tel.: 0711/8108-11609 Fax: 0711/8108-13609 eMail: r.rauser@kdrs.de
Bayern	Bayerisches Landesamt für Digitalisierung, Breitband und Vermessung IT-Dienstleistungszentrum Bayern St.-Martin-Straße 47 81541 München	Herr Thomas Maltan Tel.: 089/2119-2735 Fax: 089/2119-2522 eMail: thomas.maltan@ldbv.bayern.de eMail: servicelineVPS.RZ-Sued@ldbv.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: Herr Peter Fröhlich Tel.: 030/90269 2241 Fax: 030/90269 2097 eMail: Peter.Froehlich@labo.berlin.de eMail CC: christian.peters@labo.berlin.de technisch: Herr Matthias Teubner Tel.: 030/90222 6629 eMail: Matthias.Teubner@itdz-berlin.de eMail CC: christian.peters@labo.berlin.de eMail: vps@itdz-berlin.de
Brandenburg	Brandenburgischer IT-Dienstleister (ZIT-BB) Dortustrasse 46 14467 Potsdam	Herr Thomas Hein Tel.: 0331/39 724 Fax: 0331/39 10724 eMail: thomas.hein@zit-bb.brandenburg.de
Bremen	Governikus GmbH & Co. KG Am Fallturm 9 28359 Bremen	Herr Oliver Mania Tel.: 0421/204 95 944 Fax: 0421/204 95 11 eMail: oliver.mania@governikus.com
Hamburg	Dataport Anstalt des öffentlichen Rechts Billstraße 82 20539 Hamburg	Herr Martin Maßmann Tel.: 040/42846-2014 eMail: martin.massmann@dataport.de eMail: DataportGovernikus-Support@dataport.de
Hessen	ekom21 KGRZ Hessen Carlo-Mierendorff-Str. 11 35398 Gießen	Herr Christoph Kirchner Tel: 0641/9830-1540 eMail: christoph.kirchner@ekom21.de
Mecklenburg-Vorpommern	DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH Lübecker Straße 283 19059 Schwerin	Herr 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	Frau Bea Tiemens Herr Fabian Tiede Tel.: 0511/616-11333 Fax: 0511/616-11081 eMail: ewo@hannit.de Herr Ulrich Jestrzembski Tel.: 0511/616-11112 Fax: 0511/616-11081 eMail: Ulrich.Jestrzembski@hannit.de
	ITEBO Dielingerstraße 39/40 49074 Osnabrück	Herr 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	Herr Frank Slotta Tel.: 0441/9714-209 Fax: 0441/9714-17209 eMail: slotta@kdo.de eMail: dvdv@kdo.de
	KDS Paulinerstr. 14 37073 Göttingen	Frau Carola Mohr-Pawlik Tel.: 0551/400-4138 Fax: 0551/400- 4180 eMail: mohr-pawlik@kds.de
	ITEBS GmbH Frankfurter Straße 4 38122 Braunschweig	Herr Jörg Billewicz Tel.: 0531/48005-16 Fax: 0531/48005-77 eMail: billewicz@itebs.de Herr Bernd Newe Tel.: 0531/48005-81 Fax: 0531/48005-77 eMail: newe@itebs.de
	LK Heidekreis Vogteistraße 19 29683 Bad Fallingbostel	Herr F. Patzlee Tel.: 05162/970-285 Fax: 05162/970-900285 eMail: f.patzlee@Heidekreis.de
	Stadt Wolfsburg Porschestraße 49 38440 Wolfsburg	Herr Wolfgang Beuermann Tel.: 05361-28-2702 Fax: 05361-28-2972 eMail: wolfgang.beuermann@stadt.wolfsburg.de Herr Hubert Lux Tel.: 05361/281982 Fax: 05361/28-2550 eMail: Hubert.Lux@stadt.wolfsburg.de Herr Mirko Kratzer Tel.: 05361/281763 Fax: 05361/28-2550 eMail: Mirko.Kratzer@stadt.wolfsburg.de

Bundesland	Name und Anschrift	Kontakt
	adKOMM Software GmbH & Co. KG Stadtweg 14 85134 Stammham	Fachbereich BAU/ÖSI Tel.: 08405/9286-0 Fax: 08405/9286-100 eMail: bau-oesi@adKOMM.de
	citeq, Stadt Münster Scheibenstraße 109 48153 Münster	Herr Frank Helmer Tel.: 0251/492-1826 Fax: 0251/492-7710 eMail: helmer@citeq.de
Nordrhein-Westfalen	citeq - Stadt Münster Scheibenstr. 109 48153 Münster	Herr Frank Helmer Tel.: 0251/492-1826 Fax: 0251/492-7710 eMail: helmer@citeq.de
	KRZN 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
	KDVZ Citkomm Griesenbraucker Str. 4 58640 Iserlohn	Herr Michael Kampmann Tel.: 02371/439-228 eMail: kampmann.m@kdvz.de Herr Norbert Jung Tel.: 02371/439-227 eMail: jung@kdvz.de
	KRZ Minden/Ravensberg/Lippe Am Lindenhaus 21 32657 Lemgo	Herr 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	Herr Thomas Schulz Tel.: 0681/9264341 Fax: 0681/9264349 eMail: thomas.schulz@ego-saar.de eMail: vermittlungsstelle@ego-saar.de
Sachsen	Staatsbetrieb Sächsische Informatik Dienste Riesaer Straße 7 Haus D 01129 Dresden	Herr Robert Schenkel Tel.: 0351/20545280 eMail: esv@sid.sachsen.de
Sachsen-Anhalt	Dataport Anstalt öffentlichen Rechts Niederlassung Halle Barbarastraße 2 06110 Halle (Saale)	Herr Gunter Willimsky Tel.: 0345/1304 816 eMail: gunter.willimsky@dataport.de
	KID Magdeburg GmbH (KID) Alter Markt 15 39104 Magdeburg	Herr Marco Hauffe Tel.: 0391/24464-120 Fax: 0391/24464-400 eMail: marco.hauffe@kid-magdeburg.de

Bundesland	Name und Anschrift	Kontakt
	adKOMM Software GmbH & Co. KG Stadtweg 14 85134 Stammham	Fachbereich BAU/ÖSI Tel.: 08405/9286-0 Fax: 08405/9286-100 eMail: bau-oesi@adKOMM.de
	ITEBS GmbH Frankfurter Straße 4 38122 Braunschweig	Herr Jörg Billewicz Tel.: 0531/48005-16 Fax: 0531/48005-77 eMail: billewicz@itebs.de Herr Bernd Newe Tel.: 0531/48005-81 Fax: 0531/48005-77 eMail: newe@itebs.de
	KDRS Baden-Württemberg Krailenshaldenstr. 44 70469 Stuttgart	Herr Rainer Rauser Tel.: 0711/8108-11609 Fax: 0711/8108-13609 eMail: r.rauser@kdrs.de
Schleswig-Holstein	Dataport Anstalt des öffentlichen Rechts Billstraße 82 20539 Hamburg	Herr Martin Maßmann Tel.: 040/42846-2014 eMail: martin.massmann@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 6: Liste der Registrierungsstellen der DOI-CA

Stand: November 2011

<table>
<tr><th>Bundesland</th><th>Kontakt der
zuständigen Registrierungsstelle</th><th>Login für die Web-Seiten der DOI-CA</th></tr>
<tr><td>Baden-Württemberg</td><td rowspan="9">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</td><td rowspan="9">Login: XPersonenstand
Passwort: holemawa38</td></tr>
<tr><td>Bayern</td></tr>
<tr><td>Bremen</td></tr>
<tr><td>Hamburg</td></tr>
<tr><td>Hessen</td></tr>
<tr><td>Nordrhein-Westfalen</td></tr>
<tr><td>Rheinland-Pfalz</td></tr>
<tr><td>Saarland</td></tr>
<tr><td>Sachsen</td></tr>
<tr><td>Schleswig-Holstein</td></tr>
<tr><td>Berlin</td><td>Landesamt für Bürger und Ordnungsangelegenheiten
Friedrichstr. 219
10958 Berlin
eMail: DOI-XhD@labo.berlin.de</td><td rowspan="6">Die Zugangsdaten erfragen Sie bitte bei Ihrer zuständigen Registrierungsstelle</td></tr>
<tr><td>Brandenburg</td><td>Brandenburgischer IT-Dienstleister
Dezernat Infrastrukturservice
Dortusstr. 46
14467 Potsdam</td></tr>
<tr><td>Mecklenburg-Vorpommern</td><td>DVZ Datenverarbeitungszentrum
Mecklenburg-Vorpommern GmbH
Lübecker Str. 283
19059 Schwerin</td></tr>
<tr><td>Niedersachsen</td><td>IT.Niedersachsen
- SignaturCard Service -
Göttinger Chaussee 209
30459 Hannover
Tel.: 0511/120 3990
eMail: SignaturCard-Service@lskn.niedersachsen.de</td></tr>
<tr><td>Sachsen-Anhalt</td><td>Oberfinanzdirektion Magdeburg,
Landesrechenzentrum, PKI - Zentrale Stelle
Barbarastraße 2
06110 Halle (Saale)
Tel: 0345/13043852/3862
eMail: PKILSA-ZRA@liz.sachsen-anhalt.de</td></tr>
<tr><td>Thüringen</td><td>Thüringer LandesRechenZentrum
Bereich Vermittlungsstelle
Ludwig-Erhard-Ring 8
99099 Erfurt</td></tr>
</table>

Anhang 7: Glossar

Vorbemerkungen

Der AG Sterbefallmitteilungen ist bewusst, dass dieser Leitfaden auf einige technisch geprägte Bezeichnungen und Abkürzungen nicht verzichten kann. Das bringt die Einführung eines bundesweiten 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.

Datenschutz und Datensicherheit

Die Datenschutzbeauftragten des Bundes und der Länder begrüßten in 2005 ausdrücklich die Nutzung von OSCI-Transport für die Übermittlung von personenbezogenen Daten in eGovernment-Projekten. Sie empfahlen darüber hinaus den Ausbau einer flächendeckenden OSCI-basierten Infrastruktur, um eine Ende-zu-Ende-Sicherheit in der Datenübermittlung zu erreichen. In 2013 forderten die Datenschutzbeauftragten des Bundes und der Länder den IT-Planungsrat auf, die Nutzung von Standards zur Ende-zu-Ende-Verschlüsselung (wie bspw. OSCI-Transport) verbindlich vorzugeben und diese Standards kontinuierlich weiterzuentwickeln.

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.. Die Regelungen des § 3 IT-Netz-Gesetzes bleiben unberührt..

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 Behörden 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

Insbesondere im Rahmen der OSCI-Kommunikation 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 ermöglichen es, die Authentizität und Unverfälschtheit der hiermit signierten Daten zu prüfen.

Die qualifizierte elektronische Signatur ist eine 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.

Zertifikatsfunktionen
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.

Um die Nachricht zu 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").

Anhang 8: Vorschlag für eine rechtliche Regelung

(1) Die nach Landesrecht für die Führung der Personenstandsregister zuständigen Stellen übermitteln den nach Landesrecht für den Empfang des nichtvertraulichen[i] Teils der ärztlichen Bescheinigung über den Tod (Todesbescheinigung) zuständigen Stellen bei Sterbefällen im Inland[ii] nach der Beurkundung des Sterbefalles folgende beurkundeten[iii] Daten:

a. Standesamt
b. Personenstandsregisternummer
c. Familienname
d. ggf. Geburtsname
e. Vorname
f. Anschrift (Str., Hausnr., PLZ, Wohnort, Kreis)
g. Geburtsdatum
h. Geburtsort
i. Geschlecht
j. Staatsangehörigkeit[iv]
k. Todeszeitpunkt sonst Todeszeitraum[v]
l. Sterbeort (Str., Hausnr., Ort, Kreis)[vi].

(2) Die Übermittlungen erfolgen elektronisch soweit die technischen Voraussetzungen hierfür geschaffen sind. Die elektronische Übermittlung der Daten erfolgt durch strukturierte Datensätze. Hierfür sind das Datenaustauschformat XPersonenstand und das Übertragungsprotokoll OSCI-Transport in der vom Bundesministerium des Innern im elektronischen Bundesanzeiger bekannt gemachten jeweils gültigen Fassung zugrunde zu legen.

(3) Innerhalb von Rechenzentren und in besonders gesicherten verwaltungseigenen Netzen kann auf die Verwendung von OSCI-Transport verzichtet werden, wenn durch technische und organisatorische Maßnahmen sichergestellt wird, dass die durch die Verwendung von OSCI-Transport erzielten Sicherheitseigenschaften anderweitig in gleicher Qualität gewährleistet werden.

Die nachfolgend beschriebenen Erläuterungen sollten in die Erläuterungen/Begründung der bestattungsrechtlichen Regelung aufgenommen werden:

[i] In einigen Bundesländern wird nur der vertrauliche Teil der Todesbescheinigung an die Gesundheitsbehörde weitergeleitet. Diesem Umstand muss bei der Formulierung Rechnung getragen werden.

[ii] Nur für Sterbefälle, die sich im Inland ereignen, wird eine Todesbescheinigung ausgestellt. Daher erhalten auch die Gesundheitsämter nur eine Mitteilung, wenn der Sterbefall sich im Inland ereignet hat.

[iii] Durch diese Formulierung wird herausgestellt, dass das Standesamt nur die zur Beurkundung verwendeten und schließlich beurkundeten Daten weitergibt. Die Daten des nicht vertraulichen Teils der Todesbescheinigung sind nicht Grundlage der Beurkundung. Das Standesamt übernimmt hiervon insbesondere nicht die persönlichen Daten der verstorbenen Person. Diese ergeben sich aus anderen Personenstandsurkunden oder einem Pass oder Personalausweis.

[iv] Diese Angabe gehört nicht zum Inhalt eines Sterberegistereintrags und ist auch nicht in einem Sterberegistereintrag beurkundet. Eine Übermittlung könnte folglich durch das Standesamt nur erfolgen, wenn diese Angabe nicht durch dieses überprüft werden muss und damit kein Anspruch auf Richtigkeit einhergehen soll.

[v] Der Todeszeitpunkt enthält die Daten der festgestellten Todeszeit so genau wie möglich. Dabei kann es auch vorkommen, dass nur ein Jahr oder nur ein Monat und ein Jahr angegeben wird. Als Todeszeitpunkt kann auch das Datum der Leichenauffindung, wie er in den bestattungsrechtlichen Regelungen definiert ist, gelten. Der Todeszeitraum bezeichnet den Zeitraum zwischen dem Zeitpunkt, zu der eine Person zuletzt lebend gesehen wurde, und dem Zeitpunkt, zu dem die Person mit Sicherheit verstorben war. Er ist anzugeben, wenn der Todeszeitpunkt nicht eindeutig feststellbar ist.

[vi] Als Sterbeort gilt auch der Ort der Leichenauffindung entsprechend der bestattungsrechtlichen Regelungen.