Länderübergreifende elektronische Rückmeldung im Meldewesen

Vorstudie für den Aufbau einer technischen Infrastruktur auf Basis von OSCI

Januar 2003

1 Einleitung

1.1 Autoren

Dieses Dokument wurde durch die Arbeitsgruppe 2 des Projekts *"OSCI–XMeld 1.0"* in der Zeit von November 2002 bis Januar 2003 erstellt.

Die Mitwirkenden waren

Tabelle 1:

Dirk Christiansen	Datenzentrale Schleswig-Holstein
Markus Ernst	bremen online services
Markus Hofmann	Anstalt für kommunale Datenverarbeitung in Bayern
Wolfgang Korseska	Anstalt für kommunale Datenverarbeitung in Bayern
Sönke Maseberg	datenschutz nord
Günther Meyer	MSI
Uwe Schläger	datenschutz nord*
Martin Schlöter	ekom 21
Andreas Schmidt	Bundesamt für Sicherheit in der Informationstechnik
Frank Schweizer	Kommunales Rechenzentrum Niederrhein*
Eike Seidel	OSCI-Leitstelle
Gerd Teipelke	KAI (Kommunale Anwendergemeinschaft)
Heiko Thede	Innenministerium Mecklenburg-Vorpommern**

*) nur in der ersten Sitzung

**) als Vertreter zu KoopA-Gremien

Die Ergebnisse der Arbeitsgruppe wurden qualitätsgesichert von der Abstimminstanz (AI) und abgenommen von der Entscheidungsinstanz (EI) des Projekts (s. dort)

1.2 Einführung

Im Rahmen von E-Government haben bundesweite Aktivitäten zur Realisierung entsprechender Funktionen des Meldewesens stattgefunden.

Zu diesen Aktivitäten gehören die fachlichen Spezifikationen von Prozessen und Informationen. Die Spezifikation liegt (abgestimmt in allen Gremien) in der Version 1.0 (Final) vor (*"XMeld: Das Datenaustauschformat für das Meldewesen"*). Die funktionale Ergänzung (Version 1.1) wird z.Z. erarbeitet.

Während der Erarbeitung der Version 1.0 wurde deutlich, dass im Bereich der behördeninternen Kommunikation durch Medienbruchfreiheit und elektronischen Transport erhebliche Einsparungen denkbar sind.

Die vorliegende Arbeit orientiert sich an der Anforderung der länderübergreifenden Rückmeldung des Meldewesens. Allerdings ist das entwickelte Konzept auch auf andere OSCI-Kommunikationen grundsätzlich anwendbar. Spezifisch sind insbesondere die Umsetzung sicherheitstechnischer Maßnahmen, die von Nachrichtentyp zu Nachrichtentyp unterschiedlich sein können und die zu Grunde gelegte Netzinfrastruktur.

Die Abwicklung des eigentlichen Meldewesens erfolgt unter Anwendung entsprechender Ländergesetze (Landesmeldegesetze) und unterschiedlicher (DV-)Verfahren jeweils länderspezifisch und entzieht sich damit (jedenfalls kurzfristig) einer allgemeinen Lösung. Aber die Kommunikation (Rückmeldung) zwischen den einzelnen Bundesländern ermöglicht (und erfordert) eine einheitliche Handhabung. Hierauf konzentriert sich die nachfolgende Arbeit.

Im Rahmen einer Vorstudie (grobe Eindringtiefe aber vollständige Breite) sind technische Lösungen und deren wirtschaftliche Konsequenzen erarbeitet worden.

1.3 Ziele

Im novellierten MRRG entfällt die Pflicht zur Abmeldung eines Bürgers (sofern der Umzug innerhalb Deutschlands stattfindet). Die Abmeldung bei der Wegzugsgemeinde erfolgt im Rahmen der Rückmeldung, die von der Zuzugsgemeinde an die Wegzugsgemeinde übermittelt wird. Um die Konsistenz der Melderegister zu wahren, muss die Rückmeldung zukünftig unverzüglich, jedoch spätestens drei Werktage nach der Anmeldung übermittelt werden. Dies soll möglichst auf automatisiert verarbeitbaren Datenträgern oder durch Datenübermittlung erfolgen.

Der automatisierten Rückmeldung kommt schon aus ökonomischen Gründen eine besondere Bedeutung zu. Im Projekt OSCI–XMeld 1.0 wurden daher die erforderlichen Nachrichtenstrukturen mit Priorität 1 untersucht und auch fertiggestellt (s. dort).

Neben der interoperablen Nachrichtenstruktur ergeben sich durch die automatisierte Rückmeldung aber auch weitergehende Herausforderungen an die kommunale DV-Landschaft. Insbesondere ist ein länderübergreifender Informationsverbund zwischen Fachverfahren des Einwohnermeldewesens (EWO-Fachverfahren) einzurichten, denn bisher erfolgt die Datenübermittlung noch größtenteils per Briefpost.

Es ist unstrittig, dass eine verbindliche Vorgabe für ein technisches Verfahren zur sicheren und nachvollziehbaren Übermittlung für Rückmeldungen zwischen Meldeämtern verschiedener Bundesländer erforderlich ist. Die Einigung auf ein einheitliches technisches Verfahren muss sowohl die Nachrichtenformate, als auch die Übertragungsverfahren umfassen, ansonsten werden die erhofften positiven Effekte nicht eintreten. In der novellierten Fassung der 1. BMeldDÜV wird das Transportprotokoll OSCI–Transport in Kombination mit OSCI–XMeld als verbindliche Vorgabe für die länderübergreifende elektronische Datenübertragung vorgeschrieben. Eine vom AK1 der Innenministerkonferenz eingerichtete Projektgruppe *“Meldewesen”* formuliert als realistisches Ziel

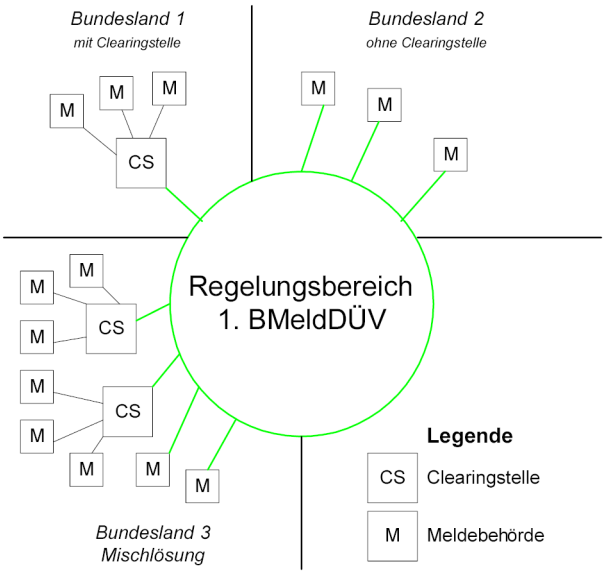
> *Die länderübergreifende Kommunikation zwischen den Meldebehörden sollte in einem Zeitraum von zwei Jahren nach Inkrafttreten der entsprechenden rechtlichen Vorschriften nur noch mittels elektronischer Datenübertragung erfolgen.*

Die darüber deutlich hinaus gehende Zielsetzung der interaktiven länderübergreifenden Anmeldung wird als mittel- bis langfristige Vision formuliert.

Das Ziel besteht darin, eine Vorstudie für die Umsetzung der Rückmeldung auf Basis von OSCI–Transport und OSCI–XMeld zu erarbeiten, mit der diese Ziele erreicht werden können.

In der Vorbereitung zu diesem Projekt haben Überlegungen stattgefunden, die Kommunikation zwischen den Meldebehörden der Kommunen wahlweise direkt oder über zentrale Clearingstelle auszuführen, die in den einzelnen Bundesländern als Datendrehscheibe fungieren können. Mögliche Varianten, die sich alle mit OSCI–Transport realisieren lassen, sind im nachfolgenden Bild dargestellt.

Bild 1 Mögliche Anbindung von Meldebehörden



Näheres zur Aufgabe und der Funktion von ist in Abschnitt 2.2. dargestellt.

1.4 Allgemeine Annahmen und Voraussetzungen

In den nachfolgenden Kapiteln wird im Sinne einer Vorstudie eine Lösung für ein technisches Verfahren für die elektronische und, so weit möglich, automatisiert erfolgende zwischen-behördlichen Kommunikation von Meldebehörden beschrieben.

Im folgenden Abschnitt werden zunächst die grundlegenden Rahmenbedingungen und Annahmen hinsichtlich technischer und organisatorischer Voraussetzungen zusammengestellt, die bei der Erarbeitung dieser Vorstudie unterstellt wurden.

1.4.1 OSCI–Transport

Der länderübergreifende Datenaustausch von Meldebehörden wird durch die erste Bundesmeldedatenübermittlungsverordnung (1. BMeldDÜV) geregelt. Die novellierte Fassung dieser Verordnung, die zur Zeit erarbeitet wird und voraussichtlich im Laufe des Jahres 2003 in Kraft tritt, schreibt als technisches Übertragungsverfahren für den länderübergreifenden elektronischen Datenaustausch zwischen Meldebehörden die Verwendung des Transportprotokolls OSCI–Transport 1.2 verbindlich vor.

Somit war die Bereitstellung aller für den spezifikationskonformen Versand und Empfang von OSCI-Nachrichten benötigten Funktionalitäten für die Meldebehörden eine der wesentlichen und grundlegenden Anforderungen bei der Erarbeitung der vorliegenden Vorstudie.

Dabei wird davon ausgegangen, dass diese Funktionalitäten in Form einer plattformunabhängigen OSCI-Bibliothek über entsprechende Schnittstellen zur Verfügung stehen (s. Protokoll der KoopA-Sitzung vom 28.11.2002, TOP 3) .

Neben den auf Seiten des Senders und des Empfängers vorhandenen weiteren und für eine OSCI-konforme Kommunikation benötigten Funktionalitäten und Komponenten werden im Sinne dieser Vorstudie als verfügbar vorausgesetzt. Dies betrifft insbesondere den OSCI-Intermediär mit seinen gemäß der OSCI–Transport-Spezifikation geforderten Funktionen.

1.4.2 OSCI–XMeld

Um eine automatisierte und medienbruchfreie Verarbeitung der übermittelten Meldedatensätze durch die Fachverfahren zu gewährleisten, werden die Meldedaten mittels des speziell für die Kommunikationsbeziehungen des Meldewesen entworfenen XML-basierten Datenaustauschformats OSCI–XMeld strukturiert. Im Rahmen der länderübergreifenden Kommunikation wird die Verwendung von OSCI–XMeld ebenfalls durch die novellierte Fassung der 1. BMeldDÜV verbindlich vorgeschrieben. Zum Bearbeitungszeitpunkt lag XMeld in der Version 1.0 vor.

Im weiteren wird unterstellt, dass die Fachverfahren in der Lage sind, XMeld-konforme Datensätze für die OSCI-konforme Nachrichtenübermittlung bereitzustellen. Eine Konvertierung der Datensätze von den unterschiedlichen fachverfahrensspezifischen Datenformaten in das XMeld-Format bzw. die Rückformatierung obliegt somit den Fachverfahren und liegt nicht im Funktionsumfang der hier beschriebenen Lösung.

Allerdings sei bemerkt, dass eine konkrete Realisierung dieser Funktionalität nicht zwangsläufig durch das Fachverfahren zur Verfügung stehen muss, sondern auch an eine sogenannte Clearingstelle delegiert werden kann. Näheres zur Aufgabe von wird im Abschnitt 2.2 genannt.

1.4.3 Public-Key-Infrastrukturen

Die Sicherung der Vertraulichkeit und Integrität der zu übermittelnden Meldedatensätze, sowie der Nachweis der Authentizität der an der Kommunikation Beteiligten erfolgt in OSCI–Transport durch Techniken und Methoden der Public-Key-Kryptographie. Dies erfordert den Betrieb einer geeigneten Public-Key-Infrastruktur (PKI) bestehend aus Registrierungs- und Zertifizierungsinstanzen, die es den Kommunen erlaubt, ihre Meldebehörden mit den benötigten Signier- und Chiffrier-Zertifikaten auszustatten.

Zudem besteht für die hier betrachtete, länderübergreifende elektronische Kommunikation die Anforderung, dass zum Zweck der Adressierung und Verschlüsselung die Chiffrier-Zertifikate sowie für die Prüfung und Verifikation von Signaturen der Gültigkeitsstatus der Signatur-Zertifikate der Kommunikationspartner in den jeweils anderen Ländern abrufbar zur Verfügung stehen.

Zur Erfüllung dieser Anforderungen wird daher im Weiteren unterstellt, dass in den Bundesländern eine unter der Wurzel-Zertifizierungsinstanzder PKI-1-Verwaltung des BSI betriebene Domänen-PKI zur Verfügung steht, die gemeinsam die PKI der öffentlichen Verwaltung bilden.

Eine solche Domänen-PKI unter der PKI-1-Verwaltung kann von den Verwaltungen

- Mit einer eigenen Zertifizierungsstelle,
- Mit einer eigenen *"virtuellen"* Zertifizierungsstelle, die bei einem TrustCenter-Dienstleister beauftragt ist,
- Mit einer Zertifizierungsdienstleistung eines kommerziellen TrustCenters,
- Mit einer Zertifizierungsdienstleistung in Form einer *"virtuellen"* Zertifizierungsstelle (Beispiele: TESTA-CA, IVBB-CA) eines kommerziellen TrustCenters,

die jeweils in die PKI-1-Verwaltung eingebunden bzw. einzubinden sind, realisiert werden.

Die PKI-1-Verwaltung verfügt als zusätzlichen Bestandteil über einen zentralen Verzeichnisdienst, so dass die benötigten PKI-Informationen wie Zertifikate und Sperrliste länderübergreifend zur Verfügung gestellt werden und somit eine gesicherte länderübergreifende Kommunikation gewährleistet ist.

1.4.4 Eigenschaften des Trägernetzes

Sowohl zwischen den einzelnen Ländern als auch landesintern zwischen den Kommunen besteht hinsichtlich der infrastrukturellen Ausstattung sowie der Nutzung von Kommunikationsnetzen eine Heterogenität, wobei insbesondere keine allgemein gültigen Aussagen bzgl. der Sicherheitsfeatures der jeweils genutzten Kommunikationsnetze möglich sind. Für die hier vorgestellte Lösung sind keine Voraussetzungen an das Trägernetz gemacht worden. Es ist also denkbar, dass normale - und damit sehr unsichere - Internet-Leitungen oder aber mit TESTA das deutlich sicherere Behördennetz genutzt werden kann. Diese Variabilität impliziert, dass die Sicherheit von TESTA für die Betrachtung der Gesamtsicherheit nicht gesondert berücksichtigt wird. Dies hat insbesondere Auswirkungen auf die Verwendung der optionalen OSCI-Sicherheitsmechanismen, die im Abschnitt 2.5 beschrieben werden.

2 Das Kommunikationsmodell

Entsprechend des Projektauftrags war es das Ziel dieser Vorstudie ein technisches Verfahren für die Abwicklung der Rückmeldung im länderübergreifenden Bereich mittels automatisierter elektronischer Datenübermittlung und auf Basis von OSCI–Transport und OSCI–XMeld zu entwickeln. Diese Aufgabe umfasst zunächst die Entwicklung eines technischen Systems, dass die für eine spezifikationskonforme OSCI-Kommunikation benötigten Funktionen

für die Meldebehörden zur Verfügung stellt. Zum anderen werden neben den eigentlichen OSCI-spezifischen Funktionen zusätzliche und ergänzende Maßnahmen benötigt, die sich im wesentlichen aus der Bereitstellung der PKI und Funktionen für deren Nutzung ergeben.

Um den Anpassungsaufwand bei den verwendeten Fachverfahren so gering wie möglich zu halten, sieht die vorliegende Grobspezifikation eine vollständige funktionale Trennung zwischen den eigentlichen Aufgaben der Fachverfahren und den zusätzlich gemäß OSCI benötigten Kommunikationsaufgaben vor.

In der Folge dieses Ansatzes wurde bald deutlich, dass es sich bei den umzusetzenden Anforderungen und Aufgaben für das zu entwickelnde Kommunikationssystem weder um rein rückmeldungsspezifische noch um allgemein meldebehördenspezifische Anforderungen handelt. Vielmehr handelt es sich um generelle, kommunikationsspezifische Anforderungen, die unabhängig vom zu transportierenden fachlichen Inhalt bei der Umsetzung von E-Government-Verfahren auf Basis von OSCI zu erfüllen sind.

Dieser fachverfahrensunabhängige Ansatz wird zusätzlich durch die Forderung gestützt, dass die Bereitstellung der fachspezifischen Daten zum Funktionsbereich des jeweiligen Fachverfahrens gezählt wird. Dabei ist es aus Sicht des OSCI–Transportprotokolls unerheblich, in welchem konkreten Datenformat die zu übermittelnden Fachdaten vorliegen. Neben einem standardisierten und XML-basierten Datenaustauschformat wie es mit XMeld für das Meldewesen bereits vorliegt, kann es sich hierbei ebenso um proprietäre und (fach-) verfahrenspezifische Datenformate handeln, die jedoch in analoger Weise unter Verwendung von OSCI–Transport rechtskonform und sicher zuzustellen sind.

In diesem Sinne und in Erweiterung des eigentlichen Projektauftrags wird mit der hier vorgelegten Lösung ein generelles Verfahren für die Zustellung von allgemeinen Verwaltungsnachrichten im zwischenbehördlichen Verkehr und auf Basis des OSCI–Transportprotokolls vorgestellt. Für die Gesamtheit dieses System wurde die Bezeichnung OSCI-Message-Handler (OMH) eingeführt.

2.1 Akteure und Rollen mit ihren Aufgaben

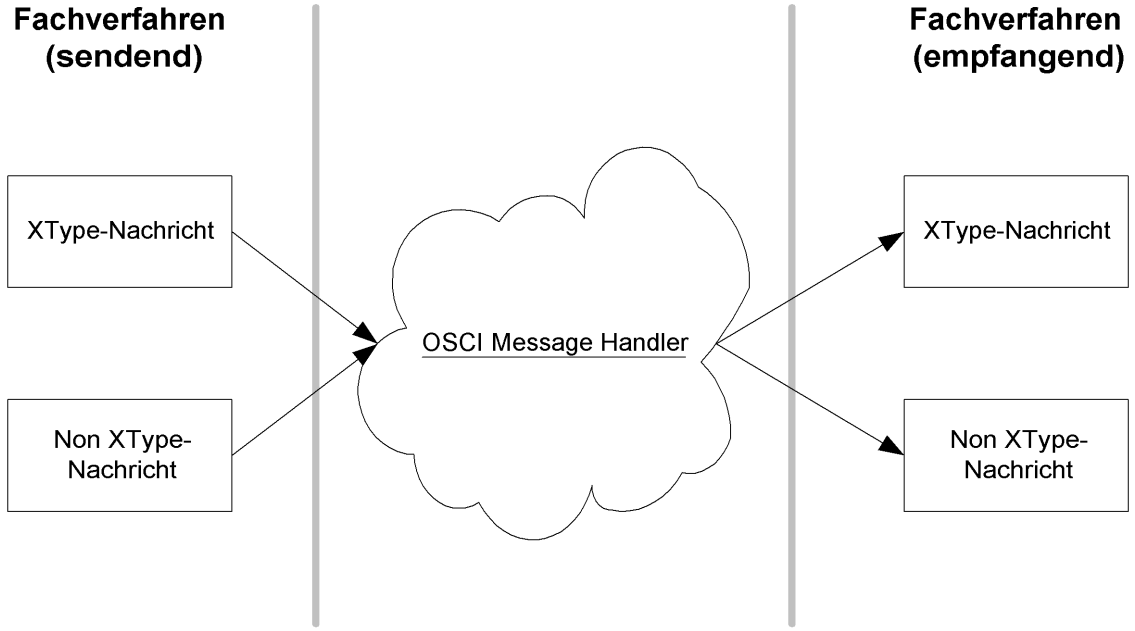
OSCI–Transport ermöglicht als Anwendungsprotokoll die sichere, d.h. vertrauliche und authentische, und rechtsverbindliche Abwicklung von Transaktionen im Bereich des E-Governments über den Betriebsweg Internet und auf Basis der digitalen Signatur.

Dabei berücksichtigt OSCI–Transport sowohl die Kommunikation der öffentlichen Verwaltung mit ihren Kunden (Bürger und Unternehmen) als auch die behördeninterne Kommunikation zwischen unterschiedlichen Verwaltungen bzw. Verwaltungsbereichen. Aufgrund der vielfältigen Anwendungsszenarien in diesem Umfeld ergeben sich vielfältige funktionale und sicherheitstechnischen Anforderungen, die zu einem sehr spezifischen Kommunikations- bzw. Rollenmodell bei OSCI führen.

Mit der Entwicklung des OMH wird das Ziel verfolgt, unter Berücksichtigung sowohl der Gegebenheiten und Voraussetzungen der derzeitigen Praxis in den Meldebehörden als auch der Prinzipien des OSCI–Transportprotokolls ein vollständiges Werkzeug für die im Verlauf der Kommunikation zu erfüllenden Aufgaben zur Verfügung zu stellen.

Dies bedeutet, dass neben den auf Sender- und Empfängerseite benötigten Funktionen durch den OMH auch der Zugang zu den zusätzlichen und für die OSCI-Kommunikation benötigten infrastrukturellen Komponenten wie dem Verzeichnisdienst zur Ermittlung von Zertifikaten und physikalischen Adressen und dem die Kommunikation vermittelnden OSCI-Intermediär ermöglicht wird. Auf einer groben Ebene stellt sich die Kommunikation wie in der folgenden Abbildung dar.

Bild 2 grobes Kommunikationsmodell



Als inhaltsneutrales Transportprotokoll bietet OSCI–Transporteine am deutschen Teledienstegesetz orientierte Trennung zwischen Nutzungs- und Inhaltsdaten. Während der eigentliche Nachrichteninhalt, die sogenannten Inhaltsdaten, die im hier betrachteten Szenario durch den mittels XMeld strukturierten Meldedatensatz gebildet werden, Ende-zu-Ende verschlüsselt übermittelt werden kann, erlauben die separat chiffrierbaren Nutzungsdaten die Zwischenspeicherung und Vermittlung von Nachrichten ohne Vertraulichkeitsverlust.

Diese Trennung findet sich durch die Unterscheidung der Rollen des Autors und des Senders auf der Seite des Nachrichtensenders (der sendenden Meldebehörde) sowie der Rollen des Empfängers und des Lesers auf der Seite des Nachrichtenempfängers (der empfangenen Meldebehörde) wieder.

Im klassischen OSCI-Bild ist ein Autor diejenige Instanz, die Inhaltsdaten generiert. Dies sind üblicherweise die schon im Einsatz befindlichen Fachverfahren. Als Inhaltsverantwortlichem obliegt es ebenfalls dem Autor in Abhängigkeit der Sicherheitsanforderungen des jeweiligen Geschäftsvorfalls die Inhaltsdaten (XMeld-Datensatz) zu signieren. Dies setzt den Besitz eines Signatur-Zertifikats beim Autor voraus.

Um einerseits bei der Umstellung auf die elektronische Kommunikation einen möglichst geringen Anpassungsaufwand bei den Fachverfahren zu verursachen und andererseits den OMH möglichst nicht fachspezifisch zu entwikkeln, reduziert sich i. A. der durch den OMH realisierte Autor auf den Inhaltsverantwortlichen im Sinne des Signierenden, während die Inhaltsdaten durch das Fachverfahren generiert dem Autor angeliefert werden.

Sofern die Inhaltsdaten in Form eines standardisierten, fachspezifischen Austauschformats wie bspw. dem XMeld-Format übermittelt werden, obliegt die Aufgabe der Datenkonvertierung ebenfalls dem Fachverfahren.

Weiterhin liefert das Fachverfahren Angaben, anhand derer die für die elektronische Zustellung erforderlichen Informationen, wie die Chiffrier-Zertifikate und physikalischen Adressen ermittelt werden können. Im Falle der Meldewesenkommunikation sind dies der amtliche Gemeindeschlüssel der empfangenen Meldebehörde sowie der der Nachricht zugrunde liegende Geschäftsvorfall in Form einer Produktkennzahl. Letztere wird gemäß den Vorgaben der Nachrichtenkennung, wie sie die XMeld-Spezifikation vorsieht, gebildet.

Die Inhaltsdaten sind an einen Leser gerichtet. Bei Bedarf können die Inhaltsdaten so verschlüsselt werden, dass sie nur durch den Leser entschlüsselt werden können. Dies setzt den Besitz eines Chiffrier-Zertifikats beim Leser voraus. Die Aufgabe der Inhaltsdaten-Verschlüsselung wird durch den Autor wahrgenommen. Die dazu notwendige Ermittlung des Chiffrier-Zertifikats des Lesers erfolgt im Rahmen des Adressierungsverfahren, das unter 2.2 gesondert beschrieben wird, und kann wahlweise durch den Sender oder durch den Autor erfolgen.

Vor dem Versand werden die Inhaltsdaten um die Nutzungsdatenzur Gesamtnachricht ergänzt. Die Nutzungsdaten werden benötigt, um die Nachricht technisch an den Empfänger übermitteln zu können. Zusätzlich erlauben die Nutzungsdaten die Nachvollziehbarkeit der Übermittlung und enthalten Elemente um einen Dialog steuern und überwachen zu können. Die Generierung der Nutzungsdaten sowie der Aufbau der Gesamtnachricht erfolgt durch den

Sender. Optional können die Nutzungsdaten ebenfalls signiert und verschlüsselt werden, wobei Signatur und Verschlüsselung in diesem Fall durch den Sender erfolgt. Die Signatur der Nutzungsdaten setzt den Besitz eines Signatur-Zertifikatsbeim Sender voraus.

Bei OSCI erfolgt sämtliche Kommunikation ausschließlich vermittelt durch einen sogenannten Intermediär. Dieser erfüllt die Aufgaben der Protokollierung des Datenflusses, der Prüfung der Zertifikate sowie der Erbringung weiterer Mehrwertdienste. Für eine detailliertere Darstellung der Aufgaben des Intermediärs sei auf das Teildokument *"Entwurfsprinzipien, Sicherheitsziele und -mechanismen"* der OSCI–Transport 1.2 Spezifikation verwiesen.

Die Nutzungsdaten-Verschlüsselung erfolgt für den jeweils nächsten Kommunikationsbeteiligten in der OSCI Infrastruktur. Insbesondere sind also diese Daten für den Intermediär lesbar und auch von ihm zu modifizieren. Die Ermittlung der Chiffrierzertifikate des Intermediärs und des Empfängers erfolgt durch den Sender im Rahmen des im Abschnitt 2.2 beschriebenen Adressierungsverfahrens.

Nach Erfüllung der durch den Intermediär zu versehenden Aufgaben wird die Nachricht mit aktualisierten Nutzungsdaten, die unter anderem um die Ergebnisse der durch den Intermediär durchgeführten Zertifikatsprüfungen ergänzt wurden, an die Empfangsbehörde zugestellt. Auch der Intermediär verfügt über ein Signatur-Zertifikat um die Nachricht bei entsprechendem Bedarf zu signieren. Ebenso besteht die Möglichkeit der Verschlüsselung der Nachricht für den Nachrichtenempfänger. Das hierfür benötigte Chiffrier-Zertifikat des Empfängers entnimmt der Intermediär den Nutzungsdaten der Nachricht.

Für die durch den Intermediär vermittelte Zustellung einer Nachricht stehen per OSCI drei unterschiedliche Arten der Übermittlung zur Verfügung. Zwei dieser Nachrichtenübermittlungen dienen der Realisierung eines *One-Way*-Szenarios, während es sich bei dem weiteren um die Abbildung eines dialogartigen *Request-Response*-Szenarioshandelt. Mit Einschränkung auf den Geschäftsvorfall länderübergreifende Rückmeldung, in der (auf Ebene der Inhaltsdaten) keine unmittelbare Reaktion auf eine zugestellte Nachricht erwartet wird, werden hier nur die beiden Versionen für die One-Way-Kommunikation beschrieben und diskutiert.

Bei dem Szenario **One Way, aktiver Empfänger** wird eine Nachricht von einem Sender an einen Empfänger übertragen, wobei der Empfänger selbst aktiv werden muss, um die Zustellung zu erhalten. Die Übertragung wird nachvollziehbar protokolliert. Dieses Szenario bietet sich an, wenn nicht sichergestellt werden kann, dass der Empfänger ständig erreichbar ist. Die Nachricht wird in einem beim Intermediär befindlichenPostfach zwischengespeichert. Der Empfänger muss aktiv werden, um die Nachricht aus dem Postfach abzuholen. Dies erfolgt in Form eines expliziten Abholauftrags an den Intermediär. In dem Moment, in dem die Nachricht das Postfach des Empfängers erreicht hat, ist sie in dessen Verfügungsbereich übergegangen. Wie im richtigen Leben liegt es in der Verantwortung des Empfängers, regelmäßig in seinen Briefkasten zu schauen, ob Nachrichten für ihn vorhanden sind.

In dem Szenario **One Way, passiver Empfänger** wird eine Nachricht von einem Sender an einen Empfänger übertragen, wobei die Zustellung ohne Zutun des Empfängers an diesen weitergeleitet. Die Übertragung wird nachvollziehbar protokolliert. Dieses Szenario bietet sich an, wenn der Empfänger die Zustellung ohne Verzögerung erhalten soll. Der Empfänger muss in diesem Szenario also ständig unter einer URL erreichbar sein.

Die oben dargestellten Übertragungsvarianten stellen unterschiedlich hohe Anforderungen an die Verfügbarkeit der Nutzer einer OSCI Infrastruktur. Bei der Variante One Way - passiver Empfänger müssen die Empfänger ständig verfügbar sein, sonst scheitert die Übermittlung. Diese Variante kommt also nur für Diensteanbieter im Bereich der öffentlichen Verwaltung in Frage, die durch technische und organisatorische Maßnahmen (Betrieb mit ausfallsicheren Systemen, etc.) die dauernde Empfangsbereitschaft sicherstellen können.

Sofern die permanente Empfangsbereitschaft eines Empfängers nicht sichergestellt werden kann, besteht der entscheidende Nachteil dieser Variante darin, dass ein Sender seine Nachricht nicht zustellen kann. Dies bedingt auf Senderseite die Notwendigkeit eines Überwachungs- und Verwaltungssystems für nicht zustellbare Nachrichten, inklusive eines geeigneten Eskalationsmechanismus, wenn für die Zustellung einzuhaltende Fristen ablaufen.

Im Gegensatz dazu bestehen bei der Variante des aktiven Empfängers keine Anforderungen hinsichtlich seiner Empfangsbereitschaft. Der Empfänger bestimmt selbst, wann er die an ihn gerichteten Rückmeldungen für die Weiterverarbeitung empfangen möchte, und der Sender hat stets die Gewissheit, Nachrichten fristgerecht zustellen zu können. Zusätzlich erlaubt diese Variante Nachrichten bzw. Rückmeldungen zu fest definierten Zeitpunkten (bspw. nachts) gebündelt beim Intermediär abzurufen werden, und anschließend im Batchverfahren zu verarbeitet, ohne das eine zusätzliche Speichermöglichkeit auf Empfangsseite vorgehalten werden muss.

Voraussetzung für dieses Verfahren ist jedoch die Verfügbarkeit der Postfachfunktionalität beim Intermediär. Technische Umsetzungen hierfür werden in der Regel auf Datenbanken basieren, und können je nach gewähltem Produkt sehr kostenintensiv sein. Insbesondere wird der Kostenaufwand für die Realisierung von Postfächern beim Intermediär erheblich höher eingeschätzt als die Kosten, die beim Sender und Empfänger für die Umsetzung des passiven Empfängers aufzuwenden sind. Diese Schätzung unterstellt jedoch, dass auf Empfangsseite keine Hoch-

verfügbarkeit gewährleistet werden muss, sondern die fristgerechte Zustellung durch angemessene Eskalationsmechanismen durch den Sender zugesichert werden kann (etwa Zustellung der Rückmeldung auf dem Postweg nach wiederholt fehlgeschlagener Zustellung).

Im Sinne einer robusten Auslegung der OSCI-Infrastruktur ist zu fordern, dass jeder Teilnehmer über ein durch einen Intermediär zur Verfügung gestelltes Postfach verfügt. Dann kann man als Sender sicher sein, dass die Zustellung einer Nachricht mindestens in der Variante des aktiven Empfängers sichergestellt ist.

Im Sinne einer möglichst preisgünstigen und schnellen flächendeckenden Umsetzung der länderübergreifenden Rückmeldung wäre jedoch der passive Empfänger zu favorisieren, sofern die Postfachfunktionalität nur mit hohen zusätzlichen Kosten für die Kommunen umsetzbar ist.

Es sei allerdings darauf hingewiesen, dass diese Vorgehenswiese sehr stark von den Anforderungen des Geschäftsvorfalls Rückmeldung geprägt ist. Trotz der hohen Relevanz der flächendeckenden Umsetzung der Rückmeldung sollte durch die jetzt vorzunehmenden infrastrukturellen Maßnahmen auch die Anforderungen anderer Fachlichkeiten abgedeckt sein und der Nutzen für diese bei der Bewertung der zu erbringenden Investitionen berücksichtigt werden.

In Analogie der Rollenaufteilung auf der Senderseite unterscheidet man auf der Empfangsseite zwischen dem Empfänger für die Verarbeitung der Nutzungsdaten und dem Leser der die Verarbeitung der Inhaltsdaten leistet.

In Abhängigkeit der Sicherheitsanforderungen des zu Grunde liegenden Geschäftsvorfalls besteht das Aufgabenspektrum des Empfängers in der Dechiffrierung der Nachricht, der Prüfung der Intermediärs-Signatur sowie der Dekomposition der Nachricht.

Weiterhin leistet der Empfänger eine Überprüfung der Sendeberechtigung. Hierbei wird zunächst geprüft, ob dieses betrachtete Kommunikationsszenario innerhalb einer geschlossenen Benutzergruppe stattfindet und ggf. die Zugehörigkeit des Senders zu dieser Benutzergruppe verifiziert. Nur bei positivem Ergebnis wird mit der Verarbeitung der Nachricht fortgefahren. Kann die Zugehörigkeit zur geschlossenen Benutzergruppe nicht bestätigt werden, wird die Nachricht bereits durch den Empfänger verworfen, ohne das der Leser in Erscheinung tritt.

Damit der Empfänger feststellen kann, ob dem vorliegenden Geschäftsvorfall eine geschlossenen Benutzergruppe zu Grunde liegt, wird dieser durch eine entsprechende Betreff-Angabe in den Nutzungsdaten der Nachricht gekennzeichnet. Für diesem Zweck wird durch OSCI–Transport ein optionales Subject-Element vorgesehen. Für XMeld-Anwendungen wird dieses Element mit der entsprechenden Nachrichtenkennung der XMeld-Spezifikation versehen.

OSCI berücksichtigt sowohl die Kommunikation zwischen Bürger und Dienstleistern und Verwaltung, als auch die Kommunikation zwischen verschiedenen DV-Verfahren der Verwaltungen untereinander. Im Unterschied zum Geschäftsvorfall länderübergreifende Rückmeldung kann in diesem allgemeinen Szenario der Kreis der potentiellen Kommunikationspartner nicht eingeschränkt werden. Daher verfügt OSCI über keine explizite Benutzerverwaltung, sondern arbeitet mit einer offenen Benutzergruppe.

Die für die Bildung einer geschlossenen Benutzergruppe benötigten Mechanismen für eine sichere und zweifelsfreie Identifizierung der Kommunikationspartner werden daher auf Basis der durch die PKI zur Verfügung gestellten Mittel realisiert. Dazu wird der im X.509-Zertifikatvermerkte *Subject-Distinguished Name* (Subject-DN) des Zertifikatsinhabers in Übereinstimmung mit den Namenskonventionen der PKI-1-Verwaltungum ein zusätzliches *organisation-unit-Attribut* (ou-Attribut) ergänzt, das im Anschluss an evt. bereits vorhandene ou-Attribute eingefügt wird und mit dem Wert *ou=EWO_OSCI* belegt wird. Da es sich bei dem Zertifikat des Senders um ein Serverzertifikat handelt, das durch eine unter der Wurzel-CA der PKI-1-Verwaltung betriebenen Domänen-PKI herausgegeben wurde, muss der Wert des *Common-Name-Attribut* (cn-Attribut) des Subject-DN des Zertifikats einen entsprechenden GRP-Zusatz enthalten. GRP steht für den automatisierten IT-Prozess entsprechend PKI-1, z.B. cn=GRP: Intermediär, cn=GRP: Leser oder cn=GRP: Empfänger.

Insgesamt wird die Mitgliedschaft der geschlossenen Benutzergruppe der Meldebehörden durch die folgenden Kriterien belegt:

- Zertifikat gehört zu eine vertrauenswürdigen PKI, die unterhalb der CA der PKI-1-Verwaltung betrieben wird
- Das letzte ou-Attribut des Subject-DN hat den Wert ou=EWO_OSCI
- Wert des cn-Attribut des Subject-DN des Zertifikats enthält den Zusatz GRP zur Kennzeichnung eines Serverzertifikats

Dem Leser obliegt die Dechiffrierung der Inhaltsdaten sowie die Überprüfung der durch den Autor applizierten Inhaltsdatensignatur.

Entsprechend der bereits geführten Argumentation wird die im klassischen OSCI-Bild ebenfalls durch den Leser wahrgenommen Aufgabe der eigentlichen Inhaltsdatenverarbeitung im Sinne einer möglichst generischer Verwendbarkeit des OMH durch das adressierte Fachverfahren geleistet. Dies betrifft insbesondere auch die ggf. notwendige

Konvertierung der Inhaltsdaten in das spezifischen Datenformat des Fachverfahrens. Insofern besteht die durch den Leser zu leistenden Verarbeitung neben der Dechiffrierung und der Prüfung der Signatur der Inhaltsdaten lediglich darin, diese an das Fachverfahren als dem Abnehmer weiterzuleiten.

Neben den eigentlichen Inhaltsdaten übergibt der Leser dem Fachverfahren auch den, die gesamte Kommunikation dokumentierenden Laufzettel für Archivierungszwecke.

2.2 Adressierung

Die Adressierung umfasst die Prozesse der Ermittlung der physikalischen Adressen des Intermediärs und des Empfängers in Form ihrer IP-Adressen, sowie die Beschaffung der benötigten Chiffrier-Zertifikate. Zur Zeit gibt es keine Möglichkeit, um von den durch das Fachverfahren bereitgestellten und im bisherigen konventionellen Verfahren für die Adressierung verwendeten Informationen in Form des amtlichen Gemeindeschlüssel(AGS) auf die im elektronischen Verfahren benötigten Informationen zu schließen. Um dies zukünftig zu ermöglichen wird das nachfolgend beschriebene Verfahren vorgeschlagen.

Dieses Verfahren beruht auf der Nutzung des durch die PKI-1-Verwaltungbereitgestellten zentralen Verzeichnisdienst der Verwaltung (VDV), der es allen Mitarbeitern der angeschlossenen Domänen erlaubt, die notwendigen PKI-Informationen (Zertifikate und Sperrlisten) domänenübergreifend abzufragen.

Die Ermittlung der physikalischen Adressen des Intermediärs und des Empfängers lässt sich durch eine geeignete und durch das Namenskonzept der PKI-1-Verwaltung zulässigen Erweiterung in den jeweiligen Zertifikaten auf die Zertifikatsermittlung zurückführen. Dazu wird durch die Zertifikats-Extension *subjectAltName* mit *GeneralName*ein Server-Name (dNSName) in das Zertifikat eingebunden. Somit können durch eine einfache DNS-Abfrage die IP-Adressen der Kommunikationsbeteiligten ermittelt werden. *GeneralName* lässt neben einem Server-Namen (dNS-Name) auch eine explizite IP-Adresse zu, so dass sich ohne DNS-Auflösung der gewünschte Rechner direkt adressieren ließe. Praktische Erfahrungen haben allerdings gezeigt, dass dieses Verfahren nicht praktikabel ist, da IP-Adressen häufig wechseln.

Das derzeitige Konzept des VDV ist begrenzt auf die verzeichnisdienstspezifischen Voraussetzungen für produktive Lösungen zur allgemeinen Bereitstellung von Sperrlisten, CA-Zertifikaten und Teilnehmer-Zertifikaten zur Verschlüsselung von E-Mail. Um den Abruf von Server-Chiffrierzertifikaten für die OSCI-Kommunikation per LDAP-Anfrage zu ermöglichen, müssen die Teilnehmer-Entries, die unter anderem die Zertifikate enthalten, um diejenigen Informationen ergänzt werden, die bei einer entsprechenden Anfrage als Suchparameter verwendet werden können. Hierzu zählen zunächst der amtliche Gemeindeschlüssel sowie die Unterscheidung der beteiligten Kommunikationspartner, also des Intermediärs, des Empfängers und des Lesers.

Da es durchaus denkbar ist, dass ein Fachverfahren seine Dienste über unterschiedliche Server zur Verfügung stellt, muss zudem die Angabe des adressierten Dienstes bei der Zertifikatsabfrage möglich sein. Im Bereich der Kommunikation im Meldewesen erfolgt dies anhand der in der XMeld-Spezifikation vorgenommenen Nachrichtenkennung, aus der der Anlass der Kommunikation eindeutig hervorgeht und somit auf den zuständigen Server geschlossen werden kann.

Der zulässige Inhalt der Teilnehmer-Entries wird im Directory-Schema konfiguriert. Auf diese Struktur muss im Hinblick auf XMeld und weitere OSCI-Anwendungen Einfluss genommen werden und es müssen ggf. Änderungen erfolgen. Konkrete Vorschläge sollten im Rahmen des Umsetzungsplans mit dem BSI diskutiert werden.

2.3 Clearingstellen

Die Bereitstellung des in den letzten Abschnitten aufgezeigten Funktionsumfangs liegt vollständig in der Verantwortung der Meldebehörden. Für Meldebehörden, die nicht über die technische Ausstattung verfügen, um den aufgezeigten Funktionsumfang zu realisieren, besteht jedoch die Möglichkeit, diese Aufgaben teilweise oder vollständig an eine sogenannte Clearingstelle zu delegieren. Dies betrifft sowohl die Gewährleistung der technischen Erreichbarkeit einer Meldebehörde in Form einer beauftragten Clearingstelle, als auch die für die kommunikationsspezifische Verarbeitung von OSCI–XMeld Nachrichten benötigten Funktionen (Kryptographie, Adressierungsfunktionalitäten, etc.). Eine Clearingstelle stellt somit eine zusätzliche, optionale technische Komponente dar, die im Auftrag einer Meldebehörde tätig wird, um eine OSCI-konforme Kommunikation im länderübergreifenden Bereich zu gewährleisten. Eine Clearingstelle in diesem Sinne agiert folglich im Sinne eines Erfüllungsgehilfen für die Meldebehörden. Darüber hinaus besitzt eine Clearingstelle keine eigene und von einer Meldebehörde unabhängige Funktion. Insbesondere handelt es sich bei einer Clearingstelle nicht um einen Intermediär im Sinne des OSCI-Kommunikationsmodells, sondern die durch eine Clearingstelle bereitgestellten Funktionen und übernommenen Aufgaben entsprechen denen des Autors und Senders auf Seiten einer sendenden Behörde bzw. des Empfängers und Lesers auf Seiten einer empfangenen Behörden. Zusätzlich kann eine Clearingstelle Aufgabe übernehmen, die in der oben beschriebenen Kommunikationsmodell dem Fachverfahren zugeteilt war, wie bspw. die Konvertierung der Datenformate.

Die Kommunikation zwischen Clearingstelle und einer sie beauftragenden Kommune liegt deshalb außerhalb des Betrachtungsbereichs und wird als vertrauensvoll vorausgesetzt.

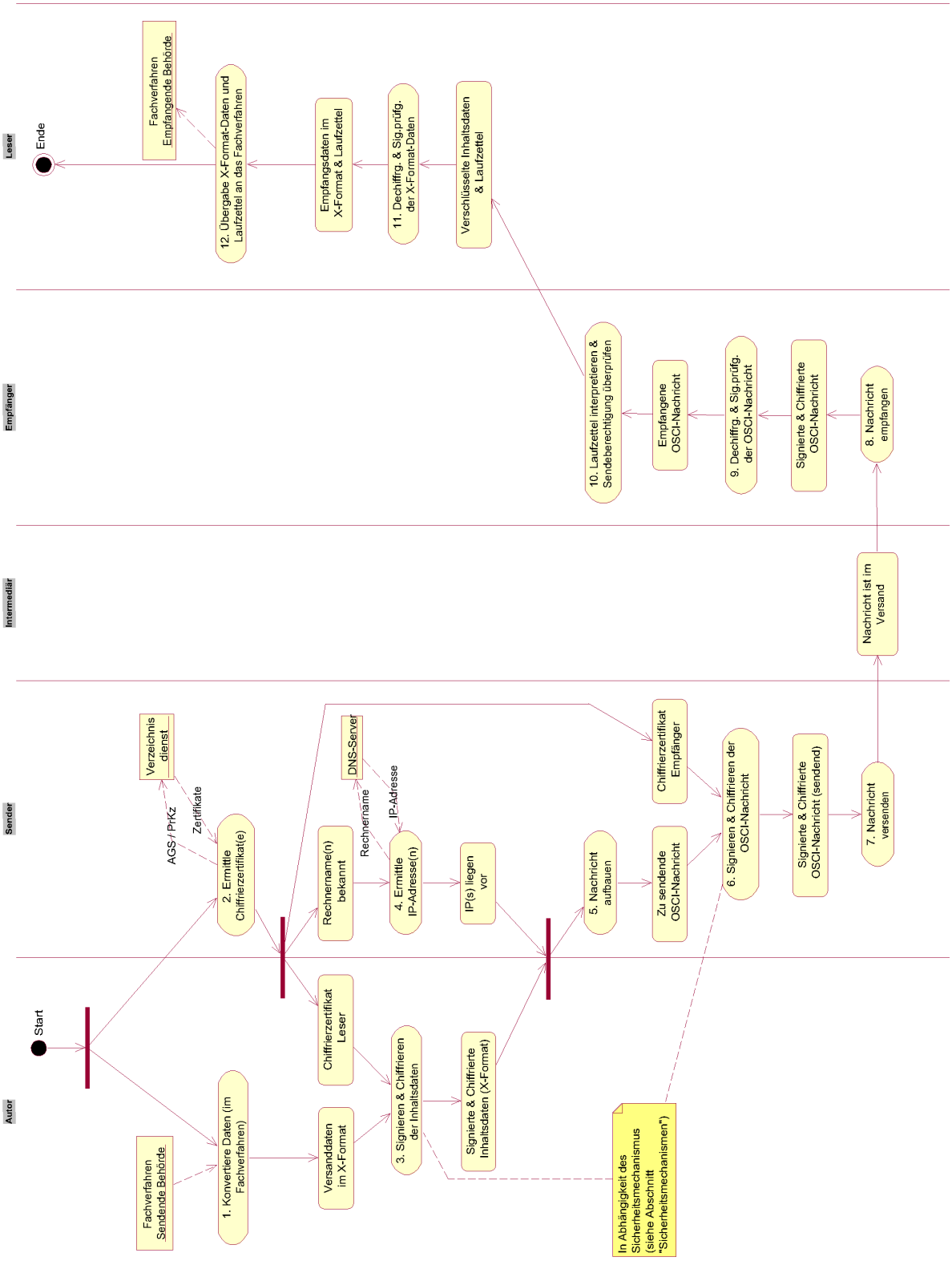
2.4 Kommunikationsablauf

Zur besseren Übersicht wird in der nachfolgender Tabelle der gesamte Kommunikationsablauf in chronologischer Ordnung nochmals dargestellt. Zusätzlich wird der Ablauf in Form eines Aktivitätsdiagramm veranschaulicht. Die in dem Diagramm verwendeten Nummerierungen für die Aktivitäten

Tabelle 2: Kommunikationsablauf

	Akteur	**Aktivität**
1.	Fachverfahren	Erzeugen und konvertieren der Inhaltsdaten
2.	Sender	Ermitteln der Chiffrier-Zertifikate des Intermediärs, des Empfängers und des Lesers
3.	Autor	Signieren und verschlüsseln der Inhaltsdaten (optional in Abhängigkeit des Geschäftsvorfalls)
4.	Sender	Ermitteln der IP-Adressen durch DNS-Abfragen
5.	Sender	Aufbauen der Gesamtnachricht
6.	Sender	Signieren und verschlüsseln der Gesamtnachricht (optional in Abhängigkeit des Geschäftsvorfalls)
7.	Sender	Versenden der Nachricht
8.	Empfänger	Empfangen der Nachricht
9.	Empfänger	Dechiffrieren und prüfen der Signatur
10.	Empfänger	Prüfen der Sendeberechtigung und interpretieren des Laufzettels
11.	Leser	Dechiffrieren und prüfen der Signatur der Inhaltsdaten
12.	Leser	Übergeben der Inhaltsdaten und des Laufzettels an das Fachverfahren

Bild 3 Aktivitätsdiagramm für die Kommunikation von Meldebehörden



2.5 Sicherheitsmechanismen

Durch OSCI–Transport 1.2 kann die Vertraulichkeit, Integritätund Authentizität der Inhalts- und Nutzungsdaten, die Nichtabstreitbarkeit der Autorenschaft und des Kommunikationsvorgangs sowie die Zurechenbarkeit von Nutzeraktivitäten sichergestellt werden (vgl. OSCI–Transport 1.2, Kap. 5.1). Dies wird realisiert durch Verschlüsselungs- und Signiermechanismen, durch Mechanismen der Zertifikatsprüfung, durch Quittungsmechanismen, durch eine Dialoginitialisierung, Challenge-Response-Mechanismen sowie durch Vergabe einer Message-Identifikation (vgl. OSCI–Transport 1.2, Kap. 6).

Für XMeld 1.0 wird die Anwendung *"Rückmeldung"* zwischen Meldeämtern betrachtet. Mit der Rückmeldung werden Informationen über den Umzug eines Bürgers von der Zuzugs- zur Wegzugsgemeinde übermittelt, sofern die beiden Gemeinden in unterschiedlichen Bundesländern liegen.

In diesem Abschnitt werden für die Rückmeldung in einer Sicherheitsanalyse die Sicherheitsziele definiert und die für die Realisierung nötigen OSCI-Sicherheitsmechanismen benannt.

In XMeld 1.0 wurde eine Verallgemeinerung auf weitere X-Typ-Nachrichten bereits berücksichtigt. Gleichwohl ist diese Sicherheitsanalyse sowie die Ableitung der OSCI-Sicherheitsmechanismen der Rückmeldung gewidmet. Für eine andere Anwendung müssen entsprechende Überlegungen angestellt werden, die sich allerdings an der hier angewandten Vorgehensweise orientieren können.

2.5.1 Sicherheitsanalyse

In diesem Abschnitt wird eine Sicherheitsanalyse für die Rückmeldung durchgeführt. Eine abschließende Bewertung (Relevanz, Vollständigkeit,...) müssen die Meldebehörden aufgrund ihres Verantwortungsbereichs vornehmen. Ein Vorschlag ist, im Rahmen der Feinkonzeption diese Aufgabe durch Hinzuziehung von Fachleuten (AK1 der IMK) zu bearbeiten.

Es sind folgende Sicherheitsziele identifiziert worden:

- Vertraulichkeit der Rückmeldung
- Integrität und Authentizität der Rückmeldung
- Nachweisbarkeit der Autorenschaft der Rückmeldung
- Authentizität/Identifikation der Kommunikationspartner
- Nachweisbarkeit der Kommunikation
- Zeitliche Bestimmtheit der Kommunikation
- Beweissicherung

Schutzbedarfsklassen

Entsprechend dem OSCI–Transport 1.2 Betriebshandbuch werden drei Schutzbedarfsklassen anhand der möglichen Schadensauswirkungen definiert:

Schutzbedarfsklasse	Beschreibung
Keine bis gering	Ein besonderer Schutz ist nicht notwendig, da keine Schadensauswirkungen zu erwarten sind.
Mittel	Die Schadensauswirkungen sind begrenzt und überschaubar. Ein Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen, ein möglicher Ansehensverlust einer Behörde ist gering.
Hoch bis sehr hoch	Die Schadensauswirkungen können beträchtlich sein und ein existentiell bedrohliches, katastrophales Ausmaß annehmen, der Ansehensverlust für eine Behörde ist beträchtlich.

Sicherheitsziel: Vertraulichkeit der Rückmeldung

Bei der Übermittlung von Rückmeldungen werden personenbezogene Daten übermittelt. Dazu ist sicherzustellen, dass diese nicht von unberechtigten Dritten mitgelesen werden können.

Schutzbedarfsklasse: hoch bis sehr hoch.

Sicherheitsziel: Integrität und Authentizität der Rückmeldung

Durch die Sicherung der Integrität der Rückmeldung wird das Ziel verfolgt, diese Informationen vor einer gezielten Manipulation zu schützen bzw. deren Unverfälschtheit nachweisbar feststellen zu können.

Schutzbedarfsklasse: mittel.

Sicherheitsziel: Nachweisbarkeit der Autorenschaft der Rückmeldung

Es ist notwendig, dass eine übersandte Rückmeldung zweifelsfrei einem konkreten Meldeamt zuzuordnen ist.

Schutzbedarfsklasse: mittel.

Sicherheitsziel: Authentizität/Identifikation der Kommunikationspartner

Die Kommunikationspartner müssen die behaupteten sein (Authentizität) und sie müssen Meldeämter sein (Identifikation). Dies dient dem Ziel, *Man-in-the-middle-* und *Replay-* Attacken erkennen bzw. vermeiden zu können.

Schutzbedarfsklasse: mittel.

Sicherheitsziel: Nachweisbarkeit der Kommunikation

Ein weiteres Sicherheitsziel - wenn auch kein vorrangiges - ist die Nachweisbarkeit der Kommunikation, wodurch der Sender nachweisen kann, eine Rückmeldung abgeschickt zu haben. Der Nachweis des Empfängers, eine Rückmeldung empfangen zu haben, wird über die obigen Sicherheitsziele abgedeckt.

Schutzbedarfsklasse: gering.

Sicherheitsziel: Zeitliche Bestimmtheit der Kommunikation

Die Protokollierung von Zeitpunkten dient der Möglichkeit, die Kommunikation einem Zeitpunkt zweifelsfrei zuordnen zu können. Dies ist insbesondere bei der Wahrung von Fristen zum Zweck der Nachweisbarkeit erforderlich. Für die Rückmeldung ist eine Frist von drei Tagen vorgeschrieben.

Schutzbedarfsklasse: mittel.

Sicherheitsziel: Beweissicherung

Die Revisionsfähigkeit, mit der festgestellt werden kann, wer wann welche personenbezogene Daten in welcher Weise verarbeitet hat, ist datenschutzrechtlich notwendig. Daher ist die Protokollierung und Archivierung aller ein- und abgehenden Daten sowie Protokoll- und Loggingdaten für eine gewisse Zeitdauer nötig.

Schutzbedarfsklasse: mittel.

Sicherheitsziel: Vertraulichkeit der Kommunikationspartner

Bei der Rückmeldung kommunizieren Meldeämter miteinander. Ihre Vertraulichkeit ist kein Sicherheitsziel, da die Informationen der Rückmeldung selber vertraulich behandelt werden.

Schutzbedarfsklasse: keine oder gering.

2.5.2 Ableitung der OSCI-Sicherheitsmechanismen

Es wird angenommen, dass sowohl auf der Seite der Zuzugs- als auch der Wegzugsgemeinde zwischen Autor und Sender sowie zwischen Empfänger und Leser ein Vertrauensverhältnis herrscht und die Kommunikation dazwischen als sicher einzustufen ist.

Diese Annahmen haben für die Rückmeldung direkten Einfluss auf die Sicherheitsmechanismen. Diese Überlegungen gelten auch für andere Architekturen, wenn etwa die jeweiligen Fachverfahren als *"Lieferant"* und *"Abnehmer"* auftreten oder wenn Clearing-Stellen Aufgaben der Meldeämter übernehmen. Es wird dann angenommen, dass die Kommunikation bei diesen Architekturen auf besondere Weise abgesichert wird, die hier out-of-scope ist. Es sind bei diesen 1:1-Beziehungen - etwa zwischen Meldeamt und Clearingstelle - auch keine Public-Key-Methoden zwingend notwendig, sondern aufgrund der 1:1-Beziehung ist auch denkbar, dass die Teilnehmer auf andere Weise geheime Schlüssel ausgetauscht haben.

Im folgenden Text werden die OSCI-Sicherheitsmechanismen vorgestellt:

Verschlüsselung der Inhaltsdaten

Die Verschlüsselung der Inhaltsdaten gewährleistet die Vertraulichkeit der Rückmeldung und die Authentizität der Kommunikationspartner.

Vertraulichkeit der Rückmeldung

Bei der Übermittlung von Rückmeldungen ist sicherzustellen, dass diese nicht von unberechtigten Dritten mitgelesen werden können.

Notwendig ist ferner eine strikte Trennung von Inhalts- und Nutzungsdaten, siehe Anforderungsdokument *"OSCI–Transport 1.2 - Entwurfsprinzipien, Sicherheitsziele und -mechanismen"* der datenschutz nord GmbH, Seite 8: *"Aufgrund der in OSCI vorgenommenen Trennung von Inhalts- und Nutzungsdaten ist [...der Einsatz des Intermediärs, der an zentraler Stelle vorgesehen ist und an den Prüfaufgaben delegiert werden,...] ohne Verletzung der datenschutzrechtlich gebotenen Vertraulichkeit der Inhaltsdaten möglich."*

Dieser Schutz der Vertraulichkeit wird bei XMeld (Rückmeldung) durch eine Verschlüsselung der Inhaltsdaten gewährleistet: Der Zweck der Inhaltsdatenverschlüsselung besteht in der Realisierung einer Ende-zu-Ende-Verschlüsselung zwischen den Autoren und den Lesern einer Nachricht. Die Verschlüsselung erfolgt durch den/die Autor/en einer Nachricht unter Verwendung des/der öffentlichen Chiffrierschlüssels des/der Leser, so dass nur diese in der Lage sind, die Nachricht zu entschlüsseln. Somit gewährleistet die Inhaltsdatenverschlüsselung die Vertraulichkeit der Inhaltsdaten sowohl auf dem Transportweg als auch gegenüber dem Intermediär.

Authentizität der Kommunikationspartner (hier: Empfänger und Intermediär)

Die Authentifikation der Kommunikationspartner dient dem Ziel, *"Man-in-the-middle-"*und *"Replay-"*Attacken erkennen bzw. vermeiden zu können.

Die Authentizität der Kommunikationspartner wird einerseits durch Mechanismen der OSCI-Kommunikation und andererseits durch Verschlüsselungen und Zertifikate mit besonderen Einträgen gewährleistet:

- Fehlerfreier OSCI-Dialog:

  Innerhalb der OSCI-Kommunikation sind Dialoge und Nachrichten durch spezielle Identifizierungskennzahlen gekennzeichnet, die in den Nutzungsdaten einer Nachricht eingestellt werden, so dass bei Empfang einer Nachricht diese Kennzahlen einer entsprechenden Plausibilitätsprüfung unterzogen werden.
- Verschlüsselung:

  Zwar dient eine Verschlüsselung der Inhaltsdaten in erster Linie der Sicherung der Vertraulichkeit der Inhaltsdaten, doch kann damit auch eine Authentifikation der Kommunikationsteilnehmer in geschlossenen Benutzergruppen erreicht werden, so dass nur der berechtigte Leser in der Lage ist, die Inhaltsdaten zu entschlüsseln. Eine geschlossene Benutzergruppe zeichnet sich dadurch aus, dass der Kreis der potentiellen Sender anhand eines eindeutigen Merkmals identifizierbar ist. Dieses Identifizierungsmerkmal wird im Rahmen eines Registrierungsprozesses vergeben.

  Denn:

  Für die Verschlüsselung wird der öffentliche Schlüssel des Lesers benötigt, welches auf einem Chiffrierzertifikat angegeben ist. Das Chiffrierzertifikat enthält darüber hinaus Angaben zum Leser, dem Zertifikatsinhaber. Es stellt sich damit nun die Frage, ob der Empfänger den Angaben des Zertifikats glaubt, insbesondere, ob der Leser/Zertifikatsinhaber ein Meldeamt ist (Identifikation). Der Empfänger glaubt den Angaben des Zertifikats, wenn er dem Aussteller des Zertifikats - also der Zertifizierungsinstanz - vertraut. Vertraut er ihr und ist im Zertifikat der Subject-DN mit dem Eintrag *"EWO_OSCI"* versehen, so kann der Empfänger davon ausgehen, dass der Besitzer des öffentlichen Schlüssels tatsächlich ein OSCI-fähiges EWO-Fachverfahren im angegebenen Meldeamt ist. Dabei ist notwendig, dass diese Zertifizierungsinstanz nur tatsächlichen OSCI-fähigen EWO-Fachverfahren diese Eigenschaft zertifiziert.

Signatur der Nutzungsdaten

Die Signatur der Nutzungsdaten gewährleistet die Integrität der Rückmeldung, die Authentizität der Rückmeldung, die Nachweisbarkeit der Autorenschaft und die Authentizität der Kommunikationspartner:

Integrität der Rückmeldung

Durch die Signatur der Nutzungsdaten wird die Integrität der Rückmeldung gewährleistet, um die Rückmeldung vor einer gezielten Manipulation zu schützen bzw. deren Unverfälschtheit nachweisbar feststellen zu können.

Für die Rückmeldung reicht die Signatur der Nutzungsdaten aus, weil

- die Inhaltsdaten in einem separaten Umschlag in die Nutzungsdaten eingebettet sind und die Signatur der Nutzungsdaten auch einen Integritätsschutz für die Inhaltsdaten bewirkt, und weil
- sowohl auf Seiten der Zuzugs- als auch der Wegzugsgemeinde zwischen Autor und Sender sowie zwischen Empfänger und Leser ein Vertrauensverhältnis herrscht und die Kommunikation dazwischen als sicher einzustufen ist. Diese Überlegungen gelten auch für andere Architekturen, wenn etwa die jeweiligen Fachverfahren als *"Lieferant"*und *"Abnehmer"* auftreten oder wenn Aufgaben der Meldeämter übernehmen.

Dabei ist folgendes zu beachten:

- Der Intermediär übernimmt auf Transportebene für den Empfänger die Prüfung der Signaturen und Zertifikate entlang der Zertifikatskette.
- Die Prüfung beinhaltet eine Verifikation und eine Validierung:

- Verifikation:

  Der öffentliche Schlüssel, der zur Signaturprüfung verwendet wird, stammt aus einem Zertifikat, das im Auftrag übermittelt wird. Es werden alle Zertifikate der Zertifikatskette geprüft. Geprüft wird letztlich gegen den beim Intermediär sicher abgelegten Sicherheitsanker, d. h. den öffentlichen Schlüssel der Zertifizierungsinstanz, dem der Intermediär vertraut. Der Sicherheitsanker kann z. B. in Form eines CA-Selbstzertifikats vorliegen. Der Intermediär greift dazu u. U.auf zentralen Verzeichnisdienst (VDV) bzw. auf Kopien der Daten im lokalen Verzeichnis zurück, falls Zertifikate oder Sperrlisten eingeholt werden müssen.
- Validierung:

  Eine Validierung, d. h. die Prüfung, ob ein Zertifikat zum gegenwärtigen Zeitpunkt gültig und nicht gesperrt ist, kann über eine Sperrliste (Certificate Revocation List - CRL) oder eine Online-Zertifikats-Status-Abfrage (Online Certificate Status Protocol - OCSP) erfolgen. Im zentralen Verzeichnisdienst der PKI-1-Verwaltung (VDV) sind zur Zeit nur Sperrlisten vorgesehen. Für die Nutzung von OCSP müsste ein Dienst geschaffen werden, der z. B. auf Basis der Daten des VDV´s ein OCSP-Response erzeugt.
- Die Ergebnisse dieser Prüfung werden in einem Laufzettel als Protokoll mit Zeitpunkten der Einreichung, Weiterleitung, etc., ggf. mit einem kryptographischen Zeitstempel zusammen mit der noch verschlüsselten Rückmeldung an den Empfänger weitergeleitet.
- Der Empfänger kann auf diese Weise auf die Verifikation und Validierung einiger Signaturen und Zertifikate der Zertifikatskette verzichten. Notwendig ist allerdings, dass der Empfänger die Prüfergebnisse des Intermediärs prüft.

• Diese Prüfung beinhaltet die Verifikation und Validierung der Signatur des Laufzettels sowie dessen Auswertung:
  - Verifikation:

    Der Empfänger verifiziert die Signatur des Intermediärs auf mathematische Korrektheit mit dem mitgelieferten Zertifikat des Intermediärs. Darüber hinaus verifiziert der Empfänger die Signatur des Intermediärs-Zertifikat auf mathematische Korrektheit mit dem lokal abgelegten Sicherheitsanker.
  - Validierung:

    Der Empfänger sollte das Intermediärs-Zertifikat auf ihre gegenwärtige Gültigkeit validieren. Allerdings würde dadurch eine Intention des Intermediärs verloren gehen, nämlich, dass der Intermediär dem Empfänger Online-Gültigkeitsprüfungen abnimmt. Deshalb wird hier bei der Validierung des Laufzettels keine Online-Validierung mit Sperrliste oder OCSP durchgeführt. Es wird festgelegt, dass wenn das Intermediärs-Zertifikat gesperrt werden sollte, die betroffenen Empfänger mit *"out-of-band"*-Mechanismen darüber unterrichtet werden. Da es sich um Behörden - und damit um eine geschlossene Benutzergruppe - handelt, wären dort etablierte Kommunikationsmechanismen geeignet und ihre Nutzung legitim, in diesem wahrscheinlich seltenen Fall - auch mit Medienbruch - zurückzugreifen.
  - Interpretieren des Laufzettels samt Fehlerbehandlung.

Authentizität der Rückmeldung

Neben der Integrität der Rückmeldung wird durch die Signatur der Nutzungsdaten die Authentizität der Rückmeldung gewährleistet: Unter den oben gemachten Annahmen, dass

• zwischen den verschiedenen Komponenten auf Seiten der Zuzugs- und Wegzugsgemeinde jeweils ein besonderes Vertrauens- und Sicherheitsverhältnis herrscht und

• über den Subject-DN der X.509-Zertifikate eine geschlossene Benutzergruppe definiert wird,

kann man annehmen, dass die Rückmeldung tatsächlich von einem OSCI-fähigen EWO-Fachverfahren in einem Meldeamt stammt. Allerdings lässt sich eine aufgrund veränderter Inhaltsdaten fehlerhafte Nutzungsdatensignatur nicht auf diese Ursache zurückführen. Eine Signatur der Nutzungsdaten erfolgt durch den Sender einer Nachricht. Da die Rollen des Senders und des Autors einer Nachricht von unterschiedlichen Personen/Instanzen wahrgenommen werden können, gewährleistet eine Nutzungsdatensignatur nur einen Integritätsschutz der Inhaltsdaten auf dem Transportweg. Eine Veränderung auf dem Weg vom Autor zum Sender bzw. vom Empfänger zum Leser kann durch eine Nutzungsdatensignatur nicht festgestellt werden. Insbesondere kann durch eine Nutzungsdatensignatur keine Inhaltsverantwortung für die Inhaltsdaten geltend gemacht werden.

Nachweis der Autorenschaft und des Sendens

Die Signatur der Nutzungs- und nicht der Inhaltsdaten führt selbstverständlich dazu, dass hierüber keine Nachweisbarkeit der Autorenschaft erfolgen kann, weil nicht der Autor die Inhalte, sondern der Sender die Nutzungsdaten signiert. Unter Berücksichtigung des engen Vertrauensverhältnisses und der eingesetzten Sicherheitsmechanismen zwischen Autor und Sender kann allerdings aus der Signatur der Nutzungsdaten (und der Nachweisbarkeit des Sendens) eine gewisse Nachweisbarkeit der Autorenschaft abgeleitet werden.

Authentizität der Kommunikationspartner (hier: Intermediär und Sender)

Die Authentifikation der Kommunikationspartner dient dem Ziel, *"Man-in-the-middle-"* und *"Replay-"*Attacken erkennen bzw. vermeiden zu können.

Die Authentizität der Kommunikationspartner wird einerseits durch Mechanismen der OSCI-Kommunikation und andererseits durch Signaturen und Zertifikate mit besonderen Einträgen gewährleistet:

- Fehlerfreier OSCI-Dialog:

  Innerhalb der OSCI-Kommunikation sind Dialoge und Nachrichten durch spezielle Identifizierungskennzahlen (s. OSCI-Spezifikation Transport Version 1.2: Abschnitt 4.5 und 4.6) gekennzeichnet, die in den Nutzungsdaten einer Nachricht eingestellt werden, so dass bei Empfang einer Nachricht alle Kennzahlen einer entsprechenden Plausibilitätsprüfung unterzogen werden.
- Signatur:

  Eine Signatur der Nutzungsdaten eignet sich für die Authentifikation der Kommunikationsteilnehmer in geschlossenen Benutzergruppen. Eine geschlossene Benutzergruppe zeichnet sich dadurch aus, dass der Kreis der potentiellen Sender anhand eines eindeutigen Merkmals identifizierbar ist. Dieses Identifizierungsmerkmal wird im Rahmen eines Registrierungsprozesses vergeben.

  Denn:

  Durch die digitale Signatur unter einer Rückmeldung kann der Empfänger prüfen, dass der Zertifikatsinhaber im Besitz des privaten Schlüssels ist, welcher zum im Zertifikat angegebenen öffentlichen Schlüssel gehört. Es stellt sich damit nun die Frage, ob der Empfänger den Angaben des Zertifikats glaubt, insbesondere, ob der Sender/Zertifikatsinhaber ein Meldeamt ist (Identifikation). Der Empfänger glaubt den Angaben des Zertifikats, wenn er dem Aussteller des Zertifikats - also der Zertifizierungsinstanz - vertraut. Vertraut er ihr und ist im Zertifikat der Subject-DN mit dem Eintrag *"EWO_OSCI"* versehen, so kann der Empfänger davon ausgehen, dass der Besitzer des öffentlichen Schlüssels tatsächlich ein OSCI-fähiges EWO-Fachverfahren im angegebenen Meldeamt ist.

  Dabei ist notwendig, dass diese Zertifizierungsinstanz nur tatsächlichen OSCI-fähigen EWO-Fachverfahren diese Eigenschaft zertifiziert. Eine Verfälschung der Daten aufgrund einer *"Man-in-the-middle"*-Attacke wird entweder durch eine fehlerhafte Signatur oder, falls durch den Angreifer eine neue Signatur erstellt wurde, im Rahmen des Identifizierungsprozesses anhand einer unberechtigten Identität erkannt.

Protokollierung/Logging

Die Nachweisbarkeit der Kommunikation gliedert sich in die Unterziele Nachweisbarkeit des Sendens und Nachweisbarkeit des Empfangs von Nachrichten. Letzteres lässt sich durch eine Signatur der Nutzungsdaten realisieren. Für die Nachweisbarkeit des Sendens sind die Protokoll- und Loggingdaten ausreichend, weil für die Rückmeldung in Analogie zur heutigen Praxis (*"Shoot-and-Forget"*) die Schutzbedarfsklasse als *"gering"* eingestuft wurde.

Für die zeitliche Bestimmung der Kommunikation sind die Zeitangaben in Protokoll- und Loggingdaten ausreichend, weil für die Rückmeldungdie Schutzbedarfsklasse als *"gering"* eingestuft wurde.

Archivierung

In Analogie zur bisherigen Praxis werden die für die Nachvollziehbarkeit der Kommunikation relevanten Informationen bei den Fachverfahren für eine gewisse Zeit archiviert. Eine genaue Spezifikation muss in der Feinspezifikation erfolgen, weil dazu eine Beteiligung der Fachverfahrensanbieter erforderlich ist.

Zusammenfassung

Im Ergebnis sind für die Erfüllung der identifizierten Schutzbedarfsklassen die OSCI-Sicherheitsmechanismen in folgender Weise anzuwenden:

Tabelle 3: Sicherheitsmechanismen für XMeld (Rückmeldung)

Mechanismus		Verwendung für Kommunikationspartner
Verschlüsselung der Inhaltsdaten	ja	Vertraulichkeit der Rückmeldung, Authentizität der Kommunikationspartner
Signatur der Inhaltsdaten	nein	
Verschlüsselung der Nutzungsdaten	nein	

Mechanismus			Verwendung für Kommunikationspartner
Signatur der Nutzungs-daten	Sender:	ja	Integrität der Rückmeldung, Authentizität der Rückmeldung, Nachweisbarkeit der Autoren-schaft und des Sendens, Authentizität der Kom-munikationspartner
	Intermediär:	ja	
Protokollierung	ja		Beweissicherung, Zeitliche Bestimmtheit durch Zeitstempel
Archivierung	ja		Beweissicherung

2.5.3 Sicherheitsmechanismen weiterer X-Typ-Nachrichten

Neben XMeld und der Rückmeldung sind weitere X-Typ-Nachrichten denkbar, z. B. die einfache Melderegisterauskunft. Bei einer einfachen Melderegisterauskunft kann die aktuelle Anschrift zu einer Person erfragt werden. Dazu ist nicht notwendig, dass die anfragende Person in der Anforderung eindeutig identifiziert wird. Eine Signierung ist nicht nötig.

Da Anfrage und Antwort zu einer einfachen Melderegisterauskunft personenbezogene Daten enthalten und u. U. über unsichere Netze transportiert werden, ergibt sich, dass die Inhaltsdaten verschlüsselt werden müssen.

3 Technikarchitektur

3.1 Ziele des Architekturentwurfs

Der Abschnitt Kommunikationsmodell geht unter Punkt 2.1 ausführlich auf die OSCI-Rollen Autor, Sender, Empfänger und Leser ein und ordnet diesen eindeutig Aufgaben zu. Eine vollständige Abbildung dieses Rollenmodells auf Softwarearchitektur und Betriebskomponenten einer realen OSCI-Implementierung wurde jedoch bewusst nicht vorgenommen. Damit wird für Entwickler und Betreiber von Softwareprodukten ein maximaler Freiheitsgrad bei der Realisierung von OSCI-Lösungen garantiert und gewährleistet, dass sich möglichst viele Anbieter kurzfristig ss zu einer derartigen Lösung entschließen können.

Die Vielzahl der unterschiedlichen Fachanwendungen, die für eine OSCI-Kommunikation in Frage kommen, macht es notwendig, eine derart flexible Lösung zu wählen. Eine Clearingstelle wird dabei - je nach Reifegrad der zu bedienenden Fachanwendung - völlig unterschiedliche Rollen im Kommunikationsmodell wahrnehmen müssen. So wird es häufig erwünscht sein, dass die Clearingstelle Signatur und Verschlüsselung der Inhaltsdaten übernimmt, eine Aufgabe, die bei strenger Auslegung des OSCI-Rollenmodells eigentlich dem Autor einer Nachricht und damit strenggenommen der Fachanwendung obliegt. In diesem Fall sind allerdings Maßnahmen zum Schutz der personenbezogenen Daten erforderlich.

Fehlende Funktionen in der Fachanwendung oder eine Infrastruktur, die dem Backendverfahren den Zugriff auf Zertifikate zur Verschlüsselung verbietet, machen es notwendig, derartige Funktionen in die Clearingstelle vorzuziehen und dort unter Umständen auch auf einem Server zu konzentrieren. Die Rollen von Autor und Sender, aber auch von Empfänger und Leser werden daher in der Praxis häufig an einer Stelle zusammengefasst werden müssen und dort nur noch schwer nach dem reinen OSCI-Modell getrennt erkennbar sein. Diesen Forderungen trägt das vorgeschlagene Architekturmodell Rechnung.

Während der Erarbeitung des Architekturmodells hat es sich außerdem als zweckmäßig erwiesen, die eigentliche Fachanwendung vollständig von der OSCI-Kommunikation abzukapseln. Sie wird in der Gesamtbetrachtung somit nur zum Datenlieferanten und Datenabnehmer, benötigt aber ssssselbst keinerlei OSCI-Funktionalität. Damit wird der Sorge der Softwarehersteller Rechnung getragen, OSCI-Funktionen aufwändig in die eigene Fachanwendung integrieren zu müssen.

Fertige OSCI-Systeme können die Fachanwendung von außen ergänzen und sie so vollständig von zusätzlichen Aufgaben entlasten. Der Name *"OSCI Message Handler"* (OMH) wird als Bezeichnung für ein derartiges System eingeführt. Ein OMH beinhaltet alle notwendigen Komponenten, um eine OSCI-Kommunikation zwischen zwei Fachanwendungen vollständig abzuwickeln.

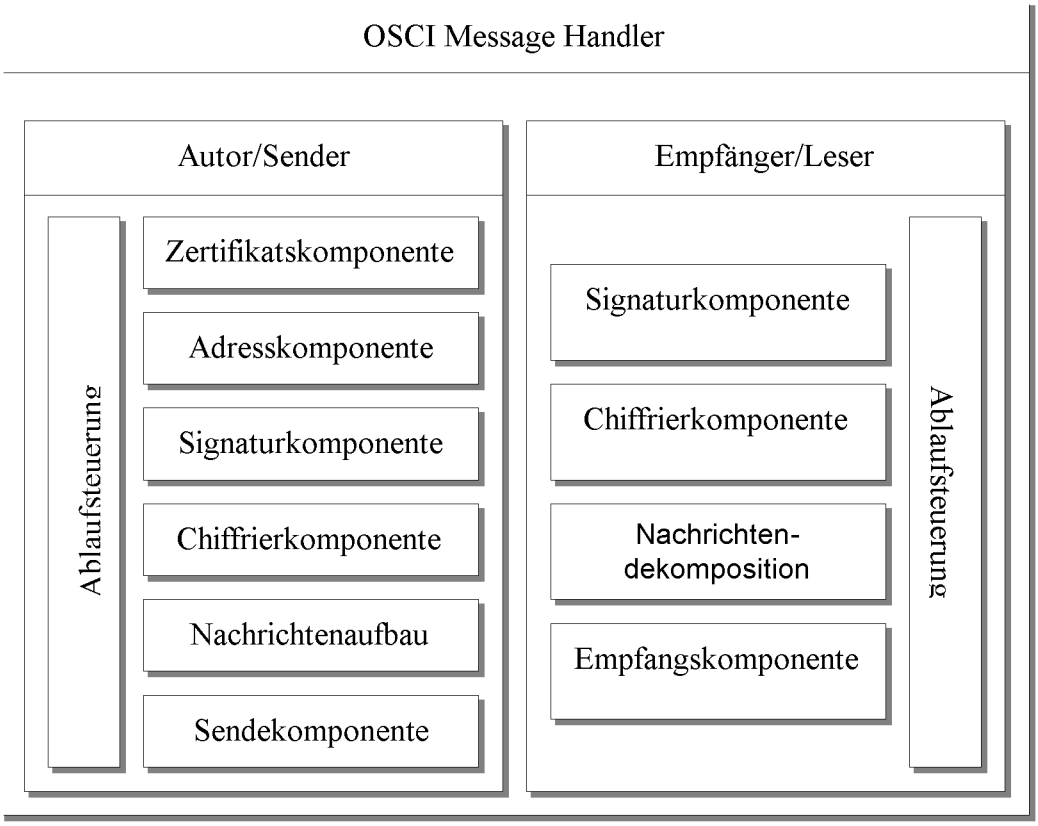
3.2 Voraussetzungen

Voraussetzung für eine kurzfristige Realisierung jeglicher OSCI-Lösungen ist die Verfügbarkeit einer plattformunabhängigen OSCI-Bibliothek, die alle OSCI-Funktionen laut Spezifikation 1.2 über Schnittstellen zur Verfügung stellt. Eine derartige Bibliothek sollte auf Basis der SAGA-Empfehlungen (s. www.bund.de/saga) realisiert werden und damit zunächst zumindest für JAVA-Umgebungen zur Verfügung stehen.

3.3 Architekturüberblick

Die folgende Abbildung gibt einen Überblick über die Komponenten eines OSCI Message Handlers. Dabei wird wie unter 3.1 beschrieben über die Lage der einzelnen Komponenten keine Aussage getroffen. Sie können sich gemeinsam auf einem System innerhalb einer Clearingstelle befinden, aber auch über mehrere Systeme verteilt betrieben werden.

Bild 4 Architekturmodell



Die Abbildung trifft keine Aussage über den Datenfluss zwischen den Komponenten. Vielmehr stellt jede Komponente eine Sammlung von Funktionen/Methoden zur Verfügung, die von der Ablaufsteuerung bei Bedarf aufgerufen werden.

Komponenten können als Services realisiert sein, die von der Ablaufsteuerung angesprochen werden und über ein entsprechendes Protokoll mit Daten versorgt werden bzw. ihre Ergebnisse abliefern. Als Protokoll zum Datenaustausch zwischen den Services wird SOAP empfohlen, jedoch nicht vorgeschrieben. In diesem Fall wird die Ablaufsteuerung nicht zwingend als eigene Komponente vorausgesetzt. Sie kann auch Bestandteil der Einzelkomponenten sein, die dann selbständig untereinander kommunizieren.

Alternativ stehen die Einzelkomponenten als lokale Bibliotheken zur Verfügung, die von der Ablaufsteuerung aufgerufen und mit Daten versorgt werden. In diesem Fall ist die Ablaufsteuerung als eigene Komponente obligatorisch, da ihr allein die Steuerung des Gesamtvorganges obliegt.

Die Schnittstelle zum Fachverfahren bildet immer die Ablaufsteuerung. Sie übernimmt die Daten in Form eines XML-Datenstromes aus dem Fachverfahren bzw. liefert sie als XML-Datensatz beim Fachverfahren ab. Die Schnittstelle der Ablaufsteuerung ist damit der einzige Punkt, an dem eine Anpassung von einem OSCI Message Handler zu den unterschiedlichen Fachverfahren erfolgen muss.

3.4 Beschreibung der Einzelkomponenten

Der nachfolgende Text stellt einen Vorschlag und keine verbindliche Vorgabe dar.

3.4.1 Adresskomponente

Die Beschaffung der Zieladressen für Intermediär und Empfänger wird bei jeder OSCI-Kommunikation zu den ersten Schritten gehören. Die hierzu notwendigen Funktionen/Methoden werden durch die Adresskomponente*OMH-Adress* zur Verfügung gestellt. Der zuständige Verzeichnisdienst-Server, der für die Anfrage verwendet werden soll, wird über das Attribut *directoryServer* festgelegt.

OSCITransport::OMHAdress
+directoryServer:String
+getDestAdress(ags:int, messageType: String):String +getIMAdress(ags:int, messageType:String):String +getIPAdress(hostname:String):String

getDestAdress liefert den Rechnernamen inklusive Domainerweiterung des Empfängers, der über den amtlichen Gemeindeschlüssel *ags* identifiziert wird, als String. Um für verschiedene Nachrichtentypen unterschiedliche Intermediäre (oder auch) ansprechen zu können, wird mit *messageType* zusätzlich der Nachrichtentyp übergeben.

getIMAdress wird wie *getDestAdress* versorgt und liefert als Ergebnisden Rechnernamen des zum *ags* und zum Nachrichtentyp gehörenden Intermediärs.

getIPAdress liefert zu einem mit *getDestAdress* oder mit *getIMAdress* erhaltenen Rechnernamen die zugehörige IP-Adresse. Die Funktion wird in Standardinstallationen dabei normalerweise auf die vom Betriebssystem gelieferten Routinen zur Namensauflösung zurückgreifen.

3.4.2 Zertifikatskomponente

Die Zertifikationskomponente liefert Funktionen, um alle für einen Vorgang benötigten Zertifikate von einem Verzeichnisdienst zu beschaffen. Der zuständige Verzeichnisdienst-Server wird über das Attribut *directoryServer* festgelegt.

OSCITransport::OMHCertificate
+directoryServer:String
+getDestCertificate(ags:int, messageType: String):userCertificate +getIMCertificate(ags:int, messageType:String):userCertificte +checkCertificate(certificate:userCertificate):boolean

Der Datentyp userCertificate beschreibt ein X.509-konformes Serverzertifikat. *getDestCertificate* liefert das zum AGS *ags* und zum Nachrichtentyp*messageType* gehörende Empfängerzertifikat.

getIMCertificate liefert das Zertifikat des Intermediärs, der für den angegebenen ags und Nachrichtentyp zuständig ist.*checkCertificate* überprüft das übergebene Zertifikate Certificate auf Gültigkeit. Dabei wird neben der mathematischen Prüfung eine Kontrolle verfügbarer Sperrlisten durchgeführt.

3.4.3 Signaturkomponente

Die Signaturkomponente sorgt für die OSCI-konforme Signatur von Inhaltsdaten und Gesamtnachricht. Der Zugriff auf den privaten Schlüssel *privateKey* ist implementierungs- und umgebungsabhängig und von außen nicht sichtbar.

```
OSCITransport::OMHSignature
+signXML(privateKey:int, xmlData: String):String
+checkXMLSignature(certificate:userCertificate,
         xmlData:String):boolean
+signMessage(privateKey:int, MessageData:String):String
+checkMessageSignature(certificate:userCertificate,
         MessageData:String):boolean
```

signXML signiert beliebige, OSCI-konforme Inhaltsdaten xmlData und liefert den signierten Datenstring zurück.

checkXMLSignature prüft OSCI-konforme, signierte Inhaltsdaten auf die Gültigkeit der Signatur. Das übergebene Zertifikat sollte vorher mit *OMHCertificate.checkCertificate* geprüft werden.

signMessage signiert die fertige Gesamtnachricht *MessageData* und liefert den signierten Datenstring zurück.

checkMessageSignature prüft OSCI-konforme, signierte Nachrichten auf die Gültigkeit der Signatur.

Es wird vorausgesetzt, dass alle Funktionen vollständig durch eine OSCI-Bibliothek zur Verfügung gestellt werden und daher nicht im OMH implementiert werden müssen.

3.4.4 Chiffrierkomponente

Die Chiffrierkomponente ist für die korrekte Ver- und Entschlüsselung von Inhaltsdaten und Gesamtnachricht zuständig. Das Zertifikat *Certificate*des Nachrichtenempfängers (Intermediär oder Leser der Nachricht) muss X.509-konform vorliegen. Üblicherweise wurde es vorher mit *OMHCertificate* beschafft.

```
OSCITransport::OMHCrypt
+encryptXML(Certificate:int, xmlData:String):String
+encryptMessage(Certificate: userCertificate
        messageData:String):String
+decryptXML(privateKey:int, xmlData: String):String
+decryptMessage(privateKey:int, messageData:String):
        String-getPrivateKey():int
```

encryptXML verschlüsselt beliebige, OSCI-konforme Inhaltsdaten *xmlData* und liefert den verschlüsselten Datenstring zurück.

encryptMessage verschlüsselt die fertige Gesamtnachricht *messageData*und liefert den verschlüsselten Datenstring zurück.

Auch hier wird vorausgesetzt, dass die beiden Funktionen vollständig durch eine OSCI-Bibliothek zur Verfügung gestellt werden und daher nicht im OSCI Message Handler implementiert werden müssen.

Die Dechiffrierfunktion ist das Gegenstück zur Chiffrierfunktion und sorgt für die Entschlüsselung von Nachrichten und Inhaltsdaten. Der Zugriff auf den privaten Schlüssel *privateKey* ist implementierungs- und umgebungsabhängig und von außen nicht sichtbar.

decryptXML entschlüsselt beliebige, OSCI-konforme Inhaltsdaten *xmlData* und liefert den entschlüsselten Datenstring zurück.

decryptMessage entschlüsselt die verschlüsselte Gesamtnachricht*messageData* und liefert den entschlüsselten Datenstring zurück.

Auch diese beiden Funktionen sind OSCI-Kernfunktionen, die vollständig von einer OSCI-Bibliothek zur Verfügung gestellt werden müssen. Ihre Implementierung ist daher nicht Bestandteil des OMH.

3.4.5 Nachrichtenaufbau

Die Komponente zum Nachrichtenaufbau erzeugt aus den XML-Inhaltsdaten*xmlData* (verschlüsselt oder unverschlüsselt, signiert oder unsigniert), eine unverschlüsselte und unsignierte Gesamtnachricht, die jederzeit über *OHMEncrypt* bzw. *OHMSign* verschlüsselt bzw. signiert werden kann. Die Nachricht wird dem in *messageType* festgelegten Nachrichtentyp entsprechend erstellt.

OSCITransport::OMHBuildMessage
+buildOSCIMessage(xmlData: String, messageType:String):String

buildOSCIMessage erzeugt aus dem Inhaltsdaten *xmlData* eine dem Nachrichtentyp *messageType* entsprechende OSCI-Gesamtnachricht und liefert sie als String zurück.

3.4.6 Nachrichtendekomposition

Die Komponente geht davon aus, dass die Nachricht bereits in unverschlüsselter Form vorliegt und die Nachrichtensignatur ggf. bereits mit *OHMSignature.checkMessageSignature* geprüft wurde. Sie liefert als Ergebnis die in der Nachricht eingebetteten Inhaltsdaten.

OSCITransport::OMHReadMessage
`+checkMessage(messageType:String):boolean` `+getXML(messageData: String):String`

checkMessage überprüft, ob die Nachricht dem in *messageType* angegebenen Nachrichtentyp entspricht.

getXML extrahiert die Inhaltsdaten aus der Nachricht *messageData* und liefert sie als String zurück.

3.4.7 Sendekomponente

Die Sendekomponente verschickt eine fertige OSCI-Gesamtnachricht an den in *imAdress* angegebenen Intermediär.

OSCITransport::OMHSendMessage
`+sendMessage(messageData:String, imAdress:String):boolean`

sendMessage verschickt die fertige Nachricht an den Intermediär *imAdress*. Dabei kann die Adressangabe als Rechnername oder IP-Adresse erfolgen. Bei erfolgreicher Ausführung erfolgt eine positive Rückmeldung.

3.4.8 Empfangskomponente

Der Empfang einer neuen Nachricht löst die im Kommunikationsmodell beschriebenen Schritte aus, führt also auf der Empfängerseite zum Durchlaufen aller für diesen Nachrichtentyp notwendigen Funktionen, um die Inhaltsdaten schließlich geprüft und entschlüsselt als XML-Strom an das Anwendungsverfahren zu übergeben.

Die Empfangskomponente lässt sich daher besonders gut in der Ablaufsteuerung integrieren. Diese nimmt neue Nachrichten als aktiver oder passiver Empfänger entgegen, löst deren Weiterbearbeitung aus und überwacht diese.

Der Aufbau der Komponente Nachrichtenempfang hängt stark vom gewählten Empfängertyp ab. Bei einem passiven Empfänger muss die Komponente als Listener realisiert werden. Die Ablaufsteuerung wartet in diesem Fall als Service auf neu eingehende Nachrichten und startet dann deren Weiterbearbeitung durch Aufruf der benötigten Funktionen.

Beim aktiven Empfänger überprüft die Ablaufsteuerung in festen Zeitintervallen das Eintreffen neuer Nachrichten im Postfach auf dem Intermediär. Auch in diesem Fall werden die Nachrichten nach ihrer Abholung durch Aufruf der benötigten Funktionen weiterverarbeitet und schließlich an das Fachverfahren übergeben.

3.5 Realisierungsempfehlungen

Für den OSCI Message Handler mit allen Komponenten und die Bibliothek von OSCI-Funktionen wird eine Implementierung nach SAGA-Richtlinien empfohlen. Für die Durchführung von Pilotprojekten wird eine Realisierung in Java empfohlen.

4 Umsetzungsplan

Das Ziel des Umsetzungsplans ist

- die Definition der weiteren notwendigen Aktivitäten zur Entwicklung und Einführung von technischen Einrichtungen und organisatorischen Voraussetzungen, um eine zeitgerechte Umsetzung der Rückmeldung bundesweit bis 2005 zu erreichen.

- Die Einschätzung der mit der Realisierung und dem Betrieb entstehenden Kosten und der entstehenden Nutzen und die sich daraus ergebenden wirtschaftlichen Konsequenzen

4.1 Aktivitätenplan

Für die Umsetzung der Rückmeldung auf Basis von OSCI–Transport und OSCI–XMeld sind die folgenden Aktivitäten erforderlich.

1. Pilotprojekt durchführen
2. Fachliche Feinspezifikation erstellen
3. Produkte entwickeln, die den OSCI-Message-Handler (OMH) realisieren
4. Umsetzung der Novellierung des MRRG in den Landesmeldegesetzen
5. Aufbau der PKI-Strukturen in den Ländern und Kommunen
6. Produkteinführung in den Kommunen
7. Betrieb

4.1.1 Pilotprojekt durchführen

Zur Absicherung des in dieser Vorstudie vorgesehenen Systementwurfs und der damit verbundenen Annahmen ist eine prototypische Erprobung angeraten.

Ein Pilotprojekt sollte unter Beteiligung von zwei EWO Fachverfahrensherstellern und eines potentiellen Herstellers des OSCI-Message-Handlers erfolgen. Eine Beteiligung von Kommunen wird als nicht notwendig erachtet, da durch die Verfahrenshersteller die Möglichkeit über Testdatenbestände zu verfügen, gegeben ist.

Ziel des Pilotprojektes ist die Erprobung der in der Vorstudie vorgeschlagenen Verfahren und Lösungen für die Adressierung inkl. des Betriebs eines exempl. Verzeichnisdienstes nach Vorgaben des VDVs, die Verwendung der Zertifikate für die Identifizierung in einer geschlossenen Benutzergruppe und die funktionalen Anforderungen an das Gesamtsystem OMH. Voraussetzung für die Durchführung des Pilotprojekts ist die Verfügbarkeit einer OSCI-Bibliothek. Das Vorhaben sollte in üblicher Projektorganisation durchgeführt werden. Als Auftraggeber sollte der KoopA in der Entscheidungsinstanz vertreten sein. Als Abstimminstanz zur Qualitätssicherung sollten Vertreter von späteren Software-Anbietern und späteren Anwendern in den Kommunen fungieren.

Für die Durchführung wird ein Aufwand von 95 Personentagen (PT) veranschlagt, der sich wie folgt ergibt:

Tabelle 4: Pilotprojekt durchführen

1.	Testplan erstellen	5 PT
2.	XML-Konverter erstellen	20 PT
3.	Aufbau eines exempl. LDAP-Servers	5 PT
4.	Zertifikate erstellen	5 PT
5.	Testkommunen einrichten	10 PT
6.	OMH implementieren	30 PT
7.	Test durchführen	10 PT
8.	Test auswerten	10 PT
	Gesamt	**95 PT**

Die Finanzierung des Pilotprojektes muss entweder über eine öffentlichen Förderungen oder durch den privaten Invest der beteiligten Pilotprojektpartner erfolgen. Nur im ersten Fall kann jedoch eine öffentliche Verfügbarkeit der Ergebnisse, insbesondere des zu entwickelnden Sourcecodes für den OMH sichergestellt werden.

4.1.2 Fachliche Feinspezifikation für den OMH erstellen und abstimmen

Auf Basis der Erkenntnisse des Pilotprojektes soll im Anschluss eine Feinspezifikation erarbeitet werden. In diesem Zusammenhang müssen auch Konzepte für die Produkteinführungen und den Betrieb in den Kommunen sowie entsprechende Übergangsregelungen erarbeitet werden.

Aus Gründen der Arbeitseffizienz sollte die Arbeitsgruppe nicht mehr als 10 Personen umfassen. Um andererseits einem großen Kreis Betroffener (Fachverfahrenshersteller, sonstige Software-Hersteller für OSCI-Produkte, Kommunen, etc.) die Möglichkeit zu geben, Einfluss auf die Arbeitsergebnisse zu nehmen, werden für die Erarbeitung der Feinspezifikation 2 Phasen vorgesehen. Somit können alle Interessierten und Betroffenen als Mitglieder der Abstimminstanz im Rahmen der Qualitätssicherung berücksichtigt werden.

Insgesamt wird für die Feinspezifikation ein Aufwand von 298 PT veranschlagt, der sich wie folgt ergibt:

Tabelle 5: Fachliche Feinspezifikation für den OMH erstellen und abstimmen

	Anzahl Mitglieder	**Kickoff**	**PT/Phase u. Person**	**Summe**
AG	10		8 PT	160 PT
AI	30	1 PT	1 PT	90 PT
EI	8	1 PT	1 PT	24 PT
Moderation/Dokumentation				24 PT
Gesamt				**298 PT**

Die Abstimmung der Anforderungen an den Verzeichnisdienstmit den Verantwortlichen des BSI wird im Rahmen der Projektarbeit durch eine Teilgruppe der Arbeitsgruppe wahrgenommen und führt zu einem Aufwand von etwa 60 PT (Finanzierung s. 4.3.1)

4.1.3 Produkte entwickeln, die den OMH realisieren

Wir gehen davon aus, dass auf Basis der erstellten Feinspezifikation durch Software-Hersteller Produkte entwickelt werden, deren Entwicklungskosten von den Herstellern getragen werden, weil diese Absatzchancen im Markt der öffentlichen Verwaltung erkennen werden.

Zum Betrieb der Produkte ist der Verzeichnisdienst mit den neuen Anforderungen zu realisieren

4.1.4 Umsetzung der Novellierung des MRRG in den Landesmeldegesetze

Aus den jeweiligen Umsetzungen der Landesmeldegesetze können sich für die Kommunen gewissen Einschränkungen bzw. Einflussparameter ergeben, die bei den jeweiligen Realisierungen zu berücksichtigen sind. Insbesondere können sich Vorgaben hinsichtlich der Architektur der landesinternen Infrastruktur ergeben, die z. B. Auswirkungen auf den Betrieb von haben können.

4.1.5 Aufbau der PKI-Strukturen in den Ländern und Kommunen

OSCI–Transport 1.2 setzt implizit voraus, dass die generischen Anforderungen für die vertrauenswürdige Benutzung von Public-Key-Kryptographieerfüllt sind. D.h., wie stets bei Benutzung von Public-Key-Kryptographie ist die Existenz einer vertrauenswürdigen Zertifizierungsinstanz nötig, die die verschiedenen Nutzer registriert, die Zugehörigkeit von Identität und öffentlichem Schlüssel des Nutzers beglaubigt und die dabei angemessen starken Registrierungs- und Zertifizierungsrichtlinien einhält. In diesem Sinne wird der wesentliche Teil des OSCI-Schlüsselmanagements von der zugrunde liegenden PKI geleistet. Wie unter Abschnitt 1.4.3 beschrieben, wird für die hier betrachtete zwischenbehördliche Verwaltungskommunikation in den Ländern der Betrieb einer PKI unter der Wurzelregistrierungsinstanz der PKI-1-Verwaltung vorausgesetzt, wobei zusätzlich die in diesem Dokument beschriebenen Anforderungen hinsichtlich der Zertifikatsausprägung zu erfüllen sind.

4.1.6 Produkteinführungen

Zur Vorbereitung des Betriebs müssen alle zur Kommunikation notwendigen Komponenten (OMH, Intermediär, XMeld-Konverter der Fachverfahren) in den Kommunen eingeführt werden. D.h. pro Kommune muss die Entscheidung über den Betrieb in eigener Regie oder der Anschluss an eine Clearingstelleerfolgen und daraus folgend müssen entsprechende Aktivitäten (Implementierung und/oder Schulung) stattfinden.

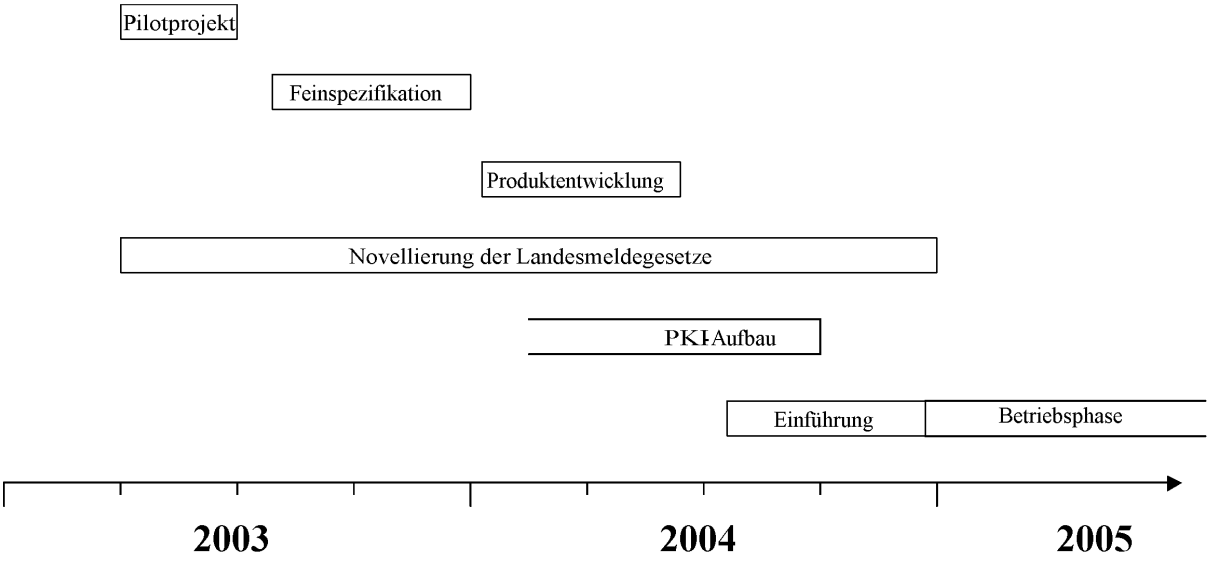
4.1.7 Betrieb

Ab dem Jahr 2005 sollen die Rückmeldungen ausschließlich elektronisch stattfinden.

4.2 Zeitplan

Die vorstehenden Aktivitäten sollten nach folgendem Zeitschema stattfinden:

Bild 5 Umsetzungszeitplan



Der Zeitplan macht deutlich, dass zur Erreichung des Betriebs in 2005 nur wenig Spielraum besteht. Aus diesem Grunde ist eine schnelle Entscheidung über das weitere Vorgehen erforderlich.

4.3 Wirtschaftlichkeit der elektronischen Rückmeldung

Ausgehend von großen Nutzungsunterschieden (kleine Kommune bis Großstadt, viel oder wenig Rückmeldungen, unterschiedliche DV-Ausstattung) sind die zu betrachtenden Kosten und Nutzen sehr unterschiedlich. Im folgenden Text sind deshalb verschiedene Modelle und Kategorien aufgezeigt, die es ermöglichen, in jeder Kommune eigene Rechnungen zur Wirtschaftlichkeit anzustellen.

4.3.1 Einmalkosten

Zum Betrieb der elektronischen Rückmeldung sind im Vorweg die im vorigen Abschnitt aufgezählten Entwicklungsarbeiten notwendig. Da hier unterschiedliche Interessen von den Partnern (Bund/Länder, Kommunen und Software-Hersteller) zum gemeinsamen Ziel gebündelt werden können, ist eine Kostenübernahme nach folgendem Schema denkbar.

Tabelle 6: Einführungskosten(einmalig)

Einführungskosten(einmalig)	Bund/Länder	Kommune	SW-Hersteller
Pilotprojekt durchführen	6 PM ca. 120 T Euro		
Fachliche Feinspezifikation 300 T Euro gemäß Kostenermittlung	100 T Euro	100 T Euro	100 T Euro
Spezifikation des VDV	30 T Euro		30 T Euro
Produktrealisierung	10 T Euro		250 T Euro /Hersteller

Die aufgezeigten Kosten bestehen zum großen Teil aus Personalkosten, die durch die Mitarbeit der Partner am gemeinsamen Entwicklungsprozess entstehen. Diese sind in der Kalkulation allerdings als Vollkosten kalkuliert. Sollten Kommunen bereits über entsprechende technische Voraussetzungen verfügen, dann sind hier nur die durch die Rückmeldung entstehenden Kosten anzusetzen.

4.3.2 Betriebskosten

Laufende Betriebskosten sind nur von den Kommunen zu tragen. Dabei wurde unterschieden, ob der Betrieb vollständig in Eigenleistung erbracht wird bzw. ob der Betrieb an einen Intermediärs- bzw. Clearingstellenbetreiber beauftragt wird. Nicht berücksichtigt wurden Kosten, die für eine Firewall-Absicherung und andere zu treffende Sicherheitsvorkehrungen anfallen.

Die aufgezeigten Kosten können sich nur an vagen Abschätzungen orientieren: d.h.

- Die Kosten für den Intermediärsbetrieb ist am Produkt Governikus von bos aus Bremen festgemacht, weil derzeit kein anderes OSCI-Produkt zur Verfügung steht. Das Produkt ist heute ausschließlich in größeren Kommunen eingesetzt und kennt deshalb nur einen Preis für Kommunen bis 250.000 Einwohnern. Ob und inwiefern preislich andere Angebote für kleinere Kommunen offeriert werden, konnte nicht ermittelt werden. Es ist zu erwarten, dass mittelfristig weitere Produkte angeboten werden.
- Die Lizenzkosten für den Einsatz der OMH-Software sind grobe Einschätzungen. Hier gibt es weder artikulierte Vorstellungen der Software-Hersteller noch sind Analogien benutzbar.
- Die Telekommunikationskosten ergeben sich aus folgender Betrachtung:
  1. Eigenlösung

     Variante 1:

     Direkter Anschluss am TESTA Netz.

     Die verschiedentlich aufgeführte Variante mit Wählverbindung beinhaltet im wesentlichen einen TESTA-Client mit SmartCard. Bei dieser Variante ist ein bidirektionaler Verbindungsaufbau wie zwischen Sender und Empfänger erforderlich nicht möglich. Aus diesen Grund scheidet diese preiswertere Lösung aus. Die günstigste Festverbindungsvariante mit 64 Kbit/sec ohne IPSEC Verschlüsselung ist im

     CITY-Bereich 936,-- pro Monat

     Country-Bereich 1.166,-- pro Monat

     Variante 2:

     Anschluss an ein Länder-Behördennetz (am Beispiel Bayerisches Behördennetz BYBN) mit Nutzung des dort verfügbaren zentralen TESTA Anschluss. Wählleitungsanschluss 64 Kbit/s mit Rückruf (ist erforderlich für bidirektionalen Verbindungsaufbau) 140,-- pro Monat ohne ISDN-Basisanschluss und Verbindungskosten, Stand 1.4.2001.
  2. Anschluss an eine Clearingstelle

     Wählleitungsanschluss 64 Kbit/s mit Rückruf (ist erforderlich für bidirektionalen Verbindungsaufbau)

     52,-- pro Monat ohne ISDN-Basisanschluss und Verbindungskosten,Stand 1.12.2002

     (Dieser Preis von 52,-- kann nur als Anhaltspunkt genommen werden, da jede Clearingstelle hier eine eigene Kalkulation durchführen wird)

Entsprechend wurden die folgenden Zahlen für die jährlichen Betriebskosten ermittelt:

Tabelle 7: Betriebskosten

Kostenart	Eigenlösung	Anschluss an Clearingstelle/Intermediärsbetreiber
PKI-Kosten	100 Euro/Zert. = 600 Euro * einmalig	100 Euro/Zert. = 600 Euro* einmalig
Intermediärsnutzung	Bspw. 40 T Euro Volllizenz Governikus für Kommunen bis 250 T E.(**) Bei einer Laufzeit von 5 Jahren beträgt dies 8.000 ? /Jahr Je zus. 100 / E. 10 T Euro Lizenz Ab 850 T E. 0,1 Euro/E. Jeweils plus 18% Wartungskosten	Kosten sind analog zu Eigenlösung

Kostenart	Eigenlösung	Anschluss an Clearingstelle/Intermediärsbetreiber
Telekommunikationskosten	ca. 12.000 Euro für direkten TESTA-Anschluss 1.680 Euro zzgl Verbindungskosten für Anschluss an Landesbehördennetz	624 Euro - zzgl. Verbindungskosten
OMH-Betrieb	l 3.600 Euro (**) (600 Euro SW-Lizenz, 3000 Euro HW-Betrieb)	0,3 Euro/ Nachricht

Die mit (*) gekennzeichneten Kosten stellen Investitionen dar, die auch für weitere elektronische EWO-Dienste (Kommunikation zu anderen Behörden, anderen Kommunikationspartnern in der Wirtschaft) genutzt werden können.

Die mit (**) gekennzeichneten Kosten stellen Investitionen dar, mit denen eine Basis für eine generelle OSCI-Kommunikation geschaffen wird.

Trotz dessen sind beide Kosten in der Kalkulation voll angesetzt worden, obwohl diese eher Basisinvestitionen darstellen. Auch hier sind eigentlich nur die Teilkosten anzusetzen, die auf die Rückmeldung entfallen, während die Nutzung auch zu anderen Zwecken dann diesen zugerechnet werden müssen.

4.3.3 Nutzen durch die Einführung der elektronischen Rückmeldung

Mit der elektronischen Rückmeldung sind eine Reihe von Nutzenpotentialen verbunden.

Nicht quantifizierbare Nutzen

Mit einer elektronischen Aktualisierung der Melderegister entstehen Vorteile gegenüber der heutigen Verfahrensweise. Die Zeitverkürzung (max. 3 Tage) führt zu einer besseren Aktualität des Melderegisters und die Vermeidung von Medienbrüchen führt zur Vermeidung von Fehlern und damit zu einer höheren Integrität des Melderegisters. Als Folge davon entstehen bessere Auskunftsfähigkeit und Planungssicherheit für die Kommunen. Eine Bewertung dieser Vorteile ist nicht erfolgt.

Quantifizierbarer Nutzen

Mit der elektronischen Rückmeldung entstehen Nutzen im Bereich der Sachkosten und Personalkosten.

Sachkosten:

Entfall von

- Papier
- Druckaufbereitung
- Kuvert
- Porto

Hiervon wird das Porto den größten Teil ausmachen. Je nach Anfall von Sammelsendungen an jeweils eine Empfängerkommune dürfte das Porto in der Größenordnung von 0,5 liegen. Mit den Kosten für das Material und die Druckaufbereitung ergibt sich ein geschätzter Nutzen von 0,6 pro Rückmeldung.

Personalkosten:

Die Erstellung der Rückmeldung wird sich kostenneutral darstellen, da lediglich der Versand automatisiert wird.

Bei einer zukünftigen Ausweitung der elektronischen Abwicklung auf weitere Geschäftsvorfälle wie bspw. die Fortschreibung der Melderegister oder die Registerauskunft werden deutliche geringere Kosten bei einer Poststelle als weiteres Einsparpotential zu erwarten sein.

Da die Rückmeldung künftig automatisch in das Melderegister eingestellt wird, entfällt der für die Bearbeitung (Erfassung) notwendige Aufwand. Dieser Aufwand wird mit 3-5 Min. pro Rückmeldung eingeschätzt.

4.3.4 Einsparpotential

Auf Basis der quantifizierbaren Nutzenpotentiale ergibt sich das in folgender Tabelle dargestellte Einsparpotential durch die Nutzung der elektronischen Rückmeldung unter der Voraussetzung, dass OSCI–XMeld flächendeckend verfügbar ist und angewandt wird (in Praxis frühestens ab 2005).. Dabei liegen die folgenden Annahmen zu Grunde:

Nettoleistung eines Sachbearbeiters der Meldebehörde: 180 Tage/Jahr

Kosten eines Sachbearbeiters in Euro: 54 000 /Jahr = 300 /Tag

Bearbeitungszeit pro Rückmeldung: 3 Minuten

Das jährliche Volumen der Rückmeldungen pro 1000 Einwohnern ergibt sich aus verschiedenen Quellen, die sich aus Recherchen der Arbeitsgruppenmitgliedern in ihren Organisationen ergaben. Aufgrund der hohen Streuung wurden die Ergebnisse mit allen ermittelten Werten erarbeitet.

Tabelle 8: Einsparpotential

Einwohner	**Rückmeld./Jahr und 1000 E.**			**Sachkostenersparnis in Euro/Jahr**			**Personalkostenersparnis in Euro/Jahr**			**Gesamtersparnis in Euro/Jahr**		
	13	36	50									
5000	65	180	250	39	108	150	121	337	468	160	445	618
15000	195	540	750	117	324	450	365	1012	1406	482	1336	1856
250000	3250	9000	12500	1950	5400	7500	6093	16875	23437	8043	22275	30937
1000000	13000	36000	50000	7800	21600	30000	24375	67500	93750	32175	89100	123750

Eigene Berechnungen der AKDB in München und des LEA in Berlin bestätigen die Schätzungen im Wesentlichen.

Die möglichen Einsparpotentiale sind heute noch nicht realisierbar. Im Gegenteil wird für eine Übergangszeit eine gewisse Mehrbelastung eintreten, weil die Kommunen sich eineseits internetfähig machen und andererseits die herkömmlichen Techniken und Abläufe parallel vorhalten müssen.

4.3.5 Resümee

Durch die elektronische Rückmeldung werden Kosten induziert, die bei kleinen und mittleren Kommunen durch den erzielbaren Nutzen nicht erbracht werden. Insbesondere die notwendigen Basisinvestionen und hohen Telekommunikationskosten bei geringer Nutzung führen dazu, dass keine Vorteile entstehen.

Eigene Lösungen potenzieren das Problem noch, so dass für kleinere und mittlere Kommunen nur der Betrieb über eine Clearingstelle sinnvoll ist.

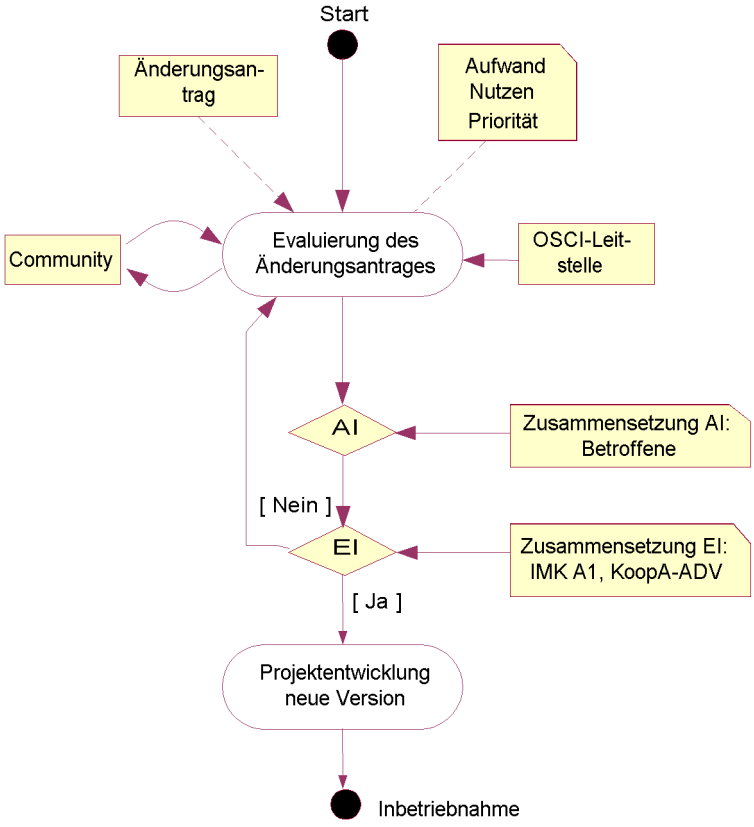
Für mittelgroße und große Kommunen entstehen erhebliche Einsparpotentiale.

5 Verfahren zur Weiterentwicklung der Standards

Die Standards für OSCI–Transport und XMeld sind in der Vergangenheit im Rahmen von Projekten definiert worden. Andere X-Standards (XKasse ?, XKfz ?, werden folgen müssen, um die weitergehenden Einführungen von E-Government zu ermöglichen.

Nach der erstmaligen Entwicklung werden Fortschreibungen aus Gründen rechtlicher, verwaltungstechnischer und technischer Änderungen notwendig werden. Hierfür ist ein Verfahren notwendig, mit dem ausgehend von Ideen und Ansprüchen eine koordinierte Weiterentwicklung erfolgt. Mit dem nachstehenden Bild sind die Grundzüge eines entsprechenden Changemanagement-Verfahrens (CM-Verfahren) aufgezeigt.

Bild 6 Change-Management-Verfahren



5.1 Verfahrensablauf

Interessierte Anwender stellen ihre Änderungswünsche in Form eines Antrags, der Angaben zum betroffenen Standard (OSCI–Transport, XMeld,..), den Änderungswunsch selbst aber auch Aussagen über die Relevanz des Wunsches (Betroffene, Nutzen, ...) enthalten sollte, an die OSCI-Leistelle, die als Administrator für alle Standards fungiert.

Administrator heißt in diesem Zusammenhang, dass von ihm alle koordinierenden Aufgaben zur Abwicklung des CM-Verfahrens übernommen werden. Hierzu gehören:

- Die Evaluierung des Änderungswunsches hinsichtlich
  - seiner Relevanz (Handelt es sich wirklich um eine Änderung, ist diese berechtigt,...)
  - des voraussichtlichen Aufwands
  - seiner zeitlichen Dringlichkeit
- Die Bereitstellung des abgeklärten Antrags zur Diskussion unter Interessierten im Rahmen einer Community
- Sammeln und sortieren der Anträge nach bestimmten Kriterien
  - Aufwand (klein - mittel - groß)
  - Dringlichkeit
  - Nutzen (klein - mittel - groß)
- Konfiguration der sortierten Änderungsanträge zu Weiterentwicklungsvorhaben nach folgendem Muster
  - Patch-Level
    zur Fehlerkorrektur
  - Release
    für funktionale Ergänzungen, Umweltanpassungen
  - Version
    für funktionale Erweiterungen
  - Produkt

für neue Standards

- Initiierung entsprechender Weiterentwicklungsvorhaben (Projekte) - und damit verbunden - die Etablierung bzw. Wiederbelebung der für die Weiterentwicklung der Standards vorgesehenen Gremien (Arbeitsgruppe, Abstimminstanz, Entscheidungsinstanz)
- Leitung der Projekte zur Weiterentwicklung
- Integration der Weiterentwicklungen in die bestehenden Standards
- Einführung der weiterentwickelten Standards bei den Anwendern

5.2 Gremien

Für jeden Standard wird (außer der Arbeitsgruppe) die Besetzung der Gremien (Abstimminstanz und Entscheidungsinstanz) schematisch (welche Institution ist vertreten) und werden die beteiligten Personen festgelegt.

Die Arbeitsgruppe wird je nach vorliegender Aufgabe und dem sich daraus ergebenden Qualifikationsbedarf jeweils pro Entwicklungsvorhaben bestimmt.

5.2.1 Entscheidungsinstanz

In der Entscheidungsinstanz sind die Auftraggeber vertreten, die Verantwortung tragen für die inhaltliche Ausprägung des Standards und der oder die Geldgeber (falls nicht identisch). Sie entscheidet über die Beauftragung des Weiterentwicklungsvorhabens auf Basis von (Projekt-) Aufträgen (definiert von der OSCI-Leistelle), steuert das Vorhaben durch Abnahme von Phasenergebnissen und nimmt das Endergebnis ab.

Für die bestehenden Standards könnte die schematische Besetzung sein:

- OSCI–Transport-KoopA
- XMeld-IMK- AK1

5.2.2 Abstimminstanz

In der Abstimminstanz sollten die durch den Standard Betroffenen repräsentativ vertreten sein. Hier ergibt sich für jeden Standard eine spezifische Besetzung.

Am Beispiel XMeld könnte die Besetzung aus Vertretern der Meldebehörden aus unterschiedlichen Ländern und Kommunengrößen, den Datenschutzvertretern, dem BSI, Software-Herstellern, etc. bestehen.