OSCI-Transport, Version 2

– Funktionale Anforderungen und Entwurfsziele –

OSCI Leitstelle

Status: Final

Edition 1, veröffentlicht am 4. Juni 2009

Disclaimer

Dieses Dokument fasst die Anforderungen und Entwurfsziele an die Version 2 des Transportprotokolls **O**nline **S**ervices **C**omputer **I**nterface (OSCI) zusammen. Ziel ist, die Spezifikation bis Anfang 2009 fertig zu stellen.

Der vorliegende Dokumentestand ist eine abgestimmte Version, die von interessierten Vertretern aus Bund, Ländern, Kommunen, Wirtschaft und Wissenschaft unter Federführung der Bremer „OSCI-Leitstelle“ im Auftrag des KoopA-ADV erarbeitet wurde.

Gegenüber der im März 2008 verabschiedeten Version wurden lediglich kleine Aktualisierungen – wie z.B. Referenzen – vorgenommen.

Sollten sich für OSCI Transport 2 in Zukunft weitere Anforderungen ergeben, so wird dies in weiteren Editionen dieses Dokuments publiziert werden.

Editor dieses Dokuments:

Jörg Apitzsch, bos bremen online services GmbH & Co. Kg, ja@bos-bremen.de

Qulitätsicherung:

Thilo Schuster, cit GmbH, thilo.schuster@cit.de

Weiter Beteiligte an der Erarbeitung der Spezifikation sind im Kapitel [6.4] aufgeführt.

Kommentierungen und Anregungen nehmen die OSCI Leitstelle sowie der Editor dieses Dokuments dankend entgegen.

Fortschreibungen (nach Edition 1)

Edition	Datum	Autor	Vorgenomme Änderungen

Inhaltsverzeichnis

1 Zweck und Aufbau des Dokuments

1.1 Einordnung von OSCI Transport 2

Online **S**ervice **C**omputer **I**nterface (OSCI) ist ein Nachrichten-Standard für das E-Government, der seit 2002 in der Version 1.2 in Deutschland von der öffentlichen Verwaltung, Teilen der Wirtschaft sowie ihren Kunden zunehmend für vertrauliche und rechtsverbindliche Kommunikation über das Internet genutzt wird[1]. Auch im europäischen Ausland wird OSCI inzwischen in einigen Projekten genutzt.

OSCI wurde mit dem Ziel entworfen, die vollständige und rechtsverbindliche Abwicklung von Transaktionen im Bereich des E-Government über den Betriebsweg Internet und auf Basis der digitalen Signatur zu ermöglichen. Es werden aber auch Szenarien für Nachrichten- und Dokumentenaustausch unterstützt, die nicht unbedingt hohen Anforderungen in Hinsicht auf Rechtsverbindlichkeit unterliegen, dennoch aber einen gewissen Bedarf an Vertraulichkeit, Nachweisbarkeit und Integritätssicherung der Kommunikation haben. Dies erfordert eine umfangreiche Interoperabilität sowohl auf der Ebene der Inhaltsdaten, als auch auf der Ebene der Transport- und Sicherheitsfunktionen. Zusätzlich sind die Regularien und Reglementierungen zu berücksichtigen, denen der Bereich des öffentlichen Handels unterworfen ist. Die hieraus erwachsenden Anforderungen haben die Entwurfsziele von OSCI bestimmt.

In diesem Dokument werden die Anforderungen an eine Fortschreibung des OSCI Transport Protokolls und die umsetzende Infrastruktur beschrieben, die

- auf Basis der Erfahrungen mit der Version 1.2 und gewonnen werden konnten
- inzwischen als neue Anforderungen zusätzlich sichtbar geworden sind
- in Teilen zu einer Modifikation der ursprünglichen Bewertung von Anforderungen führen.

Dabei wird hier Gewicht darauf gelegt, mögliche Realisierungen soweit möglich noch nicht in Betracht zu ziehen.

Die Umsetzung der Anforderungen wird in weiteren Dokumenten

(1) „OSCI Transport 2 – generelle Architektur“

und

(2) „OSCI Transport 2.0 – Specification“

dargelegt.

Aus den auf OSCI Transport 1.2 basierenden Einsatzszenarien heraus wurde eine Reihe von Unzulänglichkeiten des Protokolls ersichtlich, die eine grundsätzliche Überarbeitung des ursprünglichen Ansatzes nötig machen, um sowohl die Basis für eine breitere Nutzung dieses Konzepts zu legen, als auch Voraussetzungen für die Effektivierung von existierenden Einsatzszenarien und ihren jeweiligen Implementierungen zu schaffen.

Wesentliche Entwurfsmuster von OSCI Transport 1.2 referenzieren und profilieren Standards für die Web-basierte Kommunikation, die in 2002 als stabil und allgemein anerkannt anzusehen waren; eine Reihe spezifischer Anforderungen fanden allerdings noch keine Entsprechung in international akzeptierten Spezifikationen, OSCI konzipierte hier eigene Lösungen. Dies hat sich inzwischen dramatisch geändert; sehr viele dieser Spezifikationen haben den Status „anerkannter Industriestandard“ und sind z.T. umgesetzt in breit genutzter Infrastruktur für die Kommunikation über das Internet. Im Fokus der

[1] Siehe [OSCI]

Fortschreibung von OSCI Transport steht daher auch eine möglichst breite Nutzung des aktuellen Stands der relevanten internationalen Standards für die Umsetzung der hier dargestellten funktionalen Anforderungen. Damit soll eine verbesserte Interoperabilitätsbasis mit Lösungen der Wirtschaft wie auch ähnlichen Standardisierungsaktivitäten in anderen EU-Ländern geschaffen werden.

Diese grundsätzliche Überarbeitung wird in einem breit getragenen, gemeinsamen Diskussions- und Kooperationsprozess von interessierten Vertretern aus Bund, Ländern, Kommunen, Wirtschaft und Wissenschaft unter Federführung der Bremer „OSCI-Leitstelle“ im Auftrag des KoopA-ADV durchgeführt. In die Koordination mit entsprechenden Aktivitäten in anderen EU-Ländern ist das Generaldirektorat für Informatik der EU-Kommission im Rahmen des Programms „**I**nteroperable **D**elivery of European eGovernment Services to public **A**dministrations, **B**usinesses and **C**itizens" (IDABC)[2] eingebunden.

1.2 Aufbau des Dokuments

Das vorliegende Dokument als Teil der Spezifikation „OSCI Transport, Version 2“ beschreibt die funktionalen Anforderungen und aus diesen abgeleiteten generellen Entwurfsziele, die aus Sicht des E-Government an OSCI gestellt werden.

Kapitel 2 grenzt den generellen Einsatzzweck und daraus abgeleitete allgemeine Anforderungen an Mechanismen ein, die beim Nachrichtenaustausch über OSCI Transport unterstützt werden müssen.

Kapitel 3 stellt zunächst ausgewählte typische Anwendungsfälle dar, um die unterschiedlichen Einsatzszenarien und Anforderungen zu verdeutlichen.

Kapitel 4 erläutert die möglichen Kommunikationsszenarien mit ihren jeweiligen Anforderungen. Hieraus ergeben sich eine Reihe von Rollen und Diensten, die durch eine OSCI Transport Infrastruktur abzudecken sind, als auch solche, die selbst nicht im Fokus von OSCI Transport stehen, aber für OSCI Transport zur Verfügung stehen müssen.

Im letzten Kapitel werden – im Wesentlichen übernommen aus Version 1.2 der OSCI Transport Spezifikation - Sicherheitsrisiken sowohl externer als auch interner Art in Form von Szenarien dargestellt. Hieraus werden Sicherheitsziele abgeleitet, die bei der Konzeption des OSCI-Standards zu berücksichtigen sind.

Für die Unterscheidung von zwingend erforderlichen und optionalen Funktionalitäten sind Anforderungen in folgender Notation ausgezeichnet und durchnumeriert, es wird auf eine für Spezifikationen gebräuchliche Notation nach RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels" verzichtet:

MUSS nn: diese Anforderung muss von einer OSCI Transport Infrastruktur erfüllt werden.

OPT nn: es handelt sich um eine optionale Funktionalität.

Alle hier aufgeführten Funktionalitäten müssen in der Spezifikation abgebildet sein; die Umsetzung von optionalen Funktionalitäten liegt im Ermessenspielraum von Realisierern bzw. Betreibern von Komponenten für die OSCI Transport Infrastruktur.

1.3 Begriffsdefinitionen, Nomenklatur

Mit Hinsicht auf die intendierte Internationalisierung von OSCI Transport werden in diesem Dokument teilweise international übliche englischsprachige Begriffe verwandt. Damit soll erleichtert werden, den Bezug zu anerkannten Industriestandards mit ähnlichem Anwendungsfokus herzustellen. Genutzte Begriffe und Abkürzungen aller Dokumente zu dieser Spezifikation sind erläutert in einem gesonderten Dokument „OSCI Transport 2 – Glossar“.

[2] http://ec.europa.eu/idabc/en/chapter/3

2 Einsatzzweck und generelle Anforderungen

OSCI-Transport beschreibt das Datenaustauschformat und Mechanismen für die sichere Übertragung von Nachrichten über das Internet oder andere vergleichbare, offene und potentiell unsichere Kommunikationsmedien. Im Fokus von OSCI steht vor allem auch die Unterstützung rechtsverbindlicher elektronischer Kommunikation.

MUSS 1:

OSCI muss sowohl den Austausch strukturierter als auch unstrukturierter bzw. binärer Daten im Rahmen synchroner und asynchroner Kommunikationsszenarien unterstützen. Es muss sowohl eine „one-way"-Übertragung von Nachrichten als auch eine einfache Anfrage/Antwort-Kommunikation bis hin zum multiplen, wechselseitigen Nachrichtenaustausch realisierbar sein.

MUSS 2:

OSCI Transport ist dabei anwendungsunabhängig; Aufbau und Strukturierung der Inhaltsdaten sind für den Transport transparent („opaque Body" der Nachricht). Inhaltsdaten müssen unverändert vom jeweiligen Sender zum Empfänger transportiert werden.

MUSS 3:

Von einer OSCI-Infrastruktur müssen Mechanismen zum Transport beliebig großer Nachrichten vorgehalten werden (bei Bedarf Partitionierbarkeit, Sequenzierung).

OPT 1:

Implementierung bzw. Betreiber von OSCI-Infrastrukturen können Volumen und Frequenzen von Nachrichten beschränken. Solche Begrenzungen müssen öffentlich in einer strukturierten Form abrufbar sein.

MUSS 4:

Eine vollständige und klare Fehlerprotokollierung sowie der Austausch von Fehler- und Statusmeldungen zwischen den Kommunikationsknoten muss Bestandteil der Spezifikation sein. Sie müssen von Implementierungen einheitlich umgesetzt werden.

MUSS 5:

Nachrichten werden zwischen zwei Endpunkten (initialer Sender und ultimativer Empfänger) transportiert. Dabei können die Nachrichten Zwischenstationen („Intermediäre") durchlaufen, die für bestimmte Kommunikationsszenarien benötigte Mehrwertdienste erbringen (dargestellt in Kapitel [4]).

Es werden von OSCI Transport folgende Mechanismen gefordert, wobei die Nutzung der einzelnen Mechanismen gem. Anforderungen konkreter Kommunikationsszenarien skalierbar ist:

MUSS 6: Mechanismen für Adressierung von Kommunikationspartnern und Routing:

> OSCI Transport muss Mechanismen zur Adressierung der Empfänger, der benötigten Intermediäre für die Mehrwertdienste als auch der Sender für die Rückadressierung (Antworten, Statusmeldungen und Fehlerquittungen) bereitstellen.

MUSS 7:

> Es muss ein für alle Knoten einheitliches Interface zur Lokalisierung dieser Adressierungsdaten vorgehalten werden.
>
> **Hinweis:** *Nicht* Bestandteil von OSCI Transport ist die Spezifikation der Verzeichnisdienste für die Bereitstellung der Adressierungsdaten!

OSCI Transport macht keine Festlegungen bzgl. Format, Größe und Inhalt der transportierten Inhaltsdaten; diese per OSCI übermittelten Daten und Dokumente können jedoch signaturgesetzkonform elektronisch unterschrieben werden. Hieraus leitet sich folgende Anforderung ab:

MUSS 8: Erstellen und Prüfen von Signaturen auf Inhaltsdatenebene; Signaturgesetzkonformität:

> OSCI Transport bzw. entspr. Implementierungen müssen die Erstellung und Prüfung fortgeschrittene und qualifizierte elektronische Signaturen gemäß Signaturgesetz auf Inhaltsdatenebene unterstützen.
>
> Für Erstellung, Format und Prüfung qualifizierter Signaturen gelten hierbei die Vorgaben der Spezifikationen [COMPKI] und [AlgCat] in der jeweils aktuellen Version.

OSCI ist für beliebige Geschäftsprozesse einsetzbar und ermöglicht signaturgesetzkonforme elektronische Unterschriften und die sichere Übertragung elektronischer Dokumente zwischen öffentlicher Verwaltung bzw. Unternehmen und ihren Kunden, woraus sich folgende weitere Anforderungen und Entwurfsziele ableiten:

MUSS 9: Interoperabilität und Plattformunabhängigkeit:

> OSCI-Nachrichten werden in XML-Notation spezifiziert, wodurch Interoperabilität zwischen Implementierungen in unterschiedlichen Technologien sowie Ablauffähigkeit auf unterschiedlichen Trägersystemen gesichert werden kann.

MUSS 10: Skalierbarkeit bzgl. unterschiedlicher Sicherheitsanforderungen:

> OSCI Transport ermöglicht die Anwendung unterschiedlicher Kommunikationsszenarien und in diesen benötigter Sicherheitsniveaus. Entsprechend skalierbar müssen die Anforderungen an Vertraulichkeit, Signaturniveau und Einbindung der optionalen Dienste (vgl. Kapitel [4, 5.2) sein.

Diese allgemeinen Anforderungen werden ergänzt durch eine Reihe von Sicherheitsanforderungen, die in Kapitel [5.2] zusammengefasst erläutert sind.

Entscheidenden Einfluss auf das Sicherheitskonzept von OSCI hat dabei die durchgängig umgesetzte Plattformunabhängigkeit. Hiermit verbunden ist das Ziel, Sicherheit möglichst weitgehend auf OSCI-Transport-Ebene umzusetzen, weitestgehend unabhängig vom Sicherheitsstandard anderer Kompo-

nenten, beispielsweise des Trägernetzes sowie der lokal beim Bürger eingesetzten Ablaufumgebungen.

Plattformunabhängigkeit bedeutet jedoch nicht, dass keinerlei Anforderungen an die Systeme der OSCI-Infrastruktur, insbesondere an den Betrieb der OSCI-Services (vgl. Kapitel [4.9]) gestellt werden. Ein ordnungsgemäßer Betrieb der jeweiligen Systeme ist vielmehr Grundvoraussetzung für OSCI und ist daher in einem gesonderten Betriebskonzept dargestellt.

Diese allgemeinen Anforderungen legen - entsprechend dem aktuellen Stand der Technik - eine Modellierung der mit OSCI adressierten Kommunikationsszenarien als Ausprägung von Web Services nahe. Entsprechende internationale Standardisierungsbemühungen, namentlich denen von w3c[3] und OASIS[4], sind daher in der OSCI-Spezifikation ganz wesentlich zu berücksichtigen.

[3] World Wide Web Consortium; www.w3c.org

[4] Organization for the Advancement of Structured Information Standards, www.oasis-open.org

3 Ausgewählte Anwendungsszenarien

OSCI berücksichtigt sowohl die Kommunikation der öffentlichen Verwaltung mit ihren Kunden (Bürgern und Unternehmen) durch das Anbieten und die Abwicklung von Verwaltungsdienstleistungen über das Internet, als auch die interne Kommunikation zwischen unterschiedlichen Verwaltungen bzw. Verwaltungsbereichen.

Im Folgenden ausgewählte Szenarien mit jeweils unterschiedlichen Anforderungen dargestellt, die auf Basis von OSCI Transport 1.2 im produktiven Einsatz bzw. in Planung sind. Diese Darstellung konkreter Einsatzszenarien mit ihren jeweiligen Charakteristika vor allem bzgl.

- asynchroner und synchroner, formgebundener und unstrukturierter Kommunikation
- Sicherheitsanforderungen bzgl. Signaturniveau und Verschlüsselung
- Nachweis- und Quittungsmechanismen
- Anbindung von Verzeichnisdiensten zu Zwecken der Gewinnung von Adressierungsdaten und anderen Attributen der Kommunikationspartner sowie der Authentisierung
- implizierten Vertrauensstellungen von Sendern und Empfängern zu Intermediärsdiensten

soll der Verdeutlichung der Anforderungen dienen, die in den Folgekapiteln erläutert sind.

Die grafische Darstellung der Anwendungsfälle lehnt sich an eine UML-Notation an; es wurde eine Mischform verschiedener UML-Diagramme gewählt, um jeweils in einer Grafik den Anwendungsfall, beteiligte Komponenten und Nachrichtenflüsse darstellen zu können. Eine UML-konforme Ausdifferenzierung ist für das Architekturdokument vorgesehen.

3.1 Elektronische Datenübermittlung im Meldewesen

Für den elektronische Datenaustausch im Meldewesen wurde von der OSCI-Leitstelle auf Inhaltsdatenebene der Standard OSCI-XMeld entwickelt, für den Datentransport kommt flächendeckend OSCI Transport in der Version 1.2 zum Einsatz.

Für die unterschiedlichen Anwendungsszenarien definiert OSCI-XMeld detaillierte Austauschformate in Form von XML-Schemadateien; die jeweiligen Use-Cases sind in der Spezifikation OSCI-XMeld 1.3.2 detailliert dokumentiert. Es wird hier auf eine Darstellung dieser einzelnen Use-Cases verzichtet, sondern die allgemeinen Anforderungen an OSCI-Transport dargestellt, wie sie in der OSCI-XMeld-Spezifikation festgehalten sind (siehe [XMeld], „OSCI-Transport-Profil für OSCI-XMeld“, S. 849 ff.).

Dieses Szenario zeichnet sich aus durch die Einbindung eines speziell geschaffenes „Deutsches Verwaltungsdiensteverzeichis“ (DVDV), in dem Behörden Informationen zu angebotenen Diensteimplementierungen publizieren können; im Kontext des Meldewesens ist dies verbindlich. Es handelt sich somit um einen geschlossenen OSCI-Kommunikationsverbund aller Meldebehörden in Deutschland; alle Endpunkte und Knoten müssen im DVDV registriert werden (für diesen Zweck existiert eine spezielle Anwendung „Pflegeclient“; die Kommunikation zwischen diesem und DVDV ist ebenfalls über OSCI abgesichert).

In Form von WSDL-Beschreibungen der Dienste sind u.a. folgenden Attribute abrufbar:

- Technische Adressierungsdaten (URL) der Endpunkte
- Angebotener Kommunikationstyp (Punkt-zu-Punkt oder asynchron über Zwischenspeicherung der Nachrichten)
- Verschlüsselungs- und Signaturzertifikate der Knoten und Endpunkte
- Erfordernis und Niveau der Signatur auf Kommunikations- bzw. Inhaltsdatenebene

- Verschlüsselungserfordernis auf Kommunikations- bzw. Inhaltsdatenebene
- Schema der Inhaltsdaten, Struktur der Inhaltsdatencontainer („Paketierung“)

Da nicht alle Meldebehörden einen 24h / 365 Tage Betrieb anbieten können, ist der asynchronen Kommunikationstyp mit Zwischenspeicherung der Nachrichten verbindlich vorgeschrieben (d.h. Eingangsnachrichten müssen vom Adressaten aktiv gepollt werden).

Da es sich in der Mehrzahl der Kommunikationsvorgänge um einen Nachrichtenaustausch zwischen DV-Systemen von Einwohnermeldeämtern (EWO) handelt, könnte dieser in Zukunft auch über direkte Punkt-zu-Punkt Kommunikation und – wenn es der Geschäftsvorfall zulässt – dann auch synchron realisiert werden.

Weiter ist u.a. festgelegt:

- Inhaltsdaten müssen fortgeschritten signiert werden (dies dient der Authentisierung der jeweiligen Meldebehörde)
- Inhaltsdaten müssen für die adressierte Behörde verschlüsselt werden
- Es kommen für Signatur und Verschlüsselung ausschließlich von der CA PKI-1-Verwaltung herausgegebene Zertifikate zum Einsatz
- Kommunikationsdaten **können** signiert werden, **müssen** für den jeweils nächsten Knoten verschlüsselt werden
- Eine Struktur für die Paketierung der Inhaltsdaten zur Sicherung der Interoperabilität.

Für die bis heute produktiv umgesetzten elektronischen Kommunikationsszenarien existiert ein geringer Bedarf an der Nachweisbarkeit der Kommunikation; die implizit mit OSCI Transport 1.2 bereitgestellten Zustellnachweise werden hier nicht benötigt – vor allem auf ein längerfristig Vorhalten solcher Nachweise nicht. Reaktionszeiten zur Annahme einer Anfrage – genauer Rückübermittlung einer Antwort - sind durch entsprechende Vorschriften des Meldewesens geregelt.

Folgende Abbildung zeigt das Gesamtszenario:

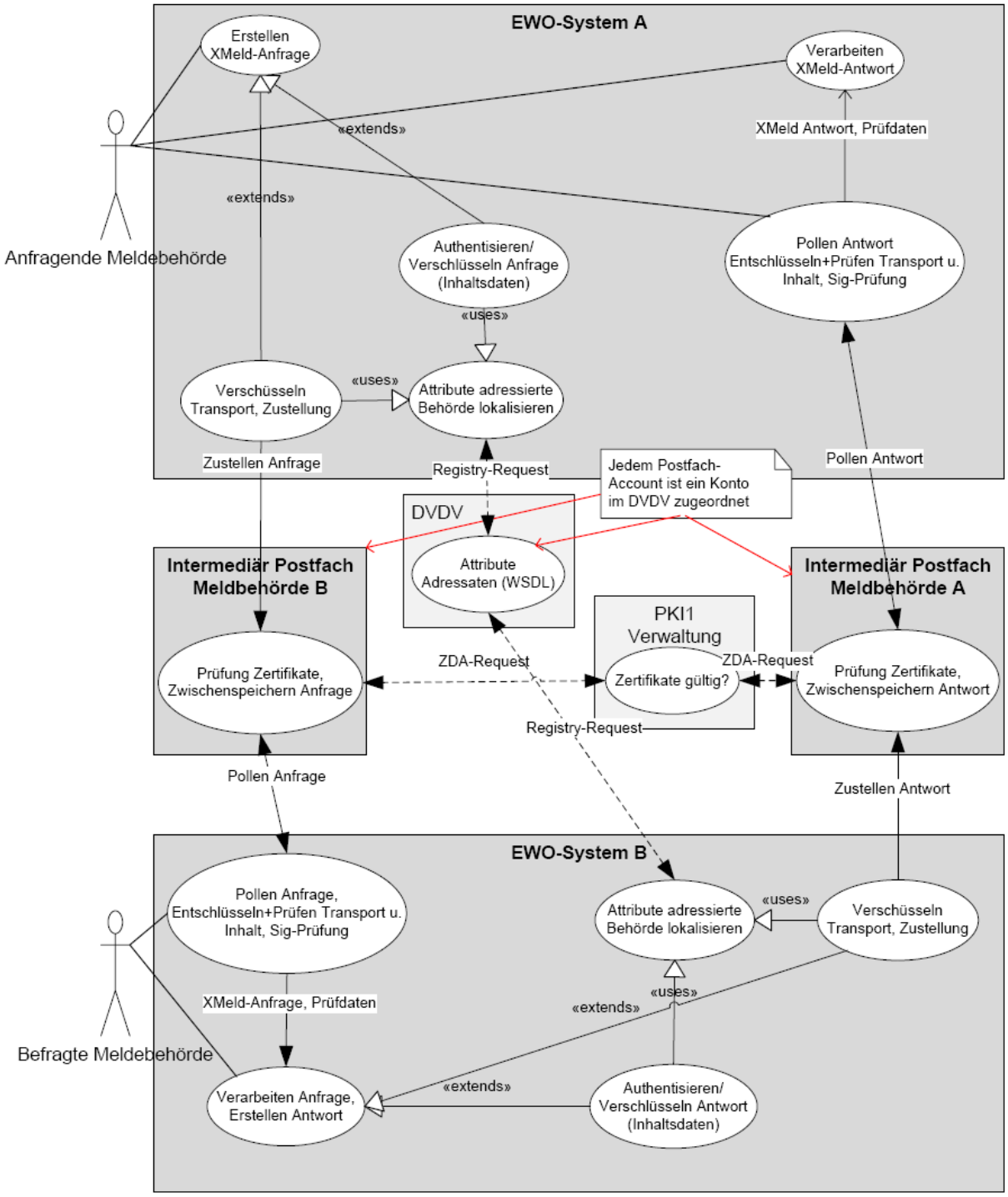

Abbildung 1: Übersicht elektronische Datenübermittlung im Meldewesen

In folgender tabellarischer Darstellung des Anwendungsfalls ist die anfragende Meldebehörde A mit „MA“ bezeichnet, die adressierte (und ggf. antwortende) Meldbehörde B mit „MB“. „Ausführend“ ist initial i.d.R. ein Mitarbeiter der Meldebehörde, getriggert durch spezifische Geschäftsvorfälle wie z.B. den Meldevorgang eines Bürgers. Dabei bedient sich der Mitarbeiter eines EWO-Systems mit direkt angebundenen oder separat aufrufbaren Anwendungen für die OSCI-Kommunikation; entsprechend kann der Automatisierungsgrad der einzelnen Aktivitätsschritte stark differieren.

Aktivität	Ausführung	Handlung	Ergebnis	Anmerkung
XMeld-Anfrage erstellen	Mit-arbeiter/EWO -System MA		Inhaltsdaten Anfrage in valider XMeld-Struktur	
Anfrage elektronisch signieren	OSCI-Client MA	Die Anfrage muss mit einer fortgeschrittene elektronisch Signatur versehen werden	Digital signierte XMeld-Nachricht	
Attribute zu adressierter Meldebehörde einholen	OSCI-Client MA/ DVDV	Request an DVDV	WSDL MB	Damit liegen alle o.g. benötigten Attribute für MB vor
Zuordnung einer eindeutigen Message-Id	OSCI-Client MA/ Intermediär MB	Message-Id wird in OSCI 1.2 von einem Server-Dienst (Intermediär) vergeben	Um Message-Id ergänzte Nachricht	Jede Nachricht erhält eine eindeutige Id
Anfrage verschlüsseln	OSCI-Client MA	Die Anfrage muss für MB verschlüsselt werden	Verschlüsselte u. digital signierte XMeld-Nachricht	
Nachricht an adressierte MB übermitteln	OSCI-Client MA	Aufbau der Adressierungsdaten; optional Sicherung der Gesamtnachricht durch Transportsignatur. Verschlüsselung Gesamtnachricht für nächsten Transportknoten (Intermediär Postfach MB)	Verschlüsselte OSCI-Nachricht wird übermittelt und im Postfach MB abgelegt	
Prüfen Unversehrtheit des Transportpakets	Intermediär MB	Entschlüsseln und ggf. Signaturprüfung der Kommunikationsdaten	Ggf. Fehlermeldung an Sender, Abbruch der Kommunikation	
Protokollierung des Eingangszeitpunkts	Intermediär MB	Zur Nachricht wird der Eingangszeitpunkt (Serverzeit) festgehalten.	Um Eingangszeitpunkt ergänzte Nachricht	
Prüfen aller Signatur- und Verschlüsselungszertifikate	Intermediär MB	Initiierung und Protokollierung der Online-Gültigkeitsprüfung aller Zertifikate.	Nachricht ist um die Prüfergebnisse ergänzt	Ausschließliche CA: PKI-1 Verwaltung

Aktivität	Ausführung	Handlung	Ergebnis	Anmerkung
Abholen und Annahme der Nachricht vom Intermediäre MB	OSCI-Client MB, Intermediär MB	Authentisierung MB beim Intermediär dieser MB, bei Erfolg Verschlüsselung der OSCI-Nachricht für MB und Übermittlung, bei Erfolg wird der Abholzeitpunkt (Serverzeit) festgehalten. Technische Annahme der Nachricht, Prüfung der Kommunikationsdaten; Entschlüsselung und Signaturprüfung der Inhaltsdaten	Nachricht liegt beim Empfänger MB entschlüsselt und geprüft bzgl. Kommunikationsdaten und Signatur Inhaltsdaten vor.	
Nachricht wird inkl. Prüfinformationen an EWO-System MB übergeben	OSCI-Client MB, EWO-System MB	Bereitstellung zur weiteren Bearbeitung		
Qualitätsprüfung Inhaltsdatenpaket	Eingangspunkt EWO-System MB	Prüfung auf Vollständigkeit und syntaktische Korrektheit der XMeld-Nachricht	Inhaltsdaten konnten auf Korrektheit geprüft werden.	Im Fehlerfall Rückmeldung an *MA* (Nachricht vom Typ „Return to Sender“)
Weitere Abarbeitung im Fachverfahren	Mitarbeiter/EWO-System MB	Fachspezifischer Vorgang - hier nicht näher betrachtet.		

Tabelle 1: Tabellarischer Use-Case „Anfrage Meldebehörde an Meldebehörde“

Die Erstellung der Antwort erfolgt - spiegelbildlich zur Erstellung und Übermittlung der Anfrage - von Meldebehörde B zu Meldbehörde A, auf eine detaillierte Darstellung wird daher verzichtet.

3.2 Emissionsberichterstattung an die Deutschen Emissionshandelsstelle (DEHSt)

Die beim Umweltbundesamt angesiedelte Deutsche Emissionshandelstelle (DEHSt) ist die in Deutschland zuständige Stelle für den Handel mit Emissionsberechtigungen. Betreiber von Anlagen, die das Klima schädigende CO_2 ausstoßen, müssen seit 2005 ihren aktuellen Ausstoß melden, diesen durch Sachverständige begutachten lassen und auf dieser Grundlage Anträge auf die Zuteilung von Emissionsberechtigungen stellen.

Basis des späteren Emissionshandels ist die Eröffnung eines entsprechenden Kontos in einem Registrierungsserver für alle Verfahrensbeteiligten in diesem Kommunikationsverbund- es handelt sich also um eine geschlossene Benutzergruppe bestehend aus

- der DEHSt
- in das Verfahren eingebundenen zuständigen Landesbehörden
- den Anlagenbetreibern

- sowie anerkannten Sachverständigen zur Begutachtung der Berichte der Anlagenbetreiber.

Zur Kontoeröffnung übermitteln Anlagenbetreiber einen Kontoeröffnungsantrag mittels einer speziellen Anwendung an die DEHSt und erhalten einen Bescheid über die erfolgreiche Kontoeröffnung. Diese ist verbunden mit einem individuellen Verschlüsselungszertifikat für alle Kommunikationsteilnehmer, welches als Basis der Adressierung und generell gehandhabter Ende-zu-Ende Verschlüsselung aller Kommunikationsvorgänge.

3.2.1 Verfahrensübersicht

Kennzeichnend für das Verfahren sind:

- Genereller asynchroner Nachrichtenaustausch unter Nutzung von Postfächern mit Ende-zu-Ende (Sender zu Empfänger) Verschlüsselung.
- Es existiert eine zentraler Postfachdienst („DEHSt-Intermediär“) für alle Teilnehmer des Kommunikationsverbundes.
- Der Einsatz der qualifizierten Signatur ist mandatorisch für die Akteure Anlagenbetreiber und Sachverständige; derzeit werden XML-Signaturen auf Inhaltsdatencontainer appliziert (keine PKCS#7-Signaturen auf Attachments).
- Signaturprüfung inkl. Online-Zertifikatsprüfung muss von den Endpunkten aus möglich sein.
- Im Ablauf des Gesamtverfahrens entstehen komplexe, verschachtelte Inhaltsdatencontainer, da ggf. signierte Inhaltsdaten vorangegangener Kommunikationsvorgänge in neue Nachrichten aufgenommen werden[5]. Bei der Visualisierung der Prüfergebnisse von Signaturen müssen diese den Nutzern entsprechend hierarchisch präsentiert werden.
- Es sind für die unterschiedlichen Geschäftsvorfälle, Kommunikationsvorgänge und jeweilige Rolle der Akteure 22 unterschiedliche Nachrichtentypen definiert, die auf Ebene der Kommunikationsdaten sichtbar sind. Sie dienen der Steuerung des Ablaufs in den eingesetzten Sende-/Empfangsclients und als Selektionsmöglichkeit in einem Postfach[6].
- Es existiert aufgrund der Fristbindung für die Berichterstattung für Anlagenbetreiber ein hoher Bedarf an Zustellungsnachweisen.

Für die Einreichung wird der Emissionsbericht vom Anlagenbetreiber mittels Fachverfahrenssoftware erstellt und einem Sachverständigen zur Bestätigung/Verifizierung vorgelegt. Der Sachverständige signiert den Emissionsbericht qualifiziert und übersendet ihn zurück an den Anlagenbetreiber.

Der Anlagenbetreiber kann die enthaltenen Informationen überprüfen und gegebenenfalls - unter erneuter Abstimmung und qualifizierter Signierung mit dem Sachverständigen - ändern.

Sind alle Inhalte abgestimmt und liegen vom Sachverständigen signiert vor, signiert der Anlagenbetreiber seinerseits den Emissionsbericht. Anschließend wird der Bericht verschlüsselt an die zuständige Landesbehörde übersendet.

Die Landesbehörde prüft stichprobenartig den Bericht und übersendet ihn ihrerseits verschlüsselt und signiert oder unsigniert (Schriftformerfordernis ist zwischen Behörden in diesem Verfahren nicht vorgeschrieben) an die DEHSt.

[5] Eine spezieller Aufbau der Inhaltsdaten soll von OSCI Transport nur bedingt generisch unterstützt werden., dies ist Sache spezieller Anwendungen wie im diesem Falle des so genannten „DEHSt-Clients“.

[6] Für OSCI 2.0 ist geplant, Nachrichtentypen über Ausdifferenzierung von Postfächern abzubilden

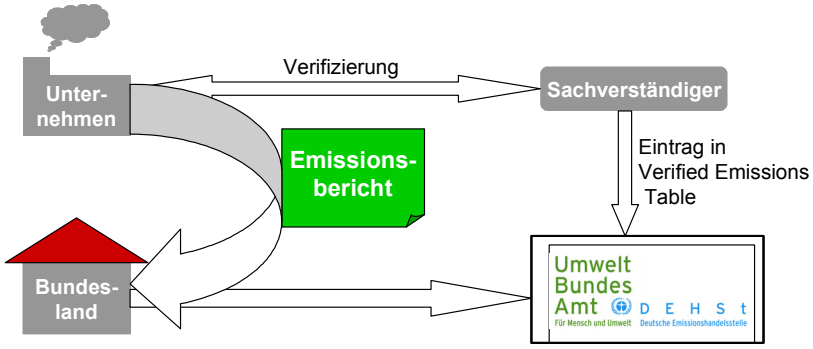

Abbildung 2: Emissionsberichterstattung: Übersicht Beteiligte und Kommunikationsfluss

3.2.2 Ablauf der Kommunikationsvorgänge

Beispielhaft ist hier nur die Erstellung und Übermittlung des Emissionsberichts vom Anlagenbetreiber an den Sachverständigen detailliert dargestellt. In den Folgeschritten des Verfahrens sind die Rollen von Sender und Empfänger der Nachrichten jeweils auszuwechseln; die Fachlichkeit – Erstellung und Bearbeitung der Inhaltsdaten - wechselt entsprechend der jeweiligen Rolle, in der die diese bearbeitet bzw. um weitere Informationen ergänzt werden. Auch die Anforderung an eine qualifizierte Signatur der Inhaltsdaten kann je nach Rolle wechseln – diese ist bei Übermittlung von Landesbehörde an DEHSt nicht vorgeschrieben.

Da alle Akteure als Sender und Empfänger von Nachrichten auftreten können, verfügen alle Akteure über eine einheitliche Anwendung, die die in folgender Abbildung dargestellten Funktionalitäten von Sende- und Empfangsclient vereinigt.

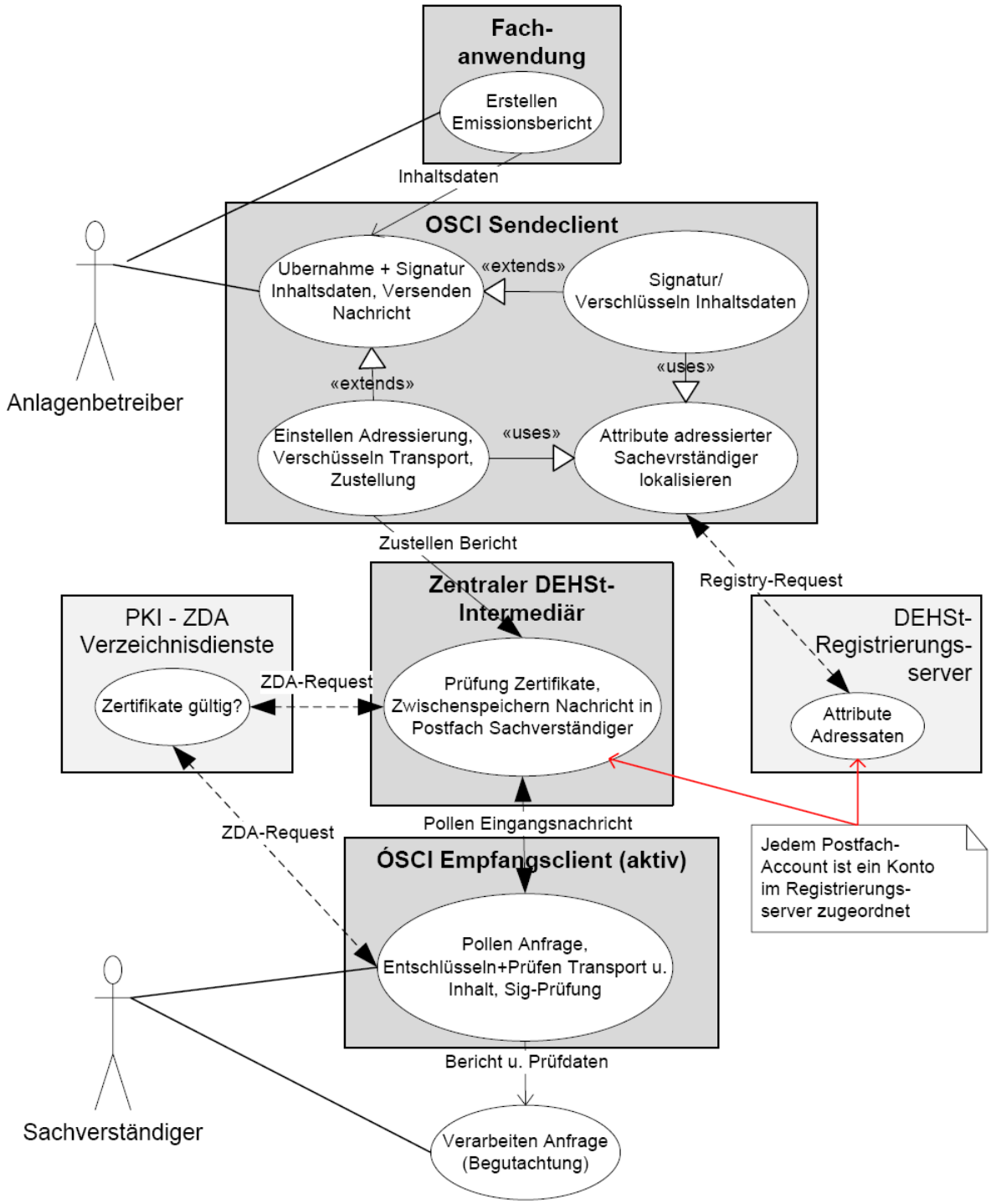

Abbildung 3: Übersicht Übermittlung Emissionsbericht vom Anlagenbetreiber an Sachverständigen

Bei der DEHSt wird der übermittelte Emissionsbericht mit den Prüfdaten zu Signaturen zur weiteren Bearbeitung direkt in ein Dokumenten-Management-System übergeleitet.

Ergänzend ist anzumerken, dass für die einzelnen Akteursrollen unterschiedliche Sichtbarkeiten bzgl. der Teilnehmer des gesamten Kommunikationsverbundes im DEHSt-Registrierungsserver existieren. So können z.B. Anlagenbetreiber keine anderen Akteure in eben dieser Rolle sehen – ein Nachrichtenaustausch zwischen Anlagenbetreibern direkt wird damit ausgeschlossen.

Aktivität	Ausführung	Handlung	Ergebnis	Anmerkung
Erstellen Emissonsbericht	Anlagenbetreiber		Inhaltsdaten Emissionsbericht	
Bericht elektronisch signieren	Anlagenbetreiber, Einsatz OSCI-Client	Der Bericht muss mit einer fortgeschrittene qualifizierten Signatur versehen werden	Digital signierter Emissionsbericht	XML-Signatur auf OSCI 1.2 Inhaltsdaten-Container
Attribute zu adressiertem Sachverständigen einholen	Anlagenbetreiber, Einsatz OSCI-Client	Request an DEHSt-Registrierungsserver, Aufbau Kommunikationsdaten	Attribute werden genutzt, die OSCI-Kommunikationsdaten aufzubauen	Knoten DEHSt-Intermediär, Postfach Sachverständiger (Verschlüsselungszertifikat)
Zuordnung einer eindeutigen Message-Id	OSCI-Client Anlagenbetreiber/ Intermediär DEHSt	Message-Id wird in OSCI 1.2 von einem Server-Dienst (Intermediär) vergeben	Um Message-Id ergänzte Nachricht	Jede Nachricht erhält eine eindeutige Id
Inhaltsdaten verschlüsseln	OSCI-Client Anlagenbetreiber	Die Anfrage muss für Sachverständigen verschlüsselt werden	Signierte und verschlüsselte OSCI-Nachricht	
Nachricht an adressierten Sachverständigen übermitteln	OSCI-Client Anlagenbetreiber	Aufbau der Adressierungsdaten; Sicherung der Gesamtnachricht durch Transportsignatur. Verschlüsselung Gesamtnachricht für nächsten Transportknoten (Intermediär Postfach Sachverständiger)	Verschlüsselte OSCI-Nachricht wird übermittelt und im Postfach des Sachverständigen abgelegt	Fortgeschrittene Transport-Signatur
Prüfen Unversehrtheit des Transportpakets	Intermediär DEHSt	Entschlüsseln und ggf. Signaturprüfung der Kommunikationsdaten	Ggf. Fehlermeldung an Sender, Abbruch der Kommunikation	
Protokollierung des Eingangszeitpunkts	Intermediär DEHSt	Zur Nachricht wird der Eingangszeitpunkt (Serverzeit) festgehalten.	Um Eingangszeitpunkt ergänzte Nachricht	
Prüfen aller Signatur- und Verschlüsselungszertifikate	Intermediär DEHSt	Initiierung und Protokollierung der Online-Gültigkeitsprüfung aller Zertifikate.	Nachricht ist um die Prüfergebnisse ergänzt	Zertifikate aller angezeigten und akkreditierten ZDAs sind zugelassen

Aktivität	Ausführung	Handlung	Ergebnis	Anmerkung
Abholen und Annahme der Nachricht vom Postfach des Sachverständiger	Sachverständiger unter Nutzung OSCI-Client, Intermediär DEHSt	Authentisierung Sachverständiger beim Intermediär DEHSt, bei Erfolg Verschlüsselung der OSCI-Nachricht für Sachverständigen und Übermittlung, bei Erfolg wird der Abholzeitpunkt (Serverzeit) festgehalten. Technische Annahme der Nachricht, Prüfung der Kommunikationsdaten; Entschlüsselung und Signaturprüfung der Inhaltsdaten	Nachricht liegt beim Empfänger (Sachverständiger) entschlüsselt und geprüft bzgl. Kommunikationsdaten und Signatur Inhaltsdaten vor.	
Erneute Prüfung Signatur(en) incl. Online-Zertifikatsprüfung	Sachverständiger unter Nutzung OSCI-Client,	Prüfung der Signatur(en)		Muss Optional möglich sein
Begutachtung Emissionsbericht	Sachverständiger	Fachspezifischer Vorgang - hier nicht näher betrachtet.		

Tabelle 2: Tabellarischer Use-Case „Übermittlung Emissionsbericht vom Anlagenbetreiber an Sachverständigen“

3.3 Elektronischer Rechtsverkehr Deutschland

Mit dem elektronischen Gerichts- und Verwaltungspostfach („EGVP“)[7] wird allen Bürgern, Verwaltungen und Unternehmen die Möglichkeit einer rechtsverbindlichen (signaturgesetzkonformen) Kommunikation mit Gerichten und anderen Justizbehörden geboten. Es können sowohl strukturierte Daten[8] als auch unstrukturierte Schriftsätze und andere Dokumente in elektronischer Form rechtswirksam ausgetauscht werden.

Basis der Teilnahme an diesem geschlossenen Kommunikationsverbund ist die Eröffnung eines entsprechenden Kontos in einem zentralen Registrierungsserver für alle Teilnehmer. An Rollen werden hier unterschieden

- Behörden (Gerichte, sonstige Justizbehörden)
- Verfahrensbeteiligte (Notare, Anwälte, Firmen)
- Sog. „Slaves“, dies sind nachgeordnete Organisationseinheiten innerhalb der Behörden.

Zur Zugangseröffnung wird eine spezielle Funktionalität des EGVP-Clients genutzt. Während Behördenkonten vom Administrator des Registrierungsservers authentifiziert und aktiviert werden, werden Konten von Verfahrensbeteiligten ohne weitere Authentifizierung direkt aktiviert. Für die einzelnen Rollen werden jeweils spezialisierte Instanzen des EGVP-Clients zur Verfügung gestellt.

[7] Details siehe www.egvp.de

[8] Um dies zu ermöglichen, hat die Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz (BLK) den Datensatz XJustiz entwickelt, siehe www.xjustiz.de

„Slaves“ sind Instanzen innerhalb der Behörden, an die Nachrichten vom EGVP-Eingangsknoten („Empfänger“ der Behörde) selektiert nach unterschiedlichen Geschäftsszenarien (unterschieden durch „EGVP-Nachrichtentypen“) weitergeleitet werden können – damit ist eine Behörde nach außen ***eine*** sichtbare Instanz des Kommunikationsverbundes mit einem OSCI-„Behördenpostfach“ als Eingangspunkt, innerhalb dieser kann nach Zuständigkeiten verteilt werden („Dispatcher“-Funktion). Die Weiterleitung innerhalb der Behörde erfolgt nicht mittels OSCI-Transport, sondern jeweils individuellen festgelegten Verfahren der jeweiligen Behörde (z.B. Ablage im Netz, ftp(s)…).

Die Sichtbarkeit der Teilnehmer des EGVP-Kommunikationsverbundes differiert nach jeweiliger Rolle – Verfahrenbeteiligte sehen sich untereinander nicht, die Behörden sind für alle Beteiligten sichtbar.

Zusätzlich gibt es die Möglichkeit anonymer Zugangseröffnung – konzipiert für den Anwendungsfall, in dem ein Bürger einmalig Dokumente an eine Behörde vertraulich und ggf. signiert übermitteln will. Eine Rückantwort ist bei anonymer Zugangseröffnung nicht möglich, da für solche Teilnehmer kein Eintrag im Registrierungsserver erzeugt wird. Die Behörde hat allerdings die Möglichkeit einer Authentisierung übermittelter Dokumente, falls diese vom „anonymen“ Übermittler signiert wurden.

3.3.1 Verfahrensübersicht

Kennzeichnend für das Verfahren sind:

- Genereller asynchroner Nachrichtenaustausch untere Nutzung von Postfächern mit Ende-zu-Ende (Sender zu Empfänger) Verschlüsselung.
- Es existiert eine zentraler Registrierungs- und Verzeichnisdienst („EGVP-Registrierungsserver“) für alle Teilnehmer des Kommunikationsverbundes[9].
- Behörden (oder Behördengruppen) betreiben eigene Intermediäre für den Postfachdienst (Eingangsnachrichten).
- Es existiert ein zentraler Intermediär für den Postfachdienst der übrigen Verfahrenbeteiligten.
- Es sind für die unterschiedlichen Geschäftsvorfälle und zugeordnete Kommunikationsvorgänge unterschiedliche Nachrichtentypen definiert, die auf Ebene der Kommunikationsdaten sichtbar sind. Sie dienen der Steuerung der des Ablaufs in den eingesetzten Sende-/Empfangsclients und als Selektionsmöglichkeit[10] in einem Postfach. Dies Szenarien sind derzeit:
    - **„normale“ EGVP-Nachrichten** - dies umfasst formfreien Austausch von Nachrichten als auch einen Mix von strukturierten und unstrukturierten Nachrichteninhalten (XJustiz-Datensatz, der in entsprechenden Fachanwendungen erzeugt/verarbeitet wird ggf. ergänzt um signierte oder unsignierte Dokumente aus Text- und Bildverarbeitungsanwendungen – z.B. Klageschriften, Beweismittel).
    - **Handelregistermeldungen** – dies ist bis dato ein „one-way“-Szenario, auf Registermeldungen hin erfolgen keine Antwortnachrichten der Registergerichte.
    - **Mahnanträge** – hier werden klassische Dateien auf früheren Datenträgeraustauschverfahren als Attachment übermittelt, ergänzt um eine Metainformationen. Auf die Übermittlung von Mahnanträgen hin erfolgt weiterer Nachrichtenaustausch zwischen Antragsteller und Mahngericht; u.a. wird dem Antragsteller eine Eingangsquittung (auf Inhaltsdatenebene) des Mahngerichts zugestellt.

[9] Stand Mai 2009 sind über 30 000 Teilnehmer registriert

[10] Die soll in OSCI 2.0 über eine differenziertere Adressierungsmöglichkeit gelöst werden, siehe Anforderungen **MUSS 17:** und **MUSS 27:** in Kapitel [4].

- Es existiert aufgrund Fristbindung in einer Reihe der hier abgebildeten Geschäftsvorfälle für die Verfahrensbeteiligten ein hoher Bedarf an Zustellungsnachweisen und Nachvollziehbarkeit der Kommunikation.
- Für die Einzelszenarien ist profilierbar, ob – und wenn ja, fortgeschrittene oder qualifizierte – Signaturen einzusetzen sind. Neben XML-Signaturen auf Ebene der Inhaltsdatencontainer sind bei der Signaturprüfung von Nachrichten auch PKCS#7-Signaturen von Attachments zu berücksichtigen (diese werden derzeit von separaten Anwendungen außerhalb des EGVP-Clients erzeugt).
- Signaturprüfung inkl. Online-Zertifikatsprüfung muss von den Endpunkten aus möglich sein.
- Die Paketierung der Nachrichten kann aufgrund der enthaltenen (ggf. signierten) Attachments komplex sein. Bei der Visualisierung der Prüfergebnisse von Signaturen müssen diese den Nutzern entsprechend den Nachrichtenbestandteilen zugehörig präsentiert werden.

3.3.2 Ablauf der Kommunikationsvorgänge

[Abbildung 4] zeigt das von den konkret bedienten Geschäftsvorfällen abstrahierte Gesamtszenario. Auf eine detaillierte tabellarische Übersicht der Anwendungsfälle wird hier verzichtet. Das Grundmuster entspricht jeweils dem im vorgehenden Kapitel geschilderten Anwendungsfall – hier allerdings unter Nutzung unterschiedlicher Instanzen von Postfach-Diensten. Aufgrund der differierenden Profile vor allem bzgl. der Signaturerfordernisse weichen die Einzelschritte in den einzelnen Kommunikationsszenarien voneinander ab.

Bzgl. der Nachweiserfordernisse Zustellung/Empfang differieren die Anforderungen bzgl. der konkreten Kommunikationsvorgänge. In OSCI Transport 1.2 ist nur der generelle Mechanismus des „Laufzettels“ vorgesehen, der nicht szenarienbezogen skalierbar ist. Eine Empfangsquittung des Empfängers ist nicht explizit vorgesehen, nur der Abholzeitpunkt aus dem Postfach ist sichtbar, eine Empfangsquittung muss daher – wie bei den Online-Mahnanträgen – über die Fachlogik abgebildet werden.

Ein weiteres Manko der Version 1.2 ist, dass die Zustellquittung des Postfach-Dienstes keinen Nachweis enthält, welche Inhaltsdaten mit der quittierten Nachricht übermittelt wurden.

Beide Anforderungen sollen in OSCI Transport 2 berücksichtigt werden.

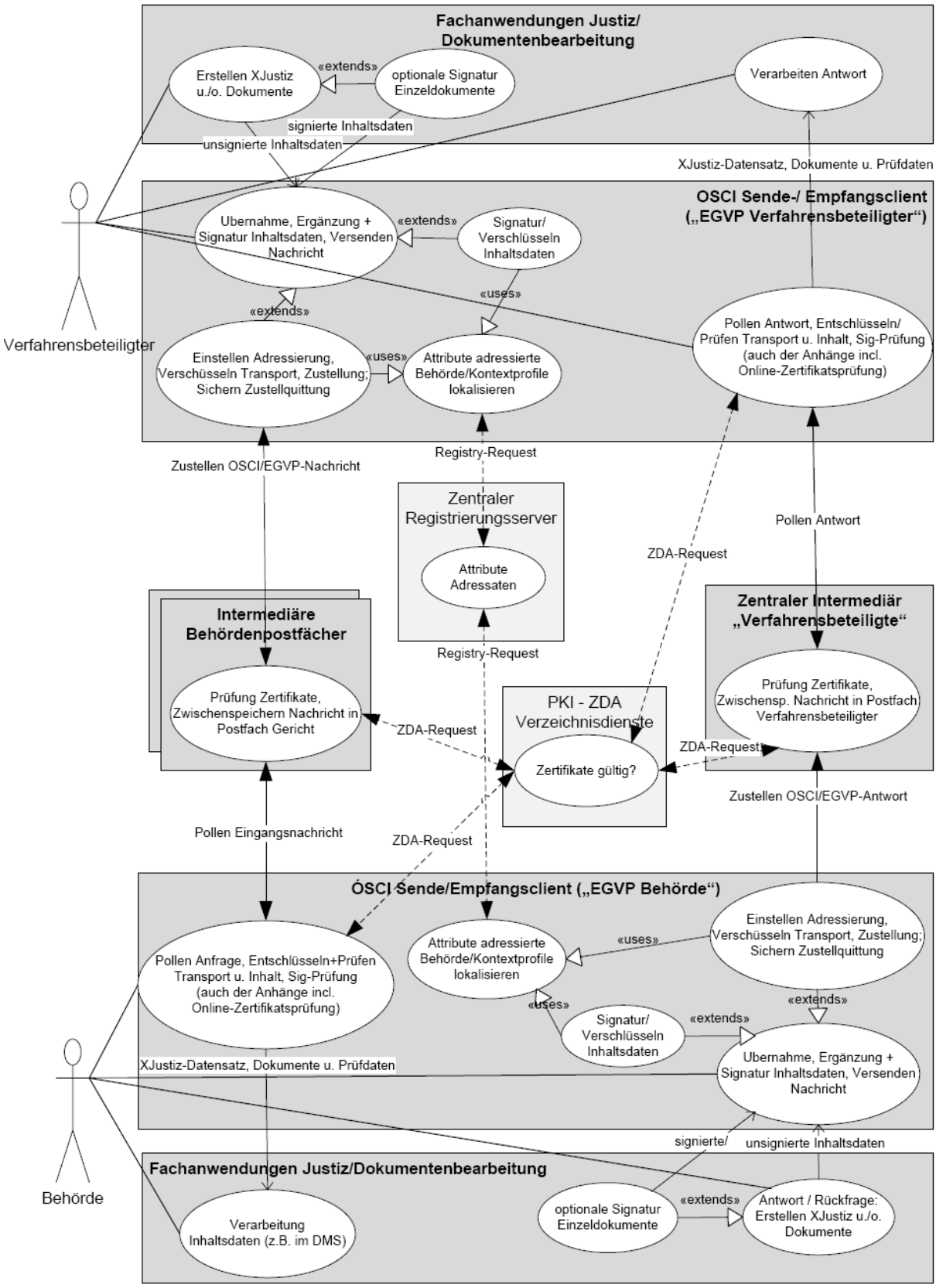

Abbildung 4: Übersicht „Elektronisches Gerichts- und Verwaltungspostfach“ (EGVP)

3.4 Deutsches Patent- und Markenamt: Schutzrechtsanmeldung (DPMAdirekt)

Das Deutschen Patent- und Markenamt bietet mit „DPMAdirekt“ ein Anwendungsbündel zur elektronischen Anmeldung von Schutzrechten an. Diese Art der Anmeldung stellt eine Alternative zur "klassischen" Anmeldung in Papierform dar, und ermöglicht es dem Anmelder, eine rechtswirksame Schutzrechtsanmeldung online vorzunehmen.

Elektronisch eingereicht werden können:

- Patentanmeldung
- Markenanmeldung
- Gebrauchsmusteranmeldung
- Europäische Patentanmeldung
- PCT – Patentanmeldung.

Weiterhin sind elektronisch möglich:

- Einspruch in Patentsachen
- Beschwerde in Patent- und Markensachen.

3.4.1 Verfahrensübersicht

Folgende Abbildung[11] gibt eine grobe Übersicht über das Verfahren:

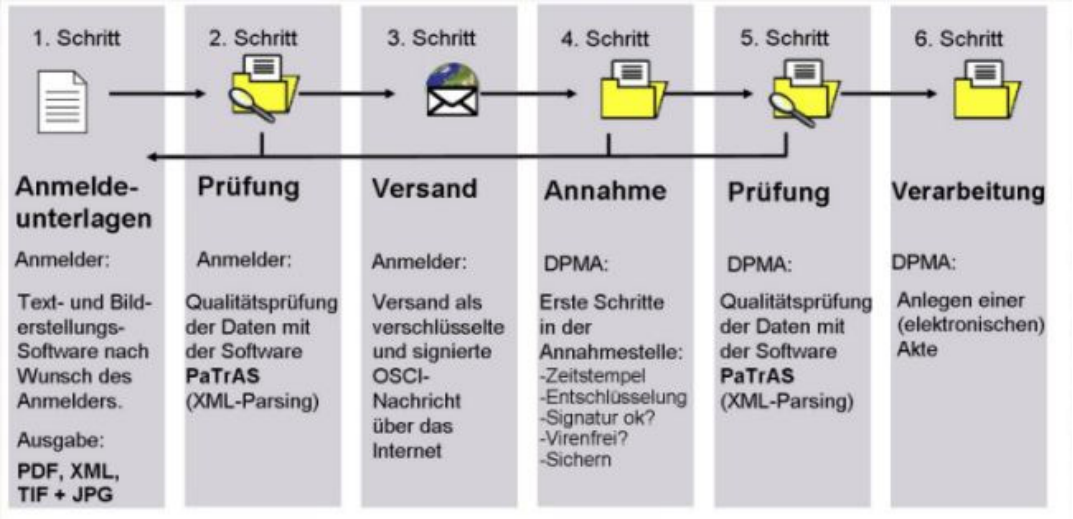

Abbildung 5: Übersicht DPMAdirekt

Es handelt es sich um ein OSCI 1.2- basiertes Szenario mit einem Mix von dem synchronen und asynchronen Kommunikationsvorgängen. Zunächst wird eine synchrone Request-Response-Folge mit direkter Anbindung der Fachverfahrenslogik durchlaufen – der Sender erhält das Resultat einer Prüfung der Kommunikationsdaten sowie eine Eingangsbestätigung. Es folgt ein asynchroner Schritt – dem Sender werden Ergebnisse der Qualitätsprüfung der Inhaltsdaten sowie eine Anmeldebestätigung aus dem Fachverfahren heraus zugestellt, die zur Abholung im Postfach des Senders bereit gestellt werden.

[11] Die Abbildung ist dem Web-Portal des DPMA entnommen

Zum Einsatz kommt *eine* zentrale Intermediärsinstanz mit den Diensten für Postfächer und Anbindung der Zertifikatsprüfung.

Da das DPMA die Eingangsnachrichten (Anträge) in einer „elektronischen Annahmestelle“ (EAST) entgegennimmt, prüft und dem Antragsteller synchron mit einer Annahmebestätigung antwortet, könnte für diese Kommunikationsvorgänge auf eine Intermediärsinstanz verzichtet werden. Die Zertifikatsprüfung müsste bei synchroner Punkt-zu-Punkt Kommunikation vom Antragsteller zum OSCI-Eingangspunkt EAST dort vorgenommen werden.

Ein Postfachdienst wird dennoch für nachfolgende Kommunikationsvorgänge benötigt, bei denen den Antragstellern aus dem Fachverfahren heraus weiter asynchron Nachrichten zugestellt werden.

In diesem Verfahren ist als einem der ersten der Einsatz qualifizierter Zeitstempel geplant. Qualifizierte elektronische Signaturen sind mandatorisch für die Antragsteller; die DPMA-Annahmestelle setzt fortgeschrittene Signaturen ein.

3.4.2 Ablauf der elektronischen Schutzrechtsanmeldung

Die folgende eine tabellarische Aufstellung beschreibt die Abläufe der Antragserstellung, -übermittlung und –annahme im Detail. Der Antragsteller eines Schutzrechtsantrags tritt in zwei Rollen auf:

- als Autor des Antrags bei der Antragserstellung
- als Sender bei der Signatur, Verschlüsselung und Übermittlung der Daten.

Nicht berücksichtig ist die Übermittlung nachfolgender weiterer asynchroner Nachrichten aus dem Fachverfahren an dis Antragsteller, die diese aktiv aus ihrem jeweiligen Postfach abholen müssen (dies ist eine implizite Funktionalität des OSCI-Clients für die Antragssteller).

Aktivität	Ausführung	Handlung	Ergebnis	Anmerkung
Anmelde-unterlagen erstellen	Autor	Ausfüllen der Formulare, ggf. ergänzen um Anhänge	Elektronische Unterlagen zur Schutzrechts-anmeldung	Hierfür stellt das DPMA kostenlos Programme für das erstellen der Daten zur Verfügung
Unterlagen prüfen	Autor	Die Anmeldeunterlagen werden mittels der Validierungssoftware PaTrAS auf Vollständigkeit hin überprüft	Geprüfte Elektronische Patentanmeldeunterlagen	
Antrag elektronisch signieren	Autor	Die Anmeldeunterlagen müssen mit einer qualifizierten elektronisch Signatur versehen werden	Digital signierte elektronische Patent-anmeldeunterlagen	Die Visualisierung der Daten vor Signatur muss möglich sein. Der Nutzer muss alle qualifizierten Signaturzertifikate einsetzen können.
Datenpaket an Annahmestelle des DPMA übermitteln	Sender	Aufbau der Adressierungsdaten; optional Sicherung der Gesamtnachricht durch Transportsignatur. Verschlüsselung Gesamtnachricht für nächsten Transportknoten (Intermediär		Verschlüsselungszertifikate aller Kommunikationsknoten müssen zur Verfügung stehen (sie werden auch zur Adressierung/Rückadressierung genutzt)

Aktivität	Ausführung	Handlung	Ergebnis	Anmerkung
		Eingang DPMA)		
Prüfen Unversehrtheit des Transportpakets	Intermediär Annahmestelle	Entschlüsseln und ggf. Signaturprüfung der Kommunikationsdaten	Ggf. Fehlermeldung an Sender, Abbruch der Kommunikation	
Zuordnung einer eindeutigen Message-Id	Intermediär Annahmestelle	Jede Nachricht erhält eine eindeutige Id	Um Message-Id ergänzte Nachricht	
Protokollierung des Eingangszeitpunkts	Intermediär Annahmestelle	Zur Nachricht wird der Eingangszeitpunkt (Serverzeit) festgehalten.	Um Eingangszeitpunkt ergänzte Nachricht	Geplant ist die Applikation eines qualifizierten Zeitstempels in diesem Schritt
Prüfen aller Signatur- und Verschlüsselungszertifikate	Intermediär Annahmestelle	Initiierung und Protokollierung der Online-Gültigkeitsprüfung dieser Zertifikate. Es müssen die signierten Originalauskünfte von den Verzeichnisdiensten der ZDAs protokolliert werden.	Nachricht ist um die Prüfergebnisse ergänzt	Es müssen mindesten alle Verzeichnisdienste der in Deutschland angezeigten oder akkreditierten ZDAs angebunden sein
Weiterleitung der Nachricht an Eingangsknoten Annahmestelle (= von Sender adressierter Empfänger)	Intermediär Annahmestelle	Weiterleitung der Nachricht, bei Erfolg wird der Weiterleitungszeitpunkt (Serverzeit) festgehalten.	Nachricht ist an den Empfänger überstellt; der Zeitpunkt wird in der Nachricht festgehalten.	
Annahme der Nachricht am Endpunkt „Annahmestelle“; Erzeugen Eingangsbestätigung an den Sender	Transport-Eingangsknoten Annahmestelle („Empfänger“)	Technische Annahme der Nachricht, Prüfung der Kommunikationsdaten; Entschlüsselung und Signaturprüfung der Inhaltsdaten; Zuordnung einer „Document Reference Number“ (DRN, eindeutiger Identifier aus Sicht des Fachverfahrens)	Nachricht liegt beim Empfänger entschlüsselt und geprüft bzgl. Kommunikationsdaten und Signatur Inhaltsdaten vor. Synchrone Eingangsbestätigung mit Eingangszeitpunkt, DRN an den Antrag-	Im Fehlerfall schon hier Rückmeldung an den Sender. *Die Nachricht wird (fortgeschritten) signiert und für den Sender verschlüsselt. Das Verschlüsselungszertifikat des Senders muss vorliegen (Dies gilt auch für alle folgende Rückmeldung an den Sender!). Abschluss des Request-Response-Szenarios*

Aktivität	Ausführung	Handlung	Ergebnis	Anmerkung
			steller.	
Nachricht wird inkl. Prüfinformationen an elektronische Akte übermittelt	Transport-Eingangsknoten Annahmestelle	Bereitstellung zur weiteren Bearbeitung		Von der Antragsübermittlung und -eingangsprüfung entkoppelter Prozess. Aus diesem heraus können weitere Nachrichten an den Autor resultieren, die diesem asynchron übermittelt und zur Abholung im Knoten Intermediär Annahmestelle werden.
(Asynchrone) Übernahme der Nachricht in Fachverfahren	Eingangsknoten Fachverfahren Annahmestelle	Aufnahme der weiteren Abarbeitung im Fachverfahren	Siehe folgende Schritte	
Qualitätsprüfung Inhaltsdatenpaket	Eingangsknoten Fachverfahren Annahmestelle	Virenprüfung der Inhaltsdaten; Duplikatsprüfung; Ermittlung des Vorgangstyps; Prüfung auf Vollständigkeit und syntaktische Korrektheit (wiederum durch das Programm PaTrAS)	Inhaltsdaten konnten auf Korrektheit geprüft werden.	Im Fehlerfall Rückmeldung an den Sender
(Rechtsverbindliche) Anmeldebestätigung an den Sender	Eingangsknoten Fachverfahren Annahmestelle	Zur Eingangsnachricht wird eine „rechtlich verbindliche Eingangsbestätigung“ an den Sender erstellt“	Sender empfängt verbindliche Anmeldebestätigung, die die eindeutige Dokumentenreferenznummer und den Annahmezeitpunkt enthält; Status: erfolgreiche Antragsstellung	Asynchrone Zustellung in das Postfach des Senders. Die Nachricht wird (fortgeschritten) signiert und für den Sender verschlüsselt. Das Verschlüsselungszertifikat des Senders muss vorliegen.
Weitere Abarbeitung im Fachverfahren	Fachverfahren DPMA	Fachspezifischer Vorgang - hier nicht näher betrachtet.		Aus der Folgeverarbeitung heraus können weitere Nachrichten an den Antragsteller resultieren, die diesem asynchron übermittelt und zur Abholung im Knoten Intermediär An-

Aktivität	Ausführung	Handlung	Ergebnis	Anmerkung
				nahmestelle bereit gestellt werden.

Tabelle 3: Tabellarischer Use-Case „Schutzrechtsanmeldung“

3.5 eBologna – rechtsverbindlicher elektronischer Austausch bescheinigter Prüfungsleistungen

Zur Schaffung eines europäischen Hochschulraumes im Bologna-Prozess haben die beteiligten Länder der EU gemeinsame Ziele zur Restrukturierung von Studiengängen und Abschlüssen an Hochschulen und Universitäten vereinbart, insbesondere die Einführung international kompatibler gestufter Studiengänge/Abschlüsse und die Modularisierung von Studiengängen, dieses verbunden mit einer verbesserten internationalen Anerkennung von Prüfungs- und Studienleistungen. Die internationale Mobilität von Studierenden und Lehrenden soll so gefördert werden. Ferner wird die internationale Transparenz und Kompatibilität von Studienabschlüssen durch die Ausstellung eines Diploma Supplements zusätzlich zum nationalen Hochschulzeugnis gefördert.

Bei Auslandssemestern bescheinigen die jeweiligen Gasthochschule den Studierenden Prüfungsleistungen auf Papier als so genannte „Transcripts of Records (TOR)“ entsprechend der Bologna-Richtlinien. Zurück an den Heimathochschulen, legen die Studierenden dort das jeweilige TOR zur Anerkennung als Prüfungsleistung vor. Im praktischen Einsatz behindern die jetzige Papierform mit unzureichenden Standards und unzureichende Sicherungen einen effizienten, sicheren und rechtsverbindlichen Prüfungsdatentransfer.

3.5.1 TOR-Austausch unter Nutzung von OSCI

Der Austausch von Prüfungsdaten TOR im Bologna-Prozess zwischen der Gasthochschule und der Heimathochschule wird nunmehr vollelektronisch unter Nutzung von OSCI Transport ermöglicht. Als „OSCI-eTOR“ strukturierte Inhaltsdaten werden rechtsverbindlich signiert und mittels OSCI Transport Ende-zu-Ende verschlüsselt. zwischen den Beteiligten ausgetauscht. Im Projekt SeDiGov an der Hochschule Harz wurden entsprechende Realisierungen und Demonstratoren unter Einsatz professioneller E-Government-Werkzeuge erstellt.

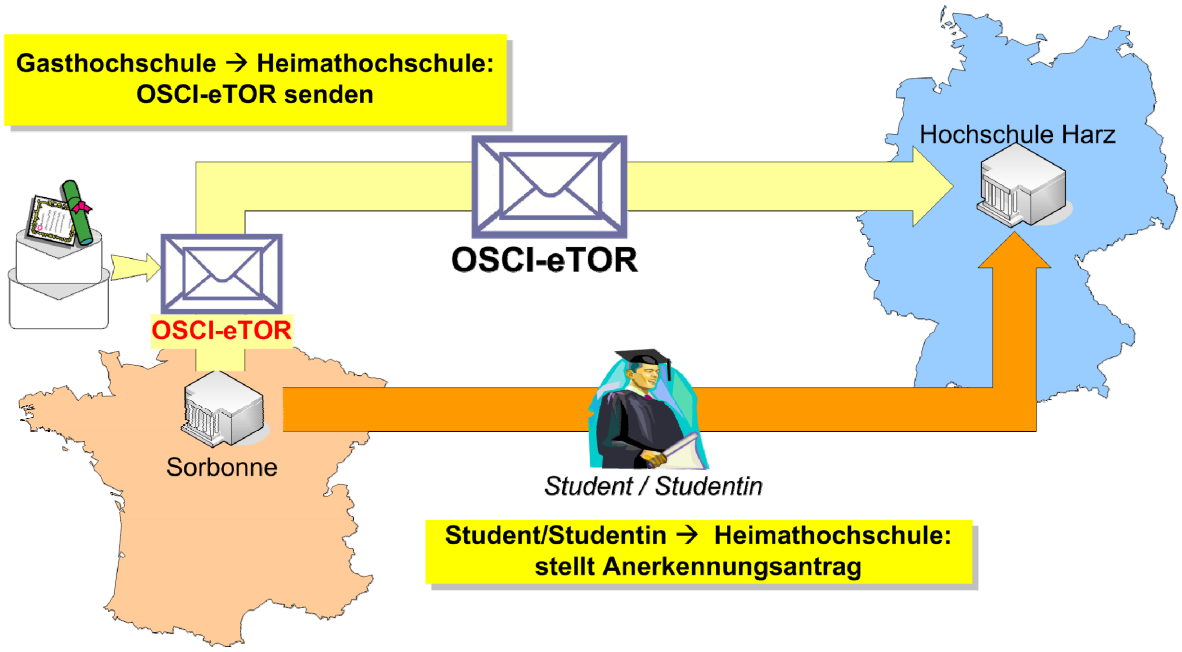

Abbildung 6: OSCI-eTor: Beispielhafter Kommunikationsfluss

Für die Organisation des Prüfungsdatenaustausches via OSCI sind generell verschiedene Hauptszenarien zu unterscheiden:

1. Prüfungsdatenaustausch national (Deutschland) zwischen Gast- und Heimathochschule
2. Prüfungsdatenaustausch international (EU) zwischen Gast- und Heimathochschule
3. Prüfungsdatenaustausch national/international in kooperativen Studiengängen (bis hin zu Mehrfachabschlüssen an verschiedenen Hochschulen).
4. Homogene oder inhomogene E-Government-Protokollverteilung zwischen den nationalen/ internationalen Hochschulen, verschiedene Providermodelle.

Entsprechend dem zugrunde liegenden Geschäftsvorfalls „Austausch bescheinigter Prüfungsleitungen“ sind sämtliche Szenarien asynchron.

3.5.2 Besondere Anforderungen des eTOR-Verfahrens

Der Studierendenaustausch wird üblicherweise durch eine Vornominierung der auszutauschenden Studierenden zwischen den Hochschulen vorbereitet, inzwischen dabei oft bereits durch eine elektronische Vornominierung der Studierenden vorbereitet/unterstützt. In Zukunft sollen auch elektronisch gesicherte Identitäten/Authentisierungen und Credentials der Studierenden aus Effizienzgründen eingesetzt werden (Studenten sollten z.B. auch in elektronischen Systemen an beiden Hochschulen Prüfungsdatentransfers/eTORs entschlüsseln und authentisieren können).

Da in näherer Zukunft eine flächendeckende internationale elektronische Studenten-Identität kurzfristig kaum zu erwarten ist, wird also bis dahin eine „beglaubigte Zuordnung“ der verschiedenen elektronischen Hochschulidentitäten der Studierenden erforderlich, auch beim eTOR-Austausch. Bezogen auf die Authentisierung beim Zugriff auf OSCI-Nachrichten müssen daher verlässliche Korrelierungen der verschiedenen Studenten-Identitäten (Leser) möglich sein und Inhaltsdaten ggf. entsprechend mehrfach verschlüsselt werden.

Je nach homogener oder inhomogener internationaler E-Government-Protokollverteilung beim eTOR-Austausch ergeben sich ggf. Forderungen nach entsprechenden Gateway-Ansätzen zwischen den Protokollen sowie nationaler Lokalisierung der Status- und Fehlermeldungen von OSCI Transport.

3.6 Elektronische Auftragsvergabe (Mehrfachverschlüsselung)

Dieses Anwendungsszenario existiert in sehr unterschiedlichen Ausprägungen, auf deren detaillierter Darstellung hier verzichtet wird. Gemeinsam ist einer Mehrzahl der OSCI-Transport basierten Lösungen, dass ein Bieter seine elektronisch übermittelten Angebote zweifach verschlüsselt (Überschlüsselung), die ausschreibende Vergabestelle dafür das Verschlüsselungszertifikat ihres Eingangsknotens zur Verfügung stellt sowie ein weiteres – oft pro Vergabeverfahren generiertes.

Mit organisatorischen Mittel ist in der Vergabestelle sichergestellt, dass die für die komplette Entschlüsselung benötigten privaten Schlüssel erst zum Submissionstermin bereitgestellt werden. I.d.R. steht der Schlüssel zur Authentisierung gegenüber einem Postfachdienst ständig zur Verfügung (d.h. Angebote können aus dem Postfach sofort nach Eingang abgeholt werden), die innere Verschlüsselung kann aber erst gelöst werden, wenn der dem Vergabeverfahren zugeordnete private Schlüssel bereitgestellt wird. Vorstellbar ist auch, dass der Zugang zum erstgenannten privaten Schlüssel erst zum Submissionstermin ermöglicht wird – in diesem Fall können eingegangene Angebot erst anschließend auf dem Postfach der Vergabestelle abgeholt werden.

4 Kommunikationsszenarien und Dienste

4.1 OSCI-Rollenmodell

Die vielfältigen Anwendungsszenarien mit jeweils unterschiedlichen funktionalen und sicherheitstechnischen Anforderungen erfordern ein geeignetes Rollen- und Funktionsmodell, welches entsprechend flexibel skalierbar ist.

Die einzelnen Rollen werden im Folgenden sowohl mit ihren deutschen als auch englischen Bezeichnungen belegt. In den Dokumenten zur Archikturübersicht und Spezifikation beschränken wir uns auf die englischen Bezeichnungen.

Grundlage jeglicher elektronischer Kommunikation ist die Übermittlung von Daten von einem Sender zu einem Empfänger. Dabei ist jedoch zu berücksichtigen, dass im Allgemeinen mehrere Personen durch gemeinschaftliches Verfassen bzw. durch Genehmigung und Abzeichnung für den Inhalt von Nachrichten verantwortlich sind, während der eigentliche Versand einer Nachricht nur von einer Person veranlasst werden kann. Beide Rollen sind mit unterschiedlichen Verantwortlichkeiten verbunden. So liegt die Inhaltsverantwortung bei den Autoren (die sich zur Erstellung der Inhaltsdaten ggf. einer „Source Application“ bedienen), während der Sender (Initiator) für den fristgerechten Versand an den richtigen Empfänger (Recipient) verantwortlich ist. Analog ist auch auf der Empfangsseite zwischen dem Empfänger (Recipient) als demjenigen, der eine Nachricht entgegennimmt und den Lesern (ultimate Recipient) einer Nachricht, die die eigentlichen Inhalte (ggf. unter Nutzung einer „Target Application“) verarbeiten, zu unterscheiden. Für die Unterscheidung dieser Rollen und der damit verbundenen Verantwortlichkeiten differenziert OSCI zwischen den so genannten Inhaltsdaten und den Kommunikationsdaten einer OSCI Nachricht.

Insgesamt wird bei OSCI folgendes Rollenmodell zu Grunde gelegt (vgl. [Abbildung 7]):

4.1.1 Source Application (Autor(en))

Die Inhaltsdaten können von mehr als einer Instanz erzeugt werden. Jede Instanz, die Inhaltsdaten generiert, wird als Source Application einer OSCI-Nachricht bezeichnet.

MUSS 11:

Die Autoren können bei Bedarf die Inhaltsdaten elektronisch signieren und verschlüsseln. Das Signieren und Verschlüsseln der Inhaltsdaten erfolgt damit bei OSCI optional. Das Signieren von Inhaltsdaten von mehreren Autoren wird eine Mehrfachsignatur der Inhaltsdaten realisiert.

MUSS 12:

Inhaltsdatensignaturen müssen die Anforderungen von [SigG] und [SigV], konkretisiert in den Vorgaben von **Fehler! Verweisquelle konnte nicht gefunden werden.**, erfüllen. Als Formate müssen XML Digital Signature und – für Attachments auch – PKCS#7 unterstützt werden. Autoren müssen die Möglichkeit haben, Attributzertifikate in die Signaturen aufzunehmen und Signaturen mit fortgeschrittenen Zeitstempeln zu versehen. Ergänzende Informationen zu Signaturen müssen die Vorgaben von [XAdES] bzw. [CAdES] erfüllen.

OPT 2:

Implementierungen können Autoren das Einholen qualifizierter Zeitstempel bei Signaturerstellung anbieten.

4.1.2 Target Application (Leser, ultimate Recipient)

MUSS 13:

Die Endpunkte, für die die Inhaltsdaten verfasst sind, werden als Target Application einer OSCI-Nachricht bezeichnet. Es können mehrere Target Applications pro Nachricht existieren. Source Applications verschlüsseln bei Bedarf die Inhaltsdaten daher so, dass sie nur durch die jeweilige Target Application entschlüsselt werden können.

Das optionale Verschlüsseln von Inhaltsdaten für mehrere Target Applications setzt bei OSCI-Transport eine Mehrfachverschlüsselung der Inhaltsdaten voraus.

4.1.3 Sender (Initiator) und Empfänger (Recipient) einer OSCI-Nachricht

Der Nachrichtentransport findet zwischen den Instanzen Sender und Empfänger statt, die auf Basis von Kommunikationsdaten ohne Kenntnis der Inhaltsdaten die Transportfunktionalität erbringen.

MUSS 14:

Zum Transport einer Nachricht müssen die Inhaltsdaten vor dem Versand um Kommunikationsdaten ergänzt werden, die sich u.a. aus Adressierungs- und Rückadressierungsdaten, Absender- und Empfängerzertifikaten, Authentisierungsinformationen des Senders und Anforderungen an Quittierungsmechanismen sowie ggf. auch Bezügen zu vorgehenden Nachrichten zusammensetzen.

MUSS 15:

Die Kommunikationsdaten müssen optional elektronisch signiert werden können.

MUSS 16:

Die Kommunikationsdaten müssen optional verschlüsselt werden können. OSCI-Infrastrukturen müssen Mechanismen zur Verschlüsselung zwischen zwei Knoten der Kommunikation vorsehen für den Fall, dass eine vertrauliche Nachrichtenübermittlung nicht durch die genutzte Transport-Infrastruktur gewährleistet werden kann [12].

4.1.4 Intermediäre

Die Kommunikationsdaten steuern auch das Erbringen von optionalen Mehrwertdiensten auf dem Transportweg (zusammenfassend in Kapitel [4.9] dargestellt); die Kommunikationsdaten werden von Teilen der Mehrwertdienste ergänzt.

[12] Z.B. https oder über VPN gesicherte Verbindungen

4.1.5 Zusammenfassung

Nachfolgende Abbildung gibt eine schematische Übersicht zum Rollenmodell von OSCI: Source Application(s) und Sender am initiierenden Endpunkt der Kommunikation, Empfänger und Target Application(s) auf der anderen Seite. Zwischen den Endpunkten sind Knoten zur Erbringung der Mehrwertdienste frei positionierbar.

Alle Knoten müssen die Möglichkeit zum Zugriff auf Profile bzw. Policies der Endpunkte haben; hier müssen Attribute der Endknoten zur Adressierung, Fähigkeit zur synchronen/asynchronen Kommunikation, Sicherheitsprofile etc. abgefragt werden können, Nicht Gegenstand von OSCI Transport ist Spezifikation von Verzeichsdiensten für diese Profile der Endpunkte.

Die Überprüfung Identitäten und Autorisierungen (in Form von Security-Token) bei Identity Providern, Attribute Services oder CAs muss von allen Knoten aus möglich sein. Für die Ausstellung solcher Token ist ein einheitliches Protokoll/Interface vorzusehen. Die Erfahrungen aus OSCI 1.2-Einsatzszenarien zeigen, dass Endpunkte und Knoten eines OSCI-Kommunikationsverbundes ggf. unterschiedlichen Vertrauensdomänen zuzuordnen sind; spätestens ein Nachrichtenaustausch über die Grenzen solcher Kommunikationsverbünde hinweg erfordert Vorkehrungen zum Austausch und der Prüfmöglichkeiten von elektronischen Identitäten und Berechtigungen.

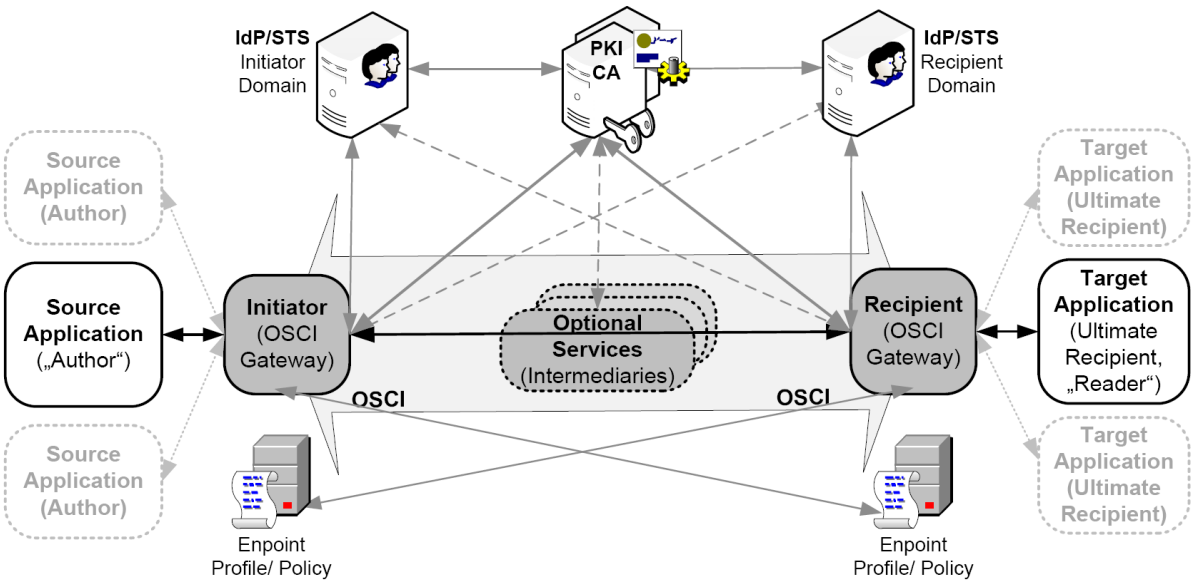

Abbildung 7: Rollenmodell

Die Instanzen Source Application und Target Application, die die eigentlichen Inhaltsdaten erzeugen bzw. verarbeiten, können beliebige Fachverfahren oder Dialoganwendungen sein. Diese Instanzen benötigen Funktionalitäten, die getrennt vom eigentlichen Nachrichtentransport zu sehen sind, aber von einer OSCI-Infrastruktur zur Verfügung gestellt werden müssen[13]:

- Signaturerstellung und –prüfung
- Visualisierungsfunktion für die Signaturerstellung
- Visualisierungsfunktion für Prüf- und Nachweisinformationen (Prüfung Signaturen, Gültigkeit von Credentials etc.)

[13] Diese Funktionen können auch von den Fachapplikationen selbst implementiert werden. Ziel ist, mit diesen von OSCI-Implementierungen zur Verfügung gestellten Diensten Fachapplikationen von der Komplexität der aufgeführten Funktionalitäten zu entlasten; auch ist eine Zentralisierung an zentralen Stellen der OSCI-Infrastruktur ein Faktor zur Sicherung der Interoperabilität.

- Ggf. Zeitstempelerzeugung und -prüfung
- Ver- und Entschlüsselung von Inhaltsdaten
- Zum jeweiligen Endpunkt müssen bestimmte Profilinformation zur Verfügung gestellt werden können (Verschlüsselungszertifikate, Anforderungen bzgl. Signaturerfordernissen, ggf. Profilierungen der Inhaltsdaten bzgl. der vom jeweiligen Leser bedienten Geschäftsszenarien).

Die eigentliche Nachrichtenübermittlung und damit Aufbau und Interpretation der Kommunikationsdaten findet zwischen den Instanzen Sender und Empfänger statt.

4.2 Kommunikationsszenarien

Der Kontakt des Bürgers und der Wirtschaft mit der Verwaltung erfolgt im Rahmen des E-Government auf vielfältige Weise. Bürgerfreundlichkeit und eine höhere Effizienz sind in der Regel nur erreichbar, wenn eine synchrone Kommunikationsphase einen Dialog zwischen der Client-Komponente beim Bürger und der Server-Komponente auf Seiten der öffentlichen Verwaltung erlaubt. Durch den Zugriff auf vorhandene Datenbestände in den Fachverfahren der öffentlichen Verwaltung wird die Fehlerrate der Kundennachrichten verringert, die Qualität erhöht und die Attraktivität der angebotenen Dienstleistungen der Verwaltung gesteigert. Am Ende dieses Dialogs steht dann in der Regel ein vom Kunden elektronisch signiertes Formular, dessen strukturierte Inhaltsdaten an die Verwaltung gesendet werden. Die Antwort hierauf ist wiederum Gegenstand einer neuen Nachricht, bei der die Rollen der Endpunkte getauscht sind.

Bei der Kommunikation zwischen Verwaltungen und Wirtschaft/Verwaltung kommen zunehmend auch Verfahren zum Einsatz, bei denen Nachrichten direkt zwischen Fachverfahren ausgetauscht werden können. Hier existieren sowohl synchrone Request-Response Szenarien als auch asynchrone, bei denen von einer Source Application Daten zur zeitversetzten Bearbeitung an eine Target Application übermittelt werden; das Bearbeitungsergebnis wird zu einem späteren als neue Nachricht (oder auch Nachrichtenfolge) an die Source Application übermittelt.

Interoperable strukturierte Kommunikation ist nur möglich, wenn die zugrunde liegenden Strukturen den Endpunkten bekannt sind. Auf fachlicher Ebene ist dies i.d.R. ein „Handshake“ auf der Ebene von Schema-Beschreibungen der Datensätze und somit nicht im Fokus des Transportprotokolls. Erfahrungen z.B. aus dem elektronischen Meldewesen haben allerdings gezeigt, dass über die fachliche Strukturierung hinaus Endpunkten auch Metainformationen zur zulässigen Paketierung der Inhaltsdaten innerhalb eines „opaque Body“ bekannt sein müssen, um diese Pakete am Übergabepunkt zwischen Empfänger und Target Application(s) korrekt zur Verfügung stellen zu können; entsprechendes gilt für den Paketaufbau am Übergabepunkt Source Application zu Sender. Solche Paktierungsprofile beschreiben, aus welchen Bestandteilen ein opaque Body in einem konkreten Kommunikationsszenario bestehen kann/muss (z.B. ist im Meldewesen - elektronische Rückmeldung - ein bestimmter strukturierter XML-Datensatz zwingend vorgeschrieben, die Übermittlung zusätzlicher Anhänge in beliebigen Formaten ist optional möglich; diese müssen aber von Empfängern nicht verarbeitet werden können).

Es empfiehlt sich daher, für Geschäftsszenarien mit hohem Automatisierungsgrad Profile für Klassifizierung der bedienten Geschäftsvorfälle und ggf. erforderliche Paketierung der Inhaltsdaten zu definieren[14] und diese den Endpunkten zuzuordnen, die die jeweiligen Dienste erbringen. Die Profile sollten die Paketierung formal beschrieben und durch die OSCI-Leitstelle in Ergänzung zu OSCI Trans-

[14] Mit dem „XMeld-Profil für OSCI Transport“ liegt bereits ein solches Profil für das elektronische Meldewesen bzgl. OSCI Transport 1.2 vor

port standardisiert und veröffentlicht werden. Wünschenswert ist eine Profilierung einer Auswahl von Standard-Kommunikationsszenarien, die sich in vielen Geschäftsvorfällen der Verwaltung wieder finden lassen[15].

Für OSCI Transport ergibt sich dann:

MUSS 17:

> Es müssen Mechanismen vorgesehen werden, die Sender und Empfänger einer Nachricht in die Lage versetzen, Nachrichten bei Bedarf klassifizierten Geschäftsszenarien zuzuordnen. Ein Diensteanbieter kann in einem online abrufbaren Profil hinterlegen, welche Geschäftszenarien er bedient und diese durch eindeutige Bezeichner differenzieren („Typ“ oder auch Ausdifferenzierung der zugeordneten Nachrichten-Eingangspunkte). Ein Sender muss bei Übermittlung einer Nachricht bzgl. dieses Geschäftszenarios dieses Attribut in die Nachricht einstellen; es muss für Knoten der OSCI-Kommunikation sichtbar sein, um ggf. an diese Attribute gebundene Operationen[16] ausführen zu können.

►***Empfehlung für die Interkation zwischen Source- und Target-Application:*** *Wenn Geschäftsszenarien es erfordern, sollte Komposition und Dekomposition des „opaque Body“ entsprechend Paketierungsprofilen von den involvierten Instanzen Source- und Target-Application unterstützt werden. Das Profil sollte mit dem Typ der Nachricht korrelieren (siehe **MUSS 17:**).*

Viele Prozesse des E-Government so beschaffen, dass sie durch eine Nachricht des Kunden zwar angestoßen werden, aber nicht vollständig maschinell bearbeitbar sind. Häufig sind manuelle Tätigkeiten von Sachbearbeitern auf Seiten der öffentlichen Verwaltung erforderlich. Dabei muss auch die Rückrichtung von der Verwaltung zum Bürger bedacht werden. In diesem Fall kann aber nicht vorausgesetzt werden, dass der Nachrichtenempfänger stets online erreichbar ist. OSCI unterstützt daher nicht nur den synchronen, sondern auch den asynchronen Austausch von OSCI Nachrichten.

Bzgl. der adressierten Endpunkte (Sender, Empfänger) in OSCI Transport wird daher unterschieden zwischen solchen, die i.d.R. online erreichbar sind (z.B. Dienste von Wirtschaft und Verwaltung, die auf Fachverfahren mit Internetanbindung basieren) und solchen, die gezielt eine Online-Verbindung aufbauen (z.B. Client-Anwendungen von Bürgern und Dienstleistern).

OSCI Transport unterstützt folgende asynchrone und synchrone Nachrichtenszenarien:

MUSS 18:

> Einfache Übermittlung einer Nachricht (Request, „one way message“), wobei ggf. eine asynchrone Antwort (Response) auf die Nachricht erwartet wird. Die Antwort ist ebenfalls eine „one way message“, diese muss den Bezug zum zugehörigen Request ausweisen.

MUSS 19:

> Request-Response-Folge(n) innerhalb einer Verbindung; dieser Nachrichtentyp ist nur nutzbar bei online erreichbaren Empfängern.

Für beide Szenarien ist sicherzustellen:

MUSS 20:

[15] In Dänemark wurden 5 bereits solcher Szenarien identifiziert, mittels derer sich die große Mehrzahl der Geschäftsvorfälle im E-Government modellieren lassen.

[16] Dies können beim Empfänger z.B. Dispatcher-Funktionen zur Übergabe der Nachricht an die passende Target Application sein; ein Postfachdienst könnten die Informationen zur Untergliederung eines Postfachs nutzen.

Sichere und einmalige Zustellung der Nachricht („exactly once“).

MUSS 21:

Eindeutige Identifizierbarkeit der Nachricht (z.B. eindeutige Message-Id, GUID).

MUSS 22:

Sicherstellung korrekter Nachrichten- und Request-Response-Folgen („in order“).

4.3 „Postfach“-Dienst für asynchrone Szenarien

MUSS 23:

Für Endpunkte, die nicht online erreichbar sind, ist die Funktionalität eines „Postfach-Dienstes“ vorzusehen, an den Nachrichten übermittelt werden können und dort für den adressierten Empfänger zur Abholung bereit gestellt werden. Der vom Sender adressierte Endpunkt einer Nachricht ist in diesem Falle das Postfach des Empfängers. Es müssen Funktionen zur Abholung dieser Nachrichten durch berechtigte Empfänger (bzw. ursprünglicher Sender bei asynchronen Rückantworten) vorgehalten werden.

MUSS 24:

Die Dauer des Vorhaltens einer asynchronen Nachricht bei einem Postfachdienst muss in der Policy eines solchen Dienstes abrufbar sein.

MUSS 25:

Im Falle des Zwischenspeicherns von Nachrichten in „Postfächern“ sind die Inhaltsdaten für die adressierte(n) Target Application(s) zu verschlüsseln (Ende-zu-Ende-Verschlüsselung), eine Einsichtnahme der Inhaltsdaten durch Dritte darf nicht möglich sein.

MUSS 26:

Eine OSCI-Nachricht muss bzgl. der Zeit ihrer Gültigkeit (“time to live”) parametrierbar sein. Hiermit wird der Zeitpunkt aus Sicht des Senders kennzeichnet, bis zu dem eine Nachricht – auch im asynchronen Fall - den Empfänger erreicht haben soll. Dieses Attribut kann vom Postfach-Dienst des Empfängers interpretiert werden (Fehlermeldung an anfordernden Sender, wenn nicht unterstützt). Die Policy des Dienstes muss darüber Auskunft geben, was nach Überschreiten des Zeitpunkts mit der Nachricht geschieht.

MUSS 27:

Ein Postfachdienst muss Funktionen zum Selektieren und Abholen der Nachrichten über eine für alle Instanzen solcher Dienste einheitliche Schnittstelle bereitstellen. Der Zugriff auf die Postfächer darf nur den jeweiligen Empfängern möglich sein.

Nachrichten müssen über folgende Kriterien selektierbar sein:

- Message-Id

Oder bei Neueingängen über eine Und-Kombination folgender Kriterien:

- Bezogene Nachricht (Message-ID) (z.B. Quittungen für eine versandte Nachricht)
- Typ der Nachricht (abgebildet in der Adressierungshierarchie eines Postfachs; siehe auch **MUSS 17:**).

Nachrichten werden aus der Ergebnisliste einer Selektion nach dem FIFO-Prinzip jeweils einzeln abgeholt.

MUSS 28:

Ein Postfachdienst muss dem Besitzer des Postfachs (Empfänger) auf Anforderung eine Liste der gespeicherten Nachrichten liefern mit den Attributen:

- Message-Id
- Status
- Initiator (URL des Endpunkts)
- Zeitpunkt Eingang, Abholung (0, wenn noch nicht geschehen)
- Typ der Nachricht (abgebildet in der Adressierungshierarchie eines Postfachs; siehe **MUSS 17:**)
- Verfallsdatum (so unterstützt; siehe **MUSS 26:**)
- Größe der Nachricht im KB.

Als Suchkriterien für diese Liste müssen unterstützt werden.

- Message-Id (Vektor von Ids, von-bis)
- Status (Neueingang, abgeholt)
- Eingangszeitpunkt (von-bis)

Der „Typ“ der Nachricht ist abgebildet in der Adressierungshierarchie eines Postfachs; siehe auch **MUSS 17:**).

4.4 Quittungs- und Nachweismechanismen

Je nach Nutzungsszenario gibt es einen differenzierten Bedarf an Quittungs- und Nachweismechanismen für Kommunikationsvorgänge; hierbei können die Bedarfe ggf. zwischen Sender und Empfänger bzgl. eines Kommunikationsvorgangs auch unterschiedlich sein.

MUSS 29:

Ein vom Sender adressierter Endpunkt muss auf Anforderung des Senders diesem einen Zustellnachweis („DeliveryReceipt“) der Nachricht zur Verfügung stellen. Inhalte: Message-Id, Zeitpunkt, Sender, Empfänger und Hash des Bodies (Inhaltsdaten incl. aller Attachments; i.d.R. verschlüsselt). Der adressierte Endpunkt kann auch das Postfach eines Empfängers sein, in diesem Fall ist der Zustellnachweis von dem Knoten zu erstellen, der den Postfachdienst für den Empfänger erbringt.

MUSS 30:

Ein Postfachdienst muss auf Anforderung des Senders diesem eine Benachrichtigung („FetchedNotification“) übermitteln, wenn der Besitzer des Postfachs (adressierter Empfänger) die Nachricht aus dem Postfach abholt[17]. Inhalte: Message-Id, Zeitpunkt, Sender, Empfänger. Dise Benachrichtigung ist in das Postfach des Senders oder ein andere von diesem angegebene Adresse zu übermitteln.

[17] Hierdurch erlangt der Senders Kenntnis, wann bzw. ob überhaupt die Nachricht aus dem Empfängerpostfach abgeholt wurde, auch wenn der Empfänger keine Empfangsquittung übermittelt.

Wollen Autoren bzw. Sender zu einem späteren Zeitpunkt die Möglichkeit des Nachweises haben, welche Inhalte sie mit der Nachricht zugestellt haben, sollten sie im Falle einer Verschlüsselung für die Target Application in diesem Fall die Nachricht auch für sich selbst verschlüsseln und sichern. Diese Verschlüsselungselemente sind in den Body der Nachricht aufzunehmen und werden somit in den Zustellnachweis aufgenommen. Für die OSCI-Infrastruktur resultiert:

MUSS 31:

Source Applications und Sender müssen die Möglichkeit haben, Nachrichten auch für sich selbst zu verschlüsseln und die Gesamtnachricht lokal für Nachweiszwecke zu sichern.

MUSS 32:

Ein Sender kann vom Empfänger einen Empfangsnachweis („ReceptionReceipt“) der Nachricht und zu den übermittelten Inhaltsdaten anfordern. Inhalt: Message-Id, Zeitpunkt, Sender, Empfänger ergänzt durch eine Quittierung, welche Inhaltsdaten empfangen wurden (z.B. Hash über die entschlüsselten Inhaltsdaten). Können beim Empfänger nicht alle Inhaltsdaten entschlüsselt werden, erhält der Sender eine Fehlermeldung (keine Empfangsnachweise für Daten, die beim Empfänger nicht entschlüsselt werden können). Empfangsnachweise sind in das Postfach des Senders oder ein andere von diesem angegebene Adresse zu übermitteln (separate Antwortnachricht auf die Zustellung bei synchroner Kommunikation zwischen Sender und Empfänger).

Es obliegt es den jeweiligen Endpunkten Sender bzw. Empfänger, bei Bedarf die Quittierungen für spätere Nachweiszwecke zu sichern.

MUSS 33:

Implementierungen müssen eine Funktionalität anbieten, Quittierungen abzuspeichern.

OPT 3:

Knoten und Endpunkte können qualifizierte Zeitstempel für das Ausstellen von Zustell- und Empfangsnachweise anbieten. Dies ist im jeweiligen Profil zu hinterlegen. Nur in diesem Fall kann ein Sender zu einem Nachweis einen qualifizierten Zeitstempel anfordern; ansonsten erhält dieser eine Fehlermeldung.

4.5 Adressierung von Endpunkten, Anbindung von Verzeichnisdiensten

Das Prinzip der „Offenen Benutzergruppe“ von OSCI Transport 1.2 wird eingeschränkt zugunsten einer Lösung, in der davon ausgegangen wird, dass alle Endpunkte eines OSCI-Kommunikationsverbundes in entsprechenden Verzeichnisdiensten (Identity Provider, Dienstleverzeichnis) registriert sein müssen. Ausnahmen sind explizit in einem Profil zu benennen.

Damit wird für den Eintritt in einen OSCI-Kommunikationsverbund die Funktionalität einer Zugangseröffnung benötigt. Die Zugangseröffnung ist nicht Gegenstand der Spezifikation von OSCI Transport.

OPT 4: Optionaler anonymer Zugang

Über OSCI-Transport erreichbare Dienste müssen in ihrem Profil hinterlegen, ob eine anonyme Inanspruchnahme zugelassen ist. In diesem Fall muss ein Initiator der OSCI-Kommunikation („Requestor“ des Dienstes) nicht bei einem IdP registriert sein; der Dienst

prüft die Zulässigkeit der Anfrage mit eigenen Mitteln. Die Anforderungen zur Authentisierung (Kapitel 4.6) gelten beim anonymen Zugang nicht.

Die anonyme Adressierung mittels Verschlüsselungszertifikaten aus OSCI Transport 1.2 wird aufgegeben.

MUSS 34:

Es muss für den Sender vor dem Versand einer Nachricht möglich sein, durch **eine** entsprechende zu spezifizierende Anfrage eine Schnittstellenbeschreibung für den konkreten OSCI-Empfänger zu erhalten, die mind. folgende Informationen enthält[18]:

- URI des Empfängers (bzw. seines Postfachs)
- zu verwendende Verschlüsselungszertifikate
- Synchrone/ asynchrone Erreichbarkeit
- Informationen zum erforderlichen Signaturniveau der Inhaltsdaten[19]
- Informationen darüber, ob und welche Authentisierungsmechanismen unterstützt werden/verwendet werden müssen
- zulässige Versionen des Transportprotokolls

4.6 Authentisierung

MUSS 35:

Die Kommunikation über OSCI ist nicht ohne die Möglichkeit einer sicheren Authentifizierung der jeweiligen Endpunkte und Dienste erbringenden Knoten möglich. Dazu müssen in die Kommunikationsdaten einer Nachricht „Claims“ in Form von Authentisierungstoken aufgenommen werden, die von allen Kommunikationsteilnehmern bei Bedarf verlässlich auf Gültigkeit überprüft werden können. Die Bestätigung der Gültigkeit eines solchen Tokens muss online bei einem IdP möglich sein, dem der jeweils prüfende Endpunkt oder Knoten traut. Eine Nachricht muss zu den Authentisierungstoken auch Information transportieren, bei welchem IdP ein Token auf welche Weise überprüft werden kann.

MUSS 36:

Folgende Authentisierungstoken sind für die OSCI-Kommunikation vorgesehen:

- X509-Zertifikate; zwingend für eine Trust-Domain übergreifende Authentisierung
- SAML-Token
- UserId / Password
- Eines dieser Token *muss* eingesetzt werden bei (optionaler) Nachrichtensignatur

OPT 5:

Innerhalb einer Trust Domain sind auch Kerberos Tickets als Authentisierungstoken zulässig.

[18] Details werden im OSCI-Architekturdokument spezifiziert

[19] Dies ist ggf. je nach Geschäftsvorfall differenziert

MUSS 37:

OSCI-Nachrichten müssen einmal eingeholte Prüfinformationen zu Authentisierungstoken (als auch zu eingesetzten Verschlüsselungs- und Signaturzertifikaten) sicher transportieren können. Damit besteht die Möglichkeit, Prüfdienste ggf. zu zentralisieren; weiter vermeidbar ist damit eine Mehrfachüberprüfung identischer Token auf unterschiedlichen Stationen einer OSCI-Kommunikation.

4.7 Token und deren Validierung

Grundsätzlich sollte jeder potenzielle Empfänger von OSCI Nachrichten in der Lage sein, Signaturprüfungen und die Gültigkeitsprüfung von Security Token selbst vorzunehmen. Die Nutzung einer OSCI Infrastruktur darf nicht dazu führen, dass Knoten und Empfänger der OSCI-Nachrichten sich auf die ggf. mit der Nachricht transportierten Validierungsinformationen verlassen müssen. Es ist aber ein pragmatischer Ansatz, das Einholen solcher Informationen an zentraler Stelle vorzusehen, an die solche Prüfaufgaben delegiert werden können. Aufgrund der in OSCI vorgenommenen Trennung von Inhalts- und Kommunikationsdaten ist dies ohne Verletzung der datenschutzrechtlich gebotenen Vertraulichkeit der Inhaltsdaten möglich.

4.7.1 Public-Key Infrastruktur

Ein wesentlicher Aspekt bei der Kommunikation mittels OSCI ist die Gewährleistung der Rechtsverbindlichkeit und der Vertraulichkeit. Geschäftsprozesse, deren Abwicklung über den neuen Vertriebsweg Internet zwingend die elektronische Signatur voraussetzt, bilden einen wichtigen Teilbereich des E-Government. Die Erfüllung dieser Anforderungen basiert in OSCI auf den Techniken der Public-Key-Kryptographie. Die Gültigkeit dieser Zertifikate muss verifiziert werden, um Aussagen hinsichtlich der Authentizität treffen zu können. Die PKI nach SigG ermöglicht dem Empfänger einer signierten Nachricht diese Prüfung.

MUSS 38:

Eine OSCI-Infrastruktur muss die Gültigkeitsprüfung von X509-Zertifikaten in den Verzeichnisdiensten der ZDAs über eine einheitliche Schnittstelle allen Knoten und Endpunkten zur Verfügung stellen können.

4.7.2 Weitere Security-Token

MUSS 39:

Andere Token müssen bei Diensten eines IdP online überprüfbar sein. Die Dienste müssen über eine einheitliche Schnittstelle allen Knoten und Endpunkten zur Verfügung stehen.

4.8 Optionaler Mehrwertdienst: Nachrichten- und Nachweisarchiv

Quittierungen von Kommunikationsvorgängen sind Verbindungsdaten nach dem Telekommunikationsdienstegesetz, welche Betreiber von entsprechenden Diensten nur einen begrenzten Zeitraum aufbewahren dürfen[20]. Ein implizit längerfristiges oder sogar unbefristetes Vorhalten solcher Daten für spätere Nachweise stellt Betreiber auch vor das Problem unkalkulierbarer Datenvolumina. Auch ist es für einen Betreiber i.d.R. sicht möglich, die Aufbewahrungsdauer solcher Nachweise selektiv nach

[20] Es befindet sich aktuell in juristischer Prüfung, wie sich dies bzgl. des Laufzettels gem. OSCI 1.2 verhält

Geschäftvorfällen mit solchen Bedarfen zu steuern (z.B. im elektronischen Rechtsverkehr), da er keine Kenntnis über die Inhaltsdaten erlangen darf.

OPT 6:

Das längerfristige Vorhalten von Nachweisen zu Kommunikationsvorgängen und übermittelten Daten ist eine optionale Dienstleistung, die von Betreibern solcher Dienste Nutzern auf Basis explizit zu treffender vertraglicher Vereinbarungen angeboten werden kann. Das Übermitteln und Abrufen solcher Nachweise muss mit einheitlichen, von einer konkreten Implementierung unabhängigen Nachrichtentypen möglich sein.

4.9 Zusammenfassung: OSCI-Mehrwertdienste

Die sichere Übertragung von Daten eines Geschäftsvorfalles zwischen zwei Kommunikationspartnern muss bei Bedarf durch zusätzliche Services unterstützt werden. Diese bieten Kommunikationspartnern über den reinen Transport der Nachrichten hinaus folgende Funktionalitäten an:

- Prüfung der Gültigkeit von mit der Nachricht übermittelten Credentials (z.B. X509-Zertifikaten) in entsprechenden Verzeichnisdiensten (PKI-Verzeichnisdienste, Prüfung anderer Token bei entsprechenden Identity Providern).
- Unterstützung asynchroner Nachrichten: Service für die Zwischenspeicherung von Nachrichten inkl. Abholfunktion.
- Anbindbarkeit von Registrierungs- und Verzeichnisdiensten für Kommunikationspartner und über OSCI erreichbare Dienste über eine einheitliche Schnittstelle.
- Nachhalten (kurz- bis mittelfristig) und Abrufbarkeit von Nachweisen zur Nachrichtenübermittlung
- Service für längerfristige Archivierung und Abrufbarkeit solcher Nachweise; optional inkl. der zugehörigen Nachrichteninhalte

Für die Erbringung der OSCI-Mehrwertdienste muss von den Knoten, die die jeweilige Funktion erbringen, auf Header-Informationen zugegriffen werden können.

Die OSCI-Mehrwertdienste müssen nicht zwingend von einer dritten Instanz wahrgenommen werden; diese Funktionalität können auch einem Fachverfahren direkt vorgeschaltet werden. In diesem Fall sind zusätzliche Sicherheitsvorkehrungen bei der Stelle umzusetzen, die diese Rollen wahrnimmt.

4.10 Vertrauensbeziehungen zu Diensten der OSCI-Infrastruktur

Sender und Empfänger müssen Diensten, die durch die OSCI-Infrastruktur erbracht werden, vertrauen können. Dies gilt insbesondere für

- Dienste zur Überprüfung von Credentials (IdP, AS); bzgl. der Dienste angezeigter oder akkreditierter ZDAs kann dabei von inhärenter Vertrauensstellung ausgegangen werden
- Postfach-Provider
- Nachweisdienste
- Dienste zur längerfristigen Speicherung/Abrufbarkeit von Nachrichten inkl. Prüf- und Transportstatusinformationen (vornehmlich Übermittlungs-/Zustellungsnachweisen).

MUSS 40:

> Sender und Empfänger stehen i.d.R. in einer Vertrauensstellung zu den Instanzen der Kommunikation, die die in den jeweiligen Szenarien benötigten optionalen Mehrwertdienste erbringen. Es muss daher die Möglichkeit bestehen, diese Instanzen jeweils gem. der Vertrauensstellung der jeweiligen Endpunkte in den Nachrichtenfluss einzubinden.
>
> Die Architektur der OSCI-Infrastruktur muss so gestaltet sein, dass jeder Endpunkt für sich festlegen kann, welcher Instanz zur Erbringung von OSCI-Mehrwertdiensten er sich bedient; insbesondere muss jeder Empfänger den Provider des Postfachdienstes für sich festlegen können.

In OSCI-Architekturen müssen die Knoten zur Erbringung der Mehrwertdienste somit flexibel lokalisierbar sein – als Service auf Zwischenknoten bei Nachrichtentransport oder auch lokalisiert jeweils direkt bei den Instanzen Sender und Empfänger. I.d.R. werden unterschiedliche Instanzen dieser Dienste betrieben, jeweils für Sender und Empfänger in deren jeweiligen „Trust Domains“. Bei überlappenden Vertrauensstellungen von Sender und Empfänger bzgl. einzelner Dienste können Instanzen der Mehrwertdienste zusammenfallen – mindestens für die Verzeichnisdienste der angezeigten und akkreditierten ZDAs ist dies immanent.

5 OSCI und Informationssicherheit

Informationssicherheit hat zum Ziel den Schutz von Informationen vor Verlust der Grundwerte

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Nichtabstreitbarkeit
- Zurechenbarkeit

Dabei bedeuten

- Verlust der Vertraulichkeit:
  die Gefahr, dass Unberechtigte Inhalts- und Kommunikationsdaten zur Kenntnis nehmen;
- Verlust der Integrität:
  die Gefahr, dass Inhalts- und Kommunikationsdaten auf dem Weg vom Autor oder Absender zum Empfänger während ihrer Übertragung verfälscht werden;
- Verlust der Verfügbarkeit:
  die Gefahr, dass auf Inhalts- und Kommunikationsdaten bzw. die OSCI-Infrastrukturdienste nicht, nicht vollständig oder nicht rechtzeitig zugegriffen werden kann.
- Verlust der Authentizität:
  die Gefahr, dass Inhalts- und Kommunikationsdaten nicht vom Urheber bzw. Autor oder Absender stammen;
- Verlust der Nichtabstreitbarkeit:
  die Gefahr, dass die Autorenschaft, der Versand oder der Empfang von Inhalts- bzw. Kommunikationsdaten bestritten wird;
- Verlust der Zurechenbarkeit:
  die Gefahr, dass Aktionen nicht (nachträglich) einer Person und einem Zeitpunkt zugeordnet werden können.

Die OSCI-Transportarchitektur dient einerseits der Gewährleistung der Informationssicherheit bei der elektronischen Kommunikation in offenen Netzen. Andererseits ist eine OSCI-Infrastruktur selbst den genannten Gefährdungen der Grundwerte ausgesetzt. Diese zunächst abstrakten Gefährdungen manifestieren sich in konkreten Gefährdungsszenarien für die jeweils betroffenen Module der OSCI-Infrastruktur.

Ausführlich analysiert werden im Folgenden die konkreten Gefährdungen, denen sowohl die OSCI-Infrastrukturdienste, OSCI-Gateways zu Systemen des Anwenders als auch die OSCI-Client-Anwendungen eines der beiden Kommunikationspartner ausgesetzt sein können. Bei allen Szenarien wird von einem unsicheren Transportnetz ausgegangen, jedoch nicht von einer Kompromittierung von Hard- oder Software des Senders oder Empfängers.

5.1 Gefährdungen und Risiken

Die OSCI-Transportarchitektur ist folgenden Gefährdungen ausgesetzt:

- **Arbeiten unter falscher Identität:**

  Eine falsche Identität kann auf Anwendungsebene durch Benutzung einer fremden Kennung vorgetäuscht werden, auf Netzwerkebene durch Manipulation der Netzadresse.

  Gelingt es, OSCI-Diensten oder der Fachanwendung eine falsche Identität vorzuspiegeln, besteht die Gefahr, dass auf fremde Daten zugegriffen sowie sämtliche Privilegien des rechtmäßigen Benutzers übernommen werden können. Die falsche Identität kann durch zwei Methoden angenommen werden:

  1. Bereits bei der Benutzerauthentisierung wird – beispielsweise unter Verwendung eines abgelaufenen bzw. ungültigen Authentisierungstokens – dem System ein falscher Benutzer vorgespiegelt. Dies kann beispielsweise auch durch Wiederverwenden von (verschlüsselten) OSCI-Nachrichten zu erreichen versucht werden (Replay-Attacken).
  2. Nach einer erfolgreichen Authentisierung wird die interne Repräsentation eines anderen Benutzers dauerhaft oder zur Durchführung einzelner Tätigkeiten angenommen. (Man-in-the-Middle-Attacken)

  Während die erste Methode die Kenntnis geheimer Information oder den Besitz privater Gegenstände voraussetzt und insofern von der eingesetzten Technik relativ unabhängig ist, beruht die zweite Methode auf der Ausnutzung technischer Schwächen des eingesetzten Systems, Informationen über eine erfolgreiche Authentisierung im Dialog fälschungssicher verwalten zu können.

  Eine Manipulation der Netzwerkadresse, sei es auf der Ebene der Übertragungs-, Netzwerk- oder Transportschicht, ist für den OSCI-Transport nicht relevant, sondern betrifft die Administration der Komponenten der OSCI-Infrastruktur.

- **Erweitern von Zugriffsrechten:**

  Gelingt es, die festgelegten Zugriffsrechte zu erweitern, können personenbezogene Daten in unzulässiger Weise verarbeitet oder fremde Daten zur Kenntnis genommen werden. Neben der Möglichkeit, Rechte durch Arbeiten unter falscher Identität zu erweitern, kann versucht werden, unter der eigenen Identität zusätzliche Rechte zu gewinnen und zunächst nur temporär gewährte Rechteerweiterungen dauerhaft zu sichern.

  Dieses Szenario bezieht sich zum einen auf die Gefahr, dass sowohl Bürger mit gültigen Authentisierungstoken als auch Außenstehende versuchen, die allgemein zugänglichen Web-Server der OSCI-Serverkomponenten zu attackieren und erweiterte Rechte auf der Plattform zu erhalten. Zum anderen können Administratoren versuchen, ihre privilegierten Rechte missbräuchlich zu verwenden.

  Bezüglich OSCI-Transport sind Ressourcen zu betrachten, die von OSCI für einzelne Kommunikationspartner zur Verfügung gestellt werden, beispielsweise Postfächer.

- **Lesen von Inhaltsdaten:**

  Inhaltsdaten können während ihres Transports oder während ihrer Nutzung von Unbefugten mitgelesen werden. Dadurch können vertrauliche Informationen in unbefugte Hände gelangen. Das Mitlesen von Daten kann auf zweierlei Weise geschehen:

1. Abhören von Geräten:

   Bildschirme, Tastaturen, Drucker und andere Geräte können aus gewisser Entfernung abgehört werden, wobei ihre kompromittierende Strahlung ausgewertet wird. Auf diese Weise können verarbeitete Daten oder Zugangsinformationen zur Kenntnis genommen werden. Der für ein elektronisches Abhören erforderliche Aufwand ist allerdings in der Regel relativ hoch.

2. Abhören von Übertragungsmedien:

   Übertragungsmedien bergen das Risiko des unbefugten Mitlesens der Daten. Interne Mitarbeiter können auf broadcast-orientierten Medien, die zur Übermittlung von Daten verschiedener Netzteilnehmer dienen, sämtliche übertragenen Daten zur Kenntnis nehmen. Externe können Strecken, die innerhalb von Gebäuden verlaufen oder diese verlassen, an beliebiger Stelle zwischen den Endpunkten abhören. Der dafür erforderliche Aufwand hängt wesentlich vom verwendeten Medium und dessen Verwendung ab. Besonders problematisch sind dabei die Fälle, bei denen das Mitlesen ohne merkliche Eingriffe geschieht und insofern nicht feststellbar ist.

- **Lesen von Kommunikationsdaten:**

  Nicht nur Inhaltsdaten können während des Transports oder lokal von Unbefugten mitgelesen werden. Auch besteht die Gefahr, dass Kommunikationsdaten ausgekundschaftet und wieder verwendet werden, um hierüber Zugriff auf geschützte Systemressourcen zu erhalten. Kommunikationsdaten bestehen bei OSCI-Transport u.a. aus dem Absender- und Empfängerzertifikat, das auch zur Nichtabstreitbarkeit der Kommunikation dienen kann.

  Gelingt es, Kommunikationsdaten in größerem Umfang zu ermitteln und zu analysieren, können Benutzerprofile erstellt und gegen die Interessen der Betroffenen ohne deren Kenntnis verwendet werden. Kommunikationsdaten stehen dem Intermediär in umfangreicher Weise zur Verfügung.

- **Verändern von Inhaltsdaten:**

  Daten können lokal oder während des Transports vom Autor bzw. Absender zum Empfänger verändert werden, wenngleich das Verändern von Daten während des Transports umfangreiche Rechte auf dem Transportsystem und entsprechende Kenntnisse voraussetzt.

- **Verändern von Kommunikationsdaten:**

  Gelingt es, Kommunikationsdaten zu verändern, können Kommunikationsvorgänge sowohl vom Autor bzw. Absender einer Nachricht als auch vom Empfänger abgestritten werden. Der Streitgegenstand kann sich auch auf den Zeitpunkt des Absendens einer Nachricht oder auf deren Zustellzeitpunkt beziehen.

  Rechte zum Verändern von Kommunikationsdaten können auch dazu benutzt werden, die Spuren einer Manipulation der Inhaltsdaten zu verwischen, so dass diese unentdeckt bleibt.

- **Stören der Infrastrukturkomponenten:**

  Gelingt es, die Komponenten der OSCI-Infrastruktur zu stören, kann die Dienstleistung nicht mehr in dem geforderten Umfang zur Verfügung gestellt werden. Dies kann bei termingebundenen Zustellaufträgen ein gravierendes Problem darstellen.

  Vor allem der OSCI-Dienst für Postfächer kann durch so genannte Denial-of-Service-Attacken lahm gelegt werden. Dabei wird eine Vielzahl von Nachrichtenpaketen an einen Server geschickt, der unter der Überlast seine Arbeit einstellt bzw. keine Rückmeldungen mehr in der gewünschten Form abgeben kann.

Hinsichtlich der mit den skizzierten Gefährdungen verbundenen Risiken und potentiellen Verursachern wird im Folgenden zwischen Bürgern mit gültigen Security Token, Verwaltung und Betreibern von OSCI-Infrastrukturdiensten sowie allgemeinen Internetnutzern differenziert, wobei sich Bürger mit gültigen Authentisierungstoken und allgemeine Internetnutzer durch die Art des Systemzugangs unterscheiden. Während allgemeine Internetnutzer in der Regel anonym versuchen können, ohne Zugriffsrechte Sicherheitslücken zu erkunden, sind Teilnehmer eines OSCI-Kommunikationsverbundes durch die mit OSCI 2 obligatorische Registrierung über die zugeordneten Authentisierungstoken identifizierbar und greifen rechtmäßig auf Teilmodule der OSCI-Infrastruktur zu.

Stellen Bürger mit gültigen Authentisierungstoken bzw. allgemeine Internetnutzer bereits bei kleineren Sicherheitslücken ein ernst zu nehmendes Risikogruppe dar, da in diesem Fall jeder Zugriff auf fremde Daten einen gravierenden datenschutzrechtlichen Verstoß bedeuten würde, ist dies bei Mitarbeitern der Verwaltung und des Betriebs von OSCI-Infrastruktursystemen nur bei sensiblen personenbezogenen Daten der Fall. Andererseits haben Betreiber von OSCI-Infrastruktursystemen in der Regel weit mehr Möglichkeiten, bestehende technische oder organisatorische Schwachstellen auszunutzen. Von welchen Personengruppen die jeweiligen Risiken ausgehen, beschreibt folgende Tabelle.

Personengruppe **Sicherheitsrisiken**	Bürger	OSCI-Infrastruktur Betreiber	Verwaltung	Internet-nutzer
Arbeiten unter falscher Identität	X	X	X	X
Erweitern von Rechten	X	X	X	
Lesen von Inhaltsdaten		X		X
Lesen von Kommunikationsdaten				X
Verändern von Inhaltsdaten		X		X
Verändern von Kommunikations-daten				X
Stören der OSCI-Infrastrukturdienste				X

Tabelle 4: Gefährdungen der Informationssicherheit von OSCI-Transport

5.2 Sicherheitsziele von OSCI-Transport

Zur Reduzierung der sich aus den in Kap. 7 erläuterten Gefährdungen ergebenden Sicherheitsrisiken verfolgt OSCI-Transport zahlreiche Sicherheitsziele. Es werden jedoch nicht alle Risiken abgedeckt. Einige der Risiken erfordern zu ihrer Reduzierung bzw. Vermeidung einen sicheren Betrieb von OSCI-Infrastruktursystemen sowie eines sicheren OSCI-Gateways für die Anbindung von Fachverfahren und Clients für die OSCI-Kommunikation.

Mit OSCI-Transport werden fünf Sicherheitsziele verfolgt:

- Schutz der Vertraulichkeit
- Schutz der Integrität
- Schutz der Authentizität
- Schutz der Nichtabstreitbarkeit

- Schutz der Zurechenbarkeit

Der Bewertung des durch OSCI erreichbaren Schutzes dieser Grundwerte wird der BSI-

Standard 100-2 „IT-Grundschutzvorgehensweise“ [AlgCat] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, 17. November 2008, http://www.bundesnetzagentur.de/media/archive/14953.pdf

[COMPKI] Common PKI Specifications for interoperable Applications, Version 2.0, 20 January 2009; http://www.common-pki.org/uploads/media/Common-PKI_v2.0.pdf

[BSI1002] zugrunde gelegt. Dieser definiert die drei Schutzbedarfskategorien *norma*l, *hoch* und *sehr hoch* anhand der möglichen Schadensauswirkungen:

Normal: Die Schadensauswirkungen sind begrenzt und überschaubar.

Hoch: Die Schadensauswirkungen können beträchtlich sein.

Sehr hoch: Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Die Problematik des sicheren Datentransport in verteilten Infrastrukturen bei unterschiedlichen Schutzbedürfnissen der Anwendungsszenarien ist im Detail auch dargestellt in [FHISST1].

5.2.1 Vertraulichkeit

OSCI ermöglicht eine vertrauliche Übertragung sowohl der Inhaltsdaten als auch der Kommunikationsdaten.

MUSS 41: Vertraulichkeit der Inhaltsdaten

> OSCI stellt eine Verschlüsselung der Inhaltsdaten von Target- zu Source-Applications zur Verfügung und kann somit die Vertraulichkeit der Inhaltsdaten während der Übertragung sowie gegenüber den OSCI-Infrastrukturdiensten gewährleisten („Ende- zu Ende-Verschlüsselung“). Dabei muss es optional möglich sein, auch die Dateinamen mitgeführter Attachments verschlüsselt zu übertragen.

MUSS 42: Vertraulichkeit der Kommunikationsdaten

> Die Kommunikationsdaten können auf der Strecke zwischen Sender und OSCI-Postfachdienst sowie zwischen OSCI-Postfachdienst und Empfänger verschlüsselt übertragen werden. Die Kommunikationsdaten werden von OSCI-Infrastrukturkomponenten gelesen und ggf. ergänzt.

In Bezug auf die Vertraulichkeit der Inhalts- und Kommunikationsdaten werden von OSCI die Schutzbedarfskategorien *normal* (keine Verschlüsselung), *hoch* und *sehr hoch* (asymmetrische Verschlüsselung) unterstützt.

5.2.2 Integrität

OSCI gewährleistet sowohl eine integre bzw. manipulationssichere Übertragung der Inhaltsdaten als auch der Kommunikationsdaten.

MUSS 43: Integrität der Inhaltsdaten

> Die Inhaltsdaten werden von Source Applications mit den privaten Schlüsseln der jeweiligen Autoren signiert. Verfälschungen werden ausschließlich vom Empfänger erkannt.

MUSS 44: Integrität der Kommunikationsdaten

> Die Kommunikationsdaten werden von dem Sender mit dessen privatem Schlüssel signiert. Verfälschungen werden von Knoten für die OSCI-Dienste bzw. vom Empfänger erkannt.

In Bezug auf die Integrität der Inhalts- und Kommunikationsdaten werden von OSCI die Schutzbedarfskategorien *normal*, *hoch* und *sehr hoch* unterstützt

5.2.3 Authentizität

OSCI garantiert sowohl eine Authentisierung der Benutzer, sofern diese auf OSCI-Dienste wie Postfächer zugreifen bzw. eine Quittung ausgestellt bekommen wollen, sowie eine Authentizität der Inhalts- bzw. Kommunikationsdaten.

Sofern eine Authentisierung der Benutzer benötigt wird, um beispielsweise den Zugriff auf Postfächer zu ermöglichen, werden von OSCI die Schutzbedarfskategorien *hoch und sehr hoch* unterstützt,

MUSS 45: Authentisierung der Benutzer

> Die Inhaltsdaten können von Source Applications mit den Zertifikaten der jeweiligen Autoren signiert werden. Die Signatur wird von den adressierten Target Applications einer Verifikationsprüfung unterzogen. Die übertragenen Inhaltsdaten sind authentisch, d.h. können einer Person zugeordnet werden, die im Besitz eines zum Zeitpunkt des Absendens gültigen Zertifikats ist. Dies sind im Falle der Inhaltsdaten die Autoren. Die Authentizität wird ausschließlich von der Target Application erkannt.

Die Authentizität der Daten bezieht sich auf die Authentizität sowohl der Inhalts- als auch der Kommunikationsdaten.

MUSS 46: Authentizität der Inhaltsdaten

> Die Inhaltsdaten können von Source Applications mit den privaten Schlüsseln der Autoren signiert werden. Die Signatur wird von den Target Applications einer Verifikationsprüfung unterzogen; ob das zugehörige Zertifikat gültig ist, wird von einem vertrauenswürdigen Dienst der Target Application geprüft. Diese Prüfung kann auch schon auf einem Knoten während der Nachrichtenübermittlung stattfinden, die Prüfergebnisse werden mit der Nachricht zum Empfänger übermittelt. Die übertragenen Inhaltsdaten sind authentisch, d.h. können einer Person bzw. Source Application zugeordnet werden, die im Besitz eines zum Zeitpunkt des Absendens gültigen Zertifikats ist. Dies sind im Falle der Inhaltsdaten die Autoren. Die Authentizität wird ausschließlich von der Target Application geprüft.

MUSS 47: Authentizität der Kommunikationsdaten

> Die Kommunikationsdaten können vom Absender mit dessen privatem Schlüssel signiert werden und in diesem Fall vom Empfänger einer Signaturprüfung unterzogen werden. Die übertragenen Kommunikationsdaten sind authentisch, d.h. können einer Serverinstanz oder Person zugeordnet werden, die im Besitz eines zum Zeitpunkt des Absendens gültigen Zertifikats ist. Dies ist im Falle der Kommunikationsdaten der Absender. Die Authentizität muss von allen OSCI-Kommunikationsknoten geprüft werden.

In Bezug auf die Authentizität der Inhaltsdaten werden von OSCI die Schutzbedarfskategorien *normal* (keine oder fortgeschrittene Signatur), *hoch* und *sehr hoch* (qualifizierte/akkreditierte Signatur) unterstützt.

In Bezug auf die Authentizität der Kommunikationsdaten wird von OSCI die Schutzbedarfskategorie *normal* (keine oder fortgeschrittene Signatur) unterstützt.

5.2.4 Nichtabstreitbarkeit

Nichtabstreitbarkeit bezieht sich sowohl auf die Autorenschaft einer Nachricht als auch auf den Kommunikationsvorgang.

MUSS 48: Nichtabstreitbarkeit der Autorenschaft

> Die Nichtabstreitbarkeit der Autorenschaft unterliegt den Anforderungen der Signaturgesetzgebung, u.a. [FormVAnpG], [JKomG]. Qualifizierte Signaturen müssen dort zum Einsatz kommen müssen, wo gemäß Verwaltungsrecht Schriftformerfordernis vorgeschrieben ist.
>
> Die Nichtabstreitbarkeit der Kenntnisnahme wird nicht durch Mittel von OSCI gesichert.
>
> Die Nichtabstreitbarkeit der Autorenschaft wird durch Signierung der Inhaltsdaten und deren Archivierung einschließlich der Signatur durch den Empfänger sichergestellt. Sofern mehrere Autoren existieren, sollten diese auch das Dokument gemeinsam signieren können. Dies setzt die Unterstützung von Mehrfachsignaturen voraus.

In Bezug auf die Nichtabstreitbarkeit der Autorenschaft werden von OSCI die Schutzbedarfskategorien *normal* (keine oder fortgeschrittene Signatur), *hoch* und *sehr hoch* (qualifizierte/akkreditierte Signatur) unterstützt.

MUSS 49: Nichtabstreitbarkeit des Kommunikationsvorgang

> Die Nichtabstreitbarkeit des Kommunikationsvorgangs unterteilt sich wiederum in zwei Unterziele:
>
> - Nichtabstreitbarkeit des Absendens:
>   Die Nichtabstreitbarkeit des Absendens stellt sicher, dass der Absender nicht erfolgreich bestreiten kann, eine bestimmte Nachricht verschickt zu haben.
> - Nichtabstreitbarkeit des Empfangs:
>   Die Nichtabstreitbarkeit des Empfangs stellt sicher, dass der Empfänger den Erhalt einer Nachricht nicht erfolgreich abstreiten kann. Mit dem Erhalt einer Nachricht ist allerdings nicht automatisch auch deren Kenntnisnahme verbunden.

Die Nichtabstreitbarkeit des Kommunikationsvorgangs wird realisiert durch Signierung der Kommunikationsdaten und die beschriebenen Quittungsmechanismen. Es steht im Ermessen der Endpunkte, Nachrichten und Quittungen längerfristig zu sichern.

In Bezug auf die Nichtabstreitbarkeit des Kommunikationsvorgangs wird von OSCI die Schutzbedarfskategorie *normal* (keine oder fortgeschrittene Signatur) unterstützt.

5.2.5 Zurechenbarkeit

Die Zurechenbarkeit setzt sich aus der Zugriffskontrolle, der Beweissicherung bzw. Protokollierung sowie aus der zeitlichen Bestimmtheit zusammen.

MUSS 50: Zugriffskontrolle

> Die Zugriffskontrolle hindert Benutzer und Prozesse, die für diese Benutzer tätig sind, lesenden oder schreibenden Zugriff auf Informationen oder Betriebsmittel zu erhalten, für die sie kein Zugriffsrecht haben, beispielsweise Postfächer oder Kommunikationsnachweise.

In Bezug auf die Zugriffskontrolle werden von OSCI die Schutzbedarfskategorien *hoch* und *sehr hoch* unterstützt.

MUSS 51: Beweissicherung/Protokollierung

Die Beweissicherung erkennt, dass Aktionen, ggf. auch von Unbefugten, ausgeführt worden sind.

In Bezug auf die Beweissicherung werden von OSCI die Schutzbedarfskategorien *hoch* und *sehr hoch* unterstützt.

MUSS 52: Zeitliche Bestimmtheit

Hierdurch wird erkannt, wann (Datum, Uhrzeit) eine Aktion stattgefunden hat.

In Bezug auf die zeitliche Bestimmtheit werden von OSCI die Schutzbedarfskategorien normal, *hoch* und *sehr hoch* unterstützt.

5.2.6 Zusammenfassung

Eine Übersicht über die Schutzbedarfskategorien, die bezüglich der jeweiligen Sicherheitsziele unterstützt werden, gibt folgende Tabelle:

Vertraulichkeit der Inhaltsdaten	normal	hoch	sehr hoch
Vertraulichkeit der Kommunikationsdaten	normal		
Integrität der Inhaltsdaten	normal	hoch	sehr hoch
Integrität der Verbindungsdaten	normal		
Authentizität der Benutzer	normal	hoch	sehr hoch
Authentizität der Inhaltsdaten	normal	hoch	sehr hoch
Authentizität der Kommunikationsdaten	normal		
Nichtabstreitbarkeit der Autorenschaft	normal	hoch	sehr hoch
Nichtabstreitbarkeit des Absendens	normal		
Nichtabstreitbarkeit des Empfangs	normal		
Zugriffskontrolle		hoch	sehr hoch
Beweissicherung		hoch	sehr hoch
Zeitliche Bestimmtheit	normal	hoch	sehr hoch

Tabelle 5: Sicherheitsziele und Schutzbedarfskategorien

6 Verzeichnisse

6.1 Tabellen

6.2 Abbildungen

6.3 Literatur

[AlgCat] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, 17. November 2008, http://www.bundesnetzagentur.de/media/archive/14953.pdf

[COMPKI] Common PKI Specifications for interoperable Applications, Version 2.0, 20 January 2009; http://www.common-pki.org/uploads/media/Common-PKI_v2.0.pdf

[BSI1002] BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise, Version 1.0, Dezember 2005, http://www.bsi.de/literat/bsi_standard/standard_1002.pdf

[CAdES] ETSI TS 101 903: CMS Advanced Electronic Signatures, V1.7.3 2007-01; European Telecommunications Standards Institute, http://webapp.etsi.org/exchangefolder/ts_101733v010703p.pdf

[FHISST1] Sicherer Datentransport in verteilten Infrastrukturen – Beispiele und Erfahrungen aus dem Bereich der Gesundheitstelematik; H. Adametz, O. Boehm, J. Caumanns, U. Kriegel, Fraunhofer Institut für Software- und Systemtechnik; Berlin, März 2007

[FormVAnpG] Gesetz zur Anpassung der Formvorschriften des Privatrechts und andere Vorschriften an den modernen Rechtsgeschäftsverkehr, Bundegesetzblatt, 18. Juli 2001, http://www.pca.dfn.de/bibliothek/sigg/germany/formanpassungsgesetz-2001-07-13.pdf

[JKomG] Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz –JkomG), Bundesgesetzblatt, 22. März 2005, http://217.160.60.235/BGBL/bgbl1f/bgbl105s0837.pdf

[OSCI] OSCI Transport 1.2, Juni 2002, http://www1.osci.de/sixcms/detail.php?gsid=bremen02.c.1160.de

[RFC4122] A Universally Unique IDentifier (UUID) URN Namespace, Proposed Standard, July 2005; The Internet Engeneering Task Force, http://tools.ietf.org/html/rfc4122

[SigG] Gesetz über Rahmenbedingungen für elektronische Signaturen,16.5.2001, http://bundesrecht.juris.de/sigg_2001/BJNR087610001.html

[SigV] Verordnung zur elektronischen Signatur, 16.11.2006, http://bundesrecht.juris.de/sigv_2001/BJNR307400001.html

[XAdES] ETSI TS 101 903: XML Advanced Electronic Signatures, V1.3.2 2006-03; European Telecommunications Standards Institute, http://webapp.etsi.org/action/PU/20060307/ts_101903v010302p.pdf

[XMeld] OSCI XMeld 1.3.2 Spezifikation, 28. Februar 2007, OSCI Leitstelle – das OSCI XMeld Projekt; http://www1.osci.de/sixcms/detail.php?gsid=bremen02.c.1413.de

6.4 Beteiligte

Folgende Personen – denen für ihr freiwilliges Engagement ausdrücklich gedankt wird - haben sich an der Erarbeitung der OSCI Transport Version 2 zeitweise oder während des gesamten Spezifikationsprozesses beteiligt.

Arbeitsgruppen Anforderungen, Architektur und Spezifikation

Jörg Apitzsch (bos), Ingo Beyer (PC-Ware), Thomas Biere (BSI), Oliver Böhm (Fraunhofer ISST), Nils Büngener (bos), Dr. Peter Dettling (IBM Deutschland), Jan Füssel (cit), Clemens Gogolin (PTB), Golo Hoffmann (procilon), Marc Horstmann (bos), Christoph Karich (Hochschule Harz), Daniel Koszior (PC-Ware), Harald Krause (Dataport), Arnold Külper (DVZ Mecklenburg-Vorpommern), Raik Kuhlisch (Fraunhofer ISST), Ralf Lindemann (bos), Dr. Klaus Lüttich (bos), Fabian Meiswinkel (Microsoft Deutschland), Lutz Nentwig (Fraunhofer ISST), Lars Nitzsche (procilon), Torsten Rienaß (procilon), Martin Schacht (Microsoft Deutschland), Thilo Schuster (cit),Janos Schwellach (bos), Prof. Dr.-Ing. Hermann Strack (Hoschule Harz), Dr. Hamed Tabrizi (bos), Lutz Vorwerk (IZN Niedersachsen), Sascha Weinreuter (cit), Mario Wendt (Microsoft Deutschland)

Entscheidungsinstanz

Mitglieder der obigen Arbeitsgruppen sowie:

Marcel Boffo (LDI Rheinland-Pfalz), Carlheinz Braun (DPMA), Christoph Damm (Staatskanzlei Sachsen), Steffen Düring (UBA), Joachim Gerber (INFORA), Reto Giger (Schweizer Post), Jens Habermann (LDS Düsseldorf), Renée Hinz (UBA), Wolfgang Klebsattel (DLR), Andreas Kraft (PBEG), Svea Lahn (HSH), Dr. Christian Mrugalla (BMI), Dr. Bernhard Paul (IBM Deutschland), Maren Pohl (HABIT), Anja Riekenberg (Hannit), Martin Rost (ULD Kiel), Alexander Spohn (ITDZ), Frank Steimke (OSCI Leitstelle), Andrea Steinbeck (HSH),Heiko Thede (DVZ Mecklenburg-Vorpommern), Joachim Wille (SAP Deutschland)