

- siehe Verteiler der Email -

Auskunft erteilt Herr Steimke

Zimmer

Tel. (0421) 361 - 59 195

Fax (0421) 361 – 56 26

E-Mail frank.steimke@finanzen.bremen.de

Datum und Zeichen
Ihres Schreibens

Mein Zeichen 36-4
(bitte bei Antwort angeben)

Bremen, 30. Mai 2006

Weiterentwicklung OSCI Transport Version 1.3
Abgestimmter Projektauftrag und weiteres Vorgehen

Sehr geehrte Damen und Herren,

der KoopA ADV hat die Bewertung der im Workshop vom 28.2.06 gemeinsam erstellten Anforderungen für die Version 1.3 von OSCI Transport zur Kenntnis genommen und die OSCI Leitstelle beauftragt, bis zur nächsten Sitzung am 21/22. September 2006 Ergebnisse vorzulegen.

Anbei übersenden wir Ihnen den Projektauftrag zur Fortschreibung des Protokolls OSCI Transport. Darin sind alle diskutierten Anforderungen an eine Fortschreibung von OSCI-Transport (z. T. mit Lösungsansätzen) beschrieben. Es ist dargestellt, welche dieser Anforderungen in der Version 1.3 berücksichtigt werden, und welche nicht. Die als „Soll“ klassifizierten Anforderungen werden nur berücksichtigt, wenn die Ressourcen dies zulassen. Weiterhin werden die Projektorganisation und die Zeitplanung für die Erarbeitung der Spezifikation dargestellt.

Wie auf dem ersten Abstimmungsworkshop zu den Anforderungen an die Version 1.3 bereits angekündigt, sollen die konkreten Vorschläge zur Umsetzung der Anforderun-

Dienstgebäude
Rudolf-Hilferding-Platz 1
Kto.1070 115000
(Haus des Reichs)
Kto. 29001565
28195 Bremen
Kto. 1090653

Briefkästen
Richtweg 25

Rövekamp 12

Eingang
Rövekamp12

(Hofeinfahrt)



Telefax
(0421) 361-5626

Bankverbindungen
Bremer Landesbank (BLZ 290 500 00)

Landeszentralbank (BLZ 290 000 00)

Sparkasse Bremen (BLZ 290 501 01)

gen zu den im Projektauftrag genannten Themenschwerpunkten möglichst in Arbeitsgruppen erarbeitet werden. Wir würden uns sehr freuen, wenn Sie sich daran beteiligen würden.

Wir möchten Sie daher bitten uns **bis zum 7. Juni 2006** mitzuteilen, ob Sie sich als „Kümmerer“ für einen der benannten 6 Themenschwerpunkte oder durch Zuarbeit zu einzelnen Punkten an der weiteren Erarbeitung der Spezifikation beteiligen werden. Bitte setzen Sie sich hierzu mit Herrn Apitzsch direkt in Verbindung, der von der OSCI Leitstelle als Koordinator und Editor für OSCI Transport 1.3 beauftragt ist. (Email Adresse: japitzsch@bos.bremen.de). Beachten Sie bitte, dass ein Stimmrecht bezüglich der erzielten Ergebnisse aktive Mitarbeit an der Erarbeitung von OSCI Transport 1.3 bedingt.

Bitten teilen Sie uns kurzfristig auch mit, ob Sie den 11. Juli 2006 (oder alternativ den 12. Juli) als Termin für einen weiteren Workshop zur Abstimmung einer ersten Arbeitsversion der Spezifikation wahrnehmen können.

Mit freundlichem Gruß

i. A. Steimke

Anlage: Projektauftrag, Fassung vom 29. Mai 2006



Fortschreibung OSCI Transport zu Version 1.3

Projektauftrag

Status: Version 1.0, Final

OSCI Leitstelle

Bremen, 29. Mai 2006

INHALT:

1	Vorbemerkung	2
2	Projektziel	3
3	Anforderungen zur Fortschreibung von OSCI Transport.....	4
3.1	Allgemeine Anforderungen.....	5
3.2	Adressierung.....	10
3.3	Kommunikation, Nachrichtenhandling	14
3.4	Öffnung für weitere Zertifikatstypen, Referenzen zu den Lokationen der Applizierung im Content	18
3.5	Erweiterung des Laufzettels.....	20
3.6	Content Container, Attachments	24
4	Projektabwicklung.....	28
4.1	Projektorganisation	28
4.2	Zeitplanung	29
5	Abbildungs- und Tabellenverzeichnis	30

1 Vorbemerkung

Das im Rahmen des MEDIA@komm-Projektes entwickelte Kommunikationsprotokoll OSCI wurde im Juni 2002 in der Version vorgelegt. Die Ziele von OSCI Transport sind fixiert in dem Dokument „OSCI Transport 1.2 – Entwurfsprinzipien, Sicherheitsziele und –mechanismen“¹.

OSCI Transport wird seither in einer ständig zunehmenden Anzahl von E-Government Vorhaben der öffentlichen Verwaltung für die sichere, vertrauliche und rechtsverbindliche Kommunikation über das Internet eingesetzt. Als Basisinfrastruktur für die Umsetzung von OSCI Transport stellt der KoopA-ADV eine Implementierung des Protokolls - die „OSCI-Bibliothek“ - zur Verfügung. Sie wird in Java- und .NET-Technologie herausgegeben; ihr Einsatz in OSCI-Transport-Implementierungen stellt die Interoperabilität solcher Implementierungen sicher. Basierend auf diesen Bibliotheken sind von unterschiedlichen Herstellern Produkte entwickelt worden; darüber hinaus gibt es Lösungen, die auf anderen Implementierungen des OSCI-Transport-Protokolls basieren, deren Interoperabilität mit den auf den KoopA-Bibliotheken basierenden Produkten nur durch entsprechende Tests abgesichert werden können.

Bereits in früher Phase der Umsetzung wurde dabei ersichtlich, dass die Spezifikation OSCI Transport 1.2² in einzelnen Punkten Interpretationsspielräume zulässt, auch wurden kleinere formale Unzulänglichkeiten in der Implementierungs- und Testphase aufgedeckt. Dies und eine Reihe von zusätzlichen inhaltlichen Anforderungen sowie Änderungsvorschläge fanden ihren Niederschlag in einer Korrigenda zur Spezifikation³, die im Juni 2004 veröffentlicht wurde.

Nachfolgend wurden in einer Reihe von Projekten weitere Anforderungen sichtbar, die z.T. durch eine weitere Korrigenda zu OSCI Transport 1.2 bedient werden könnten, zum größeren Anteil jedoch eine Erweiterung der Spezifikation nötig machen.

Diese Anforderungen wurden von der OSCI-Leitstelle gesammelt und systematisiert, Anwender von OSCI Transport haben die Möglichkeit, ihre Anliegen und Vorschläge auf einem dafür vorgesehenen Forum⁴ der OSCI-Leitstelle zu platzieren.

Im Februar 2006 fand ein erster Abstimmungsworkshop der Anwender von OSCI Transport zu den bis dahin vorliegenden Anforderungen statt. Bewertet wurde, welche der Anregungen mit einer Fortschreibung der Spezifikation im Jahr 2006 umgesetzt werden sollten; Eckpunkt der Bewertung ist hier vor allem auch, dass die Fortschreibung unter der Maßgabe der Wahrung der Abwärtskompatibilität zu OSCI Transport 1.2 zu gestalten ist.

Diese Bewertung wurde vom KoopA-ADV im März 2006 zu Kenntnis genommen; er beauftragte die Projektleitung mit der Umsetzung und Vorlage der Ergebnisse⁵ zu seiner Herbstsitzung 2006. Nach der Abnahme der Ergebnisse durch den KoopA ADV wird die neue Version von OSCI-Transport durch den KoopA-ADV herausgegeben werden. Das Bundesministerium des Innern wird die Herausgabe der neuen Version bekannt geben.

¹ siehe http://www1.osci.de/sixcms/media.php/13/osci_entwurfsprinzipien_1_2.2110.pdf

² siehe http://www1.osci.de/sixcms/media.php/13/osci_spezifikation_1_2_deutsch.pdf

³ siehe http://www1.osci.de/sixcms/media.php/13/2004-06-10_OSCI1.2-Korrigenda.pdf

⁴ die Foren rund um OSCI finden sich auf: <http://www.osci.de/phpbb/index.php>

⁵ KoopA-Beschluss Nr. 4 -3/2006

2 Projektziel

Das Projektziel besteht in der Erstellung folgender Dokumente:

1. Fortschreibung des „Anforderungsdokuments“ zu OSCI Transport

Das Dokument „OSCI Transport 1.2 – Entwurfsprinzipien, Sicherheitsziele und –mechanismen“ beschreibt die E-Government Szenarien, die sich daraus ergebenden Anforderungen und abgeleitet Entwurfsprinzipien in formalisierter Prosa. Dieses Dokument ist auf Basis der vorliegenden Anforderungen entsprechend der zugrunde liegenden modifizierten und zusätzlichen Szenarien und Randbedingungen fortzuschreiben.

Es ist darzustellen, welche der mit OSCI Transport 1.3 umgesetzten Mechanismen von OSCI 1.2-Implementierungen nicht bedient werden können.

Wie das Ausgangsdokument hat auch die Fortschreibung keinen normativen Charakter.

2. Die „Spezifikation OSCI-Transport“ in der Version 1.3

Dieses Dokument ist die Fortschreibung der formalen Spezifikation. Es gelten hier die Anforderungen des Projektauftrags zu OSCI Transport 1.2⁶ mit der Modifikation der Referenzierung relevanter Standards in ihrer aktuellen Version – dies gilt insbesondere für ISIS-MTT, welche seit März 2004 in der Version 1.1 vorliegt.

Dieses Dokument hat normativen Charakter.

3. Korrigenda für OSCI Transport 1.2

Im Laufe der Erarbeitung der Spezifikation OSCI Transport 1.3 könnte ersichtlich werden, dass zur Sicherung der Kompatibilität zu Implementierungen auf Basis der Version 1.2 eine Korrigenda zu dieser Version wünschenswert ist⁷. Diese Korrigenda soll geeignete Empfehlungen für 1.2-Implementierung formal festlegen.

Alle Dokumente werden in deutscher Sprache erstellt. Eine spätere Übersetzung ins Englische wird ggfs. durch die OSCI-Leitstelle veranlasst und ist nicht Gegenstand des vorliegenden Projektauftrags.

⁶ siehe http://www1.osci.de/sixcms/media.php/13/projekt%20osci-transport%201_2.2118.pdf, Seite 2, Abschnitt 1.1

⁷ betrifft aus heutiger Sicht z.B. ergänzende Fehlermeldungen und Reaktionsvorschriften

3 Anforderungen zur Fortschreibung von OSCI Transport

Die Aufstellung der Anforderungen in diesem Dokument basiert auf der Liste, die beim 1. Workshop zur Abstimmung der Anforderungen an OSCI Transport 1.3 am 28. Februar 2006 aufgestellt wurde. Die entsprechenden Einträge im Forum zu OSCI Transport 1.3 enthalten z.T. ausführlichere Darlegungen zum Hintergrund der jeweiligen Anforderungen und den zu erwartenden Nutzen bei Umsetzung. Die Nutzendarstellung zu den Anforderungen, die mit OSCI 1.3 bedient werden, ist in die Fortschreibung des „Anforderungsdokuments“ aufzunehmen.

Im vorliegenden Dokument sind zwischenzeitlich einige weitere Anforderungen/Anregungen aufgenommen worden, denen Change Requests zum „Elektronischen Gerichts- und Verwaltungspostfach“ (EGVP) zugrunde liegen; diese sind in den Tabellen entsprechend ausgewiesen. Die Anforderungen sind gruppiert in Kategorien, die die Auswirkungen auf die entsprechenden Teile von OSCI-Transport widerspiegeln:

Allgemeine Anforderungen, die gesamte Spezifikation u./o. Policies betreffend

- Adressierung von Kommunikationspartnern
- Kommunikation, Nachrichtenhandling
- Öffnung für weitere Zertifikatstypen, zusätzlich zu führende Attribute
- Erweiterung des Laufzettels um zusätzliche Prüfinformationen und Nachweise
- Festlegungen zu Inhaltsdaten und Attachments.

Ausgewiesen ist auch jeweils die Quelle oder der Kontext, aus dem die Anforderungen stammen sowie die Bewertung durch den 1. Abstimmungsworkshop.

Die Anforderungen sind weiter grob bewertet bzgl. der möglichen Umsetzungsstrategien, wobei dies lediglich als Anregung zu verstehen ist:

- Umsetzung der Anforderung erfordert rein textuelle Schärfung der aktuellen Spezifikation, Überarbeitung der Policies und des Rollenmodells; Handlungsbedarfe bzgl. der Implementierungen sind im Einzelfall zu überprüfen.
- Anforderung könnten auch als Korrigenda zur Spezifikation OSCI Transport 1.2 umgesetzt werden (i.d.R. impliziert dies auch eine Anpassung der Implementierungen).
- Anforderung ist nur umsetzbar mit einer Erweiterung des OSCI-Transport Schemas, d.h. auch in 1.2-Implementierungen funktional nicht abbildbar.
- Anforderung ist auf Gründen des Erhalts der Kompatibilität mit 1.2-Implementierung nicht umsetzbar.

Der Vollständigkeit halber sind auch solche Anforderungen noch in der Aufstellung enthalten, die nach erster Bewertung durch den Abstimmungsworkshop oder aus technischen Gründen nicht mit dieser Fortschreibung von OSCI Transport abgedeckt werden sollen. Sie sind entsprechend gekennzeichnet. Ihre Realisierung erfolgt ggfs. in einer Folgeversion von OSCI-Transport.

3.1 Allgemeine Anforderungen

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 28.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags ⁸
1	Validierbarkeit des Schemas	div.	Nicht schemakonforme Nachrichten müssen von Implementierungen abgewiesen werden. Achtung: Performance!!	Muss für 1.3; aufwändig	Beschränken auf neue 1.3-Header, da sonst Kompatibilität zu 1.2-Implementierungen gefährdet. Wenn insgesamt, wäre Voraussetzung eine Korrigenda auch für 1.2 und der Umsetzung in Implementierungen.	Schema- Erweiterung 1.3	Ja
2	Behebung von Interpretationsspielräumen	Leitstelle	Im Detail jeweils in Einzelpunkten	Muss für 1.3;	Textliche Präzisierung der Spezifikation	Text Spec. präzisieren	Ja
3	Ein sehr wichtiger und aktuell nicht ausreichend spezifizierter Punkt ist die Klarstellung von Fehlermeldungen, vor allem deren Weiterleitung „Passiver Client -> Intermediär -> Client“. Derzeit ist z.B. unklar, ob „Interner Fehler beim Supplier“ bedeutet dass es sich um einen internen Fehler des Intermediärs (in der Supplier-Rolle) handelt, oder um einen Fehler beim passiven Client.	MediaKomm Esslingen		Muss für 1.3 Aufwand gering;	Erweiterung Fehlercodes für 1.3-Funktionalitäten auf jeden Fall nötig; diese konkrete Anforderung bedingt auch eine Korrigenda für 1.2 !	Erweiterung für 1.3 Korrigenda Text Spec. u. Implementierung 1.2	Ja

⁸ Kategorien: Ja (muss); Nein (nicht in 1.3); Soll (falls weitere Prüfung positiv und die Projektressourcen ausreichen); Neu: Anforderung wurde nach dem 28.2.06 eingereicht

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 28.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
4	Unterstützung allgemeiner XML-Signaturen: wünschenswert wäre eine Möglichkeit, nicht-OSCI XML-Signaturen (d.h. isoliert erstellte XML-Signaturen von Inhaltsdaten, die keine Elemente und Namensräume des OSCI-Spezifikation, insbesondere der Content Container enthalten) zu transportieren und zu prüfen. Hierzu gehört auch die Prüfung der beteiligten Zertifikate durch den Intermediär.	MediaKomm Esslingen	Sache der Implementierung eines Produkts, auf Transportebene können beliebige Zertifikate eingestellt werden. Es fraglich ob dann alle Signaturen geprüft werden können. ToDo: Prüfung im Kontext exklusiver Kanonisierung	OSCI nicht überlasten; wird nicht als so vordringlich bewertet			Nein
5	Unterstützung von CMS-Signaturen: Man sollte in Erwägung ziehen, mit OSCI den Transport von PKCS #7 Signaturen in Attachments zu ermöglichen. Diese Signaturen sollen soweit möglich an der OSCI-Infrastruktur teilnehmen; hierzu würden unter anderem die Prüfung der Signatur durch die Client-Implementierung und die Prüfung der beteiligten Zertifikate durch den Intermediär gehören.	MediaKomm Esslingen	Produkteigenschaft ? Problem hier: man fordert von Implementierungen (auch im Kontext mit vorhergehender Anforderung), alle möglichen Signaturformate parsen zu können – ggf. dann auch zu erstellen?	Nützlich; aber nicht gefordert von Implementierungen	Hinweis in Spezifikation (ggf. Anhang), dass hier benutzte Zertifikate in Transportebene eingestellt werden sollten, um OSCI-Infrastruktur auszunutzen (Validierung durch Intermediär) - aber nicht gefordert von Implementierungen! Siehe auch: 1.3-Container für Zertifikate mit zweiter Referenz zum Content, wo diese verwendet wurden	Korrigenda Text Spec. für 1.2	Nein

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 28.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
6	Zweckmäßig wäre eine Klarstellung, wie Nachrichten zu erkennen sind, d.h. dass der Typ einer Nachricht eindeutig in der Spezifikation durch ein kennzeichnendes Attribut oder ein Tag an einer einheitlichen Stelle in der Nachricht festgeschrieben wird	MediaKomm Esslingen	Die aktuelle Erkennung and xsi:schemaLocation ist nicht wirklich mit etablierten Internet-Standards vereinbar, andererseits ist die Erkennung anhand der Tags <storeDelivery>, etc. eigentlich zu aufwendig, da diese, je nach Typ, an verschiedenen Stellen auftreten.	Muss für 1.3; Aufwand gering	Für 1.2 möglich: Attribut im SOAP-Envelope; da in der aktuellen OSCI-Bibliothek zusätzliche Attribute nicht geparkt werden, wäre Interoperabilität mit laufenden Implementierung gesichert Weiter: Erweiterung für neue 1.3-Nachrichtentypen	Als Korrigenda zu 1.2 möglich; In jedem Fall ToDo für 1.3	Ja
7	MIME-Konformität	MediaKomm Esslingen	Die Spezifikation sollte fordern, dass (1) alle Ende-zu-Ende MIME-Header (z.B. Content-Type, Content-Description, jedoch nicht Transport-spezifische Header wie Content-Encoding) auf dem ganzen Transportwert (Client-Intermediär-Client und zurück) vollständig transportiert und (2) seitens der Client-Implementierung zugänglich sein müssen.	Muss für 1.3 Aufwand mittel (?)	Mehr Schärfe der Spezifikation an dieser Stelle.	Als Korrigenda zu 1.2 möglich; In jedem Fall ToDo für 1.3	Ja

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 28.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
8	Transport von Zertifikatsketten; OSCI sollte, ähnlich wie PKCS #7, die komplette Zertifikatskette der beteiligten Zertifikate übertragen, was vor allem die Zertifikatsprüfung einfacher, verlässlicher und im Einzelfall gar erst möglich macht.	MediaKomm Esslingen	Sollte optional sein, und dann auch als Kette gekennzeichnet. Zu welchen Zertifikaten der Kette sollen die Prüfergebnisse transportiert werden? Komplex bei verschachtelten Content Containern, Mehrfachsignaturen etc.	Erst nach Prüfung für 1.3; Wenn dann als Option in 1.3; Aufwand hoch wg. der festzulegenden Regeln. (BSI prüft)	Ketten können im X509Data-Element transportiert werden können (Spec. xmldsig); Intermediäre müssen darauf reagieren. Zusätzliche Rückmeldung.	Als Korrigenda zu 1.2 möglich	Soll
9	Festlegung Zeitstempelformat	bos, MediaKomm Esslingen	Zu präzisieren ist, worauf der Zeitstempel zu applizieren ist. Entsprechend auch für Inhaltsdatensignatur!	Muss für 1.3 Detaillierung erforderlich Aufwand mittel	Festlegung nach ETSI (bisher nur empfohlen), RFC 3161 Korrigenda 1.2 ?	Als Korrigenda zu 1.2 möglich	Ja
10	(Optionale) Aufnahme der Systemzeit in die Signatur der Inhaltsdaten	bos, Justizanwendungen		Muss für 1.3 Aufwand mittel	Präzisierung des Signaturelements Inhaltsdaten: „SignatureProperty“	Als Korrigenda zu 1.2 möglich	Ja

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 28.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
11	In bestimmten Szenarien ist die Kommunikation mit einem Intermediär nicht offen für beliebige Nutzer mit gültigen Verschlüsselungszertifikaten (wie in 1.2 gefordert), sondern beschränkt.	bos	Ggf. Fehlermeldung spezifizieren für den Fall, das Kommunikation nicht zugelassen wird oder Nachrichtentyp, der die Policies/AGB's eines Intermediärs dem Client bekannt macht.	Muss für 1.3 Aufwand gering	Anpassung der Entwurfprinzipien / Policies von OSCI Im Wesentlichen: Text zu den Policies überarbeiten	Als Korrigenda zu 1.2 möglich; In jedem Fall ToDo für 1.3	Ja
12	OSCI 1.2 gibt es Probleme mit den Namespace-Deklarationen. Die Prefixe sollten natürlich beliebig sein, die Kanonisierung, XML-Signature hat damit aber Probleme: die Signaturen werden ungültig.	bos	Problem der Abwärtskompatibilität; müsste zusätzlich oder optional sein.	Muss für 1.3 Prüfung wg. Abwärtskom- patibilität; müsste in 1.2 unterstützt werden, aufwändig in der Implemen- tierung	Wechsel auf exklusive Kanonisierung: nicht möglich bei Wahrung der Kompatibilität		Nein (nicht möglich)

Tabelle 1: Allgemeine Anforderungen

3.2 Adressierung

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 28.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
1	Die Spezifikation sollte so erweitert werden, dass es nicht zwingend notwendig erscheint, einen passiven Client über dessen physikalische URL zu adressieren. Das verursacht sowohl verwaltungstechnischen Aufwand (URLs können sich je nach System-Umgebung ändern) als auch sicherheitstechnische Probleme mit sich, da evtl. private Netzwerk-Adressen veröffentlicht werden müssen.	MediaKomm Esslingen	Siehe auch 4: Anschluss DVDV. Auflösung von URNs ist Sache einer Implementierung. Der Type dieses Attributs ist xsd:anyURI in OSCI 1.2	Muss für 1.3 Aufwand gering	Korrigenda 1.2: Spec. anpassen (schärfer formulieren). Fehlercodes anpassen.	Korrigenda 1.2	Ja
2	Ticket für ungerichteten Versand: Bei Versand von verschlüsselten Unterlagen zur Weiterbearbeitung innerhalb des Gesundheitswesens ohne genaue Kenntnis des Empfängers wird dem Patienten ein Ticket ausgehändigt, ein Schlüssel also, der es ihm ermöglicht, die verschlüsselten Daten für die Weiterbearbeitung durch Dritte freizugeben.	infora	Das scheint für OSCI 1.3 zu mächtig vom Szenario her.	Nicht in 1.3	Es wäre zu prüfen, ob ein solcher Mechanismus nicht auch in einigen E-Government-Szenarien (z.B. Justiz) sinnvoll ist und im OSCI-Protokoll vorgesehen werden sollte.		Nein

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 28.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
3	Führen des „Home Intermediary“: In verteilten Szenarien – und hier insbesondere auch den asynchronen – kann es wünschenswert sein, einem OSCI-Empfänger für die Adressierung der Antwortnachrichten nicht nur das Verschlüsselungszertifikat des Senders mitzuteilen, sondern auch URI und Verschlüsselungszertifikat des Intermediärs, auf dem ein Sender eines Requests die Antwortnachricht erwartet („Home-Intermediary“).	div.	Es ist zu spezifizieren, wie die Kommunikationsteilnehmer an den aktuellen Laufzettel kommen!	Muss in 1.3. Optionales Element; aufwändig;	Da innerhalb des OSCI 1.2-Headers eine entsprechende Erweiterung nicht möglich ist, wäre ein zusätzlicher Header zu spezifizieren, der diese Information aufnehmen kann, z.B.: from (Certificate, urn, IMed-cert., IMed-urn) to (Certificate, urn, IMed-cert., IMed-urn)	Schemaerweiterung 1.3	Ja

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 28.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
4	Anschluss Verzeichnisdienst für dynamische Gewinnung von Adressierungsdaten – DVDV für „Supplier“ und ggf. weitere für allgemeine Nutzer.	bos	Die Spezifikation eines solchen Verzeichnisdienstes und seiner Policies kann allerdings nicht Aufgabe des Transportprotokolls OSCI sein. Die Anforderungen dieses Szenarios sollten jedoch bewertet werden in Hinsicht auf die Sinnhaftigkeit eines zusätzlichen Nachrichtentyps in OSCI Transport 1.3 für die Abfrage solcher Verzeichnisse (UDDI/SAML?).	Verschoben; Konzept Verzeichnisdienst (OSCI-Adressbuch, Identity Server) ist zunächst zu entwickeln			Nein

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 28.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
5	<p>„NotificationHandler“ / Notification: In Diskussion sind Konzepte, die es erlauben Notifikationen über den Eingang von Nachrichten auf beliebigen Intermediären an die jeweiligen Empfänger zu senden. Diese Notifikationen enthalten die nötigen Adressierungsinformationen, um letztendlich einen OSCI-Abholauftrag für diese Nachrichten zu generieren.</p> <p>Diese Notifikationen können über OSCI-Nachrichten zur Verfügung zu stellen. Dies könnte über einen zentralen (ggf. auch föderierten) Intermediär geschehen, der allen Empfängern bekannt ist. Intention dieses Konzepts ist, dass alle möglichen Empfänger von OSCI-Nachrichten bei Abfrage auf Nachrichteneingang lediglich einen Intermediär kontaktieren müssen.</p> <p>An diesen Intermediär werden ausschließlich solche Notifikationsnachrichten geleitet.</p>	bos	Mai 06: BSI legt Wert auf erneute Prüfung!	Nicht für 1.3; Produktlösung	Dies könnten innerhalb der von OSCI 1.2 als spezifisch modellierter Inhaltsdatencontainer definiert werden oder alternativ in OSCI 1.3 wiederum als zusätzlicher Header. Diese Notifikationen wären direkt vom Sender einer Nachricht an den Notifikationsserver zu übermitteln (dann auch mit OSCI 1.2 möglich). Mögliche Variante für OSCI 1.3 wäre, dass der Intermediär des Senders, auf dem die Nachricht für den Empfänger persistiert wird, dem zu spezifizierenden „Notification“-Header die Informationen entnimmt, die zur Erstellung einer Notifikation an den Empfänger benötigt werden. Im Falle Notifikation über OSCI würde also ein Intermediär direkt eine Nachricht – eben diese Notifikation – an einen weiteren Intermediär senden, der in der Spezialrolle „Notifikationsserver“ ist.	Schemaerweiterung 1.3, Erweiterung Rollenmodell	Nein (bisher!)

Tabelle 2: Anforderungen zur Adressierung

3.3 Kommunikation, Nachrichtenhandling

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 18.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
1	GetMessageld-Aufträge sollten mehrere MessageIDs auf einmal einholen können.	bos	Als Erweiterung des Dialoglnit; interessant! Abwärtskompatibilität muss bewertet werden	Wünschenswert für 1.3; Alternative zu 3.3, Punkt 2 Aufwand mittel	Neues Auftragspaar im 1.3-Header; Vorschlag 3.3, Punkt 2 ist evt. vorzuziehen. Könnte optionaler Teil einer Implementierung sein.	Erweiterung Spec. 1.3	Ja
2	Beim Versenden von Nachrichten wird in einem extra Roundtrip erst eine Message-ID abgeholt bevor die Nachricht verschickt wird. Dadurch reduziert sich der mögliche Durchsatz erheblich weil sich der Propagation-Delay pro Nachricht verdoppelt (4*w statt 2*w)	SAP	MessageID müsste optional sein; Verhinderung Mehrfacheinreichung ist bei explizitem Dialoglnit durch die DialogID gesichert; alte Mimik auf jeden Fall erhalten für die Falle, wo die MessagID in den signierten Content aufgenommen werden soll. Bei implizitem Dialoglnit ist Verhinderung der Mehrfacheinreichung nicht gesichert.	Wünschenswert für 1.3; Alternative zu 3.3, Punkt 1 Kann wg. Abwärtskompatibilität nur Option in 1.3 sein, eher aufwändig	Der Sender (Client) nummeriert seine Nachrichten durch und erhält eine Empfangsbestätigung, welche dann die eindeutige Message-ID enthalten kann. Alternativ könnte der Client auch einfach eine GUID generieren und als Message-ID vorgeben. Mit seiner Quittung würde der Intermediär dann den erfolgreichen Empfang und damit die Gültigkeit der GUID bestätigen. MessageID optional; wenn nicht vorhanden, greift diese MIMIK (IMed vergibt dann); ggf. Vorgaben zum Aufbau einer MessageID festlegen. Entsprechende Ausformulierung im Text zur Spec. 1.3	Erweiterung Spec. 1.3	Ja

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 18.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
3	Erweiterung der Filtermöglichkeiten beim Laufzettel-Abholauftrag	div.		Hier nicht; Siehe Punkt 4	Oft gewünscht: Selektion nach Einträgen auf dem <subject>-Element ; Neues FetchProcessCard für 1.3; Vorschlag Tab 4, Punkt 2 vorzuziehen!	Erweiterung Spec. 1.3; Alternative auch Korrigenda zu 1.2 (gab es bereit einmal in diesem Punkt!	Ja (siehe nächste Zeile)
4	Neben dem subject-Tag wäre ein contentType-Tag für die ganze Nachricht wünschenswert	bos	Wenn dieses realisiert wird, kann 3 entfallen;	Muss für 1.3 Aufwand mittel	Header 1.3: Ggf. dann auch neuer Nachrichtentyp zur Selektion von Laufzetteln / Nachrichten über dieses Element; Name wie contextCategory ggf. besser	Erweiterung Spec. 1.3;	Ja
5	Es wäre evtl. sinnvoll, wenn eine Kommunikation möglich wäre, ohne im vorherigen Besitz der jeweiligen (Transport-) Zertifikate zu sein. (sowohl Client -> Intermediär und eigentlich auch Intermediär -> Supplier)	MediaKomm Esslingen	Dies erleichtert gerade Test-Szenarien, wo es darauf ankommt, Transport-Verschlüsselung an sich zu testen, der Ursprung bzw. das Vertrauen in die (Test-) Zertifikate jedoch unerheblich ist.	Soll für 1.3 Aufwand gering	Neues Diaognit in 1.3: Dialognit liefert erst das Zertifikat des Intermediärs. Achtung: Ist-Zustand in 1.2 auf der Strecke Sender-> IMed!	Handlungsbedarf?	Soll
6	Einführung eines „Test“-Attributs für Gesamtnachricht	bos	Zur Erleichterung der Trennung von Test- und Produktionsszenarien	Nicht in 1.3	Schon in 1.2: „CustomHeader“ in Implementierungen ausnutzen	Handlungsbedarf?	Nein

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 18.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
7	Neuer Nachrichtentyp: „Löschen“ von Nachrichten- für den Sender das Löschen der von ihm bei einem Intermediär eingestellten Nachrichten, für den Empfänger das Löschen der von ihm abgeholten / ihm zugestellten Nachrichten	bos		Zu prüfen; Aufwand eher der juristische Abstimmungsbedarf, siehe auch 8,9	Neuer Nachrichtentyp Löschanforderung	Erweiterung Spec. 1.3;	Soll
8	Möglichkeit, senderseitig die Lebenszeit einer Nachricht festzulegen	bos	Es ist weiter festzulegen, wie Nachweise für ein evt. ausgelöstes Löschen derart parametrierter Nachrichten geführt werden müssen. Soll dies unabhängig vom Betreiber eines Intermediärs (bei diesem ggf. gezielt über Auswertung des Verarbeitungsprotokolls des Intermediärs) möglich sein, muss eine entsprechende Ergänzung des OSCI-Laufzettels in einem zusätzlichen Header-Element vorgesehen werden. Die Aufbewahrungsfristen solcher Laufzettel müssen Betreiber wiederum in ihren AGB's benennen.	Soll für 1.3, Aufwand eher der juristische Abstimmungsbedarf 8,9 vorklären	Aufnahme eines zusätzlichen Attributs „<TimeToLive>“ in den Nachrichtenheader, der es Sendern ermöglicht, die max. Lebensdauer einer Nachricht zu steuern. Hier wären vor allem auch die OSCI-Policies anzupassen und z.B. auch festzulegen wie sich ein Intermediär zu verhalten hat, falls die AGB's des Betreibers eine kleinere Vorhaltezeit von Nachrichten als die vom Sender verlangte vorsehen.	Erweiterung Spec. 1.3;	Soll

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 18.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
9	Möglichkeit, senderseitig den spätesten Zeitpunkt der Eingang einer Nachricht beim Empfänger festzulegen. Benötigt wird diese Funktion in Szenarien mit definierten Fristen für die Reaktion eines Empfängers.	bos	Diese Anforderung ist eher unkritisch, da sie nur einem Eskalations-Handling dient – anders als die beiden vorgenannten Anforderungen	Soll für 1.3, Aufwand eher der juristische Abstimmungsbedarf	Aufnahme eine zusätzlichen Attributs „<LatestDelivery>“ in den Nachrichtenheader, der es Sendern ermöglicht, den spätest möglichen Zeitpunkt des Eingangs einer Nachricht beim Empfänger zu steuern. Daran zu koppeln wäre eine Warnfunktion, wenn eine Nachricht bis zu einem bestimmten Zeitpunkt nicht abgeholt wurde.	Erweiterung Spec. 1.3;	Soll
10	Reliabilty	dataport	Es wird angezweifelt, ob das derzeitige http-Binding die Anforderungen an „Reliable Messaging“ erfüllt	Zu bewerten für eine Version > 1.3	Handshake-/ Quittierungsmimik Überarbeitung		Nein

Tabelle 3: Anforderungen zur Parametrierung von Nachrichten, Nachrichtentypen

3.4 Öffnung für weitere Zertifikatstypen, Referenzen zu den Lokationen der Applizierung im Content

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 18.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
1	Authentisierungszertifikate müssen auf Transportebene einstellbar sein und geprüft werden	bos	Das Element <NonIntermediaryCertificates> keine Erweiterungen zu.	Muss für 1.3; Aufwand gering	Es muss ein weiteres 1.3-Header-Element gebildet werden; dieses sollte alle Zertifikate aufnehmen, auch jene in Kopie, die im 1.2-Header gehalten werden	Erweiterung Spec. 1.3;	Ja
2	Zeitpunkt der Applizierung der Signatur muss in die Gültigkeitsprüfung eingehen	Bos, ERV-D Anwenderkreis	Zu klären ist: welchen Prüfzeitpunkt soll ein Intermediär dann nehmen: Eingangszeitpunkt Intermediär wie bisher oder dieser vom Client behauptete Signaturzeitpunkt? Siehe auch [Allgemeine Anforderungen], Nr. 10	Neue Anforderung!	Zusätzliches Attribut im 1.3-Zertifikatscontainer (wenn nicht die ganzen Signaturelemente der Inhaltsdaten auf Header-Ebene geführt werden, wie das BSI vorschlägt!)	Erweiterung Spec. 1.3;	Neu!
3	Attributzertifikate müssen auf Transportebene einstellbar sein und geprüft werden	bos	s. (1)	Muss für 1.3; Aufwand gering	s. (1)	Erweiterung Spec. 1.3;	Ja
4	Organisationszertifikate müssen auf Transportebene einstellbar sein und geprüft werden	div.	s. (1)	Muss für 1.3; Aufwand gering	s. (1)	Erweiterung Spec. 1.3;	Ja

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 18.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
5	Überarbeitung der Referenzen von Zertifikaten zu Signatur- und Verschlüsselungselementen in Inhaltsdatencontainern. Die Referenzen sollten bidirektional sein.	bos	Die Zuordnung von Zertifikaten zu ggf. beim Empfänger noch verschlüsselten ContentContainer ist nicht möglich. Weiterleitungsfunktion an jeweilige „Reader“ dadurch erschwert (es müssen immer alle Zertifikate mit übermittelt werden)	Nur, wenn auf Basis 1.2 machbar	Ist auf Basis 1.2 nicht machbar. Wenn komplettes 1.3-Headerelement für alle Zertifikate gebildet wird, kann hier ein zusätzliches Attribut für diese Referenzen aufgenommen werden.	Erweiterung Spec. 1.3;	Soll

Tabelle 4: Anforderungen zu Zertifikaten und zusätzlichen Attributen

3.5 Erweiterung des Laufzettels

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 18.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
1	Sicherung Zusammenhang Laufzettelinformationen (MessageID, Zeitstempel) und signierte Inhaltsdatencontainer auf Sender- und Empfängerseite	CC DS	Laufzettel / Signaturen müssen doppelt geführt werden (Abwärtskompatibilität)	Muss; Alternative.: Verschlüsselung für Sender (Nachweis); TSP Laufzettel auch über MsgDigest; Lösungen müssen bewertet werden	Signaturen auf 2. Laufzettel im extra Header führen; Intermediär appliziert Zeitstempel auf diesem. Verschlüsselung auch für Sender ist vermutlich die von bos bevorzugte Lösung, wäre auch auf Basis 1.2 schon machbar; Präzisierung in Spec: TSP IMed auch über Body+Attachments	Erweiterung Spec. 1.3;	Ja

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 18.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
2	Erweiterung der Validierungsinformationen zu Zertifikaten (gem. Anforderungen Langzeitarchivierung)	CC DS, bos, LDS NRW	Sollte – wenn überhaupt (großer Overhead) - optional sein; ggf. erst von Archivierungsservice anfordern (siehe Projekt ArchiSafe); ggf. nur Originalauskunft TC (OCSP oder XKMS?)	Als Option in 1.3 Format: XAdES Aufwand hoch! Es entscheidet auch immer erst ein Empfänger (nicht der Sender), welche Daten/ Nachrichten archiviert werden!	Inspection Report, der die kompletten Informationen gem. ETSI XAdES/CAAdES enthält	Erweiterung Spec. 1.3;	Nein
3	Der Laufzettel sollte Informationen über die jeweilige Kommunikationsart enthalten (store, forward, process)	MediaKomm Esslingen	Siehe auch [Allgemeine Anforderungen], Punkt 6 (Nachrichtentyp)	Soll in 1.3 Aufwand gering	Zweck noch zu präzisieren!	Erweiterung Spec. 1.3;	Soll
4	Separate Signatur des Laufzettel	BSI		Neue Anforderung!	Siehe auch nächster Punkt; welche Signatur dann nötig? In 1.2 verfügbar: FetchProcessCard zu einer MessageID, Response dann abspeichern	Erweiterung Spec. 1.3;	Neu!

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 18.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
5	Erweiterung Prüfinformationen zu Zertifikaten	bos, BSI	OSCP-Response zum Zertifikat muss dem Empfänger zur Verfügung gestellt werden können	Neue Anforderung!	Komplette XKMS-Validate-Response zu einem Zertifikat in den Laufzettel einstellen	Erweiterung Spec. 1.3;	Neu!
6	Erweiterung <InspectionReport> um Prüfinformationen zu Attribut-Organisations- und Authentisierungszertifikaten	bos	Im Kontext der Erweiterung der Validierungsinformationen zu bewerten, ob eher in den „neuen“ Laufzettel aufzunehmen	Muss in 1.3 Aufwand gering	Ließe sich im <InspectionReport> von 1.2 abbilden, allerdings liegen die Zertifikate selbst im Header 1.3. Im Kontext eines komplexeren <InspectionReport> für 1.3 dort abzubilden	Erweiterung Spec. 1.3;	Ja
7	Der Laufzettel sollte detailliertere Informationen über (nicht) erfolgreiche Zustellung enthalten, z.B. deren Anzahl. Momentan gibt es den Forwarding-Zeitpunkt und den Empfangs-Zeitpunkt, die können aber bestenfalls Auskunft darüber geben, ob je versucht wurde, die Nachricht zuzustellen und ob sie mindestens einmal erfolgreich angekommen ist. Vor allem relevant für asynchrone Nachrichten, da diese mehrfach sowohl erfolglos (d.h. ohne implizite Bestätigung) als auch erfolgreich abgeholt werden können.	MediaKomm Esslingen	Für asynchronen Fall wäre die Sinnhaftigkeit der Anregung noch einmal zu diskutieren!	Nicht in 1.3	Anzahl Zustellversuche im Laufzettel mitführen	Erweiterung Spec. 1.3;	Nein

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 18.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
8	Es sollte möglich sein, die Tatsache, dass eine Nachricht mit Transportsignatur versehen war, auf Empfängerseite abzufragen. Ebenso sollte das dazugehörige Zertifikat dem Empfänger zur Verfügung stehen. (In OSCI 1.2 ist die einzige Möglichkeit für Empfänger, die Herkunft der Nachricht gesichert zu erkennen, eine Signatur der Inhaltsdaten in der Rolle des Autors.)	MediaKomm Esslingen	Lösung könnte sein: Flag des Intermediärs mit Referenz auf das eingesetzte Sender-Zertifikat	Muss für 1.3; Aufwand mittel	Aufnahme in einen erweiterten Laufzettel (in 1.2 <ProcessCard>) für 1.3	Erweiterung Spec. 1.3;	Ja

Tabelle 5: Erweiterte Prüf- und Statusinformationen

3.6 Content Container, Attachments

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 18.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
1	Die MIME-Types von Attachments werden nicht aufbewahrt. Dadurch sind die Inhalte nicht mehr zuverlässig bestimmbar.	SAP		Muss in 1.3; Aufwand mittel	Spezifikation hier schärfer formulieren – in 1.2 machbar	Korrigenda zur Spec 1.2 ; Umsetzung in deren Implementierungen	Ja
2	Attachments sollten zusätzliches Name-Attribut haben, damit mehrere Dateien mit gleichem Namen verschickt werden können	bos		Muss in 1.3; Aufwand mittel	Ist im Kontext 5/6 mit zu lösen (Metacontainer zu Inhaltsdaten); kann prinzipiell auch in 1.2-Implementierungen umgesetzt werden	Korrigenda zur Spec 1.2 ; Umsetzung in deren Implementierungen	Ja
3	Dateiname sollten auch bei Intermediär nicht erkennbar sein	CC DS		Muss in 1.3; Aufwand mittel	Ist im Kontext 5/6 mit zu lösen (Metacontainer zu Inhaltsdaten); kann prinzipiell auch in 1.2-Implementierungen umgesetzt werden	Korrigenda zur Spec 1.2 ; Umsetzung in deren Implementierungen	Ja
4	Abwicklung Komprimierung der Inhaltsdaten durch die Transportschicht	Leitstelle	Eher Transfer-Encoding des Bindings? Zweifel auch, ob sich verschlüsselte Daten gut komprimieren lassen.	Nicht in 1.3; Sache der Applikation; Effekt nicht groß	Sender komprimiert einen oder alle Inhaltscontainer, Empfänger dekomprimiert. Das Ganze völlig transparent für die Beteiligten als Service der Transportschicht. Durch eindeutige Vorgabe der Algorithmen als Bestandteil der OSCI Spezifikation ist Interoperabilität sichergestellt. Klären: gibt es GZIP-Transformer für die Signatur?		Nein

Nr.	Anforderung	von	Anmerkungen	Bewertung Workshop 18.2.06	Mögliche Lösung, Stand 24.5.06	Kategorie Lösung	Gegenstand des Projektauftrags
5	„Meta“-Container (Inhaltsdatenebene) für spezifische Inhaltsdaten zur Abbildung der Funktionalität von „Clearingstellen“ (Weitertransport/-Bearbeitung von Nachrichten auf der Strecke Adressee->Reader)	AWV	War in der Diskussion zu OSCI 1.2 schon angerissen und verschoben worden. Hier wird im Fachlichkeit in Transportprotokoll geholt, sollte im jeweiligen Fachkontext (XJustiz etc.) gelöst werden.	Soll in 1.3; Aber sehr beschränkt: Auszeichnung Metacontaine r; wenn machbar Vorgaben allg. Meta- Container, enthält z.B. Aufzählung Nachrichten- bestandteile, Dateinamen Attachments etc.	Zweistufig: Genereller Part (z.B. Metadaten in Anlehnung DOMEA denkbar), Informationen zu den Bestandteilen der des ContentPackage); dazu dann fachspezifischer, der „out of Scope“ des Tranportprotokolls ist	Optionalen Teil der Spezifikation 1.3, prinzipiell auch in 1.2-Implementie- rungen umsetzbar	Soll

Nr.	Anforderung	von	Anmerkungen	Bewertung durch Workshop	Mögliche Lösung, Stand 24.5.06	Kategorie mögliche Lösung	Gegenstand des Projektauftrags
6	„Meta“-Container, der Metadaten für die Langzeitarchivierung enthält:	LDS NRW	Kontext ggf. zu XArchive/DOMEA?	Nicht Sache des Transportprotokolls Es entscheidet auch immer erst ein Empfänger, welche Daten/Nachrichten archiviert werden!	Angeregt werden Überlegungen für OSCI 1.3 in Richtung notwendiger Metadaten für eine entsprechende Ablage von OSCI-Nachrichten vorzunehmen. Konkret: Welche Informationen aus OSCI-Nachrichten können/müssen für eine Metadatenbereitstellung genutzt werden, ergänzt ggf. um Möglichkeiten weitere Informationen für eine elektronische Ablage, die für das Auffinden und inhaltliche Korrelieren von Nachrichten notwendig sind.		Nein
7	Spezifikation ContentContainer unabhängig von Transportschicht. Eine zeitlich versetzte Applikation von Signaturen und ggf. auch schon anzubringende Verschlüsselung für den Leser durch einen der Autoren macht es nötig, einen OSCI Content Container zu spezifizieren, der zunächst unabhängig der der OSCI-Nutzungsdatenebene – und damit dem Transport – ist.	bos	Unabhängig von OSCI Transport 1.3.	Muss in 1.3 Wichtig! Aufwand: zu prüfen	Das ist eine Festlegung, wie der ContentContainer mit Signatur, Verschlüsselung und außerhalb geführten Zertifikaten auszusehen hat.	Kann bereits in 1.2 abgebildet werden – unabhängig vom Transport	Ja

Nr.	Anforderung	von	Anmerkungen	Bewertung durch Workshop	Mögliche Lösung, Stand 24.5.06	Kategorie mögliche Lösung	Gegenstand des Projektauftrags
8	ContentContainer: XML-Content nicht Typ <any> sondern base64	bos	Es gibt immer wieder Probleme mit „plain“ XML-Contents	Soll in 1.3; de facto abwärtskompatibel Aufwand gering		Korrigenda 1.2, Spec. schärfer	Soll

Tabelle 6: Festlegungen zu Inhaltsdaten und Attachments

4 Projektentwicklung

4.1 Projektorganisation

Die Projektorganisation erfolgt in vier Ebenen:

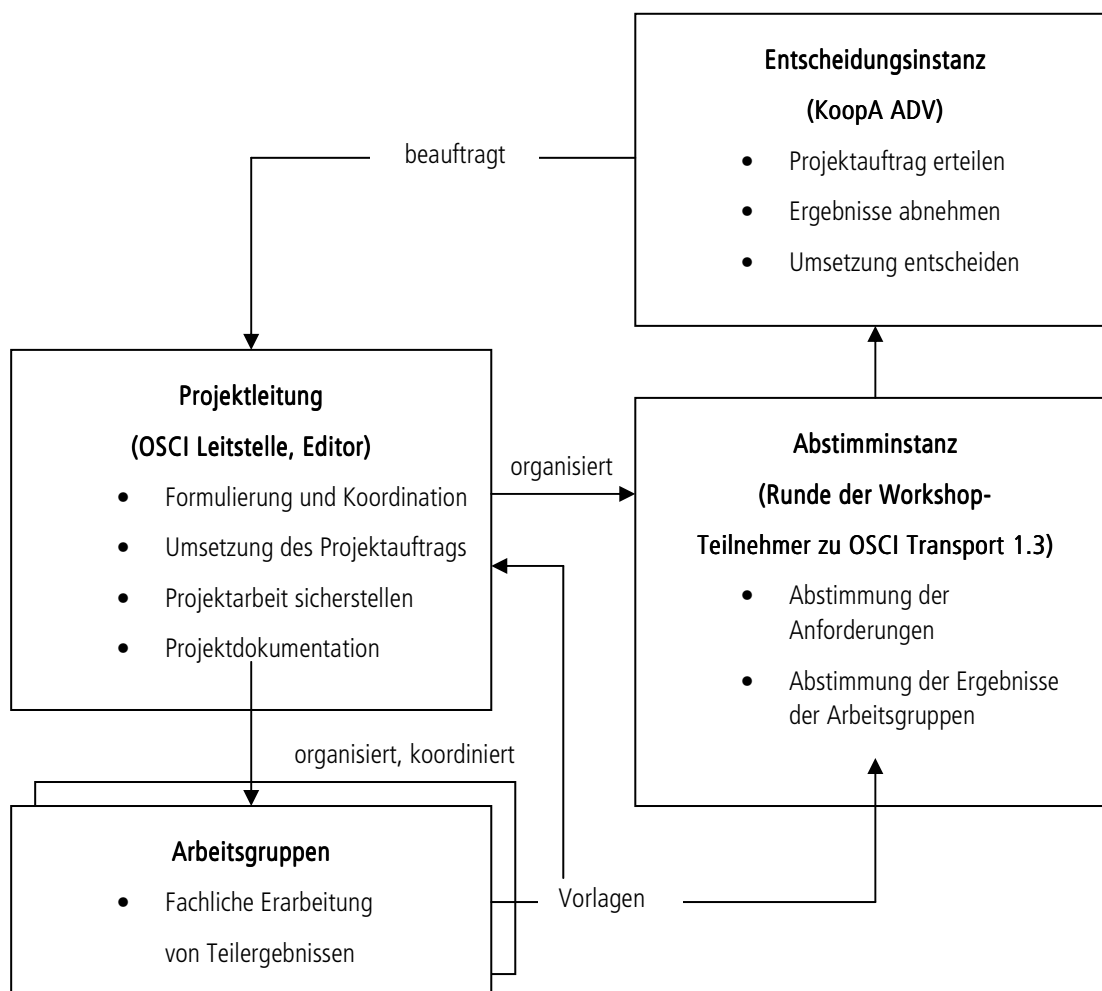


Abbildung 1: Projektorganisation

Ziel ist, zu jedem der in Kapitel 3 aufgeführten sechs Anforderungskategorien eine Arbeitsgruppe zu etablieren, die die jeweils erforderlichen Teile des Anforderungsdokuments und der Spezifikation erstellen. Die Projektleitung und der Editor übernehmen dabei die Koordination und unterstützen bei der Abstimmung und Verfeinerung der Teilergebnisse.

Die Gesamtabstimmung der Einzelergebnisse und letztlich auch der finalen Vorlage für die Entscheidungsinstanz obliegt der Runde der Workshopsteilnehmer zu OSCI Transport 1.3 als Abstimminstanz. Der Abstimminstanz ist vor allem auch für die Qualitätssicherung und die Prüfung der Realisierbarkeit zuständig.

Eine Teilnahme an den Workshops steht nach wie vor allen an OSCI Transport Interessierten offen; eine ergebnisorientierte Abstimmung der finalen Dokumente kann nur durch jene Vertreter in den Workshops erfolgen, die sich als Institution oder Person an den Arbeitsgruppen beteiligen – d.h. das Stimmrecht bedingt aktive Mitarbeit an der Erarbeitung von OSCI Transport 1.3.

Sollte keine einvernehmliche Abstimmung möglich sein, werden diese Punkte an den KoopA als Entscheidungsinstanz herangetragen.

4.2 Zeitplanung

Die abgestimmten Projektergebnisse müssen bis zum 1. September 2006 vorliegen, damit der KoopA ADV über diese auf seiner Herbstsitzung befinden kann.

Zur Erreichung dieses Ziels sind folgende Meilensteine in 2006 einzuhalten:

- (1) Kalenderwoche 22: Veröffentlichung dieses Projektauftrags auf www.osci.de; gleichzeitiges Mailing an den Verteiler, der der OSCI Leitstelle zu an OSCI Transport Interessierten vorliegt. Hier auch Aufforderung in die Community-Runde, spätestens bis zum 13. Juni Rückmeldung an die Projektleitung zu geben, zu welchen Positionen der Anforderungsliste und/oder Arbeitsgruppen konkrete Umsetzungsvorschläge eingereicht werden sollen bzw. aktive Mitarbeit in den Arbeitsgruppen möglich ist.
- (2) Kalenderwoche 24 bis 27: Erarbeitung der ersten Version der Projektergebnisse; jeweils Teilergebnisse zu den Einzelanforderungen; gesammelt als Arbeitsgruppenergebnisse.
- (3) Kalenderwoche 27, konkret 5. Juli 2006: Deadline für die Auslieferung der ersten Version bei der Projektleitung; anschließend Verteilung der Arbeitsergebnisse durch die Projektleitung an alle, die sich aktiv an der Erarbeitung von OSCI 1.3 beteiligen, Anforderungen in das Forum gestellt haben oder sich am 1. Abstimmungsworkshop teilgenommen haben.
- (4) 13. oder 14. Juli 2006: 2. Abstimmungsworkshop; Arbeitsgruppen stellen ihre Ergebnisse vor; Abstimmung der Lösungsansätze insgesamt, Klärung vor Alternativen und ggf. auch strittigen Punkten; Detailfestlegung weiteres Vorgehen
- (5) Kalenderwochen 29 bis 31: Erarbeitung der vorläufig finalen Version der Arbeitsgruppenergebnisse im Umlaufverfahren mit Unterstützung durch die Projektleitung
- (6) Kalenderwoche 32: Endredaktion durch die Projektleitung, Verteilung des Gesamtergebnisses an die Teilnehmer der Arbeitsgruppen und der Abstimmungsinstanz
- (7) Kalenderwoche 34: finaler Abstimmungsworkshop, falls nötig; ansonsten letzte Abstimmungen im Umlaufverfahren in KW 34/35.
- (8) 1. September 2006: Übergabe des Projektergebnisses an die Entscheidungsinstanz.

5 Abbildungs- und Tabellenverzeichnis

Abbildung 1: Projektorganisation	28
Tabelle 1: Allgemeine Anforderungen	9
Tabelle 2: Anforderungen zur Adressierung.....	13
Tabelle 3: Anforderungen zur Parametrierung von Nachrichten, Nachrichtentypen	17
Tabelle 4: Anforderungen zu Zertifikaten und zusätzlichen Attributen	19
Tabelle 5: Erweiterte Prüf- und Statusinformationen	23
Tabelle 6: Festlegungen zu Inhaltsdaten und Attachments.....	27