Fortschreibung des Protokolls

OSCI Transport:

Ergebnis 1. Abstimmungsworkshop zu den Anforderungen an Version 1.3

Workshop am 28. Februar 2006

OSCI Leitstelle

Bremen, 1. März 2006

Zusammenfassung der Ergebnisse durch: J.Apitzsch, bremen online services

Inhalt

1 Zusammenfassung der Workshop-Ergebnisse, weiteres Vorgehen

Der Workshop hatte primär zum Ziel, die vorliegenden Anforderungen zu bewerten in den Kategorien

- unverzichtbare Funktionalität
- Soll-Funktionalität, jedoch näher zu prüfen in Hinsicht auf Verhältnis Aufwand/Gewinn an Funktionalität
- wünschenswerte Funktionalität, Machbarkeits- /Aufwandsprüfung nötig
- Anforderung kann/soll in 1.3 nicht umgesetzt werden (bzw. ist ggf. keine an ein Transportprotokoll).

Weiter wurde versucht, den einzelnen Anforderungen bzgl. ihrer Umsetzung Aufwandsklassen (gering, mittel, hoch) zuzuordnen.

Die folgenden Abschnitte listen die gemeldeten Anforderungen, Lösungsvorschläge und Klassifizierungen durch die Workshop-Teilnehmer im Einzelnen auf.

Bzgl. der Bewertung und möglichen Umsetzung der Anforderungen konnte dieser erste Workshop angesichts der Menge der Positionen noch nicht ins Detail gehen, um das Ziel einer ersten Klassifizierung in der gegeben Zeit zu erreichen. Weitere inhaltliche Vertiefungen sollen in kleineren Fachteams erarbeitet werden.

Es sei hier angemerkt, dass die hier vorgelegte Klassifizierung der Anforderungen von den Workshopteilnehmern sehr einvernehmlich getroffen werden konnte. Die Einordnung in Aufwandsklassen ist in diesem frühen Stadium natürlich noch mit Vorbehalt zu sehen.

Bzgl. der im Anhang allgemein geschilderten und in einzelnen Anforderungen gesondert hervorgehobenen Problematik, die eine voll interoperable Gestaltung von OSCI Transport 1.3 zu 1.2 in sich birgt (siehe dazu Anhang), werden die Workshopergebnisse zunächst zu einem Summary zusammengefasst (Termin: Draft zur Abstimmung bis 10.3.06, finale Version bis 23.3.06). Es soll insbesondere dargestellt werden, welche Anforderungen und mögliche Lösungen mit welchen funktionalen Gewinnen einerseits und Aufwänden in Realisierung und/oder Betrieb andererseits verbunden sind.

Auf Basis dieses Papiers soll der KoopA ADV – möglichst auf der nächsten Sitzung Ende März 06 - über das generelle weitere Vorgehen entscheiden.

Anschließend werden Arbeitsteams konstituiert zu den Blöcken

- Generelle Anforderungen (jene aus den folgenden Abschnitten 2-5)
- Erweiterung/ Neugestaltung des OSCI-Laufzettels (Abschnitt 6)
- Anforderungen an Container für Inhaltsdaten, Umgang mit Attachments (Abschnitt 7).

In den jeweiligen Teams sollen die entsprechenden Passagen für das detaillierte Anforderungsdokument an OSCI Transport 1.3 incl. Empfehlungen zur Umsetzung erarbeitet werden. Die OSCI Leistelle übernimmt die Editor-Rolle zur Redaktion des Gesamtdokuments; letzteres soll wiederum dem KoopA ADV zur Verabschiedung vorgelegt werden.

Die Spezifikation OSCI Transport 1.3 incl. Schema-Definition soll nach Abnahme des abgestimmten Anforderungsdokuments durch den KoopA ADV erfolgen.

2 Allgemeine Anforderungen

Nr.	Anforderung	von	Lösungsvorschlag	Anmerkungen	Bewertung durch Workshop
1	Validierbarkeit des Schemas	div.		Nicht schemakonforme Nachrichten müssen von Implementierungen abgewiesen werden.	Muss für 1.3; aufwändig
2	Behebung von Interpretationsspielräumen	Leitstelle		Im Detail jeweils in Einzelpunkten	Muss für 1.3;
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	Erweiterung Fehlercodes	auch. als Korrigenda für 1.2 !	Muss für 1.3 Aufwand gering;
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	Siehe 7.7; OSCI nicht überlasten; nicht so wichtig

Nr.	Anforderung	von	Lösungsvorschlag	Anmerkungen	Bewertung durch Workshop
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	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!	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
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	Attribut im SOAP-Envelope	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
7	MIME-Konformität	MediaKomm Esslingen	Mehr Schärfe der Spezifikation an dieser Stelle	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 Siehe auch 7.1., 7.2.; Aufwand mittel (?)

Nr.	Anforderung	von	Lösungsvorschlag	Anmerkungen	Bewertung durch Workshop
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	Optional muss Kette transportiert werden können (Spec.); Intermediäre müssen darauf reagieren. Zusätzliche Rückmeldung.	Sollte optional sein, und dann auch als Kette gekennzeichnet. Zu welchen Zertifikaten der Kette sollen die Prüfergebnisse transportiert werden? Komplex bei verschachtelten ContentContainern, Mehrfachsignaturen etc.	Erst nach Prüfung für 1.3; Wenn dann als Option in 1.3 Aufwand hoch wg. der festzulegenden Regeln. H. Biere prüft im BSI
9	Festlegung Zeitstempelformat	bos, MediaKomm Esslingen	Festlegung nach ETSI (bisher nur empfohlen), RFC 3161	Zu präzisieren ist, worauf der Zeitstempel zu applizieren ist. Siehe auch Tab 5, Anforderung 1. Entsprechend auch für Inhaltsdatensignatur!	Muss für 1.3 Detallierung erforderlich Aufwand mittel
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	Anpassung der Entwurfprinzipen / Policies von OSCI	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
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	Wechsel auf exklusive Kanonisierung	Problem der Abwärtskompatibilität; müsste zusätzlich oder optional sein.	Muss für 1.3 Prüfung wg. Abwärtskompa-tibilität; müsste in 1.2 unterstützt werden, aufwändig in Implementierung (A)

3 Adressierung

Nr.	Anforderung	von	Lösungsvorschlag	Anmerkungen	Bewertung durch Workshop
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	Eine technische Möglichkeit, die bereits in verschiedenen Implementierungen realisiert ist, wäre es beispielsweise, URNs als Supplier-Adressen vorzusehen, die vom Intermediär per Konfiguration auf URLs abgebildet werden.)	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 Spec. Anpassen. Fehlercodes anpassen Aufwand gering
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	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.	Das scheint für OSCI 1.3 zu mächtig vom Szenario her.	Nicht in 1.3

Nr.	Anforderung	von	Lösungsvorschlag	Anmerkungen	Bewertung durch Workshop
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.	Da innerhalb des OSCI 1.2-Headers eine entsprechende Erweiterung nicht möglich ist, wäre ein zusätzlicher Header zu spezifizieren, der diese Information aufnehmen kann.	Es ist zu spezifizieren, wie die Kommunikationsteilnehmer an den aktuellen Laufzettel kommen!	Muss in 1.3. Optionales Element; äufwändig;
4	Anschluss Verzeichnisdienst für dynamische Gewinnung von Adressierungsdaten – DVDV für „Supplier" und ggf. weitere für allgemeine Nutzer.	bos	Kommunikationsteilnehmer müssten sich in einem solchen Verbund mit ihren Rollen, Zertifikaten und Adressierungsparametern in einem Verzeichnis registrieren; dieses Verzeichnis steht den Kommunikationspartnern als „Adressbuch" zur Verfügung, aus dem eine Sender die Adressierungs- und Verschlüsselungsinformationen entnimmt.	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?). Fraglich, ob das in 1.3 schon bewältigt werden kann, „Registrierungsserver" ist ein eigenständiges Projekt	Verschoben; Konzept Verzeichnisdienst (OSCI-Adressbuch, Identity Server) ist zunächst zu entwickeln

Nr.	Anforderung	von	Lösungsvorschlag	Anmerkungen	Bewertung durch Workshop
5	„NotificationHandler" / Notification	bos	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. 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. An diesen Intermediär werden ausschließlich solche Notifikationsnachrichten geleitet.	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 einer Notifikation an den Empfänger benötigt werden. Im Falle Notifikation über OSCI würde also ein Intermediär direkt eine Nachricht – eben diese Notifikation – an einer weiteren Intermediär senden, der in der Spezialrolle „Notifikationsserver" ist.	Nicht für1.3; Produktlösung

4 Kommunikation, Nachrichtenhandling

Nr.	Anforderung	von	Lösungsvorschlag	Anmerkungen	Bewertung durch Workshop
1	GetMessageId-Aufträge sollten mehrere MessageIDs auf einmal einholen können.	bos	Als Erweiterung des DialogInit interessant!	Abwärtskompatibilität mus bewertet werden	Wünschenswert für 1.3; Alternative zu Tab 4, Punkt 2 Aufwand mittel
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	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 müsste optional sein; Verhinderung Mehrfacheinreichung ist bei explizitem DialogInit 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 DialogInit ist Verhinderung der Mehrfacheinreichung nicht gesichert.	Wünschenswert für 1.3; Alternative zu Tab 4, Punkt 1 Kann wg. Abwärts-kompatibilität nur Option in 1.3 sein, eher aufwändig
3	Erweiterung der Filtermöglichkeiten beim Laufzettel-Abholauftrag	div.	Oft gewünscht: Selektion nach Einträgen auf dem <subject>-Element		Hier nicht; Siehe Punkt 4
4	Neben dem subject-Tag wäre ein contentType-Tag für die ganze Nachricht wünschenswert	bos	Ggf. dann auch neuer Nachrichtentyp zur Selektion von Laufzetteln / Nachrichten über dieses Element	Wenn dieses realisiert wird, kann 3 entfallen;	Muss für 1.3 Aufwand mittel
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	Dialoginit liefert erst das Zertifikat des Intermediärs	Dies erleichtert gerade Test-Szenarien, wo es darauf ankommt, Transport-Verschlüsselung an sich zu testen, der Ursprung bzw. das Vertrauen in die (Test-) Zertfikate jedoch unerheblich ist.	Soll für 1.3 Aufwand gering

Nr.	Anforderung	von	Lösungsvorschlag	Anmerkungen	Bewertung durch Workshop
6	Einführung eines „Test"-Attributs für Gesamtnachricht	bos		Zur Erleichterung der Trennung von Test- und Produktionsszenarien	Nicht in 1.3
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	Neuer Nachrichtentyp Löschanforderung		Zu prüfen; Aufwand eher der juristische Abstimmungs-bedarf, siehe auch 8,9
8	Möglichkeit, senderseitig die Lebenszeit einer Nachricht festzulegen	bos	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.	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 Abstimmungs-bedarf 8,9 vorklären A

Nr.	Anforderung	von	Lösungsvorschlag	Anmerkungen	Bewertung durch Workshop
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	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.	Diese Anforderung ist eher unkritisch, da sie nur einem Eskalation-Handling dient – anders als die beiden vorgnannten Anforderungen	Soll für 1.3, Aufwand eher der juristische Abstimmungs-bedarf
10	Reliabilty	dataport	Hanshake-/ Quittierungsmimik Überarbeitung	Es wird angezweifelt, ob das derzeitige http-Binding die Anforderungen an „Reliable Messaging" erfüllt	Zu bewerten für 1.4

5 Öffnung für weitere Zertifikatstypen, Referenzen

Nr.	Anforderung	von	Lösungsvorschlag	Anmerkungen	Bewertung durch Workshop
1	Authentisierungszertifikate müssen auf Transportebene einstellbar sein und geprüft werden	bos	Leider lässt das Element <NonIntermediaryCertificates> keine Erweiterungen zu. Es müsste eine weiteres Header-Element gebildet werden	Sieht letztlich natürlich sehr unschön aus im Schema!	Muss für 1.3; Aufwand gering
2	Attributzertifikate müssen auf Transportebene einstellbar sein und geprüft werden	bos	s. (1)	s. (1)	Muss für 1.3; Aufwand gering
3	Organisationszertifikate müssen auf Transportebene einstellbar sein und geprüft werden	div.	s. (1)	s. (1)	Muss für 1.3; Aufwand gering
4	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. Weiterleitungsfunkmtion an jeweilige „Reader" dadurch erschwert (es müssen immer alle Zertifikate mit übermittelt werden)	Nur, wenn auf Basis 1.2 machbar A

6 Erweiterung des Laufzettels

Nr.	Anforderung	von	Lösungsvorschlag	Anmerkungen	Bewertung durch Workshop
1	Sicherung Zusammenhang Laufzettelinformationen (MessageID, Zeitstempel) und signierte Inhaltsdatencontainer auf Sender- und Empfängerseite	CC DS	Signaturen auf 2. Laufzettel im extra Header führen; Intermediär appliziert Zeitstempel auf diesem	Laufzettel / Signaturen müssen doppelt geführt werden (Abwärtskompatibilität)	Muss; Alt.: Verschlüsselung für Sender (Nachweis); TSP Laufzettel auch über MsgDigest; Lösungen müssen bewertet
2	Erweiterung der Validierungsinformationen zu Zertifikaten (gem. Anforderungen Langzeitarchivierung)	CC DS, bos, LDS NRW	Inspection Report, der die kompletten Informationen gem. ETSI XAdES/CAdES enthält	Sollte – wenn überhaupt (grosser Overhead) - optional sein; ggf. erst von Archivierungsservice anzufordern (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!
3	Der Laufzettel sollte Informationen über die jeweilige Kommunikationsart enthalten (store, forward, process)	MediaKomm Esslingen		Siehe auch Tabelle 1, Punkt 7 (Nachrichtentyp) und Tabelle 3, Punkt 4 (ContentType)	Soll in 1.3 Aufwand gering
4	Erweiterung <InspectionReport> um Prüfinformationen zu Atrribut- Organisations- und Authentisierungszertifikaten	bos	Ließe sich im <InspectionReport> von 1.2 abbilden	Im Kontext der Erweiterung der Validierungsinformationen zu bewerten, ob eher in den „neuen" Laufzettel aufzunehmen	Muss in 1.3 Aufwand gering

Nr.	Anforderung	von	Lösungsvorschlag	Anmerkungen	Bewertung durch Workshop
5	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	Anzahl Zustellversuche im Laufzettel mitführen	Für asynchronen Fall wäre die Sinnhaftigkeit Anregung noch einmal zu diskutieren!	Nicht in 1.3
6	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 Flag des Intermediärs sein mit Referenz Auf eingesetztes Sender-Zertifikat		Muss für 1.3; Aufwand mittel

7 Content Container, Attachments

Nr.	Anforderung	von	Lösungsvorschlag	Anmerkungen	Bewertung durch Workshop
1	Die MIME-Types von Attachments werden nicht aufbewahrt. Dadurch sind die Inhalte nicht mehr zuverlässig bestimmbar.	SAP			Muss in 1.3; siehe ergänzend 2.8 Aufwand mittel
2	Attachments sollten zusätzliches name-Attribut haben, damit mehrere Dateien mit gleichem Namen verschickt werden können	bos	Ggf. in 5/6 mit zu lösen		Muss in 1.3; siehe ergänzend 2.8 Aufwand mittel
3	Dateiname sollten auch bei Intermediär nicht erkennbar sein	CC DS	Ggf. in 5/6 mit zu lösen		Muss in 1.3; In Ergänzung ergänzend 2.8; Aufwand mittel
4	Abwicklung Komprimierung der Inhaltsdaten durch die Transportschicht	Leitstelle	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.	Eher Transfer-Encoding des Binding? Zweifel auch, ob sich verschlüsselte Daten gut komprimieren lassen.	Nicht in 1.3; Sache der Applikation; Effekt nicht groß

Nr	Anforderung	von	Lösungsvorschlag	Anmerkungen	Bewertung durch Workshop
6	„Meta"-Container (Inhaltsdatenebene) für spezifische Inhaltsdaten zur Abbildung der Funktionalität von „Clearingstellen" (Weitertransport/-Bearbeitung von Nachrichten auf der Strecke Adressee->Reader)	AWV	Wenn dann zweistufig: Genereller Part (z.B. Metadaten in Anlehnung DOMEA denkbar), dazu dann fachspezifischer, der „out of Scope" Tranportprotokoll ist	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 Metacontainer; wenn machbar Vorgaben allg. Meta-Conatiner, enthält z.B. Aufzählung Nachrichten-bestandteile, Dateinamen Attachments etc.
7	„Meta"-Container, der Metadaten für die Langzeitarchivierung enthält:	LDS NRW	Angeregt werden Überlegungen für OSCI V1.3 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.	Kontext ggf. zu XArchive/DOMEA?	Nicht Sache des Transportprotokolls Es entscheidet auch immer erst ein Empfänger, welche Daten/Nachrichten archiviert werden!

Nr	Anforderung	von	Lösungsvorschlag	Anmerkungen	Bewertung durch Workshop
8	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	Das ist im Prinzip eine Festlegung, wie der ContentContainer mit Signatur, Verschlüsselung und außerhalb geführten Zertifikaten auszusehen hat.	Unabhängig von OSCI Transport 1.3. Siehe hierzu ergänzend auch Eintrag Tabelle 1, Punkt 4	Muss in 1.3 Wichtig! Aufwand: zu prüfen
9	ContentContainer: XML-Content nicht Typ <any> sondern base64	bos		Es gibt immer wieder Probleme mit „plain" XML-Contents	Soll in 1.3; de fakto abwärtskompatibel Aufwand gering

Anhang

Problematisierung der Kompatibilitätsanforderungen

Es ist vorrangig zu klären, wie im Detail die geforderte Kompatibilität von OSCI Transport 1.2 und 1.3 gesehen wird. Gefordert ist:

1. Implementierungen von 1.3 akzeptieren 1.2-Nachrichten und liefern die volle 1.2-Funktionaliät.
2. Implementierungen von 1.2 akzeptieren auch 1.3-Nachrichten und liefern basierend auf diesen die zugehörige 1.2-Funktionalität uneingeschränkt.

Die letzte Anforderung hat zur Folge, dass bestimmte Informationen innerhalb des Transportprotokolls in zwei Versionen eingestellt werden müssten. OSCI Transport 1.2 sieht als Erweiterungselement primär zusätzliche optionale Header-Elemente vor, während die Einzelstrukturen kaum Erweiterungen bzw. Varianten zulassen. Dies ist mit Blick auf Stabilität und Sicherheit sowie Komplexitätsminderung für Implementierungen bewusst so gestaltet worden.

Für die Umsetzung von OSCI Transport 1.3 müssten dann sowohl die Header-Elementen für OSCI 1.2 als auch die erweiterten Headern für die 1.3-Funktionalität bestückt werden. Wenn z.B. über die Anbindung von Verzeichnisdiensten wie DVDV für konkrete Kommunikationsszenarien dynamisch feststellbar ist, welche OSCI Transport Version die jeweiligen Knoten einer Kommunikationsstrecke bedienen können, ergäbe sich hieraus die Möglichkeit den der Kompatibilitätsforderung (2.) geschuldeten Overhead zu minimieren.

Weiter sollte bewertet werden, ob bestimmte Gruppen von Anforderungen an OSCI 1.3 in Form von „optional modules" gestaltet werden können, wie dies z.B. dem Konzept von ebXML zugrunde liegt. Nur Kernfunktionalitäten hätten dann einen „must"-Status. Bei dieser Variante wäre es ggf. auch möglich, eine 1.2-Kompatibilität optional zu machen.

Weiter muss geprüft werden, ob es nötig ist, in OSCI Transport 1.2 in Form einer Korrigenda ggf. zusätzliche Fehlermeldungen/Reaktionsvorschriften aufzunehmen, um die Kommunikation zwischen 1.2- und 1.3-Implementierungen sicherzustellen.

Liste der Workshopteilnehmer

1. Herr Weinreuter – CIT
2. Herr Büngener – BOS
3. Herr Bennewege – CITEQ
4. Herr Hoffmann – Procilon
5. Frau Riekenberg – HannIT
6. Herr Kremser – DZWB
7. Frau Pohl – Stadt Hagen
8. Herr Gerber – Infora
9. Herr Greska – Curiavant
10. Herr Schuster – CIT
11. Herr Damm – KOBIT / Sachsen
12. Herr Biere – BSI
13. Herr Steimke – OSCI-Leitstelle
14. Herr Apitzsch – BOS
15. Herr Krause – Dataport
16. Herr Meiswinkel - Microsoft
17. Herr Wendt - Microsoft
18. Herr Horstmann - BOS
19. Herr Dietrich – OSCI-Leitstelle