Projektauftrag *"OSCI—Transport: Version 1.2"*

Status: Final

Die PROJEKTLEITUNG

2. April 2002

```
Vers. 0.9 Draft20.3.02  fst ........Version zum Umlaufverfahren für die Entscheidungsinstanz.
                                    Muss bis 28. März verbindlich abgestimmt sein.
```

```
Vers. 1.0 Final26.3.02  fst ........Version nach Abstimmung der AG/AI am 28.3.03 bei ppi/HH, so-
                                    wie Abstimmung mit BSI am 28.3.02 in Göttingen.
```

OSCI wird im Rahmen des MEDIA@komm–Projektes für die öffentliche Verwaltung entwickelt. Der Auftraggeber ist der KOOPA – ADV, er formuliert und vertritt die Interessen der öffentlichen Verwaltung. Die OSCI - Leitstelle verantwortet und koordiniert die Entwicklung von OSCI.

Der Geltungsbereich von OSCI umfasst sowohl die Ebene der Inhaltsdaten, als auch die Ebene der Transport- und Sicherheitsfunktionen inklusive der digitalen Signatur. Die öffentlichen Verwaltung hat ein Interesse an Interoperabilität durch Standardisierung in beiden Bereichen. Die fachlich / inhaltlichen Anforderungen sind für diese beiden Ebenen aber ganz unterschiedlich, weshalb die OSCI Spezifikation in einen *"Teil A"* für die Transport- und Sicherheitsfunktionen und einen *"Teil B"* für die Inhaltsdaten aufgeteilt ist. **Projektgegenstand ist ausschließlich der Teil A von OSCI, der sich mit den Transport- und Sicherheitsfunktionen beschäftigt, sowie formale Aspekte der Inhaltsdaten, die für die inhaltsneutrale Verarbeitung der Inhaltsdaten wichtig sind.**

Die OSCI—Transport Spezifikation liegt in der Version 1.0 seit November 2000 vor. Auf dieser Basis wurden in Bremen Produkte implementiert und wichtige Erfahrungen im praktischen Einsatz gewonnen. Diese Erfahrungen führten zu neuen Anforderungen, die in einer Folgeversion der Spezifikation zu berücksichtigen sind.

OSCI—Transport basiert in wesentlichen Teilen auf internationalen Entwicklungen in zwei Bereichen:

- der Kryptographie (Algorithmen und Datenstrukturen für Verschlüsselung, Signaturen und Zertifikate) sowie ihrer Umsetzung in einschlägige Normen in Europa, insbesondere Deutschland (Signaturgesetze und -Verordnungen).
- XML und verwandte Technologien, wie sie vom W3C koordiniert werden.

Relevante Entwicklungen aus diesen Bereichen werden durch OSCI—Transport in geeigneter Weise konkretisiert und kombiniert. Dies führt zu einem leistungsfähigen Protokoll insbesondere für die Anforderugen des E – Government. In beiden Bereichen haben sich in den cirka 14 Monaten seit der Veröffentlichung von OSCI—Transport 1.0 erhebliche Fortschritte bei den einschlägigen Standards ergeben, die ebenfalls in einer Folgeversion der Spezifikation 1.0 zu berücksichtigen sind.

Schließlich haben unsere Erfahrungen in praktischen Projekten gezeigt, dass die OSCI—Transport Spezifikation in der vorliegenden Form nicht gut lesbar ist. Neben funktionalen Verbesserungen ist ein weiteres Projektziel die Konsolidierung und Verbesserung der Dokumentenlage.

1 Das Projektziel

Das Projektziel besteht in der Erstellung folgender Dokumente:

1 Das *"Anforderungsdokument"*.

Das Anforderungsdokument beschreibt E – Government Szenarien und formalisiert die sich daraus ergebenden Anforderungen an das zu spezifizierende Transportprotokoll OSCI—Transport 1.2. Lösungen werden in diesem Zusammenhang nicht beschrieben. Anforderungen, die für eine spätere Version vorgemerkt werden, werden ausdrücklich so gekennzeichnet. Die Anforderungen werden benötigt, um eine eindeutige, verifizierbare und unmissverständliche Beschreibung der umzusetzenden Konzeption zu erhalten. Die Anforderungen bilden die Grundlage für die Entwicklung der eigentlichen Spezifikation. Ferner soll in diesem Dokument auch explizit angemerkt werden, welche Anforderungen durch OSCI—Transport 1.2 nicht erfüllt werden (z.B. ein konkretes Payment-Verfahren).

Damit die Anwendungsszenarien auch von Nicht-Informatikern gelesen werden können, sind sie in formalisierter Prosa ausgeführt (unter anderem durch präzise Begrifflichkeiten). Das Anforderungsdokument hat keinen normativen Charakter.

2 Die *"Spezifikation OSCI—Transport"* in der Version 1.2

Das Dokument beschreibt präzise das OSCI—Transport Protokoll. Es dient als Grundlage für OSCI Implementierungen. Es beschreibt Lösungen für die im *"Anforderungsdokument"* genannten Anforderungen.

Die einzelnen Abläufe werden in formalisierter Prosa (u.a. präzise Verwendung von "muss", "kann", "soll", etc.) beschrieben und in geeigneter Weise durch UML - Diagramme ergänzt. Alle für eine Interoperabilität notwendigen Konkretisierungen und Festlegungen werden getroffen (zum Beispiel: Festlegung der Mindestanforderungen an konforme Anwendungen hinsichtlich Algorithmen, Schlüssellängen, Parametern etc.).

OSCI Datenstrukturen werden in Form von validen *XML Schema* Definitionen (entsprechend der *"XML Schema"* Recommendation des w3c vom 2. Mai 2001) notiert.

Soweit sinnvoll und notwendig, werden Signatur- und Prüfmechanismen gemäß *ISIS MTT* Version 1.01 vom 15. November 2001 beschrieben bzw. konkretisiert.

Sofern sinnvoll, werden (Fragmente von) XML - Dokumenten, die valide bezüglich der definierten Schemata sind, als erläuternde Beispiele in das Dokument aufgenommen.

Einschlägige Normen, Standards und sonstige relevante Dokumente (wie zum Beispiel *"XML digital signature"*) werden in der Regel nicht zitiert, sondern nur referenziert.

Das Spezifikationsdokument ist normativ.

3 Betriebsanforderungen und -empfehlungen

Nicht alle der im *"Anforderungsdokument"* (Dokument 1) genannten Anforderungen können durch das Übertragungsprotokoll OSCI—Transport gelöst werden. Zur Gewährleistung eines insgesamt sicheren Prozesses zwischen den Kommunikationspartners in einer OSCI Infrastruktur müssen Fragestellungen gelöst werden, die vom Übertragungsprotokoll unabhängig sind. Hierzu gehören zum Beispiel die PKI, die Visualisierung von Nachrichteninhalten, die sichere Auslieferung von Client - Komponenten und so weiter.

Dieses Dokument beschreibt ergänzende Massnahmen, um eine Infrastruktur aufzubauen, mit der unter Nutzung des Transportprotokolls OSCI—Transport die im *"Anforderungsdokument"* genannten Szenarien und Problemstellungen gelöst werden können.

Das Dokument hat keinen normativen Charakter.

Alle Dokumente werden zunächst in deutscher Sprache erstellt, in einem zweiten Schritt werden sie ins Englische übersetzt.[1]

1. Nicht bis Mai 2002, nicht unbedingt durch Mitglieder des Projektteams.

Das Projektziel dient der Umsetzung des Beschlusses 01-12-10 des KOOPA – ADV vom 13/14.12.2001 (Wintersitzung in Husum):

Der KoopA-ADV empfiehlt:

1 *Das im Rahmen des MEDIA@komm Projektes entwickelte Protokoll OSCI bietet die für E – Government notwendige Interoperabilität sowohl auf der Ebene der Inhaltsdaten, als auch auf der Ebene der Transport- und Sicherheitsfunktionen inklusive der digitalen Signatur. OSCI soll daher zu einem Standardprotokoll der öffentlichen Verwaltung weiterentwickelt werden und Anwendung finden, wenn im Rahmen der Realisierung von elektronischen Dienstleistungen Web-Services für offene Benutzergruppen im Bereich der medienbruchfreien Transaktionen angeboten werden.*

2 *Die OSCI Leitstelle ist verantwortlich für die Weiterentwicklung von OSCI. Sie führt entsprechende Projekte, insbesondere die bundesweite Abstimmung entwickelter OSCI-Modelle ("X....."; entsprechend XMeld), im Auftrag des KoopA-ADV durch. Sie stellt durch eine geeignete Projektorganisation sicher, dass die Beschlüsse des KoopA-ADV zur Umsetzung von E-Government realisiert werden. Im Rahmen einer Qualitätssicherung können auch kommerzielle Anbieter kommunaler Software beteiligt werden.*

3 *Vertreter des KoopA bilden die Entscheidungsinstanz für die Weiterentwicklung von OSCI.*

2 Ausgangspunkt der Projektarbeiten

Das Projektziel ist keine Neuentwicklung eines Protokolls, sondern es besteht in einer Fortschreibung und Konsolidierung bestehender Dokumente und Spezifikationen. Die Version 1.2 wird sich von der Version 1.0 wie folgt unterscheiden:

- Die Fortschreibungen einschlägiger Standards seit der Fertigstellung der Version 1.0 werden berücksichtigt;
- Es gibt funktionale Veränderungen, die mit den Erfahrungen in konkreten Projekten seit der Veröffentlichung der Version 1.0 begründet werden (zum Beispiel synchrone Transaktionen);
- Neben der Signatur nach *XML Signature* wird alternativ angestrebt, dass eine Signatur nach *ISIS MTT* möglich wird. Bis zu welchem Grad und in welchen Funktionalitäten OSCI—Transport bereits in der Version 1.2 ISIS-MTT kompatibel werden kann, muss als ein Projektergebnis erarbeitet werden.
- Die Dokumentenlage wird konsolidiert und insgesamt verbessert. OSCI—Transport wird für eine Internationalisierung vorbereitet.

Die folgenden Dokumente beschreiben die Ausgangslage:

1 Die OSCI—Transport Spezifikation in der Version 1.0 vom 30.11.2000

2 Das Dokument *"Sicherheit von OSCI"* der *datenschutz nord GmbH* vom Mai 2001

3 Das Kapitel *"Sicherheitsinfrastruktur für übergreifende, medienbruchfreie e-Government Anwendungen"* als Bestandteil des *"Kryptoleitfadens"* des BSI. Die aktuelle Version wurde auf der letzten Sitzung der *"AG KuS"* des KOOPA – ADV verabschiedet und wird mit der nächsten Version des Kryptoleitfadens veröffentlicht.

4 *"Katalog der Sicherheitsziele"* des BSI, Stand vom 28.3.03

3 Kernaspekte der Version 1.2 von OSCI—Transport

In dem folgenden Abschnitt werden die wesentlichen, charakteristischen Aspekte der nächsten Version von OSCI—Transport stichwortartig als Übersicht aufgeführt.

3.1 Das Einsatz - Szenario

OSCI—Transport ist entworfen für die sichere, nachvollziehbare und vertrauliche Kommunikation, insbesondere im Bereich E – Government. Zur Sicherstellung der Integrität und Authentizität von Nachrichten wird die elektronische Signatur genutzt.

Zusammen mit standardisierten Inhaltsdaten (OSCI Teil B) sichert OSCI—Transport die notwendige Interoperabilität für Kommunikationsvorgänge des E – Government und ermöglicht so die medienbruchfreien Weiterverarbeitung von Daten.

Der Einsatzbereich umfasst sowohl interaktive, synchrone Dialoge mit mehreren Nachrichten pro Session, als auch die asynchrone Kommunikation.

Kryptografische Mechanismen sichern die Integrität, Authentizität und / oder Vertraulichkeit der Nachrichten. Diese Mechanismen sind skalierbar, um OSCI—Transport auf die jeweiligen Einsatzbedingungen anzupassen (in der Minimalstufe: *"nicht vorhanden"*).

Ein Dialogkontext verhindert replay- und man-in-the-middle Angriffe.

Die Kommunikation mittels OSCI—Transport ist *nachvollziehbar* und zusammen mit dem Einsatz der digitalen Signatur *unbestreitbar*. Mittels Zeitstempelmechanismen läßt sich der Nachweis der Fristwahrung führen.

Die OSCI-interne Adressierung der Empfänger (natürliche Personen oder Verfahren) erfolgt anhand von X.509 Zertifikaten. Ein Mapping auf physikalische Adressen (IP-Adressen, URL etc.) wird im Dokument 3 *"Betriebsanforderungen und -empfehlungen"* geregelt. Ein Abholen von Nachrichten bedarf einer Authentisierung anhand von X.509 Zertifikaten[1].

OSCI bietet die Möglichkeit, Fremdformate zu *"tunneln"*. Für die Version 1.2 wird diese Möglichkeit in Hinblick auf *"große"* Datenvolumen optimiert.

3.2 Trennung der Nutzungs- und Inhaltsdaten

Die Nutz- und Inhaltsdaten (in der Terminologie des *Teledienstegesetzes* TDG) einer OSCI Nachricht sind getrennt, sie können kryptografisch unterschiedlich behandelt werden.

Die Nutzungsdaten einer OSCI Nachricht werden durch ein Intermediärsmodul verarbeitet. Ein Intermediärsmodul ist zwingender Bestandteil jeder Kommunikation nach OSCI—Transport. Es realisiert mindestens die Etablierung, Überwachung und den Abbau des Dialogkontextes.

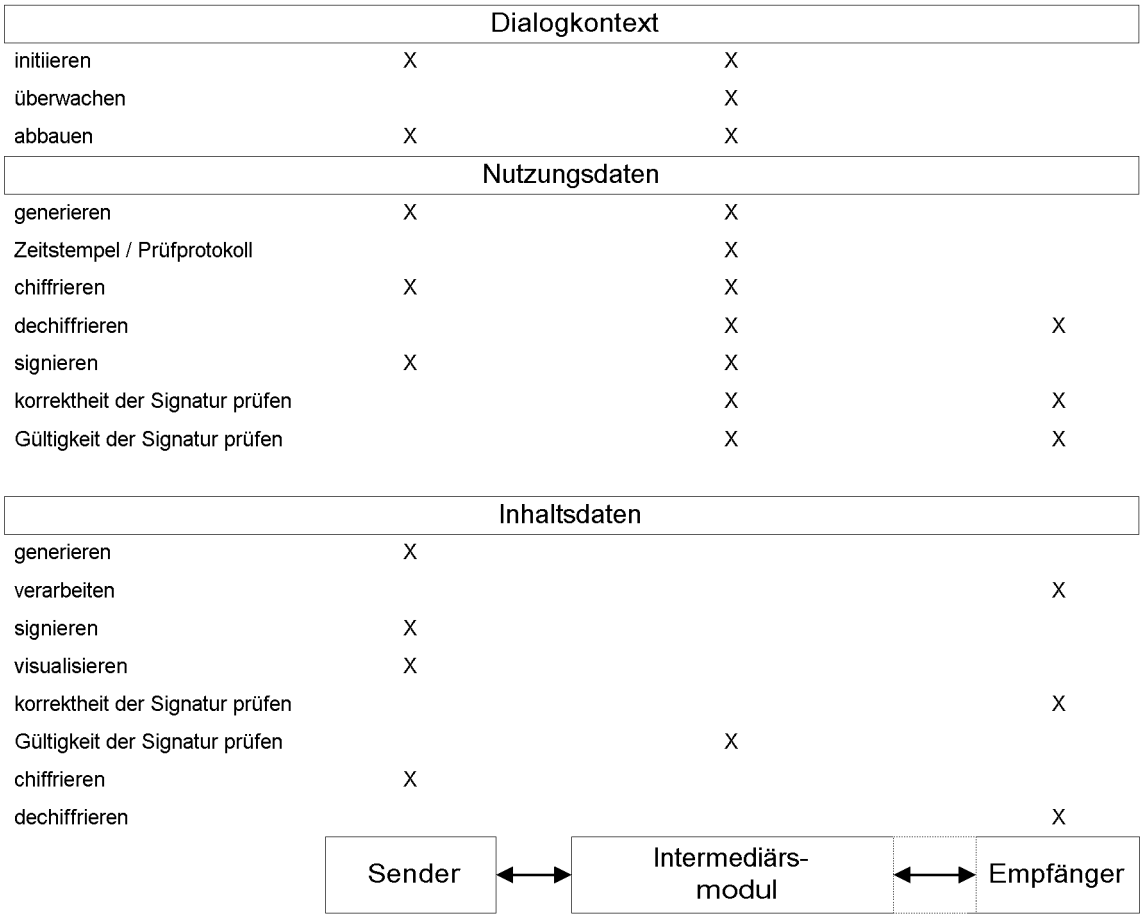
Die Inhaltsdaten sind in der Regel von den Autoren der Inhaltsdaten signiert und für die Leser der Inhaltsdaten verschlüsselt. Das Intermediärsmodul hat keinerlei Zugriff auf die Inhaltsdaten.

Das Intermediärsmodul kann als eigenständiger, zentralisierter Dienst realisiert werden, es kann aber auch unmittelbar bei einem der Kommunikationspartner installiert werden. Unterschiedliche Szenarien legen unterschiedliche Realisierungen nahe, dies soll im Dokument *Betriebsanforderungen und -empfehlungen* näher dargestellt werden.

Das Intermediärsmodul operiert stets nur auf den Nutzungsdaten, niemals auf den Inhaltsdaten.

1. Herr Schwarze macht einen Formulierungsvorschlag für eine allgemeinere Lösung, die X.509 als konkrete Ausprägung vorsieht.

Bild 1: OSCI Kommunikationsmodell



4 Sachstand und Anforderungen

Der folgende Abschnitt benennt thematisch gegliedert die für die Weiterentwicklung von OSCI identifizierten Anforderungen. Dabei erfolgt zusätzlich ein Abgleich, ob bzw. in wie weit diese Anforderungen bereits durch die OSCI Spezifikation 1.0 erfüllt sind, bzw. ob die Anforderungen bereits in der folgenden Version Version 1.2, oder in einer späteren Version zu berücksichtigen sind.

4.1 Konsolidierung und Internationalisierung der Spezifikation

Hinsichtlich der Lesbarkeit und Übersichtlichkeit hat sich der strukturelle Aufbau der Spec. als zu unhandlich erwiesen. Weiterhin liegt die Spec. nur in deutsch vor, und die XML-Strukturierung des Nachrichtenformats benutzt deutsche Elementnamen.

Tabelle 1: Konsolidierung und Internationalisierung

Version 1.0	Version 1.2	Spätere Version
Kein einheitliches Inhaltsverzeichnis, keine Zusammenfassung am Ende der Kapitel, liegt nur in deutsch vor	Zusammenhängende Kapitelstruktur mit übergeifendem Inhaltsverzeichnis, Glossar und Index erstellen, englische XML-Elementnamen, Portierung der DTD in Schema, zusätzliches Anforderungs- und Begründungsdokument in Form einer Szenarienbeschreibung, *"Betriebsanforderungen und -empfehlungen"* als eigenständiges Dokument 3, Integration eines Sicherheitskonzepts. Die englische Übersetzung der Dokumente ist Bestandteil des Projektes, muss aber nicht bis zum 1.5 vorliegen.	

4.2 Sicherheit und Anforderungen des BSI

Sicherheitsanforderungen bestehen hinsichtlich der Vertraulichkeit und der Integrität der übermittelten Nachrichten, sowie hinsichtlich der Identifikation und Authentifikation der Kommunikationspartner. Weiterhin muss die Möglichkeit der Nachweisbarkeit der Kommunikation und deren zeitliche Bestimmung möglich sein.

OSCI—Transport basiert auf dem Signaturformat *w3c digital signature*. Es muss im Projektverlauf ermittelt werden, welcher Grad von Kompatibilität zu *"ISIS MTT"* für die Version 1.2 von OSCI—Transport erreichbar ist.

Die verwendeten Sicherungsverfahren (kryptographische Komponenten sowie das Protokoll) sind mit einem vom BSI erarbeiteten Katalog von Sicherheitsanforderungen abgestimmt.

Tabelle 2: Sicherheitsaspekte

Version 1.0	Version 1.2	Spätere Version
Sicherung der Vertraulichkeit und Integrität mittels zwingender hybrider Verschlüsselung auf Basis von 3DES und RSA; Authentifikation der Kommunikationspartner durch Signatur gemäß SigG und SigV OSCI 1.0 orientiert sich an W3C XML Signature und W3C XML Encryption in der damals aktuellen Version	Aktualisierung an die weiterentwickelten einschlägigen W3C-Standards. Wenn möglich,Konformität zu XAdES-Spezifikation des ETSI herstellen; Sicherung der Vertraulichkeit und Integrität durch hybride Verschlüsselung auf Basis von AES (an Stelle oder alternativ zu 3DES) und RSA; *optionale* Verwendung von Verschlüsselung Prüfung, in welcher Form bestimmte Aspekte von *ISIS MTT* in OSCI—Transport Berücksichtigung finden können, um sich dem langfristig angestrbten Ziel der Kompatibilität zu nähern. Unterstützung unterschiedlicher Signaturniveaus von akkreditierter Signatur bis zur unsignierten Nachricht; Die Nachweisbarkeit der Kommunikation wird durch die Aufnahme zertifizierter Zeitstempel in die OSCI-Spec. 1.2 gewährleistet.	Nach der Bereitstellung der erforderlichen PKI (von der öffentlichen Verwaltung zu leisten) wird der Mechanismus der Transportverschlüsselung per SLL in OSCI aufgenommen. Erweiterung des *Prüfprotokolls* (ein Bestandteil der Nutzungsdaten) um Informationen, die eine Prüfung der Signaturen auch nach langen Aufbewahrungsfristen gewährleisten. (Langfristige Archivierung der Nutzungsdaten).

4.3 SOAP als künftiges Messaging-Protokoll

Die Kommunikation muss uneingeschränkt über Standardprotokolle des Internet möglich sein.

Tabelle 3: SOAP als Messaging-Protokoll

Version 1.0	Version 1.2	Spätere Version
Hinsichtlich des Transportmechanismus werden keine Aussagen gemacht (die Bremer Referenzimplementierung basiert allerdings auf SOAP und HTTP)	OSCI 1.2 wird als SOAP 1.2 Dialekt modelliert	

4.4 Referenzierung von Teilthemen

Um ein möglichst schlankes und übersichtliches Dokument für die Spec. zu erhalten, sollen alle Themenbereiche, für die eigenständige Spezifikationen vorliegen, nur noch in Form entsprechender Referenzen Erwähnung finden.

Tabelle 4: Referenzierung von Teilthemen

Version 1.0	Version 1.2	Spätere Version
In der Spec. 1.0 werden verschiedene grundlegende Technologien (XML, X509, etc.) erläutert.	Sofern für die in OSCI verwendeten Technologien eigenständige Spezifikationen zur Verfügung stehen, ist darauf zu referenzieren, und auf entsprechende Erläuterungen dieser Technologien in der Spec. zu verzichten; lediglich evt. darüber hinaus gehende Konkretisierungen sind zu erläutern	

Zu refenzierende Spezifikationen u.a.:

- XML
- XML Schema
- XML Signature
- XML Encryption
- SOAP
- SOAP Security
- SOAP with Attachments
- ggfs. ETSI XAdES
- X.509
- ISIS MTT (ggfs. nur einschlägige Abschnitte).
- PKCS#...

Ein abschließender Katalog der Standards wird während der Projektlaufzeit — in Abstimmung mit dem BSI — erarbeitet.

4.5 Synchrone Kommunikation mit Fachanwendungen

Tabelle 5: Synchrone Kommunikation

Version 1.0	Version 1.2	Spätere Version
OSCI 1.0 geht von einem asynchronen Modell aus, synchrone Kommunikation ist nicht vorgesehen (in der Bremer Implementierung wurde bereits ein Auftragstyp *"Transaction"* eingeführt). Im Architekturmodell wurde neben dem Intermediär ein OSCI-Backend eingeführt, an das Aufträge vom Typ *"Transaction"* und *"Zustellungsauftrag"* mittels *"push"* übertragen werden. OSCI-Antworten des Backends auf solche Auftragstypen sind zu spezifizieren).	OSCI—Transport 1.2 ist um einen Nachrichtentyp für die synchrone Kommunikation zu ergänzen. Dabei sind die in der Spec. 1.0 beschriebenen Verfahren zur Sicherung der Dialogkontexte und -folgen zu prüfen.	

4.6 Regelbasierte Übermittlung von Nachrichten

Tabelle 6: Regelbasierte Übermittlung

Version 1.0	Version 1.2	Spätere Version
OSCI sieht in der Version 1.0 einen einfachen Regelmechanismus vor, anhand dessen die Zustellung von Nachricht an Bedingungen geknüpft werden kann. Die notwendigen Bedingungen, die für die Zustellung einer Nachricht erfüllt sein müssen, sind entweder das Erreichen eines expliziten Zeitpunktes, oder die Übermittlung eines Status in einer separaten NAchricht. Die Zustellung der Nachricht erfolgt dann abhängig vom Statuswert. Die zweite Bedingung wird zur Abbildung von Payment-Abhängigkeiten genutzt.	Es wird ein *"Regelcontainer"* übermittelt, dieser ist von den Inhaltsdaten separiert, aber ebenfalls für den Empfänger (statt — wie bisher — für das Intermediärsmodul) verschlüsselt.Die Regelauswertung wird durch den Empfänger durchgeführt. Der Empfänger ist für die Beachtung und korrekte Verarbeitung der Regeln selbst verantwortlich. Durch die getrennten Container für Regeln und Inhaltsdaten kann der Empfänger die Regeln prüfen, *bevor* er die Inhaltsdaten dechiffriert und öffnet.	

4.7 Reduzierung der Interpretationsspielräume

Die Spezifikation OSCI 1.0 lässt eine Reihe von Interpretationsspielräume bei der Implementation, die mit OSCI 1.2 ausgeräumt werden sollen.

4.8 Große Attachements

Tabelle 7: Fremdformate

Version 1.0	Version 1.2	Spätere Version
OSCI 1.0 erlaubt die transparente Übermittlung beliebiger Binärdaten in BASE64 codierter Form. Es werden keine Aussagen über *"große Attachements"* gemacht.	In gewissen Geschäftsvorfällen sind sehr große Attachments zu übermitteln. Die Spezifikation wird in Hinblick auf eine bessere Implmentierbarkeit bezüglich *"großer"* Attachements überprüft und optimiert.	

4.9 Mehrfachsignatur und -verschlüsselung (geschachtelt und parallel)

Die Forderung nach Mehrfachsignaturen und Mehrfachverschlüsselung wurde seit der Fertigstellung von OSCI—Transport 1.0 bereits mehrfach erhoben. Mit der Forderung der Mehrfachverschlüsselung ist automatisch die Vorstellung verbunden, dass eine OSCI-Nachricht nicht an *eine*, sondern an *mehrere* Personen gerichtet ist. Dazu analog ist die Mehrfachsignatur dadurch motiviert, dass die Nachricht nicht *einem* Verfasser, sondern *mehreren* zugeschrieben wird.

Andererseits würde die Zulässigkeit mehrerer Sender oder mehrerer Empfängern einer OSCI-Nachricht vermutlich zu sehr komplexen organisatorischen Fragestellungen führen, zum Beispiel:

- Wenn eine Nachricht mehrere Empfänger hat: wann gilt sie als erfolgreich übermittelt (oder gar als *zugestellt*?)
- Wenn eine Nachricht mehrere Sender hat: wer erhält Quittungen über die erfolgreiche Übermittlung?

  Kann es Datenschutzprobleme geben, wenn jeder der Sender Aufschluss über Signaturen, Sendezeitpunkte etc. der anderen Sender erhalten kann?
- Wie ist es zu bewerten, wenn von mehreren Absenderzertifikaten einige, aber nicht alle positiv gegen die CA geprüft werden konnten?

Es scheint uns sinvoll zu sein, bei der Betrachtung der Mehrfachsignatur- und Verschlüsselung zwischen den Inhalts- und den Nutzungsdaten zu unterscheiden. Aus diesen Gründen präzisieren wir ein Rollenmodell der OSCI-Kommunikation sowie die Anforderungen an die Mehrfachsignatur / Mehrfachverschlüsselung wie folgt:

1 Die *Inhaltsdaten* können von mehr als einer Person signiert werden. Jede Person, die die Inhaltsdaten signiert hat, wird als *Autor* der OSCI-Nachricht bezeichnet, die diese Inmhaltsdaten transportiert.

Dies begründet die Möglichkeit der *Mehrfachsignatur der Inhaltsdaten.*

2 Die Zielgruppe, also die Personen (oder maschinelle Verfahren), für die die Inhaltsdaten verfasst werden, bezeichnen wir als *Leser*. Die Autoren verschlüsseln die Inhaltsdaten so, dass sie nur durch die Leser dechiffriert werden können. Es kann mehr als einen Leser geben.

Dies begründet die Möglichkeit der Mehrfachverschlüsselung der Inhaltsdaten.

3 Die Inhaltsdaten werden vor dem Versand in den Transportumschlag gepackt. Bestandteil des Transportumschlags sind die Nutzungsdaten, dazu gehören u. a. Zertifikate, der Laufzettel, das Prüfprotokoll und so weiter. Der Transportumschlag ist ebenfalls signiert. Den Inhaber des Signaturzertifikats, der die Nutzungsdaten signiert hat, bezeichnen wir als den *Sender*.

Um die Übertragungssituation einfach zu halten, legen wir fest, dass es auch in OSCI—Transport 1.2 nur *genau einen Sender* pro OSCI Nachricht geben kann. Es gibt kein Mehrfachsignatur der Nutzungsdaten.

4 Jede OSCI-Nachricht ist an genau einen *Empfänger* gerichtet. Sein Chiffrierzertifikat ist in der ausgezeichneten Rolle des *Empfängerzertifikats* Bestandteil der Nutzungsdaten. Die Nutzungsdaten sind für den Empfänger verschlüsselt.

Um die Übertragungssituation einfach zu halten, legen wir fest, dass es auch in OSCI—Transport 1.2 nur *genau einen Empfänger* pro OSCI Nachricht geben kann.

Es gibt kein Mehrfachverschlüsselung der Nutzungsdaten.

Tabelle 8: Mehrfachsignatur

Version 1.0	Version 1.2	Spätere Version
Mehrfachverschlüsselung und -signatur sind nicht vergesehen.	Zur Realisierung des Vier-Augen-Prinzips muss die Möglichkeit der geschachtelten Verschlüsselung der Inhaltsdaten umgesetzt werden. Zusätzlich ist die Möglichkeit paralleler Mehrfachverschlüsselung, also Verschlüsselung für mehrere Leser zu realisieren (evt. erst in einer späteren Version?). Ferner soll die mehrfache Signatur der Inhaltsdaten implementiert werden (geschachtelte und parallele Signaturen). *Alle* Signaturzertifikate sind auf der Ebene der Nutzungsdaten zugänglich, damit vom Intermediärsmodul die Mehrwert - Dienstleistung der Prüfung der Signaturzertifikate auf Gültigkeit auch im Falle der Mehrfachsignatur erbringen kann.	Realisierung paralleler Mehrfachverschlüsselung der Inhaltsdaten. Es ist zu prüfen, ob ggfs. mehr als ein Empfänger pro OSCI-Nachricht sinnvoll ist.

5 Projektorganisation

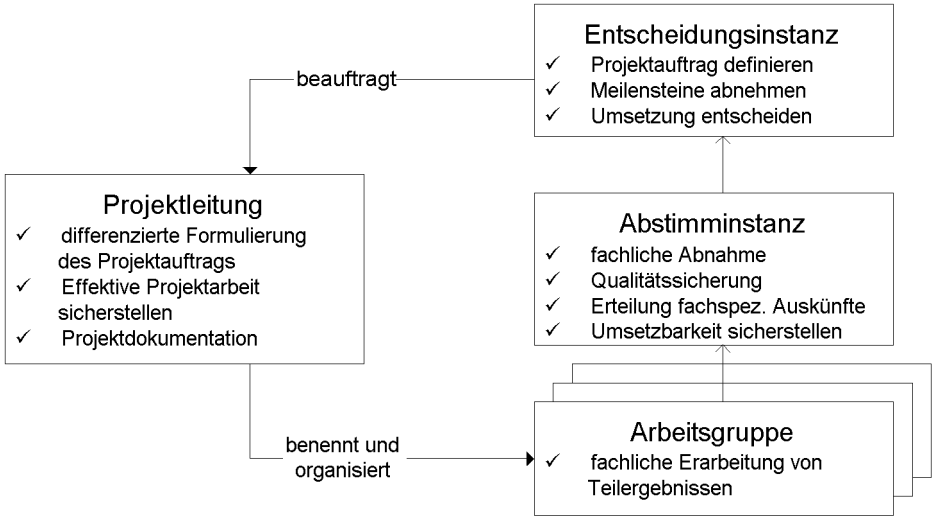
Die Projektorganisation erfolgt analog XMeld mit drei Gremien sowie der Projektleitung.

Aufgrund der zeitlichen Vorgaben des Bundes muss das Projektziel bis zum 1.5.2002 erreicht sein. Wegen der CeBiT können die meisten Beteiligten erst Ende März mit umfangreicheren Arbeiten beginnen. Die Arbeit muss im Monat April erfolgen. Daher gibt es genau drei Meilensteine:

- Verabschiedung des abgestimmten Projektauftrags durch die EI am 28.3.02
- Vorlage der Projektergebnisse *"Anforderungsdokument"* und *"OSCI—Transport Spezifikation 1.2"* durch die Arbeitsgruppe Anfang Mai 2002.

  Abnahme dieser Projektergebnisse durch die EI Anfang / Mitte Juni 2002.
- Erstellung des Dokuments *"Betriebsanforderungen und -empfehlungen"* sowie der englischen Übersetzungen aller drei Papiere bis Ende August 2002. Abnahme dieser Projektergebnisse durch die Entscheidungsinstanz und Projektende im September 2002.

Bild 2: Projektorganisation



5.1 Entscheidungsinstanz

Sie entscheidet über das Projektziel und nimmt Ergebnisse ab.

Sie wird gebildet aus Vertretern des KOOPA – ADV

Die EI trifft sich zu jedem Meilenstein, also drei Mal im Projektverlauf. Sie besteht aus:

- Herrn Krost, KBSt
- Herrn Dr. Franßen, Bayern
- Herrn Thede, Mecklenburg-Vorpommern
- Frau Schwellach, Bremen

5.2 Abstimminstanz

Sie hat die Aufgabe der Qualitätssicherung, sie prüft auf Realisierbarkeit.

Die Besetzung der Abstimminstanz wird auf der Sitzung am 27.3.02 endgültig festgelegt.

5.3 Arbeitsgruppe(n)

Die Mitglieder der Arbeitsgruppen erarbeiten die Dokumente, die als Projektziel genannt wurden.

Aufgrund der oben genannten zeitlichen Rahmenbedingungen gehen wir davon aus, dass Mitglieder der Arbeitsgruppe(n) im Monat April 2002 **60%...80% ihrer regelmässigen wöchentlichen Arbeitszeit** für das Projekt investieren müssen.

Die Besetzung der Arbeitsgruppe wird auf der Sitzung am 27.3.02 endgültig festgelegt.

5.4 Projektleitung

Die Projektleitung organisiert das Projekt und stellt eine effiziente Kommunikation zwischen den Gremien sicher. Sie organisiert die Arbeitsgruppe(n). Sie dokumentiert Arbeitsergebnisse und erstellt redaktionell die drei als Projektziel genannten Dokumente. Sie moderiert die Sitzungen der drei anderen Gremien. Sie besteht aus:

- Herrn Schunk von der Firma ppi
- Herrn Steimke von der OSCI–Leitstelle