Organisations- und Finanzierungskonzept für die Weiterentwicklung von OSCI inklusive der OSCI Bibliothek

Entsprechend KoopA - ADV Beschluss 3-11/2002

OSCI Leitstelle
Bremen, 27. März 2002

Status: Proposal

Einleitung

Mit *“E–Government”* ergeben sich bisher kaum überschaubare Potenziale für eine verbesserte und effizientere Abwicklung von Geschäftsprozessen zwischen der öffentlichen Verwaltung und ihren Kunden. Mit Hilfe der elektronischen Signatur ist es inzwischen möglich geworden, auch solche Geschäftsvorfälle über den *Vertriebskanal Internet* anzubieten, bei denen besonders hohe Anforderungen an die Integrität, Authentizität oder Vertraulichkeit der übermittelten Nachrichten gestellt werden. Die Bundesregierung hat frühzeitig erkannt, dass vor einer flächendeckenden Umsetzung dieses Potenzials noch viele technische Fragen zu klären sein werden, und hat entsprechende Projekte initiiert.

Eine dieser Initiativen ist das MEDIA@Komm-Projekt aus dem Jahre 1998, dessen Ziel wie folgt definiert ist:

> *In einem integrativen Ansatz sollen im städtischen Raum innovative multimediale Dienste und Anwendungen möglichst unter Nutzung der digitalen Signatur entwickelt und deren Möglichkeiten und wirtschaftlichen Potenziale demonstriert werden. Zwischen öffentlicher Verwaltung, Bürgern und Wirtschaft sollen rechtsverbindliche Dienstleistungen und Transaktionen vollelektronisch ohne Medienbrüche getätigt werden können (“virtuelles Rathaus”, “elektronische Akte”, “Bürgerkarte”), um so Effizienz und Transparenz von Verwaltungs- und Geschäftsvorgängen zu verbessern. Durch die modellhafte Entwicklung und Erforschung der rechtlichen, technischen und ökonomischen Voraussetzungen für die “virtuelle Stadt” sollen*
>
> - *die Arbeits- und Lebensbedingungen der Bevölkerung verbessert,*
> - *die Verwaltungen effizienter und bürgerfreundlicher,*
> - *die Unternehmen flexibler und produktiver werden.*

In dem später prämierten Konzept Bremens wurde von Beginn an darauf hingewiesen, dass sich *attraktive Angebote mit hohem Rationalisierungspotenzial* nur dann verwirklichen lassen, wenn durch Standardisierung die *medienbruchfreie Weiterverarbeitung* der übermittelten Daten erreicht wird. Zudem wird durch eine Standardisierung das Ziel der *Interoperabilität* der technischen Komponenten erreicht. Dies ist wichtig, damit der potenzielle Markt für die über das Internet angebotenen Dienstleitstungen nicht aufgrund technischer Restriktionen unnötig reduziert wird. Dieser Standardisierungsaspekt bezieht sich sowohl auf die Basisfunktionen des sicheren Transports, als auch auf fachspezifische Inhaltsdaten.

Der MEDIA@Komm-Projektträger ist dieser Argumentation gefolgt. Die bremen online services GmbH & Co. KG (bos KG) hat von der Bundesrepublik Deutschland im Rahmen des MEDIA@Komm Projektes eine Forschungs- und Entwicklungsförderung auf Kostenbasis erhalten. In diesem Rahmen wurde auch die OSCI–Leitstelle eingerichtet. Ihre Aufgabe ist es, für die identifizierten Handlungsfelder Standards zu entwickeln und bundesweit abzustimmen. Die Summe dieser Standards hat den Namen OSCI, diese Abkürzung steht für *“Online Services Computer Interface”*. Inzwischen hat die Verbreitung der OSCI Idee wesentlich weitere Ausmaße angenommen als im Forschungsantrag dargestellt und zum damaligen Zeitpunkt vermutet werden konnte.

Jeder OSCI-Bestandteil ist eine technische Umsetzung fachlicher Vorgaben, die von der öffentlichen Verwaltung definiert wurden. OSCI basiert auf *dem* generischen Beschreibungsformat XML, und jedes OSCI-Ergebnis besteht im Wesentlichen aus Nachrichtenstrukturen, die in XML-Schema definiert werden.

Da Software (nämlich die XML Schemata) erzeugt wird, sind die üblichen Regularien der Softwareerstellung anzuwenden. Es muss Fachkonzepte auf grober und feiner Ebene geben, fachliche Inhalte werden mit den heute üblichen Methoden modelliert, und die erzielten Ergebnisse gehen in einen Software-Lifecycle über. Die Anforderungen an das Change-Management und die Versionierung von Software sind aus anderen Projekten bekannt.

Dennoch ist die Situation nicht die eines gewöhnlichen Software-Erstellungsprojektes. E–Government wird seine Potenziale nur dann entfalten können, wenn der Gedanke der Standardisierung und Interoperabilität ernst genommen wird. Die zu überwindenden Grenzen sind vielfältig:

- Die föderale Struktur der Bundesrepublik führt zu landesspezifischen Normen, und damit zu landesspezifischen Daten- und Prozessmodellen
- Unterschiedliche Fachinhalte führen ebenfalls zu verschiedenen Datenmodellen. Ein Objekt *"Einwohner"* in einem DV-Verfahren des Meldewesens unterscheidet sich wesentlich von dem *"Steuerpflichtigen"* aus den Verfahren des Finanzwesens. So kommt es zu Inkompatibilitäten, wenn zwischen beiden Fachverfahren Daten über einen *Bürger* ausgetauscht werden sollen.

Die Aufgabe der Standardisierung in diesem Bereichen kann nur durch eine Kooperation zwischen den betroffenen Stellen des Bundes, der Länder und des kommunalen Bereiches erreicht werden.

Inzwischen hat OSCI einen Stand erreicht, der durch eine dauerhafte Organisationsstruktur nachhaltig gesichert und für den ein mittel - bis langfristiges Finanzierungskonzept erarbeitet werden muss.

Mit dem nachfolgenden Text wird ein Organisationsvorschlag unterbreitet, bei dem durch geeignete Projektstrukturen sichergestellt wird, dass die Weiterentwicklung von OSCI in diesem Sinne erfolgt.

Versionshistorie

Die Version 1.0 dieses Papieres wurde durch die *"OSCI Strategierunde"* erstellt, die aus den folgenden Personen bestand:

Mitglieder der OSCI Strategierunde	
Fiedler, Arno	Teletrust
Goerdeler, Andreas	BMWi
Grabow, Busso	Difu
Gröming, Erko	Deutscher Städtetag
Klein, Stephan	bremen online services (MEDIA@Komm Bremen)
Kohnert, Werner	DLR
Kraft, Andreas	MEDIA@Komm e.V. Esslingen)
Krost, Rolf	BMI, KBSt
König, Friedrich	BMWi
Schmalfeld, Uwe	Curiavant (MEDIA@Komm Nürnberg)
Schmidt, Andreas	BSI
Schulz, Arnold	DIN
Schwellach, Gisela	Senator für Finanzen, Bremen
Schwemmer, Jürgen	RegTP
Steimke, Frank	OSCI Leitstelle
Thede, Heiko	Innenministerium Mecklenburg Vorpommern
Zinke, Michael	BMWi

Die Aufgabe der Strategierunde bestand in der Unterstützung der OSCI–Leitstelle während der Übergangsphase vom MEDIA@Komm-Projekt hin zur dauerhaften Etablierung und Verankerung in bestehenden Gremien.

Die aktuelle Version 2.0 dieses Papiers differenziert stärker zwischen den infrastrukturellen Aufgaben und fachlichen Projekten. Sie berücksichtigt die zwischenzeitlich gewonnenen Erfahrungen.

Version	Inhalt	Datum / Status
1.0	Initiale Version, entstanden durch die Strategierunde.	Mai 2002
2.0	• Trennung der Verantwortlichkeiten zwischen OSCI Infrastruktur (KoopA–ADV) und Inhaltsdaten (Fachministerien). • Einführung eines *"OSCI Framework"*, um die geordnete und koordinierte Weiterentwicklung durch Stützpunkte sicherzustellen. Dies ist im Abschnitt 1.3 auf Seite 9 beschrieben. Die Vergabe der Marke und des Logos *"OSCI"* werden an die Einhaltung des Framework geknüpft. • Beschreibung der OSCI-Bibliothek als Teil der OSCI Infrastruktur auf Seite 4ff. Darstellung eines Nutzungs- und Finanzierungskonzeptes dafür. • Aufnahme der Projekte *"XBau"* und *"Grunddatensatz Justiz (XJustiz)"* in den Abschnitt *"Fachaufgaben"* (siehe Seite 6). Beschreibung von OSCI–XMeld als *"Leitprojekt"* (siehe Seite 9). • Die Überführung von OSCI in die Verwaltung ist erfolgt, es gibt keinen Bedarf mehr an der Strategierunde. • Alle Kapitel wurden aktualisiert.	• 27.3.03 Proposal

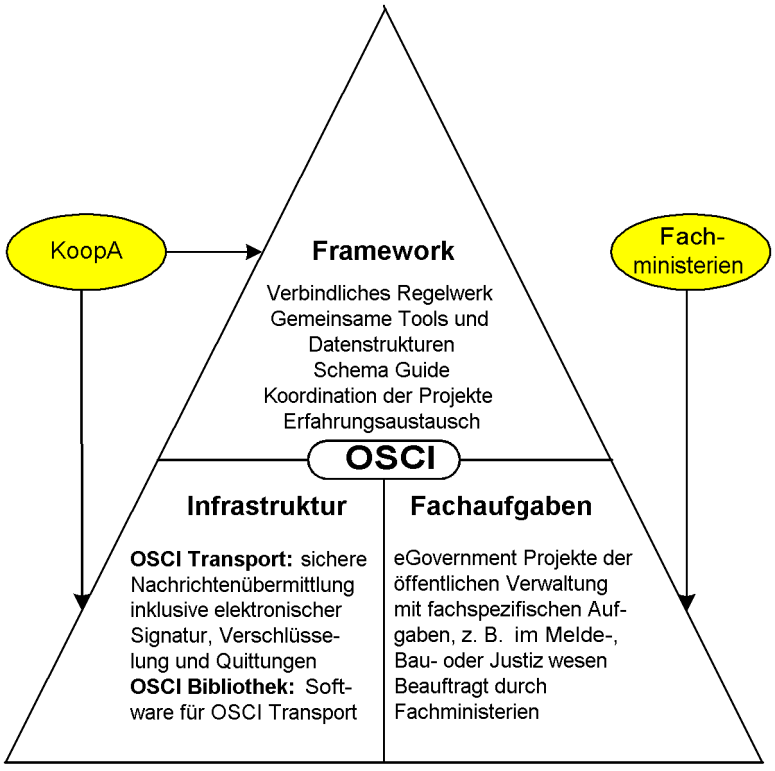
1. KAPITEL: SACHSTAND

Der Name OSCI: *"Online Service Computer Interface"* steht für eine Menge von Protokollen, deren gemeinsames Merkmal die besondere Eignung für das E–Government ist. OSCI ist ein MEDIA@Komm-Ergebnis.

Durch eine Orientierung an Entwicklungen der Kreditwirtschaft werden langfristig Synergieeffekte angestrebt: die Anforderungen an die Sicherheit der Online-Dienste der Kreditwirtschaft sind ähnlich hoch wie die an die Online-Dienste der Verwaltungen, und durch OSCI-Produkte für verschiedene Branchen sind Kosteneinsparungen möglich.

OSCI soll dazu beitragen, dass E–Government kostengünstig und effektiv in Deutschland umgesetzt werden kann, beispielsweise dadurch, dass die öffentlichen Verwaltungen bei Ausschreibungen zu E–Government-Produkten und -Dienstleistungen die jeweils für sie passenden Teile von OSCI als einzuhaltende Norm referenzieren können. Dies sichert die Vergleichbarkeit der Angebote und erhöht den Preiswettbewerb.

Bild 1 Die Elemente von OSCI



Der Geltungsbereich von OSCI umfasst sowohl die Ebene der Transport- und Sicherheitsfunktionen inklusive der elektronischen Signatur (Teil A), als auch die Ebene der Inhaltsdaten (Teil B). Die Zielsetzung von OSCI ist es, durch Standardisierung in beiden Bereichen Interoperabilität für die öffentliche Verwaltung herzustellen und damit E–Government - Anwendungen auf allen Verwaltungsebenen sowie innerhalb der Verwaltungen kostengünstig und interoperabel entwickeln oder erwerben zu können.

Damit eine möglichst optimale Wirkung erzielt wird ist es notwendig, dass alle OSCI Projekte nach abgestimmten Regeln, einem *"Framework"* ablaufen. Damit wird einerseits sichergestellt, dass übertragbare Ergebnisse auch in anderen Projekten genutzt werden, so dass innerhalb der OSCI Entwicklung mit der Zeit die Synergieeffekte größer werden. Andererseits wird damit im Rahmen des Möglichen auch gewährleistet, dass alle OSCI Projekte einem gewissen Qualitätsstandard genügen. Nur die Projekte, die unter Beachtung des abgestimmten Regelwerkes durchgeführt werden, dürfen die geschützte Marke *"OSCI"* in ihrem Namen führen, und nur solche Projekte bekommen ein projektspezifisches OSCI Logo.

In den nächsten Kapiteln werden diese drei Bestandteile von OSCI:

1. sichere Infrastruktur;
2. Fachaufgaben (ab Seite 6), und
3. das OSCI Framework in Abschnitt 1.3 auf Seite 9

dargestellt. Anschließend wird OSCI von anderen Standards (in Deutschland, in der EU und weltweit) abgegrenzt. Die geplante Zusammenarbeit mit einschlägigen Standardisierungsgremien wird dargestellt.

Im Abschnitt 2 auf Seite 20 wird die geplante Organisationsform für eine langfristige — über die Projektlaufzeit des MEDIA@Komm-Projektes hinausgehende — Etablierung der Standardisierungsaktivitäten dargestellt. Dabei wird die Trennung zwischen den infrastrukturellen und den fachbezogenen Aufgaben herausgearbeitet. Schließlich wird ein Finanzierungsvorschlag unterbreitet.

1.1 Infrastruktur

1.1.1 OSCI–Transport

OSCI–Transport bietet als Basisfunktionalität die sichere und interoperable Übermittlung elektronisch signierter Nachrichten. Die in XML beschriebene Datenstruktur bietet eine am deutschen Teledienstedatenschutzgesetz orientierte Trennung zwischen Nutzungs- und Inhaltsdaten. Während der eigentliche Nachrichteninhalt (die Inhaltsdaten) Ende-zu-Ende verschlüsselt sind, erlauben die separat chiffrierten Nutzungsdaten die Zwischenspeicherung und Vermittlung von Nachrichten ohne Vertraulichkeitsverlust. Dadurch kann eine Verwaltung ein sicheres Portal aufbauen und aufwendige Technik *"vor die Klammer"* ziehen. Ökonomisch günstige E–Government Realisierungen durch gemeinsam genutzte Ressourcen werden möglich, ohne die vom Datenschutz gebotene Trennung der Verwaltungseinheiten aufzugeben.

OSCI–Transport adressiert die sichere und medienbruchfreie Nutzung von Verwaltungsanwendungen durch *"Externe Kunden"*, die in Anhängigkeit von den — rechtlich vorgegebenen — Anforderungen der Geschäftsvorfälle durch elektronische Signaturen verschiedener Niveaus authentisiert und identifiziert werden können.

OSCI–Transport beschreibt (ab Version 1.2) die Rollen der Kommunikationsbeteiligten exakt. Es besteht die Möglichkeit, mehrere, miteinander in Relation stehende Inhaltsdatencontainer in einer Nachricht zu übermitteln. Dieser Mechanismus erlaubt eine Steuerung der Verarbeitung auf Inhaltsdatenebene. Dies ermöglich beispielsweise:

- Die regelbasierte Übermittlung von Inhaltsdaten an Empfänger (als extra Inhaltscontainer)
- Den Aufbau virtueller Poststellen mit zentralisierten Übermittlungsaktivitäten
- Die zentralisierte Abwicklung von Zahlaktivitäten

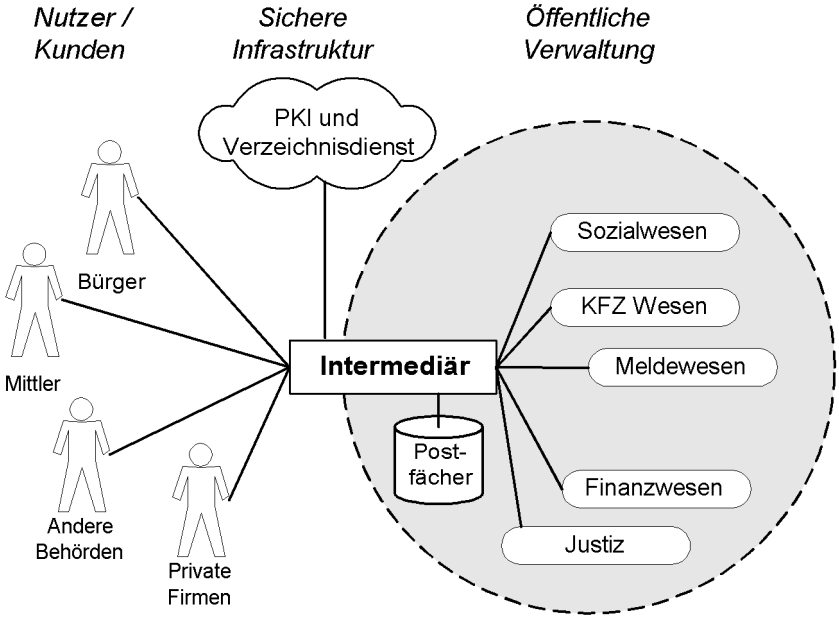
OSCI–Transport basiert auf *XML digital signature*, *XML encryption* und *SOAP*. Diese weltweit anerkannten Standards werden in geeigneter Weise konkretisiert, um die Anforderungen des deutschen Signaturgesetzes zu erfüllen und Interoperabilität sicherzustellen. Auch für die Verschlüsselungsverfahren werden genaue Vorgaben gemacht, um Interoperabilität sicherzustellen. Dabei unterstützt OSCI–Transport von der fortgeschrittenen bis hin zur akkreditierten elektronischen Signatur alle Qualitätsniveaus. In der Version 1.2 ist OSCI–Transport bezüglich der Sicherheitsmechanismen noch stärker skalierbar geworden. Dadurch ergibt sich die Eignung von OSCI–Transport auch in (verwaltungsinternen) Intranetzen.

Bezüglich der durch das Signaturgesetz vorgegebenen PKI und des Umgangs mit Zertifikaten wurden bereits im Rahmen des ISIS–MTT-Projektes Interoperabilitätsregeln definiert. OSCI bezieht sich in den einschlägigen Teilen auf die Ergebnisse von ISIS–MTT. Im Rahmen eines Expertengesprächs zwischen den Entwicklern von OSCI–Transport und ISIS–MTT wurde festgestellt, dass sich diese beiden Standards ergänzen, dies ist ab der Seite 16 im Detail beschrieben.

E–Government Anwendungen müssen für die Kunden attraktiv gestaltet werden, sonst werden sie nicht angenommen. Hierfür ist es zum Beispiel sinnvoll, dem Bürger in einem interaktiven Dialog die in den Verwaltungsverfahren bereits gespeicherten Altdaten anzubieten. Am Ende dieses Dialogs steht dann in der Regel ein vom Kunden elektronisch signiertes Formular, dessen strukturierte Inhaltsdaten an die Verwaltung gesandt werden. Die Verwaltung reagiert irgendwann mit einer ebenfalls elektronisch signierten Nachricht an den Kunden. Solange die Bearbeitung des Prozesses nicht vollautomatisch erfolgen kann, mögen zwischen dem Antrag des Kunden und dem Bescheid der Verwaltung mehrere Tage oder gar Wochen vergehen. OSCI–Transport unterstützt daher mit den gleichen Sicherheitsmechanismen sowohl die *"synchrone"* Kommunikation (für den interaktiven Dialog), als auch die zeitversetzte Nachrichtenübermittlung mit der sicheren Zwischenspeicherung von Nachrichten in Postfächern.

Der *"Intermediär"* ist ein integraler und unverzichtbarer Bestandteil jeder Nachrichtenübermittlung mittels OSCI–Transport. Der Intermediär sichert den Dialogkontext und hält Postfächer vor. Außerdem bildet er den zentralen Zugang zur PKI. Wegen der Ende-zu-Ende Verschlüsselung kann der Intermediär ausschließlich auf den Nutzungsdaten, niemals auf Inhaltsdaten operieren. Deshalb können sich auch solche Verwaltungseinheiten, die datenschutzmäßig streng voneinander zu trennen sind, einen Intermediär als gemeinsame Ressource teilen.

Bild 2 Sichere Verwaltungsportale mit OSCI



Ein Intermediär ist aus den folgenden Gründen erforderlich:

1. Aufbau und Sicherung eines Dialogkontextes. Dadurch können Transaktionen abgebildet werden, die aus mehreren Schritten bestehen (zum Beispiel: Identifikation und Authentisierung; Arbeiten auf Datenbeständen der Fachverfahren; Finales Signieren).

   Diese Funktion des Intermediärs ist in der OSCI Spezifikation fest definiert. Sender und Empfänger von OSCI Nachrichten kommunizieren niemals direkt, sondern stets vermittelt über den Intermediär.

   Eine OSCI–Transport Nachrichtenübermittlung ohne Intermediär ist nicht möglich. Dafür ist es jedoch nicht erforderlich, dass der Intermediär als eigenständiges DV-System mit eigener Hardware (Server) realisiert wird. Der Aufbau und die Überwachung des Dialogkontextes könnten auch von Softwarekomponenten wahrgenommen werden, die direkt beim Fachverfahren installiert werden. Die Installation als eigenständiges System ist dennoch in der Regel praktisch und ökonomisch sinnvoll.

2. Zentraler Zugang zu PKI und Verzeichnisdiensten. Der Zugang zu Verzeichnisdiensten und PKI-Services ist noch nicht ausreichend standardisiert, daher sind Zugangstechniken, die mit unterschiedlichen Produkten und Anbietern zurecht kommen müssen, aufwändig und teuer. Es ist ökonomisch sinnvoll, diese Techniken zu zentralisieren. Darüber hinaus ist der Zugang aus behördeninternen Netzen oft nur schwer möglich. Daher ist es praktisch, wenn der PKI-Zugang außerhalb des Behördennetzes liegt.
3. Der Intermediär verwaltet die Postfächer, die für die asynchrone Kommunikation erforderlich sind. OSCI–Transport unterstützt nicht nur die Nachrichtenübermittlung vom Kunden zur Verwaltung, sondern auch den Rückweg. Da man von den Bürgern nicht erwarten kann, dass sie ständig online sind, muss mit eMail - ähnlichen Übermittlungsverfahren gearbeitet werden.

   Im Unterschied zur *"normalen eMail"* (`smtp`) sind die OSCI Nachrichten besser geschützt. Absenderadressen können nicht verfälscht werden, und es ist sichergestellt, dass nur berechtigte Empfänger Zugriff auf ihr Postfach haben.

Die Basisfunktionalitäten (Datenstrukturen und Sicherheitsfunktionen) von OSCI–Transport wurden in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie der Begleitforschung des MEDIA@Komm Projektes erarbeitet.

Im Juli 2002 hat das BSI die Eignung von OSCI–Transport für E–Government geprüft und festgestellt:

> *Im gegeben Prüfungsumfang des Erlasses vom 28.05.02 kann für die Frage nach der Erfüllung der Anforderungen aus Sicht der Kommunikationssicherheit im E–Government festgestellt werden:*
>
> *Eine Übertragungssicherung im Sinne der ITSEC (Schutz der Daten während der Übertragung über Kommunikationskanäle) ist sichergestellt. Damit kann davon ausgegangen werden, dass die Anforderungen aus Sicht der Kommunikationssicherheit im E-Government abgedeckt werden. Produkte, die auf der Basis der vorliegenden Spezifikation implementiert wurden, können somit … die Anforderungen der Kommunikationssicherheit im E-Government erfüllen.*
>
> *Bezüglich der ebenfalls im Erlass beauftragten Frage nach der Erfüllung der Anforderungen hinsichtlich der kryptographischen Sicherheit der eingesetzten Algorithmen und Verfahren ist festzustellen:*
>
> *OSCI-Transport 1.2 sieht ohne Ausnahme die Verwendung von der Fachwelt anerkannter, nach derzeitigem Kenntnisstand kryptographisch starker Algorithmen (für die Zwecke "digitale Signatur" bzw. Ver-/Entschlüsselung) vor, wobei die verwendeten Schlüssellängen ebenfalls derzeit nicht zu beanstanden sind. Zudem orientieren sich die Vorschläge für die konkrete Realisierung der verwendeten Verfahren an bewährten, weithin eingesetzten Standards.*
>
> *Bei Einhaltung der im Text gegebenen Empfehlungen zur Implementierung kann davon ausgegangen werden, dass das von einem entsprechenden Produkt erzielbare kryptographische Sicherheitsniveau durchgängig angemessen hoch ist.*
>
> *"Angemessen hoch" heißt hier: nach aktuellem Stand der Algorithmik und der Rechentechnik liegt der vermutliche Minimalaufwand für die Erlangung der zugrundeliegenden kryptographischen Schlüssel durch Kryptoanalyse oberhalb der derzeit akzeptierten Schwelle von 2 hoch 80 Operationen.*

OSCI–Transport ist in der aktuellen Fassung von *SAGA* der *obligatorische* Standard für den Bereich der Transaktionen.

1.1.2 Die OSCI-Bibliothek

Mit der Spezifikation des Protokolls OSCI–Transport hat die OSCI–Leitstelle entsprechend dem MEDIA@Komm Projektauftrag ein sicheres, herstellerunabhängiges und interoperables Datenaustauschformat beschrieben. Es war ursprünglich nicht beabsichtigt, dass die Leitstelle auch Software herausgibt, die dieses Protokoll oder Teile davon implementiert.

Es ist jedoch deutlich geworden, dass auf Seiten der Anwender in der öffentlichen Verwaltung der Bedarf besteht, OSCI–Transport möglichst einfach und schnell implementieren zu können. Die wahren Herausforderungen liegen in der Etablierung von E–Government in den Prozessabläufen und auf der fachlichen Ebene. Die *Implementierung* der sicheren Infrastruktur muss deshalb möglichst einfach funktionieren, damit nicht technische Detailprobleme die Umsetzung der fachlichen Lösungen verhindern.

Besonders deutlich wird dies derzeit im Meldewesen. Bis 2005 sollen alle länderübergreifenden Datenübermittlungen zwischen Meldeämtern mittels OSCI stattfinden. Dies ist eine erhebliche Herausforderung. Um diesen Prozess nicht zusätzlich durch technische Probleme zu behindern, und um den Anwendern in den Kommunen einen möglichst kostengünstigen Zugang zur OSCI Infrastruktur zu ermöglichen, hat die Innenministerkonferenz eine OSCI-Bibliothek gefordert (siehe Seite 25). Da die Bibliothek ausschließlich OSCI–Transport implementiert (also unabhängig von Fachinhalten ist), handelt es sich um einen Bestandteil der OSCI Infrastruktur. Die OSCI-Bibliothek soll

in Fachverfahren (auf Verwaltungsseite) oder Clientsystemen (auf Kundenseite) implementiert werden. Mit der Entwicklung und Nutzung der Bibliothek ergeben sich nicht nur für die Anwender, sondern auch für den Anbieter (die öffentliche Verwaltung) wirtschaftliche Vorteile:

- Die OSCI–Leitstelle, durch die die OSCI-Bibliothek herausgegeben wird, kann die Weiterentwicklungen des Protokolls OSCI–Transport ind der implementierenden OSCI-Bibliothek aufeinander abstimmen. Für den Auftraggeber KoopA–ADV werden dadurch die Kosten der Weiterentwicklung planbar.
- Für eine Übergangszeit macht die Existenz von nur *einer* Implementierung dieser OSCI-Bibliothek die Erstellung eines aufwändigen und teuren *Testbed* überflüssig.

  Deshalb wird während einer Übergangszeit innerhalb der öffentlichen Verwaltung die Nutzung von OSCI–Transport an die Nutzung der OSCI-Bibliothek gekoppelt. Es wird (zunächst) kein Testbed für die Prüfung auf OSCI–Transport - Kompatibilität implementiert. Fachverfahren der öffentlichen Verwaltung müssen OSCI mittels der OSCI-Bibliothek implementieren.

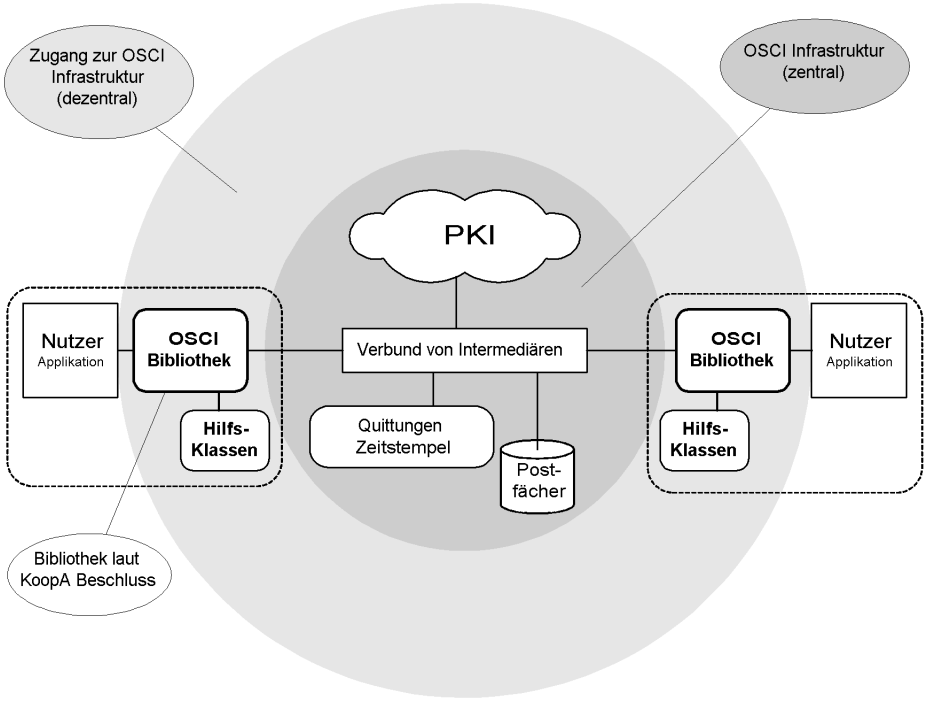
  Diese Festlegung auf eine einzige Implementierung soll bestehen bleiben, bis genügend Erfahrungen im flächendeckenden Produktiveinsatz von OSCI–Transport in heterogenen Umgebungen vorliegen (und zu einer Fortscheibung und Verbesserung der Spezifikation geführt haben), um Interoperabilität auch bei unterschiedlichen Implementierungen erreichen zu können.

Die OSCI-Bibliothek dient somit dem Ziel, die für den Einsatz von OSCI erforderliche Funktionalität und Interoperabilität für die in den öffentlichen Verwaltungen zum Einsatz kommenden Fachverfahren auf *pragmatische* Weise sicherzustellen.

Als Teil einer kompletten OSCI-Infrastruktur wird durch die OSCI-Bibliothek die Einbindung von Diensten zur Verfügung gestellt, die benötigt werden um OSCI–Transport Nachrichten zu generieren, zu versenden bzw. zu empfangen sowie diese kryptographisch zu bearbeiten. In diesem Sinne werden durch die OSCI-Bibliothek die Funktionen verfügbar, die auf Sender- und Empfangsseite immer (unabhängig von den Fachinhalten) für einen Zugang zu einer OSCI-Infrastruktur erforderlich sind.

Die Einordnung der OSCI-Bibliothek in die vollständige OSCI-Infrastruktur wird durch die folgende Abbildung veranschaulicht:

Bild 3 OSCI-Bibliothek und Infrastruktur



Die OSCI-Bibliothek wird auf Seiten der beteiligten Kommunikationspartner in vorhandene Software integriert. Sie ermöglicht einen Zugang zu einer OSCI Infrastruktur. Mit Hilfe der OSCI-Bibliothek können OSCI–Transport Nachrichten erstellt, signiert, verschlüsselt, versandt, empfangen, dechiffriert und geprüft werden.

Die Bibliothek dient *nicht* der Erstellung oder der Weiterverarbeitung der Inhaltsdaten, dies ist Sache der Clientsysteme und Fachverfahren auf Seiten der Autoren und der Leser dieser Inhalte. Im Sinne einer Modularisierung gehören zum Beispiel Kryptobibliotheken, Signaturerstellungseinheiten und Visualisierungskomponenten *nicht* zum Bestandteil der OSCI-Bibliothek. Die Schnittstellen zwischen den eben genannten externen Komponenten und der OSCI-Bibliothek werden als Interfaces exakt definiert, damit eine möglichst einfache Integration der OSCI-Bibliothek in vorhandene DV-Systeme gesichert ist.

Die Bibliothek ist kein Intermediär im Sinne der OSCI–Transport Spezifikation. Sie verfügt *nicht* über PKI-Zugänge, und sie verfügt über keine *"Postfächer"* zur persistenten Aufbewahrung von OSCI Nachrichten. Diese Funktionalitäten werden von OSCI Intermediären bereitgestellt. Die erforderlichen Schnittstellen zwischen der OSCI-Bibliothek und den Intermediären sind im Rahmen der Spezifikation bereits beschrieben (in Form des Dialoghandlings und der definierten OSCI Auftragstypen.).

1.1.2.1 Nutzungsrechte

Die OSCI-Bibliothek wird der öffentlichen Verwaltung und den Softwareherstellern durch die OSCI–Leitstelle zur unentgeltlichen Nutzung zur Verfügung gestellt werden. Hierfür werden die kombilierten Java-Klassen (Binärform) sowie die zugehörige Dokumentation zum Download über das Internet angeboten.

Die OSCI-Bibliothek soll als *Signaturanwendungskomponente* vom BSI im Wege der Amtshilfe evaluiert werden. Hierfür wird der Quellcode gegenüber der evaluierenden Stelle offengelegt.

1.1.2.2 Finanzierung und nachhaltige Pflege

Die initiale Entwicklung der Bibliothek ist durch den MEDIA@Komm Projektauftrag an Bremen bereits abgedeckt. Eine Aufwandsabschätzung der Fa. bremen online services hat zu geschätzten Entwicklungskosten in Höhe von ca. 600 Tsd. Euro geführt. Darüber hinaus wurden bereits ca. 150 Tsd. Euro verausgabt durch die Entwicklungen im Rahmen von GOVERNIKUS (mit er Realisierung der OSCI-Bibliothek wurde also bereits begonnen).

Eine Evaluierung von (Teilen der) OSCI-Bibliothek als *Signaturanwendungskomponente* ist hierbei allerdings nicht berücksichtigt, da dies durch den MEDIA@Komm Projektaufttrag nicht gedeckt ist. Die Kosten dafür sind dezeit noch nicht bekannt. Im April 2003 wird ein Workshop mit TÜV-IT durchgeführt werden, der zu einer Kostenschätzung für die Evaluierung führen wird. Zu beachten ist, dass — nach Empfehlung des BSI — die Evaluierung erst durchgeführt werden soll, wenn die Software einen *"angemessen stabilen Stand"* hat.

Pro Jahr wird für die nachhaltige Pflege ein Betrag in Höhe von 20% der Entwicklungskosten benötigt. Dies ergibt eine Summe in Höhe von ca. 120 Tsd. Euro pro Jahr.

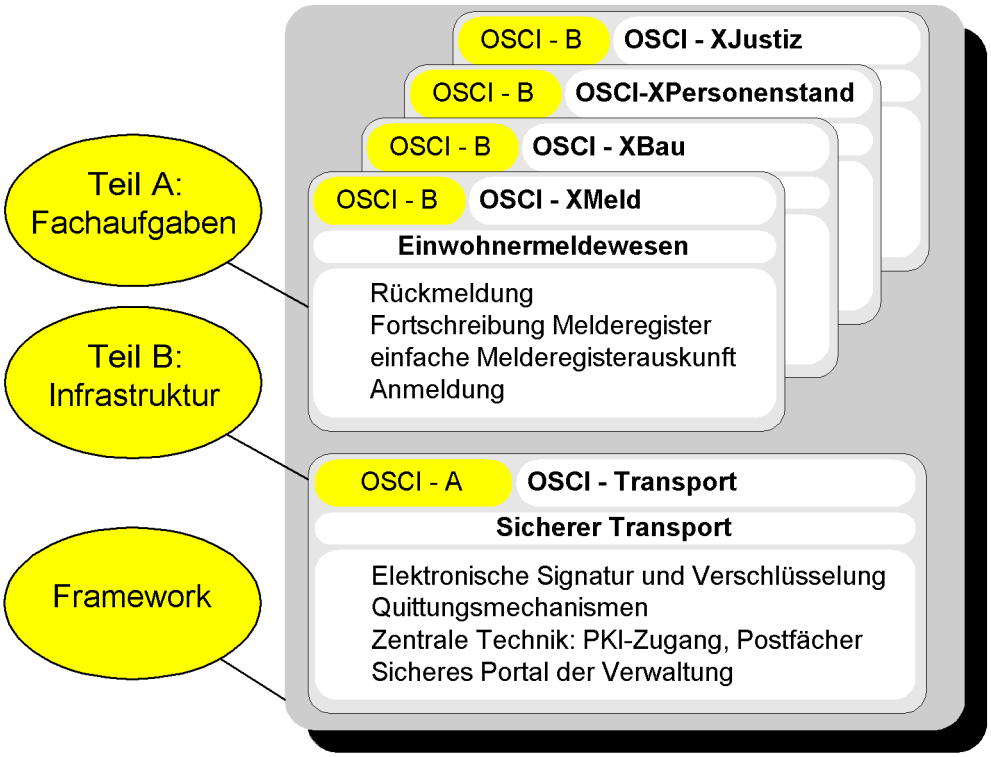
Hinzu kommen Kosten für den erforderlichen Support bei der Anwendung und Implementierung der Bibliothek durch Fachverfahrenshersteller. Hier gibt es zwei Varianten:

1. Der Support ist kostenpflichtig, er wird nach Aufwand abgerechnet.
2. Für den Planungszeitraum bis 2005 wird für den zu erwartenden Supportaufwand eine Stelle bei der OSCI–Leitstelle finanziert, entsprechend der Ziffer 5 des KoopA–ADV Beschlusses 3-11/2002. (Im Jahre 2005 muss für die länderübergreifende Rückmeldung eine flächendeckende, sichere Infrastruktur zwischen Meldeämtern etabliert sein. Die Bibliothek muss dann in allen EWO-Fachverfahren — bzw. in den Clearingstellen — installiert worden sein. Deshalb ist eine Planung bis 2005 sinnvoll.)

Um eine optimale Betreuung der Verfahrenshersteller sicherzustellen, empfehlen wir die zweite Variante. Er gibt der Leitstelle Planungssicherheit für die Zeit, in der die Infrastruktur aufgebaut wird. Im Jahre 2005 sollte der Supportbedarf überprüft und ggfs. verändert werden. In diesem Falle werden für Pflege, Wartung und Support Kosten von insgesamt ca. 190 Tsd. Euro pro Jahr erforderlich sein (120 Tsd. Euro für Wartung und Pflege, zzgl. Kosten für eine Stelle). Dieser Betrag wurde in der Gesamtplanung (Tabelle 1 auf Seite 22) für die Bibliothek eingesetzt.

1.2 Fachaufgaben

In diesem Abschnitt werden Projekte beschrieben, bei denen die Strukturierung und Standardisierung der Inhaltsdaten im Vordergrund steht. Nur durch die Übermittlung strukturierter Inhalte läßt sich deren medienbruchfreie Weiterverarbeitung in den DV-Systemen der Empfänger erreichen. Dies ist eine unabdingbare Voraussetzung für Effizienzsteigerung und Kostensenkung durch automatisierte Datenübermittlung.



In den hier beschriebenen Projekten wird von der unterliegenden Transport- und Übermittlungsschicht verlangt, dass bestimmte Sicherheitsfunktionalitäten gegeben sind. Es handelt sich dabei um

- die elektronische Signatur (in unterschiedlichen Qualitätsniveaus) für die Integrität und Authentizität;
- die Verschlüsselung zur Wahrung der Vertraulichkeit; sowie
- Quittungs- und Zeitstempelverfahren.

Dies sind Bestandteile einer *sicheren Infrastruktur*, wie sie durch OSCI–Transport gewährleistet wird. Insofern bauen die hier beschrieben OSCI-B Projekte auf den Ergebnissen von OSCI–Transport auf.

1.2.1 OSCI im Meldewesen (OSCI–XMeld)

Am 4. April 2002 wurde das Melderechtsrahmengesetz (MRRG) novelliert. Die Novellierung verfolgte unter anderem ausdrücklich das Ziel, die Nutzung neuer Medien zuzulassen, um Geschäftsprozesse des Meldewesens effizienter, effektiver und für die Kunden attraktiver anbieten zu können. Für die Umsetzung in Landesrecht stehen den Ländern zwei Jahre zur Verfügung.

In dem Projekt OSCI–XMeld werden die Datenaustauschformate für die Geschäftsvorfälle des Meldewesens definiert und normiert. Es hat bei allen Beteiligten eine große Akzeptanz gefunden. Die Version 1.0 von OSCI–XMeld wurde im März 2002 vorgestellt. Seitdem laufen Pilotprojekte zur Umsetzung unter anderem in Niedersachsen, Nordrhein Westfalen, Berlin, Baden Württemberg und Bayern. Derzeit läuft das Folgeprojekt OSCI–XMeld 1.1, es ist terminiert bis Mai 2003. Der Auftraggeber des Projektes OSCI–XMeld ist zur Zeit noch der KoopA–ADV, dies wird aber in Folgeprojekten korrigiert werden, Zuständig ist die IMK.

Von besonderer wirtschaftlicher Bedeutung ist der melderechtliche Vorgang der *“Rückmeldung”*. In einem Informationsverbund zwischen den Meldeämtern werden Nachrichten ausgetauscht, um die Konsistenz der Daten in den Melderegistern zu sochern. Bisher erfolgt die Rückmeldung (zumindest bei der nachrichtenübermittlung zwischen verschiedenen Bundesländern) konventionell, also mittels Briefpost. Dies führt zu Kosten in Höhe von ca. 2,50 Euro pro Fall. Bei mehr als 2 Millionen länderübergreifender Rückmeldungen pro jahr ist esein erklärtes Ziel des Gesetzgebers, diese Kosten durch die Nutzung moderner Technologien zu reduzieren.

Eine vom AK1 der Innenministerkonferenz eingerichtete Projektgruppe *"Meldewesen"* formuliert als *realistisches Ziel*:

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

Es ist davon auszugehen, dass in einer novellierten Fassung der 1. BMeldDÜV das Protokoll OSCI–Transport in Kombination mit OSCI–XMeld als verbindliche Vorgabe für die länderübergreifende elektronische Datenübertragung gemacht werden wird (siehe Seite 25). Mit dieser Novellierung ist im Jahre 2003 zu rechnen.

OSCI–XMeld ist die erste Standardisierung von Inhaltsdaten der öffentlichen Verwaltung im Sinne des KoopA–ADV Beschlusses 4-9-2000. Diese Standardisierung der Informationmsobjekte des Meldewesens haben eine gute Grundlage für weitere fachbezogene Standardisierungen geschaffen, weil Grunddaten wie *"natürliche Person"*, *"Anschrift"*, etc. bereits modelliert zur Verfügung stehen. Es ist offensichtlich, dass diese Informationsobjekte in weiteren Standardisierungsprojekten, wie zum Beispiel *"XPersonenstand"* genutzt werden können. Die Synergieeffekte werden dann eintreten. Der KoopA–ADV hat darauf in dem Beschluss 1-12-09 Bezug genommen.. Zur Vermeidung von Doppelarbeit und zur Schaffung eines übergreifenden OSCI-Regelwerks (Framework) müssen die bereits modellierten OSCI-Inhaltsdaten datenbankgestützt zur Verfügung gestellt werden. Es muss eine Datenbank entwickelt werden, auf die von verteilten Stützpunkten über das Internet zugegriffen werden kann. Dieser Aspekt wird im Abschnitt 1.3.1 auf Seite 9 näher erläutert.

1.2.2 OSCI in der Justiz

Die Arbeitsgruppe *"IT-Standards in der Justiz"* hat einen *"Grunddatensatz Justiz"* erstellt. Das Ziel besteht darin, zu einer einheitlichen Definition von Basisobjekten im Justizbereich zu kommen. Der Grunddatensatz soll Softwareherstellern zur Vorgabe bei Verfahrensentwicklungen gemacht werden. So soll eine effizienter Daten- und Dokumentenaustausch in Verfahren der Justiz sichergestellt werden.

Genau wie bei OSCI–XMeld werden die Informationsobjekte in XML notiert. Viele der Basisobjekte sind zu den in OSCI–XMeld definierten Informationsobjekten sehr ähnlich. Daher wurde frühzeitig mit der OSCI–Leitstelle Kontakt aufgenommen, um sicherzustellen, dass die Entwicklungen aufeinander abgestimmt werden.

Die *"Bund - Länderkommission Justiz"* hat auf Ihrer Sitzung im November 2002 beschlossen, dass (über den KoopA–ADV) Kontakt mit der Leitstelle aufzunehmen ist, um Synergieeffekte nutzen zu können. Es wird ein Betrag von ca 50 Tsd. Euro pro Jahr für die Unterstützung veranschlagt (siehe Abschnitt A.3.1 auf Seite 26).

Die Arbeitsgruppe hat ihre Arbeitsergebnisse, den in XML-Schema notierten Grunddatensatz, unter dem Aspekt der XML - Nutzung qualitätssichern lassen. Das Ergebnis hat deutlich gemacht, dass ein hoher Bedarf an *"Schema Guidelines"* (siehe Seite 14) besteht, wie sie im Rahmen des OSCI Frameworks erarbeitet werden sollen.

1.2.3 OSCI im Bauwesen (XBau)

In Esslingen wird ein Stützpunkt für OSCI im Baubereich entstehen. Unter dem Namen *"XBau"* wird eine Menge von Informationsobjekten entstehen, die für ein *Bauantragsverfahren* erforderlich sind. Hierfür ist es notwendig, die in allen Bundesländern verschiedenen Bauantragsformulare auf Gemeinsamkeiten zu untersuchen. Folgende Ziele sollen erreicht werden:

- Im Projekt XBau werden die inhaltlichen Anforderungen und Abhängigkeiten für Verwaltungsvorgänge im Bereich des Bauens analysiert und entworfen. Die Ergebnisse aus dem OSCI Projekt Datenaustauschformat OSCI–XMeld werden berücksichtigt.
- Der Standard XBau ermöglicht die interoperable Nutzung und medienbruchfreie Übergabe von Daten bzw. Informationen in heterogenen EDV-Umgebungen.
- Im Projekt XBau werden auf Grundlage vorhandener Geschäftsprozessanalysen und -optimierungen XML-Schemata entwickelt.
- XBau definiert einheitliche verbindliche Informationsbausteine als qualitative Schnittstellendefinition. Auf Grundlage dieser Standards können beliebige Formularmasken generiert werden, mit denen eine strukturierte Datenerfassung und Ausgabe ermöglicht wird.
- Die Schnittstelle legt die Grundsyntax bundesweit fest und sollte nach Möglichkeit normativen Charakter haben. Erweiterungen oder Ergänzungen können mit dem offenen Protokoll problemlos berücksichtigt werden. Auf regionale und kommunale Anforderungen sowie zukünftige Gesetzesänderungen kann flexibel reagiert werden. Alle Definitionen werden in einer zentralen öffentlich zugänglichen Datenbank dokumentiert.
- Das Projekt endet mit Vorlage der XML Schemata. Die Realisierung, z.B. XML-Codierung und Implementierung in bestehende Plattformen oder Oberflächen erfolgt in konkreten Umsetzungsprojekten.

Die Projektorganisation ist noch im Entstehen. Die Gremienbesetzung steht noch nicht fest, demzufolge gibt es auch noch keine verbindlich vereinbarten Projektauftrag.

1.2.4 OSCI im Personenstandswesen (XPersonenstand)

In der Phase 3 des Projektes OSCI–XMeld 1.1 werden die Beziehungen zwischen den Meldeämtern und den Standesämtern untersucht. Im Vorfeld ist deitlich geworden, dass es sehr wahrscheinlich ein hohes Nutzenpotenzial bei der Standardisierung von Nchrichten des Personenstandswesen (mit den Standesämtern im Mittelpunkt) geben wird.

Es gibt einen hohen Nachrichtenaustausch zwischen den Standesämtern, außerdem übermitteln die Standesämter viele ihrer Daten an andere Behörden. Aufgrund der einschlägigen gesetzlichen Grundlagen werden die meisten dieser Nachrichten elektronisch signiert sein müssen.

Eine Novellierung des Personenstandsrechts ist geplant. Dabei wird offenbar — ähnlich wie im Melderechtsrahmengesetz — der Einsatz neuer Technologien zur Effizienzsteigerung und Kostensenkung gewünscht.

Wegen der Nähe zum Meldewesen ist es sehr wahrscheinlich, dass sich viele OSCI–XMeld Ergebnisse übernehmen und weiterverwenden lassen. Nähere Untersuchungen stehen allerdings noch aus. Es gibt noch keine genauere Projektplanung.

1.3 OSCI Framework

Bei einem Vergleich der OSCI Initiative mit den Standardisierungsaktivitäten anderer Länder wird ein wichtiger Unterschied deutlich:

- In vielen Ländern wird eine E–Government-Gesamtstrategie *“von oben herab”*, also *top-down*, entwickelt. Von Regierungsseite werden globale und allgemein anwendbare Techniken, Regularien und Standards ausgewählt oder entwickelt. Diese Vorgaben müssen dann in konkreten E–Government Projekten verfeinert und angewandt werden.
- Bei OSCI wird — zumindest bisher — eher ein *bottom up* Ansatz verfolgt. Anhand einer konkreten Problemstellung, nämlich der flächendeckenden technischen Umsetzung des novellierten Melderechtsrahmengesetzes, wurden unmittelbar einsetzbare Lösungen entwickelt. Die in diesem Projekt entstandenen Techniken, Regularien und Standards sind jedoch nicht nur im Meldewesen einsetzbar. Vielmehr läßt sich vieles von dem, was im Meldewesen entwickelt wurde, auch in anderen Projekten einsetzen.

Sofern die *bottom up* Strategie beibehalten werden soll, werden auch weiterhin *“Leitprojekte”* benötigt. Nach derzeitigem Kenntnisstand bietet sich dafür das Projekt OSCI–XMeld an, zumindest bis zum Jahre 2005. (In dem Abschnitt 1.3.1 auf Seite 9 wird detailliert beschrieben, weshalb das so ist.) Bis 2005 wird die länderübergreifende Rückmeldung umgesetzt sein. Es wird dann also eine flächendeckende OSCI Infrastruktur geben müssen, um den elektronischen Informationsverbund zwischen Meldeämtern zu realisieren. In dieser Infrastruktur sind dann die heterogenen DV-Strukturen aller Bundesländer eingebunden. Es muss die notwendigen Verbindungen zu Verzeichnisdiensten und PKIen geben. Aufgrund der jetzt bereits existierenden (und teilweise weit fortgeschrittenen) Pilotprojekte ist absehbar, dass dann auch die Anwendungen zwischen den Meldeämtern und den privaten Kunden (also G2C und G2B) geben wird. Ob es nach 2005 andere Projekte geben muss, die die Rolle des Leitprojektes übernehmen, und welche das sein können, ist derzeit noch nicht absehbar.

1.3.1 OSCI–XMeld als Leitprojekt

Das Meldewesen ist derzeit eine Art *“OSCI Leitprojekt”*. Viele andere Projekte können von den Ergebnissen aus den Tätigkeiten der Leitstelle im Meldewesen profitieren. Als Gründe, warum sich derzeit gerade das Meldewesen für diese Rolle besonders gut eignet, sind zu nennen:

a. Der Bund als zuständiger Gesetzgeber hat durch die zielgerichtet Novellierung des Rahmengesetzes die Umsetzung von E–Government erst ermöglicht. Aufgrund der Rahmengesetzgebung gibt es trotz unterschiedlicher Ländergesetze einen genügend großen bundeseinheitlichen Kern.
b. Es gibt mit der *Rückmeldung* einen Geschäftsvorfall, der sich hervorragend für eine Automatisierung eignet. Die Nutzenpotenziale sind bei der Rückmeldung offensichtlich, daher gibt es ein belegbares ökonomisches Interesse der Verwaltung an der Umsetzung von E–Government.
c. Mit dem bundsweit abgestimmten DSMeld liegt ein guter Ausgangspunkt für die Erstellung eines Informationsmodells vor.
d. Im Meldewesen wird ein sehr breites Spektrum von Techniken gefordert:
    - Das Meldewesen hat Bürger (G2C), Unternehmen (G2B) und andere Behörden (G2G) als Kunden.

- Die Sicherheitsanforderungen reichen von *“unsigniert, unverschlüsselt”* (bei der einfachen Melderegisterauskunft über das Internet) bis hin zu *“qualifizierte elektronische Signatur, Ende-zu-Ende verschlüsselt”* (bei der *Anmeldung* und der *Gesamtauskunft an den Betroffenen.*
- Es gibt Geschäftsvorfälle mit Paymentfunktionalität (Melderegisterauskunft).
- Bei den Übertragungstechniken benötigt man sowohl die eMail - ähnliche *one way Message* (für die Rückmeldung und die Fortscheibung des Melderegisters), als auch die synchrone Kommunikation mittels *request - response.*

e. Im Rahmen der technischen Umsetzung des E–Governments im Meldewesen müssen Lösungen aus unterschiedlichen Bereichen zusammengeführt werden, die sonst häufig getrennt betrachtet werden. Neben der Standardisierung des Datenaustaschformats wird eine unterliegende sichere Infrastruktur und die Verbindung zu PKIen und Verzeichnisdiensten benötigt. Auf technischer Ebene sind somit OSCI–XMeld, OSCI–Transport sowie ISIS-MTT und ggfs. weitere Techniken involviert. Die DV Ausstattuneng der Bundesländer sind heterogen. In manchen Ländern wird es eine Clearingstellen geben, in anderen keine, und manchmal gibt es mehr als eine Clearingstelle. Die Frage der PKI-Anbindung und des Verzeichnisdienstes wird im Meldewesen auf anspruchsvolle Art und Weise prototypisch gelöst werden müssen. Dabei sind die *PKI-1 Verwaltung* und (vermutlich zumindest in einigen Bundesländern) das *TESTA-Netz* einzubuinden. Die dabei gemachten Erfahrungen werden anderen OSCI Projekten zu Gute kommen.

   Die flächendeckende Umsetzung der automatisierten Rückmeldung im länderübergreifenden Verkehr wird bis 2005 stattfinden. Dies erfordert eine flächendeckende Ausstattung der Meldeämter (bzw. der beauftragten Clearingstellen) mit OSCI. Um diesen Prozess möglichst pragmatisch ablaufen zu lassen, wird von der zuständigen Innenministerkonferenz eine OSCI-Bibliothek gefordert. Dies ist im Abschnitt 1.1.2 auf Seite 4 beschrieben. Es ist davon auszugehen, dass zumindest bis zu diesem Zeitpunkt noch viele Impulse für die Weiterentwicklung von OSCI–Transport aus dem Bereich des Meldewesens kommen werden.

Die im Rahmen der OSCI–XMeld Projekte entstandenen Kenntnisse über Techniken, Regularien und Standards sind zunächst unmittelbar auf das Meldewesen bezogen. Sie müssen abstrahiert, verallgemeinert und damit auch für andere Projekte nutzbar gemacht werden. Dieses *“Framework”* wird im Abschnitt 1.3 auf Seite 9 beschrieben. In der Tabelle 1 sind projektspezifische und verallgemeinerbare Ergebnisse und Erfahrungen dargestellt.

Tabelle 1: Verallgemeinerbare Erkenntnisse aus OSCI–XMeld

Thema	Meldewesen-spezifisch	OSCI allgemein
Initiierung des Projektes	1. Das Projekt wurde gestartet, weil es einen breit getragenen Konsens gab, dass durch die automatisierte Datenübermittlung im Meldewesen konkrete Nutzenpotenziale für die öffentliche Verwaltung zu erschließen sind. 2. Vor dem Beginn eines bundesweiten Projektes wurde in einem Pilotprojekt die prinzipielle Machbarkeit nachgewiesen.	1. Bundesweite OSCI Projekte können erst beginnen, wenn Vorarbeiten und Vorklärungen (zum Beispiel aus Pilotprojekten) die Machbarkeit realistisch erscheinen lassen. Es muss auf Seiten des Auftraggebers einen Konsens darüber geben, dass der für die öffentliche Verwaltung zu erwartende Nutzen die kalkulierten Kosten rechtfertigt.
Projektorganisation	1. Es wurde eine Projektstruktur mit den Gremien *"Arbeitsgruppe"*, *"Abstimminstanz"* und *"Entscheidungsinstanz"* sowie der Projektleitung etabliert, die sich als sehr zielführend erwiesen hat. 2. Es gibt klar definierte Ziele und die regelmässige Rückkopplung mit der Entscheidungsinstanz über den Projektablauf 3. Es gibt diverse Interessengruppen mit jeweils unterschiedlichen Zielen und Möglichkeiten, diese Ziele durchzusetzen.	1. Die erfolgreiche Gremienstruktur (beschrieben im Abschnitt 4 auf Seite 14) kommt generell für alle OSCI Projekte zur Anwendung. Ausgehend von den Erfahrungen mit OSCI–XMeld wird eine schematische Gremienbesetzung für OSCI Projekte benannt. Der Rolle der *Hersteller*, der *Lösungsanbieter* aus der Privatwirtschaft sowie des DIN als Standardisierungsgremium ist dabei zu klären. 2. Es gibt kein OSCI Projekt ohne einen *verantwortlichen Auftraggeber,* mit dem die *Projektziele in einen Projektauftrag verbindlich vereinbart* worden sind. 3. Es ist zu prüfen, ob man die aus OSCI–XMeld bekannten Interessen der potenziellen Projektbeteiligten (öffentliche Verwaltung, Hersteller, Nutzer etc.) hinsichtlich anderer E–Government Projekte verallgemeinern kann. Wer hat ein Interesse an *Herstellerunabhängigkeit* und *Interoperabilität*, und aus welchen Gründen besteht dieses Interesse?

Thema	Meldewesen-spezifisch	OSCI allgemein
Vorgehen bei der Modellierung	1. Es ist eine MDA (*"model driven architecture"*) Umgebung entstanden, bei der fast ausschliesslich in UML modelliert wird. Toolunterstützt werden daraus XML Schemata und ein wesentlicher Teil der Dokumentation generiert. Dabei wurde deutlich, dass der Aufwand der Ergebnisdokumentation ohne die Toolunterstützung nicht leistbar gewesen wäre.	1. Die Art der Modellierung und der Dokumentation wird auch für andere Projekte übernommen. (Formale Modellierung in UML, Beschränkung auf drei grundlegende Diagrammtypen, hochgradig automatisierte Ergebnisdokumentation …) Die Tools (für MDA und die Dokumentation) müssen hinsichtlich der Verwendbarkeit in anderen Projekten geprüft und gegebenenfalls erweitert werden. Siehe hierzu Bild 5 auf Seite 15. Die Art, wie fachliches Wissen aufgenommen, modelliert und dann in die technischen Ergebnisse umgesetzt wird, soll auch in anderen Projekten zur Anwendung kommen.
Datenstrukturen und Nachrichten in XML Schema	1. Grundlegende Datentypen 2. Nachrichten, spezifisch für das Meldewesen	1. Objekte wie *"natürliche Person"* oder *"Anschrift"* müssen auf Verwendbarkeit in anderen Projekten überprüft werden Das *"Baukastenprinzip"* hat sich bewährt. 2. Wie nutzen wir XML? Nach welchen internen Regeln setzen wir UML-Modelle in XML-Schema um? Es muss eine Art *"Schema Guideline"* (analog eines entsprechenden Dokuments der englischen eGif Initiative) für andere OSCI Projekte entwickelt werden. 3. Wie gehen wir mit den (zwingend erforderlichen) landesspezifischen Erweiterungen um? Wie behandeln wir Versionierung?
Nachhaltige Pflege und Change Management	Es gibt bisher noch wenig konkrete Erfahrungen mit der nachhaltigen Pflege und dem vorgeschlagenen Change Management Prozess. Diese Erfahrungen wird es geben, wenn der Produktivbetrieb aufgenommen wird.	Die zu erwartenden Erkenntnisse aus der Praxis müssen bei der Planung anderer OSCI Projekte berücksichtigt werden.

Thema	Meldewesen-spezifisch	OSCI allgemein
Parallele Aktivitäten	1. Neben der fachlichen Arbeit war eine permanente Aktivität im Sinne eines Marketings erforderlich. (Erläuterung der Projektergebnisse in verschiedenen Medien, Präsentationen auf unterschiedlichen Veranstaltungen, Information weiterer potenzieller Beteiligter …) Diese Aktivität war nicht nur während des eigentlichen Projektes erforderlich, sondern ständig, also auch zwischen Projektphasen. 2. Die Kommunikation mit der Fachministerkonferenz erfolgt außerhalb des eigentlichen Projektes (über die *"Würzburger Gruppe"* und den AK I).	1. Diese Aktivitäten sollten bei weiteren OSCI Projekten von vornherein geplant und bei der Aufwandskalkulation berücksichtigt werden. 2. Bei zukünftigen Projekten muss die zuständige Fachministerkonferenz bzw. ein Unterausschuß davon von Beginn an angemessen in das Projekt integriert sein.

In OSCI–XMeld wurden einige Vorgehensweisen und Techniken entwickelt, von denen andere Projekte profitieren werden. Es ist die Aufgabe der OSCI–Leitstelle, diese Methoden und Techniken so vom konkreten Projekt zu abstrahieren und zu verallgemeinern, dass andere Projekte davon Nutzen haben. Daher ist die OSCI–Leitstelle in dem Leitprojekt OSCI–XMeld auch operativ tätig. In dem Projekt, in dem die erstmalige Entwicklung stattfindet, ist der Aufwand zwangsläufig höher als in anderen Projekten mit vergleichbarem Projektauftrag.

1.3.2 Aktueller Stand des OSCI Framework

Charakteristisch für ein OSCI Leitprojekt ist die direkte, operative Beteiligung der OSCI–Leitstelle. Die Aufgabe der OSCI–Leitstelle in einem Leitprojekt besteht darin, die neuen Erkenntnisse und Erfahrungen zu abstrahieren, zu verallgemeinern und somit für andere Projekte nutzbar zu machen. Aus diesem Grunde wird der Aufwand eines OSCI Leitprojektes höher sein als der anderer Projekte mit vergleichbarem Projektauftrag. So sind im OSCI–XMeld Projekt Techniken ausprobiert und entwickelt worden, die nunmehr anderen OSCI Projekten zu Gute kommen. Derzeit profitiert das Meldewesen stark von einem hohen Engagement der OSCI–Leitstelle, andererseit profitieren die OSCI–Leitstelle (und damit auch andere OSCI Projekte) von den Erfahrungen.

Um sicherzustellen, dass in allen OSCI Projekten Synergieeffekte optimal genutzt werden können, muss — basierend auf den Erfahrungen aus konkreten Projekten — ein Framework erstellt werden, welches für alle OSCI Projekte (Teil A: Infrastruktur, und Teil B: Fachaufgaben) verbindlich ist. Es besteht aus einem Regelwerk, dem alle Projekte zu genügen haben, die die geschützte Marke *"OSCI"* in ihrem Namen führen (zum Beispiel OSCI–XMeld). Auch die Nutzung eines projektspezifischen Logos mit dem OSCI Zeichen ist an die Einhaltung dieses Regelwerkes geknüpft.

Dieses Regelwerk ist erst im Entstehen. Nach jetzigem Kenntnisstand (basierend auf den Erfahrungen aus den Projekten *"OSCI–Transport"* und *"OSCI–XMeld"* und diversen Diskussionen schlagen wir folgendes initiales Regelwerk vor.

1.3.2.1 Generell

1. OSCI Projekte werden im Auftrag der öffentlichen Verwaltung durchgeführt, um E–Government umsetzen zu können.
2. Die Standardisierungsaktivitäten erfolgen in einem offenen Prozess mit Beteiligten aus Verwaltung und Wirtschaft. Alle erzielten Ergebnisse müssen herstellerunabhängig und interoperabel sein.

   Soweit möglich, sind akzeptierte internationale Standards zu nutzen.
3. OSCI Projekte dienen dem Ziel, die sichere und medienbruchfreie Übermittlung und Weiterverarbeitung von Daten zwischen Kommunikationspartnern zu ermöglichen oder zu optimieren, damit E–Government Geschäftsvorfälle schneller, effizienter, kostengünstiger und bürgerfreundlicher abgewickelt werden können. Zu diesem Zweck wird eine sichere Infrastruktur (weiter-) entwickelt (OSCI Teil A), oder es werden Nachrichteninhalte strukturiert und normiert (OSCI Teil B). Bei der Modellierung wird der Standpunkt eines *neutralen Dritten* eingenommen.

   Es ist nicht das Ziel von OSCI, interne Prozesse der Kommunikationsbeteiligten zu standardisieren. Gleichwohl ist es erforderlich, auf grober Ebene Verfahrensabläufe festzulegen, um verbindlich zu beschreiben:

- unter welchen Umständen welche Nachrichten übermittelt werden; und
- wie auf Nachrichten reagiert werden soll.

4. Das Produkt eines OSCI–Transport Projektes sind Spezifikationen von Datenstrukturen (notiert in XML Schema) und Prozessabläufen für eine sichere Infrastruktur für E–Government.

   Das Produkt eines OSCI-B Projektes sind Spezifikationen von Datenstrukturen (notiert in XML Schema) und Prozessabläufen für die interoperable und herstellerunabhängige Übermittlung strukturierter Inhaltsdaten.

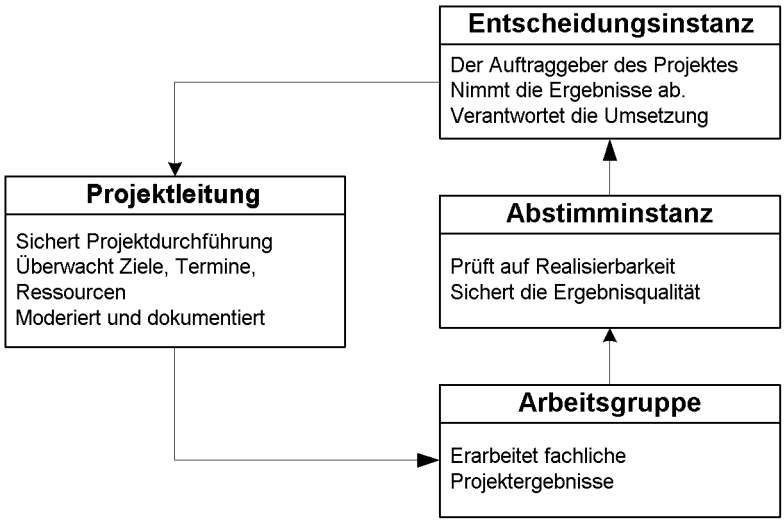
   Das Produkt von Projekten im Bereich OSCI Framework sind (innerhalb des OSCI Kontextes) allgemein verwendbare Regeln, Handlungsanweisungen oder Softwarekomponenten, die in OSCI-A oder OSCI-B Projekten genutzt werden können (und sollen).

1.3.2.2 Projektorganisation

5. Bundesweite OSCI Projekte sollten erst beginnen, wenn Vorarbeiten und Vorklärungen (zum Beispiel aus Pilotprojekten) die Machbarkeit realistisch erscheinen lassen. Es muss auf Seiten des Auftraggebers einen Konsens darüber geben, dass der für die öffentliche Verwaltung zu erwartende Nutzen die kalkulierten Kosten rechtfertigt.
6. In jedem Projekt gibt es die Gremien *“Arbeitsgruppe”*, *“Abstimminstanz”* und *Entscheidungsinstanz* sowie die Projektleitung (siehe Bild 4).

   Die Entscheidungsinstanz repräsentiert den Auftraggeber. Sie ist besetzt durch Vertreter aus der öffentlichen Verwaltung.
7. Bevor ein OSCI Projekt beginnen kann, muss es einen verbindlich mit dem Auftraggeber vereinbarten Projektauftrag geben. In diesem sind die Ziele des Projektes, das kalkulierte Budget die Beginn- und Endetermine genannt. Die Gremienbesetzung muss klar sein.
8. Bei der Planung und Aufwandskalkulation des Projektes ist die nachhaltige Pflege der Ergebnisse und der nach dem Projektende erforderliche Marketingaufwand mit zu berücksichtigen. Es muss bereits zum Projektbeginn eine Stelle geben, die als Ansprechpartner dient und für die nachhaltige Pflege und Verbreitung der Ergebnisse auch zwischen Projekten verantwortlich ist (Projektverantwortlicher).
9. Eine nachträgliche Änderung erzielter Ergebnisse (auch im Sinne einer Fehlerbehebung oder einer Weiterentwicklung) darf nicht ungeordnet erfolgen. Es ist ein definierter Change management Prozess zu beachten. Dies ist durch den Projektverantwortlichen sicherzustellen.

Bild 4 Die Gremien in OSCI Projekten



1.3.2.3 Umgang mit Ergebnissen

10. Bis zur Abnahme durch die Entscheidungsinstanz sind alle Projektergebnisse als intern zu betrachten, sie dürfen nicht nach außen gegeben werden.

    Nach der erfolgten Abnahme sind die in den Projekten erzielten Ergebnisse (XML Schema Dateien und Ergebnisdokumentation) öffentlich verfügbar. Sie werden der OSCI–Leitstelle zur Verfügung gestellt. Diese veröffentlicht die Ergebnisse im Internet.

Alle im Rahmen von OSCI Projekten erarbeiteten Dokumente und Spezifikationen müssen für alle interessierten Kreise unentgeltlich und frei über das Internet erhältlich sein. Auch die Druckerzeugnisse müssen unentgeltlich erhältlich sein.

Die Publikation der Ergebnisse in Standardisierungsgremien (zum Beispiel als *PAS*) wird nur dann unterstützt, wenn dadurch der freie, schnelle und unentgeltliche Zugang zu den Ergabnissen nicht in Frage gestellt wird.

11. Andere Projekte sollen möglichst auf bereits erzielte Ergebnisse (insbesondere bereits standardisierte, übergreifende Informationsobjekte) anderer OSCI Projekte zurückgreifen. Falls hierfür Änderungen an Ergebnissen anderer Projekte erforderlich sind, so ist ein Change Management Prozess zu initiieren.

1.3.2.4 Schema Guidelines

Die systematische Erarbeitung von*Schema Guidelines*, in denen der technische Umgang mit XML Schema geklärt wird, hat noch nicht begonnen. Das Thema ist recht neu, viele Schema - Konzepte werden kontrovers diskutiert. Eine Bearbeitung muss sorgfältig und unter Hinzuziehung von Experten erfolgen. Die Erstellung eines solchen *Schema Guide* ist aber unbedingt erforderlich, da dies eine kritische technische Bedingung für die korrekte Datenübermittlung ist, und da vor Ort (also in der Verwaltung und bei den Lösungsanbietern auf Herstellerseite) oft nur wenig Kompetenz vorhanden ist. Zudem gibt es oft mehrere Lösungswege, die alle *“richtig”* sind. Es wäre fatal, wenn in jedem OSCI-Projekt jeweils andere Lösungsalternativen gewählt würden.

Fragen, die in diesem Zusammenhang zu betrachten sind, lauten zum Beispiel:

- Welche Schema Notation? (Vorschlag: w3c Schema)
- Dokumenten- oder Datenorientiert? (Vorschlag: Datenorientiert. Kein *mixed content.*)
- Elemente oder Attribute? (Vorschlag: Elemente)
- Sprache für Tagnamen und Annotation: Englisch oder Deutsch? (Bisher verwenden wir bei OSCI–Transport Englisch, bei OSCI–XMeld Deutsch. Möglicherweiseb wäre es besser, generell Englisch zu nehmen, aber die Entscheidung darüber ist nicht einfach zu treffen.)
- Umgang mit *Namespaces* und landesspezifischen Erweiterungen.
- Umgang mit elaborierten Schema Mechanismen (redefine, restriction, extension und so weiter),

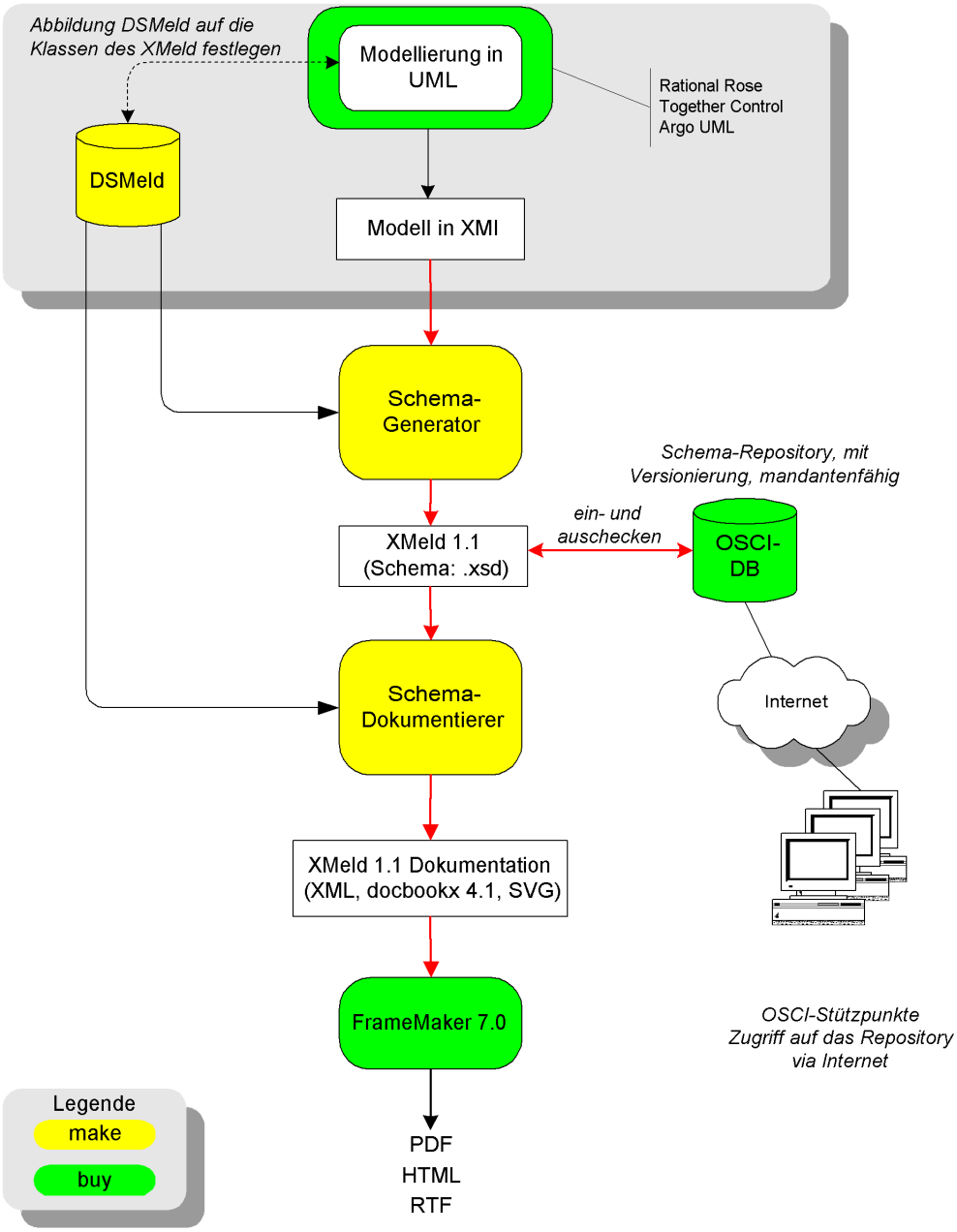
Als Vorgabe für einen eigenen *Schema Guide* kann das entsprechende Dokument aus dem englischen *eGif* Projekt dienen, darüber hinaus natürlich die in der OSCI–XMeld Praxis bewährten Entscheidungen. Außerdem gibt es einen Input aus einer externen Qualitätssicherung des *“Grunddatensatzes Justiz”*.

1.3.2.5 Tools und Applikationen

Zu dem Framework gehören außerdem Software-Tools und Anwendungen, die der Erarbeitung der OSCI Ergebnisse oder deren gemeinsamer Nutzung im Internet dienen:

- Im Rahmen des OSCI–XMeld Projektes sind Tools entstanden, die eine *model driven architecture* (MDA) unterstützen. In UML modellierte Fachmodelle werden in XMI exportiert und durch die von der OSCI–Leitstelle entwickelten Werkzeuge automatisiert in XML Schema Definitionen konvertiert.. Mittel eines Zusatztools werden wesentliche Teile der Ergebnisdokumentation automatisiert erstellt (siehe Bild 5). Diese Werkzeuge wurden so programmiert, dass sie generell bei OSCI-B Projekten eingesetzt werden können.
- Zur Koordination verschiedener OSCI Projekte ist eine Datenbank zu entwickeln, in der die unterschiedlichen Projektergebnisse (möglichst in versionierter Form) vorgehalten werden können.
- Es ist eine Internetpräsenz zu entwickeln, die als Kommunikations- und Informationsplattform über OSCI dient.

Bild 5 MDA - Tools, entwickelt im Projekt OSCI–XMeld



1.4 OSCI und andere Standards bzw. Netze

Mit OSCI wird nur der Teilbereich des E–Government adressiert, in denen für eine Kommunikation über das Internet eine Sicherheitsarchitektur und ein Sicherheitstandard bzw. -protokoll erforderlich ist, mit denen die Rechtsverbindlichkeit einschließlich elektronischer Signatur und Verlaufsprotokoll sichergestellt wird.

Es ist also eindeutig nicht das Ziel, OSCI–Transport als Ersatz für bestehende Standards im Bereich geschlossener Nutzergruppen oder auch als Zugangsstandard (Identifizierung) für einzelne Anwendungen zu etablieren. Im Krypto-Leitfaden des KoopA wird OSCI–Transport in dem Szenario "Sicherheitsinfrastruktur für übergreifende medienbruchfreie E–Government-Anwendungen" (siehe dort, Punkt 5.6) aufgeführt. Im der Version 1.1 des SAGA Dokuments wird OSCI–Transport für den Bereich der *“Transaktion / Integration”* als obligatorischer Standard genannt. Daran wird deutlich, dass OSCI nicht jedes Problem lösen soll und gleichzeitig, dass durch OSCI nicht alle anderen bereits etablierten Standards und Lösungsalternativen ersetzt werden sollen. Im Folgenden wird OSCI zu anderen Standardisierungsaktivitäten positioniert.

1.4.1 ISIS–MTT und OSCI

ISIS–MTT (mit SigG-Profil) regelt die Datenstrukturen und die Dienstprotokolle einer PKI *(Public-Key-Infrastruktur),* die als technische Basis für PKI-basierte Sicherheitsdienste im elektronischen Datenverkehr dient. Eine PKI ist die modernste und sicherste technische Lösung, um die Vertrauenswürdigkeit, die Integrität und die Authentizität der Datenübertragung in einem großen Teilnehmerkreis und über öffentlichen Übertragungskanäle — insbesondere im Internet — sicherzustellen. Neben der Regelung der allgemeinen PKI-Dienste (Zertifizierung, Verzeichnisdienste, Zertifikatsprüfung, Zeitstempel) legt ISIS–MTT (mit SigG-Profil) Nachrichtenformate für sichere E–Mail fest, die derzeit die verbreiteteste PKI-basierte Anwendung repräsentiert.

Eine weitere, wichtige Anwendung ist die elektronische Signatur nach SigG: ISIS–MTT (mit SigG-Profil) legt zusätzliche Regeln für Dienste und Client-Anwendungen fest, welche die Einhaltung der Anforderungen des Signaturgesetzes (sowohl nach nationalen als auch nach europäischen Richtlinien) sowie eine Interoperabilität der Systeme gewährleisten.

OSCI hat eine andere Zielsetzung bzw. ein anderes Zielgebiet. OSCI spezifiziert keine eigenen, OSCI-spezifischen Mechanismen oder Funktionalitäten zur Sicherung des Datenverkehrs, sondern greift auf die Dienste einer ISIS–MTT-konformen PKI zurück. In den oben genannten Anwendungen des E–Government sind also ISIS–MTT und OSCI komplementär: sie ergänzen einander, da OSCI–Transport die Transportmechanismen und die Nachrichtenformate definiert, während ISIS–MTT einen wesentlichen Teil der notwendigen Sicherheitsmechanismen abdeckt.

1.4.1.1 Kompatibilität

Da OSCI im Bezug auf Sicherheitsmechanismen vollständig auf ISIS–MTT (mit SigG-Profil) aufsetzt, gibt es generelle *keine Widersprüche oder Inkompatibilitäten* zwischen den zwei Spezifikationen.

Bisher konnte nur ein einzige Punkt isoliert werden, bei dem noch Handlungsbedarf bezüglich der Kompatibilität zwischen OSCI–Transport und ISIS–MTT besteht. Die von OSCI definierten Datenstrukturen der Transportschicht und der Applikationsschicht werden mit Hilfe von XML definiert und dargestellt, während ISIS–MTT im sicheren E–Mailverkehr und bei Dateiverschlüsselung auf das ASN.1-basierte CMS *(Cryptographic Message Syntax)* setzt. Beide Datenformate haben ihre Berechtigung und sind international weit verbreitet:

- CMS ist das traditionelle Format für sichere E–Mails und PKI-Protokolle
- XML setzt sich wegen seiner höheren Flexibilität zunehmend in modernen Web-basierten Applikationen durch

Es ist jedoch ohne Probleme möglich, ISIS–MTT-Zertifikate und Zeitstempel in XML-Dokumente einzubinden, und dadurch XML-Anwendungen an eine PKI zu binden.

Die Bildung der XML-Signatur wird derzeit von ISIS–MTT (mit SigG-Profil) noch nicht geregelt. Dieser Tatbestand stellt jedoch kein generelles technisches Hindernis und keinen prinzipiellen Widerspruch zwischen ISIS–MTT und OSCI dar.

Es gibt zwischenzeitlich einen Projektantrag des ISIS MTT Boards, ISIS MTT um die XML Signatursyntax zu ergänzen. Dabei ist sichergestellt, dass die Ergebnisse von OSCI–Transport herangezogen werden. So kann der Anschluß des XML-Anwendungsfeldes an ISIS–MTT erreicht werden kann.

1.4.1.2 Konsequenzen für Anwender

1. In Verbindung mit OSCI können ISIS–MTT-konforme Produkte (d.h. Signaturkarten, Chipkarten-Treibersoftware und PKI-Dienste) *beliebiger* Zertifizierungsdienstanbieter (z.B. Datev, D-Trust, Telesec, Signtrust, TC Trustcenter) benutzt werden;
2. Eine weitgehende Deckungsgleichheit der Konformitätsaspekte ist bereits gegeben, nur die Generierung von XML-Signaturen liegt im Moment noch außerhalb des geregelten Bereichs von ISIS–MTT (mit SigG-Profil).

1.4.2 OSCI und Entwicklungen in der EU

Wie in Deutschland wird auch im europäischen Ausland an der Entwicklung von E–Government gearbeitet. Insbesondere in UK und in Schweden liegen Konzepte vor, die einer genaueren Betrachtung bedürfen. Im Vergleich zu diesen zeichnet sich OSCI bereits durch eine vergleichsweise große Verwendung aus. Beide Ansätze werden in der IDA (Interchange data between administrations) - Group der europäischen Union diskutiert und als Vorgehensweise oder *“framework”* empfohlen.

In Bezug auf OSCI stellt sich folgendes Bild dar:

- In Schweden wird eine landesweite Transaktionsplattform SHS (im europäischen Zusammenhang eLink genannt) zur Integration verschiedener Backend-Systeme aufgebaut. Diese Plattform wurde von der schwedischen Steuerverwaltung konzipiert. Technisch werden dieselben Anforderungen wie in Deutschland gestellt (TCP/IP, http, SSL, XML, X.500 und LDAP), allerdings wird als Transaktionsprotokoll nicht SOAP eingesetzt — möglicherweise weil der Beginn der Konzeption zeitlich vor der Standardisierung von SOAP lag.

  Bisher sind (uns) keine Spezifikationen für den Bereich der sicheren und rechtsverbindlichen Transaktionen ohne Medienbrüche inkl. der elektronischen Signatur sowie praktische Erfahrungen mit elektronischen Signaturen und PKI bekannt, die aber konzeptionell auch in Schweden gefordert werden.

  Am 11.2.2003 fand in Brüssel die Sitzung der Expertengruppen *Interoperability Framework* und *eLink* statt. In der Diskussion stellte sich ein großes Interesse an OSCI–Transport heraus. Schweden teilte mit, dass die OSCI-Spezifikationen aktueller als die schwedische sei (die von 1998 stamme) und befürwortete deshalb die Übernahme der entsprechenden Inhalte. Deutschland bot an, dass die OSCI-Bibliothek auch der EU und den Mitgliedsstaaten zur Verfügung gestellt wird
- In England gibt es eine (von Tony Blair) ins Leben gerufene E–Government-Strategie mit namen eGif, die mit viel Personalkapazität (ca. 240 MA in der Zentrale) und politischer sowie wirtschaftlicher Unterstützung (z.B. Microsoft) landesweite Konzepte entwickelt und durchsetzt. Für Neuentwicklungen und Online-Dienste ist z.B. in dem umfassenden E–Government-Konzept zur Standardisierung der Einsatz von http, XML und Browser-Technologien verbindlich vorgeschrieben.

  Organisatorische Lösungen für E–Government sind ein wesentlicher Bestandteil der Konzepte, die in sogenannten Frameworks niedergelegt sind. Im *"security-framework"* (vergleichbar mit dem Handlungsleitfaden für Signaturen und Verschlüsselungen des KoopA) werden hinsichtlich der Signaturen die selben Anforderungen gestellt wie in Deutschland - auch in UK geht man davon aus, dass anwendungsbezogen das erforderliche Sicherheitsniveau festgelegt wird, wobei vier verschiedene Sicherheitsstufen vorgesehen sind.

  Im Gegensatz zu OSCI gibt es keine Integration der Signaturen als integraler Bestandteil einer Spezifikation eines Transaktionsprotokolls.

  eGif entsteht im Unterschied zu OSCI in einer *top-down* Strategie: von der Regierung werden die Regularien und Techniken auf abstrakter und allgemeiner Ebene vorgegeben, sie *müssen* dann in konkreten Projekten entsprechend den gemachten Vorgaben umgesetzt werden.

Zusammenfassend lässt sich feststellen, dass OSCI keine Konkurrenz zu den Ansätzen in UK und Schweden darstellt. Es ist jedoch notwendig, im Sinne der europäischen Interoperabilität die Entwicklung von OSCIund anderen europäischen Initiativen zu koordinieren. Dazu ist die Mitarbeit in IDA - speziell in den beiden Expertengruppen zu Interoperabilität und Standardisierung - erforderlich, die als Konsequenz aus der e-LINK-Machbarkeitsstudie von der Kommission einberufen wird und auch den Status von OSCI prüfen soll. Diese Gruppe wird sich voraussichtlich zunächst fünf Mal im Jahre 2003 treffen. Darüber hinaus wird die Durchführung von bilateralen Abstimmgesprächen mit besonders weit fortgeschrittenen Initiativen als sinnvoll angesehen - speziell mit UK, SE und FRA. Für jedes Land werden mindestens zwei Reisen mit zwei Personen in die jeweiligen Hauptstädte durch zu führen sein, unter der Annahme, dass jeweils zwei Gegenbesuche der Länder stattfinden.

Ergänzt werden sollen die Aktivitäten durch Vorstellen von OSCI und den Ergebnissen der Interoperabilitätsbemühungen auf mindestens vier Konferenzen: in Vilnius im Rahmen der Northern eDimension (Ostsee-Anrainer und IDA-Programm), Januar 2003; 2. E-Government-Konferenz der Kommission in Como, Mai oder Juni 2003; zwei weitere Veranstaltungen im Rahmen von IDA-Aktivitäten oder des Maastrichter Institute for Public Administration.

Für die Gremien und Projektarbeit in der EU ist eine personelle Kontinuität erforderlich. Es wird von einem Aufwand von jährlich 0,5 MJ ausgegangen. Die Freie Hansestadt Bremen möchte den Sitz in der IDA TAC-Gruppe für den Bundesrat übernehmen und auch finanzieren. Hiervon verspricht sie sich einen Imagegewinn, für den sie bereit wäre, 0,5 Stellen zu investieren. Die zusätzlichen Reisekosten für die OSCI/IDA-Expertgroups sind allerdings nicht im Budget, so dass diese zu finanzieren wären.

1.4.3 Internationale Standards

Viele Hersteller von Computersoftware, speziell für Internet-Anwendungen, haben ein Interesse an sicheren Transaktionsdienstleistungen. Die von OSCI gewählten Standards XML, SOAP, XML Signature und XML Encryption spielen dabei eine große Rolle. In Initiativen wie WS-I oder OASIS versuchen die *"Big Player"* wie z.B. Microsoft, SUN oder IBM, die Standardisierung entsprechender Protokolle voranzutreiben. Nach den uns vorliegenden Informationen gleichen diese in ihrer Struktur der Architektur von OSCI.

Es besteht deshalb die wahrscheinlich einmalige Möglichkeit, das in OSCI geförderte Knowhow in die Entwicklung weiterer Industriestandards aus Bereich Web-Services einzubringen. Damit würde der deutschen E–Government Branche im günstigsten Fall, bei einem Durchsetzen von OSCI in diesen Gremien, ein Wettbewerbsvorteil verschafft werden. Im schlechtesten Fall würde die OSCI–Leitstelle frühzeitig über die Entwicklung informiert und könnte evtl. entstehende Entwicklungen zeitnah umsetzen.

Konkret ist die OSCI–Leitstelle von dem Organisator des neu eingerichteten Technical Committee *"E–Government"* innerhalb von OASIS um ihre Teilnahme gebeten worden. Geprüft werden muss noch, inwieweit eine (alternative) Mitgliedschaft im Technical Committee *"WS-I"* erforderlich ist.

Personelle Ressourcen für die weltweite Etablierung von OSCI sind zur Zeit bei der OSCI–Leitstelle weder finanziell noch personell abgedeckt. Es wird geprüft, ob dieses Aktivitäten vom BSI übernommen werden könnten.

1.4.4 OSCI und HBCI (als Beispiel von Standards anderer Branchen)

OSCI sollte in Anlehnung an den Standard der Kreditwirtschaft für sichere Finanztransaktionen im Internet, den Home Banking Computer Interface (HBCI)-Standard entwickelt werden. Vom Aufbau her ist dieses auch gelungen; so stellt das Dreischichtenmodell in HBCI dieselben Schichten wie in OSCI dar. In der konkreten Spezifikationsphase von OSCI 1.0, in der Phase der Anforderungsermittlung aus insgesamt ca. 70 Anwendungen sowie durch die erste Implementierungsphase, wurde deutlich, dass das Rollenverständnis von HBCI für Online-Dienstleistungen mit der öffentlichen Verwaltung nicht ausreichend ist. Geht HBCI von dem Modell *"meine Bank und ich"* aus — also Offenlegung aller Daten bei einer Bank (alle Konten, Kredite, etc.) —, so gibt es ein solches einfaches Rollenverständnis der Verwaltung nicht. Vielmehr geht man hier immer davon aus, dass die Daten für eine Behörde nur für sie und nicht für andere Behörden bestimmt sind. Dies schreibt nicht nur das Verständnis der Bürger/-innen vor, sondern ist auch durch das Zweckbindungsgebot der Datenschutzgesetze vorgeschrieben, das nur im festgelegten Umfang eine Weitergabe von Daten an andere ermöglicht.

Somit musste die Spezifikation von OSCI ein komplexeres Rollenmodell berücksichtigen und sich damit von HBCI unterscheiden. Langfristig ist jedoch eine Angleichung von HBCI auf der Ebene Transport und Sicherheit zu erwarten, weil im Bereich der Kreditwirtschaft zunehmend Fremddienstleister (z.B. Broker) eingeschaltet werden, die nicht in Kenntnis aller Kundendaten kommen sollen. Dieser Bereich muss also weiterhin genau betrachtet werden, um Synergien herzustellen. Wird OSCI von mehreren Branchen eingesetzt, wird die Entwicklung von OSCI-konformen Produkten für Softwarehersteller einen größeren Nutzen bringen. Da häufig Verwaltungsdienstleistungen Bezahlungen, die ja auch über HBCI - Produkte abgewickelt werden können, nach sich ziehen, wären OSCI-konforme Produkte für Banken und Verwaltungen für die Nutzer erheblich ergonomischer und nutzerfreundlicher (ein Produkt für Homebanking und Verwaltungsdienstleistungen).

Die Möglichkeit, mit den Basiskomponenten einer OSCI–Transport - Infrastruktur eine *"virtuelle Poststelle"* aufbauen zu können, ist durchaus nicht nur für den öffentlichen Bereich und die Kreditwirtschaft interessant, sondern auch für andere Branchen. Überall dort, wo Vertraulichkeit verschiedener Anwendungen und deren Inhalte sowie Authentifizierung automatisiert erfolgen soll, bietet sich das Modell von OSCI–Transport an.

1.4.5 OSCI und TESTA

Das TESTA - Netz ist ein verwaltungsinternes, geschlossenes Netz. Es bietet den Anwendern aus der öffentlichen Verwaltung Mehrwertdienste, insbesondere im Bereich der Sicherheit.

Die Zielgruppe und der Fokus von TESTA ist damit ein anderer, als der von OSCI. TESTA bezieht einen wesentlichen Teil seiner Sicherheit daraus, dass es eben kein öffentliches Netz ist, sondern nur einem definierten Nutzerkreis zur Verfügung steht. OSCI hingegen legt eine Sicherheitsschicht über die im Internet gebräuchlichen Transportprotokolle (`http`) und ermöglicht damit die sichere und nachvollziehbare Datenübermittlung über öffentliche Netze. Schließlich lebt E–Government zu wesentlichen Teilen von der Kommunikation zwischen der Verwaltung und den *externen* Kunden der Verwaltung, also den Bürgern und den Unternehmen der Privatwirtschaft. *G2C* und *G2B* Kommunikation setzt ist aber mit verwaltungsinternen Netzen natürlich nicht durchführbar.

Andererseits bietet das TESTA-Netz (insbesondere in der Verbindung mit Verzeichnisdiensten und PKI-Strukturen) für den Fall der verwaltungsinternen Kommunikation Dienste an, die bei OSCI optional sind. Daher kann es zum Beispiel durchaus sinnvoll sein, dass OSCI und TESTA gemeinsam genutzt werden. Es kann in bestimmten Szenarien sinnvoll sein, dass die Vertraulichkeit der Datenübermittlung durch TESTA Basisdienste sichergestellt wird, während eine darüber liegende OSCI Schicht füe die elektronische Signatur und die Nachvollziehbarkeit mittels Quittungen realisiert.

2. KAPITEL: ORGANISATION UND FINANZIERUNG

Ein wesentlicher Leitgedanke bei dem Lösungsvorschlag ist es, aus der Projektstruktur von MEDIA@Komm heraus einen Transfer in die bestehenden Strukturen der öffentlichen Verwaltung zu organisieren und das Thema dort als dauerhafte Aufgabe zu verankern. Es wäre aufgrund der bereits zahlreich vorhandenen Gremien im Öffentlichen Dienst nicht sinnvoll, neben bestehenden Strukturen neue aufzubauen, die neue Abstimmungsnotwendigkeiten schaffen würden. Deshalb wurde sehr frühzeitig durch Bremen sichergestellt, dass Beschlüsse zu OSCI durch das für infrastrukturelle Aufgaben zuständige Gremium KoopA–ADV (Kooperationsausschuss ADV Bund/Länder/kommunaler Bereich) gefasst wurden.

Zielsetzung muss es sein, dass langfristig in den Regularien (Richtlinien für den Einsatz der ADV, Vorgaben von Normen und Standards, etc.) des Bundes, der Länder und der Kommunen OSCI als ein einzuhaltender Standard aufgenommen wird, auf den bei Ausschreibungen etc. referenziert werden kann. Nur so kann auch für die Softwareindustrie die erforderliche Planungssicherheit hergestellt werden. Die Aufnahme von OSCI–Transport als obligatorischer Standard für Transaktionen im SAGA-Papier entspricht diesem Ziel.

Unserem föderalen System wird eine Mischform mit zentralen Aufgaben und dezentralen Aktivitäten am ehesten gerecht. Hierbei muss genau abgewogen werden, welche Aufgaben als strategische Aufgaben zentral anzusiedeln sind und welche Aufgaben operativ als dezentrale Aktivitäten durchgeführt werden könnten. Im Folgenden werden Aufgaben und Rollen beschrieben, die im Zusammenhang mit OSCI langfristig anfallen.

Für den dauerhaften Betrieb von OSCI werden zwei verschiedene OSCI-Rollen mit unterschiedlichen Aufgaben im Verwaltungszusammenhang benötigt::

- Die OSCI–Leitstelle für das Framework (siehe Seite 9f) und die Querschnittsaufgaben. Hierzu gehört insbesondere die Weiterentwicklung von OSCI–Transport sowie die Herausgabe und Pflege der OSCI-Bibliothek.

  Da es sich um infrastrukturelle Maßnahmen handelt, ist auf Seiten der öffentlichen Verwaltung der KoopA–ADV zuständig. (Siehe Ziffer 2 des KoopA–ADV Beschlusses 3-11/2002, Seite 24). Der KoopA–ADV ist der Auftraggeber der Projekte zu diesen Themen.
- OSCI-Stützpunkte für fachlich abgrenzbare Bereich aus OSCI—Teil B.

  Da es sich um Fachaufgaben handelt, sind Fachministerkonferenzen und deren Untergliederungen zuständig (siehe Ziffer 3 des oben angegebenen KoopA–ADV Beschlusses). Diese fungieren als Auftraggeber der entsprechenden Projekte.

  Die OSCI–Leitstelle ist zuständig für die Koordinierung dieser fachlichen Aufgaben, um Doppelarbeiten zu vermeiden und Synergieeffekte zu optimieren. Sie sammelt und veröffentlicht die Ergebnisse an zentraler Stelle.

Die Beteiligung der darüber hinaus gehenden (verwaltungsinternen und -externen) Fachöffentlichkeit erfolgt über fest etablierte Reviews nach den Beschlussfassungen in den jeweils zuständigen Fachgremien.

Die beiden Rollen und ihre Aufgaben werden im Folgenden präzisiert.

2.1 Aufbau- und Ablauforganisation

2.1.1 OSCI–Leitstelle

Die OSCI–Leitstelle übernimmt die steuernden Aufgaben für den gesamten Standardisierungsprozess (OSCI-Teile A und B sowie *Framework*). Dort laufen alle Aktivitäten zusammen und werden von dort koordiniert.

Aufgabe	**Zuständig / Finanzierung**
Die OSCI–Leitstelle ist zuständig für die Entwicklung und nachhaltige Pflege von OSCI–Transport (siehe Abschnitt 1.1.1 auf Seite 2). Sie sammelt und priorisiert neue Anforderungen an OSCI–Transport und unterbreitet dem KoopA–ADV Vorschläge für Projekte zur Weiterentwicklung. Der KoopA–ADV entscheidet über die Projekte. Kommen sie zu Stande, so bildet der KoopA–ADV die Entscheidungsinstanz.	KoopA–ADV
Die OSCI–Leitstelle koordiniert für den KoopA–ADV die Entwicklung und nachhaltige Pflege einer OSCI-Bibliothek (Abschnitt 1.1.2 auf Seite 4). Die OSCI–Leitstelle stellt sicher, dass die Weiterentwicklungen des Standards OSCI–Transport und der OSCI-Bibliothek aufeinander abgestimmt erfolgen.	KoopA–ADV
Sie bringt OSCI in EU-weiten und internationalen Standardisierungsgremien ein (siehe Abschnitt 1.4.2 auf Seite 17).	KoopA–ADV
Sie erarbeitet im Auftrag der KoopA–ADV ein Framework (siehe Abschnitt 1.3 auf Seite 9). Dieses besteht aus einem Regelwerk, dem alle OSCI Projekte (auch die fachlich orientierten aus Teil B) zu genügen haben, sowie Tools und Anwendungen, die von allen OSCI Projekten genutzt werden können. Zu den Anwendungen gehört eine Datenbank, in der Informationen und Ergebnisse aller OSCI Projekte vorgehalten werden, sowie eine zentrale OSCI Internetpräsenz.	KoopA–ADV
Sie koordiniert im Auftrag des KoopA–ADV die Entwicklung der fachlich orientierten OSCI-B Projekte. Sie überprüft, ob die verbindlich vereinbarten Regeln des *Frameworks* in den OSCI Projekten eingehalten werden.	KoopA–ADV
Die OSCI–Leitstelle bietet Beratung, Schulung und sonstige Dienstleistungen für OSCI B Projekte an. Die OSCI–Leitstelle wird sich darum bemühen, dass sie von dem zuständigen Auftraggeber in die Projekte zur Erarbeitung und Pflege der Inhaltsdaten einbezogen wird.	Jeweils projektbezogen durch den zuständigen Auftraggeber, dies sind Fachministerkonferenzen beziehungsweise deren Untergliederungen.

2.1.2 OSCI-Stützpunkte

Sogenannte OSCI-Stützpunkte könnten in den jeweiligen Ländern, in Kommunen oder beim Bund (beziehungsweise in zuständigen Fachgremien) eingerichtet werden, Es ist auch möglich, dass Firmen diese Aufgabe im Auftrag der jeweilig ernannten Stützpunkte wahrnehmen. Hierbei muss sichergestellt werden, dass die jeweilige Verwaltungseinheit die Zusammenarbeit innerhalb der Verwaltung herstellt und die Zielsetzung vorgibt.

Diese Stützpunkte haben fachliche Verantwortung für mindestens einen Schwerpunkt (z.B. XBau, OSCI–XMeld, XJustiz, XPersonenstand …). Sie sind tätig für die zuständige Fachministerkonferenz beziehungsweise deren Untergliederung.

Die Stützpunkte werden durch die OSCI–Leitstelle eingesetzt. Dafür wird die OSCI–Leitstelle prüfen:

1. Gibt es einen Auftraggeber aus der öffentlichen Verwaltung (Fachministerkonferenz oder Untergliederung), mit dem ein Projektauftrag verbindlich vereinbart wurden ist?
2. Sind durch Projektauftrag die Projektziele, das Budget und die Laufzeit klar definiert?

3. Entspricht das Projekt dem Regelwerk im *Framework* ?
4. Ist die nachhaltige Pflege der Projektergebnisse sichergestellt?
5. Ist sichergestellt, dass es kein anderes OSCI Projekt mit gleichen oder ähnlichen Zielen gibt?

Wenn diese Kriterien erfüllt sind, wird der Stützpunkt eingesetzt. Ab dann kann die geschützte Marke OSCI und das OSCI Logo genutzt werden. Das Projekt und der Stützpunkt werden in der OSCI Internetpräsenz aufgenommen.

Die Leitstelle wird den Stützpunkten bzw. den Auftraggeber ihre Mitarbeit in den Projekten gegen Finanzierung anbieten.

2.2 Finanzierung

2.2.1 Erforderlicher Aufwand für infrastrukturelle Aufgaben

In der folgenden Tabelle sind die Aufwände genannt, die nach dem Ende des MEDIA@Komm Projektes für für infrastrukturellen Aufgaben (OSCI Teil A und Framework) anfallen werden. Das sind die Kosten, die den Ziffern zwei und vier des KoopA–ADV Beschlusses 3-11/2002 entsprechen.

Tabelle 1: Aufwände für infrastrukturelle Aufgaben

Aufgabe	Investiv (Tsd. Euro)	Jährlich (Tsd. Euro)	Zuständig
Weiterentwicklung von OSCI–Transport und OSCI Framework (ohne Software - Lizenz- und Wartungskosten): 2 Stellen		120	BMI (Finanzierungszusage liegt vor).
Entwicklung einer Datenbank für die Projektergebnisse, Aufbau einer Internet - Präsenz:	100	15	ggfs. zusammen mit SAGA, dies wird geprüft
Entwicklung, Weiterentwicklung und nachhaltige Pflege der OSCI-Bibliothek (siehe Abschnitt 1.1.2.2 auf Seite 6.	Die Entwicklung ist bereits durch MEDIA@Komm finanziert Kosten für eine Evaluierung als Signaturanwendungskomponente sind noch nicht bekannt.	120	KoopA–ADV Umlage
OSCI-Bibliothek: Support für die Entwickler, die die Bibliothek in ihre Fachverfahren einbauen werden.		60	Durch die Hersteller, die die OSCI-Bibliothek nutzen.
Mitarbeit in EU Gremien. Ein geschätzter Bedarf von 0,5 Stellen wird durch die Freie Hansestadt Bremen finanziert. Allerdings werden Reisekosten benötigt.		klären	Reisekosten müssen noch geklärt werden
Mitarbeit in weltweiten Standardisierungsgremien			Ist noch zu klären. Kann ggfs. durch BSI übernommen werden.
Summe	100	315	

Anhang A: Beschlusslage der öffentlichen Verwaltung

A.1 Beschlusslage des KoopA–ADV

A.1.1 Beschluss 5-9-99 des KoopA–ADV

Der KoopA ADV befürwortet den Aufbau eines OSCI-Standards in Kongruenz mit den HBCI-Standards der Kreditwirtschaft. Hierfür wird eine enge Kooperation der Öffentlichen Verwaltung mit der Kreditwirtschaft im Bereich der Spezifikation der (SigG-konformen) Signatur und Geldkarte, im Bereich der (SigG-konformen) Kartenleser, der dezentralen Personalisierung sowie bei der Entwicklung des OSCI-Standards angestrebt. Der KoopA ADV bittet Bremen, ihn in die inhaltliche Arbeiten einzubeziehen und in der nächsten Sitzung zu berichten.

A.1.2 Beschluss 4-9-2000 des KoopA–ADV

1. Der KoopA ADV bekräftigt, dass als wichtige Voraussetzung für den Übergang zu e-government die Entwicklung von Verwaltungsnachrichten auf der Basis von XML und ihre semantische Standardisierung notwendig und dringlich sind.
2. Priorität sollen bei dieser Entwicklung diejenigen Aufgabenfelder erhalten, in denen bereits (bundesweit) standardisierte Datenformate und -inhalte existieren (z.B. im Melde- und Kfz-Wesen oder für Ausschreibung und Vergabe von Bauleistungen) oder die in den MEDIA@Komm-Projekten als Verwaltungsleistungen in Selbstbedienung (z.B. Bauanträge) vorgesehen sind.
3. Der KoopA ADV bittet Bremen, geeignete organisatorische und technische Vorkehrungen zu treffen, um eine möglichst aktive Mitwirkung aller interessierten Stellen an diesem Vorhaben zu ermöglichen und die Ergebnisse umfassend verfügbar zu machen.

A.1.3 Beschluss 1-12-09 des KoopA–ADV

1. Der KoopA - ADV begrüßt die Erarbeitung eines Informationsmodells "XMeld" für den standardisierten Datenaustausch im Einwohnerwesen. Das Informationsmodell soll anderen, im E-Government tätigen Projekten und Gremien mit dem Ziel der Wiederverwendung definierter Objekte zur Verfügung gestellt werden
2. Der KoopA - ADV betrachtet das Informationsmodell für die Bereiche "Natürliche Person" und "Anschrift" als Basis für Neuentwicklungen im E-Government und empfiehlt den Mitgliedern, bei Ausschreibungen, in denen diese Datensätze benötigt werden, auf die Kompatibilität zu den modellierten Objekten Wert zu legen.

A.1.4 Beschluss 1-12-10 des KoopA–ADV

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 E-bene 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 Abstim-mung 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.

A.1.5 Beschluss 3-11/2002

1. Der KoopA–ADV begrüßt die grundsätzliche Bereitschaft des Bundes, die Finanzierung der für die längerfristige Etablierung des OSCI-Standards erforderlichen Infrastruktur im Sinne der folgenden Nummern 2 bis 6 zu übernehmen.
2. Der KoopA–ADV ist zuständig für infrastrukturelle IT-Entwicklungen der öffentlichen Verwaltung. Er ist deshalb für die Standardisierungsinitiative OSCI zuständig und beabsichtigt, die nachhaltige Pflege und Weiterentwicklung der OSCI-Protokolle sicherstellen; hierbei bezieht er sich auf den Teil A von OSCI (*“OSCI Transport”*), der die Infrastruktur betrifft.
3. Der Teil B von OSCI betrifft Fachaufgaben. Für die Pflege und Weiterentwicklung sind die jeweils zuständigen Fachministerkonferenzen und deren Untergliederungen zuständig. Der KoopA–ADV bietet (über die OSCI–Leitstelle) eine Koordinierung dieser fachlichen Aufgaben IT-gestützt an, um eine Wiederverwendung bereits modellierter Objekte zu ermöglichen und somit Doppelarbeit zu vermeiden.
4. Um eine möglichst schnelle, planbare und pragmatische Verbreitung von OSCI–Transport sicherzustellen erachtet der KoopA–ADV es für geboten, eine OSCI-Bibliothek zu entwickeln, zu pflegen und der öffentlichen Verwaltung zur Verfügung zu stellen. Er bittet die OSCI–Leitstelle, im Rahmen der Weiterentwicklung von OSCI–Transport bis zur nächsten Sitzung ein IT-technisches Konzept für diese Bibliothek vorzulegen und bezüglich der OSCI-Bibliothek die Nutzungsrechte und Förderkriterien zu klären bzw. bewerten.
5. Der KoopA–ADV bittet Bremen, baldmöglichst ein Organisations- und Finanzierungskonzept für die OSCI–Leitstelle zu erarbeiten.
6. Der KoopA–ADV bittet Bremen, baldmöglichst einen detaillierten Vorschlag für die Aufbau- und Ablauforganisation zu unterbreiten. Dabei soll die Trennung der Verantwortlichkeiten für infrastrukturelle Aufgaben (KoopA–ADV) und fachliche Aufgaben (Fachministerkonferenzen) deutlich herausgearbeitet werden.

A.2 Beschlusslage zu OSCI im Meldewesen

A.2.1 Beschluss des AK I der IMK vom 8.11.2002

1. Der AK I nimmt den Bericht der Projektgruppe *“Meldewesen”* (Stand: 08.11.02) zustimmend zur Kenntnis.
2. Der AK I hält ein effizient arbeitendes Meldewesen nicht nur aus Gründen der inneren Sicherheit, sondern auch als Dienstleistung für die Erfüllung einer großen Zahl von öffentlichen Aufgaben, insbesondere auch für die Wirtschaft für unverzichtbar.
3. Er spricht sich deshalb dafür aus,
   a. ab dem Beginn des Jahres 2005 die länderübergreifenden Geschäftsvorfälle der Meldebehörden, insbesondere die Rückmeldungen, nur noch elektronisch über Netze abzuwickeln, um einen möglichst hohen Grad an Aktualität der Melderegister zu gewährleisten;
   b. diese Kommunikation, wo notwendig, über Clearingstellen in den einzelnen Ländern abzuwickeln, um Routingprobleme und Störungen zu vermeiden;
   c. zur notwendigen Vereinheitlichung von Meldeinhalt und Transportprotokoll die im Rahmen des MEDIA@Komm-Projektes entwickelten Standards *“OSCI–XMeld”* und *“OSCI–Transport”* verbindlich vorzuschreiben;

   d. diese Standards nachhaltig zu pflegen und weiterzuentwickeln.
4. Der AK I beauftragt die Melderechtsreferenten der Länder und des Bundes,
   a. die Pflege des Standards OSCI-X-Meld zu übernehmen,
   b. dem AK I Vorschläge für konkrete Projekte zur Weiterentwicklung der Funktionalitäten von OSCI–XMeld zu machen und
   c. mögliche Tests von EWO-Verfahren, die OSCI–XMeld-tauglich sein wollen, zu organisieren.
5. Der AK I weist darauf hin, dass die Kosten für die betroffenen Stellen je nach der vorhandenen Ausstattung und je nach der von den einzelnen Ländern gewählten Lösung unterschiedlich sein werden.

   Der AK I hält die Setzung von Standards für den länderübergreifenden Datenaustausch für dringend erforderlich, um auf die ohnehin stattfindende und heranstehende Weiterentwicklung des Meldewesens rechtzeitig steuernd und kostenmindernd z.B. durch Rationalisierungseffekte einzuwirken.
6. Der AK I bittet die IMK, folgenden Beschluss zu fassen:
   1. Die IMK nimmt den Beschluss des AK I vom 08.11.2002 zu TOP 4 und den Bericht der Projektgruppe *"Meldewesen"* (Stand: 08.11.02) zustimmend zur Kenntnis.
   2. Die IMK hält ein effizient arbeitendes Meldewesen nicht nur aus Gründen der inneren Sicherheit, sondern auch als Dienstleistung für die Erfüllung einer großen Zahl von öffentlichen Aufgaben und insbesondere auch für die Wirtschaft für unverzichtbar.
   3. Die IMK bittet das BMI, die für die länderübergreifende Kommunikation der Meldebehörden untereinander notwendigen Standards OSCI–XMeld und OSCI–Transport verbindlich vorzuschreiben und festzulegen, dass keine Software im Einwohnermeldewesen eingesetzt werden darf, die nicht diese Standards implementiert hat.
   4. Die IMK hält den Standard OSCI–Transport für einen überaus wichtigen und unverzichtbaren Bestandteil der elektronischen Infrastruktur im Rahmen des E-Government auf Bundes- und Landesebene.

      Der KoopA–ADV wird deshalb gebeten, der IMK bis zu ihrer Sitzung im Frühjahr 2003 Vorschläge zu machen,
      - wie und in welchen Strukturen der Standard OSCI–Transport 1.2 nachhaltig gepflegt und fortentwickelt werden kann; dabei sollte darauf eingegangen werden,
      - ob und in welcher Form die OSCI–Leitstelle über das Ende des MEDIA@Komm-Projektes hinaus fortbestehen kann
      - wie eine *"Bibliothek"* zu diesem Standard bereit gestellt werden kann, die es Softwareherstellern ermöglicht, diesen Standard so schnell und kostengünstig wie möglich in ihre Verfahren zu integrieren.
7. Der AK I bittet seinen Vorsitzenden, den Vorsitzenden des AK VI über den Beschluss und die beabsichtigte Einbindung des KoopA–ADV zu unterrichten.

A.2.2 Beschluss der IMK vom 28.11.2002

1. Die IMK nimmt den Beschluss des AK I vom 08.11.2002 zu TOP 4 und den Bericht der Projektgruppe *"Meldewesen"* (Stand: 08.11.02) zustimmend zur Kenntnis.
2. Die IMK hält ein effizient arbeitendes Meldewesen nicht nur aus Gründen der inneren Sicherheit, sondern auch als Dienstleistung für die Erfüllung einer großen Zahl von öffentlichen Aufgaben und insbesondere auch für die Wirtschaft für unverzichtbar.
3. Die IMK bittet das BMI, die für die länderübergreifende Kommunikation der Meldebehörden untereinander notwendigen Standards OSCI–XMeld und OSCI–Transport im notwendigen Umfang verbindlich vorzuschreiben und festzulegen, dass keine Software im Einwohnermeldewesen eingesetzt werden darf, die nicht diese Standards implementiert hat.
4. Die IMK bittet die Projektgruppe *"Meldewesen"*,
   - Für das Meldewesen unter Berücksichtigung von OSCI offene (d.H. für jeden zur Nachentwicklung veröffentlichte), sachgerechte und wirtschaftliche technische Standards für die Kommunikation
     - zwischen den Meldeämtern
     - zwischen Meldeämtern und Cxlearingstellen
     - zwischen den Clearingstellen

     zu definieren, als Entwurf zu veröffentlichen und der IMK zur Beschlussfassung vorzuschlagen;
   - Organisation und Kosten für die Fortentwicklung der fachlichen und technischen Standards des Meldewesens und für die Clearingstellen zu konzipieren und dieses Konzept der IMK vorzulegen.

5. Die IMK hält den Standard OSCI–Transport für einen überaus wichtigen und unverzichtbaren Bestandteil der elektronischen Infrastruktur im Rahmen des E–Government auf Bundes- und Landesebene.

   Der KoopA–ADV wird deshalb gebeten, der IMK bis zu ihrer Sitzung im Frühjahr 2003 Vorschläge zu machen, wie und in welchen Strukturen der Standard OSCI–Transport 1.2 nachhaltig gepflegt und fortentwickelt werden kann. Dabei sollte darauf eingegangen werden,

   - ob und in welcher Form die OSCI–Leitstelle über das Ende des MEDIA@Komm-Projektes hinaus fortbestehen kann
   - wie eine *"Bibliothek"* zu diesem Standard bereit gestellt werden kann, die es Softwareherstellern ermöglicht, diesen Standard so schnell und kostengünstig wie möglich in ihre Verfahren zu integrieren.

A.3 Beschlusslage zu OSCI in der Justiz

A.3.1 Beschluss der *"BLK Justiz"* am 11/12. November 2002

- Die BLK nimmt den Zwischenbericht der Arbeitsgruppe *"IT-Standards in der Justiz"* zur Kenntnis.
- Die BLK bittet die Arbeitsgruppe *"IT-Standards in der Justiz"* mit dem KoopA–ADV Kontakt aufzunehmen, um die technische Führung, Betreuung und Integration des Grunddatensatzes für den elektronischen Rechtsverkehr mit seinen fachlichen Erweiterungen (XJustiz) unter Berücksichtigung anderer zentraler (XML-) Datensätze (z.B. OSCI–XMeld) im Rahmen der geplanten Betreuungsstelle beim KoopA–ADV vorzubereiten.
- Der auf die Justiz entfallende Kostenanteil beträgt ca. 50.000 Euro / Jahr, der nach dem Königsteiner Schlüssel auf die Landesjustizverwaltungen umgelegt wird. Das BMJ prüft eine Beteiligung.
- Die Arbeitsgruppe *"IT-Standards in der Justiz"* wird beauftragt, die genauen Kosten, die Leistungsbeschreibung und die vertraglichen Rahmenvorgaben mit dem KoopA–ADV zu klären und der BLK vor der nächsten Sitzung zur Abstimmung vorzulegen.

Anhang B: DV-technisches Konzept der OSCI-Bibliothek

B.1 Übersicht und Zielsetzung

Mit Blick auf die Fachverfahrensintegration bildet die Schnittstelle der OSCI-Bibliothek den Zugang zu einer kompletten OSCI-Infrastruktur und ist somit der einzige Punkt, an dem eine Anpassung zu den unterschiedlichen Fachverfahren erfolgen muss.

OSCI ist eine XML-Anwendung. Die Strukturen einer OSCI-Nachricht werden durch XML-Schemata beschrieben.

Die zentrale Aufgabe der OSCI-Bibliothek besteht in der Komposition valider OSCI-Nachrichten für den Versand, sowie der Dekomposition von OSCI-Nachrichten bei deren Empfang und der Prüfung ihrer syntaktischen Korrektheit. Weiter werden alle kryptografischen Funktionen zur Signaturerzeugung und -prüfung sowie Ver- und Entschlüsselung über Funktionen der Bibliothek verwaltet - wobei die eigentliche Abarbeitung kryptografischer Aufgaben incl. der Zugriffe auf Krypto-Token durch entsprechende Drittimplementierung zur Verfügung gestellt werden müssen.

In diesem Sinne werden durch die OSCI-Bibliothek alle für den vollständigen Aufbau einer OSCI-Nachricht benötigten Objekte wie die eigentlichen Inhaltsdaten, die Signatur- und Verschlüsselungszertifikate aller Kommunikationsbeteiligten und deren physikalische Adressen in Form entsprechende Klassen bzw. deren Attribute bereitgestellt.

Die Erstellung und Weiterverarbeitung von Inhaltsdaten ist nicht Aufgabe der OSCI-Bibliothek, sondern muss durch die Clientsysteme und Fachanwendungen erfolgen. Durch die Klassen und Methoden der Bibliothek wird lediglich sichergestellt, dass diese schemakonform in die Nachrichtenobjekte eingebettet werden.

Eine weitere wesentliche Aufgabe der OSCI-Bibliothek besteht in der Steuerung und Überwachung des Kommunikationsvorgangs. Für diesen Zweck stellt die Bibliothek Klassen und Methoden zur Verfügung, anhand derer die Plausibilität einer Kommunikation überprüft und dokumentiert werden kann.

Methoden für den technischen Versand und Empfang von OSCI-Nachrichten auf Basis des HTTP-Protokolls, die Bereitstellung kryptografischer Funktionen für die Signatur und Verschlüsselung von Nachrichten sowie die Visualisierung signierter Nachrichtenbestandteile sind nicht Bestandteil der OSCI-Bibliothek. Diese Funktionalitäten müssen durch separate Module realisiert werden und werden durch Java-Interfaces der OSCI-Bibliothek eingebunden. Dies erlaubt den Einsatz unterschiedlicher Module für den jeweiligen Aufgabenbereich.

Außerhalb des Funktionsumfangs und der Kontrolle der Bibliothek liegt die *TrustViewerService* Implementierung zur sicheren Visualisierung zu signierender Inhaltsdaten.

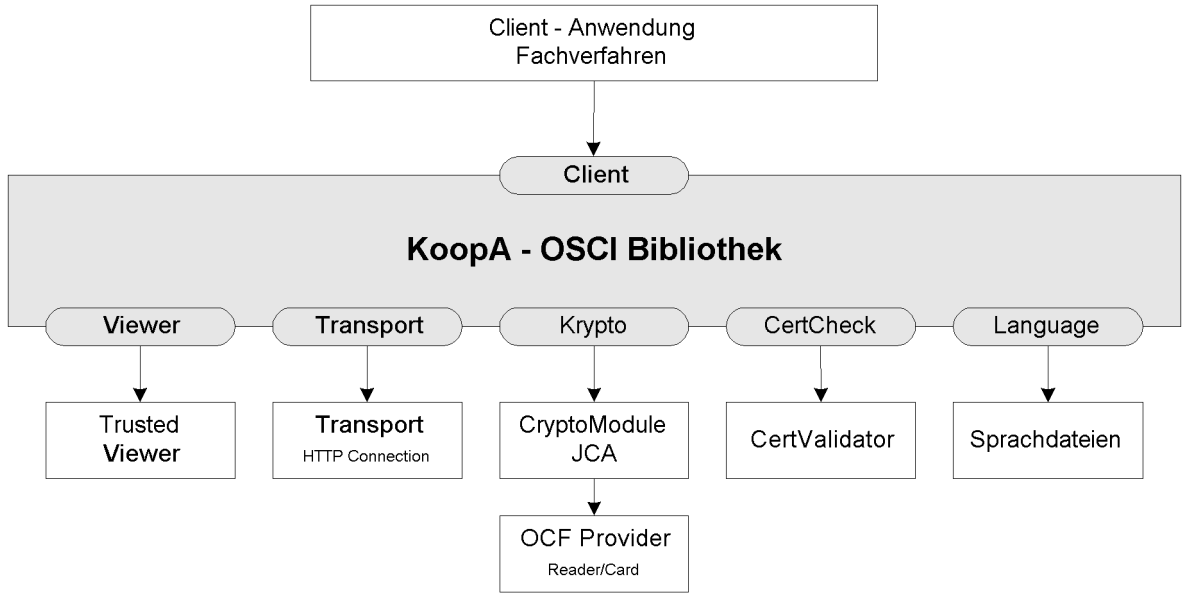
OSCI Transport 1.2 lässt beliebig viele Inhaltsdatencontainer zu. Die Bibliothek stellt lediglich die Funktionalitäten zur Verfügung, diese Inhaltsdatencontainer konform zur OSCI-Spezifikation aufzubauen.

Diese Container können von der OSCI-Bibliothek einem *TrustedViewer* übergeben werden, der in der Lage ist, die jeweiligen Inhalte konform zu den Forderungen des Signaturgesetzes darzustellen. Dieser konkrete Viewer ist bei Aufruf der Signaturfunktionen von der Anwendung jeweils anzugeben.

Damit ist eine konkrete OSCI-Implementierung in der Lage, hier beliebigen Nutzerkomfort und mit jeweils probatem GUI zur Verfügung zu stellen. Bei Bedarf können so von der Anwendung auch unterschiedliche, jeweils passende Visualisierungskomponenten für die einzelnen Inhaltsdatencontainer einer OSCI-Nachricht angezogen werden.

In dem Bild 1 sind die Interfaces und Klassen, um die es geht, dargestellt. Im Bild 2 auf Seite 31 werden die internen Strukturen gezeigt.

Bild 1 Bibliothek und Interfaces



B.2 Objekte der OSCI-Bibliothek

Die Objekte der Bibliothek sowie von dieser referenzierte Objekte einer konkreten voll funktionsfähigen Implementierung lassen sich in folgende Gruppen gliedern:

B.2.1 Konfiguration

Ein Konfigurationsobjekt stellt die statische Information einer konkreten Implementierung zur Verfügung. Es sind Interfaces definiert, deren Implementierung (nicht Bestandteil der Bibliothek !) folgende benötige Funktionen verfügbar machen muss:

- **`CertificateValidatorService`** - Dienst zur Validierung von Zertifikaten (bzw. Anbindung einer solchen Dienstes)
- `CryptoServices` - Implementierung der kryptografischen Funktionen

Zusätzlich werden hier Attribute der konkreten Implementierung geführt, die sich in der Regel während einer Session bzw. auch darüber hinaus nicht ändern - wie z.B. das bediente OSCI-Schema, zu benutzende Algorithmen für Normalisierung, Signaturerstellung und Verschlüsselung etc.

Im Standardumfang der Bibliothek wird eine Implementierung für den **`CertificateValidatorService`** zur Verfügung gestellt, die lokale (offline) Zertifikatsprüfung ermöglicht.

B.2.2 Dialog Handler

Das zentrale DialogHandler Objekt dient

1. der Verwaltung der OSCI-Sicherheitsmechanismen zur Absicherung des Dialogs. Dazu dienen Methoden zur Einstellung und zum Check von
   - *Challenge-Response*
   - *Sequence-Number* und *Conversation-Id* der Nachricht
2. der Festlegung konkreter Einstellungen für das jeweilige *Request-/Response* Tupel (bzw. auch die gesamte Session) wie

- Attribut **`checkSupplierSignature`** - Signatur des Transportumschlags von Responses prüfen (optional für einen Client).

3. *TransportModule* - Implementierung der Transportschicht (SOAP with Attachments/http)

Weiter werden hier die Referenzen gehalten auf folgende Akteurs-Objekte einer OSCI-Kommunikation (s.u.):

- Originator (Sender der Nachricht)
- Intermediär.

Eine jede OSCI *Request-/Response* Folge erhält die Referenz auf die **`DialogHandler`** Instanz, um im konkreten OSCI-Request die entsprechen aktuellen Attributwerte zu setzen und die korrespondierenden Werte der jeweiligen Response auf Korrektheit gem. OSCI-Spezifikation zu prüfen. Nach erfolgreicher Prüfung werden die Attribute zur Dialogabsicherung jeweils sofort auf die Werte gesetzt, die für die nächste *Request-Response* Sequenz gefordert sind.

Für die Initiierung einer neuen Dialogabfolge können die Attributwerte mit `startNewDialog()` initialisiert werden.

B.2.3 Akteure

Die Akteure gem. Rollenmodell der OSCI-Spezifikation werden in folgenden Objekten gehalten; für die Attribute existieren - wo benötigt - jeweils entsprechende `get` / `set` Methoden (teilweise können diese über den Konstruktor gesetzt werden):

- **`Intermediary`** - als Attribute für die Kommunikation und Verschlüsselung werden URI des Intermediärs, Verschlüsselungszertifikat und ein Name für die symbolische Adressierung benötigt.
- **`Originator`** - geführt werden müssen Signatur- und Verschlüsselungszertifikate sowie auch Anforderungen an die Qualität der jeweiligen Zertifikate (hier: Speichermedium des Kryptotokens). Bzgl. der benötigten Pin's sind zwar Attribute vorgesehen, um die prinzipielle Möglichkeit des Caching von Pin's nicht auszuschließen. Aus Sicherheitsgründen sollten die Attribute jedoch i.d.R. nicht gesetzt werden, so dass beim Zugriff auf private Schlüssel über die Krypto-Implementierung generell ein Mechanismus zur Abfrage der Pin hochgezogen wird.
- **`Adressee`** - für den Empfänger der Nachricht werden auf Seite des zustellenden Clients lediglich das Verschlüsselungszertifikat (öffentlicher Schlüssel) und ggf. ein symbolischer Name benötigt. Im Szenario Empfang eines Weiterleitungs- bzw. Abwicklungsauftrags muss das Objekt Adressee Zugriff auf private Schlüssel (Verschlüsselung und Signatur) haben.
- **`Author`** - für einen Autor müssen identische Kryptotoken wie bei Origniator verfügbar gemacht werden. Im Unterschied zum Originator können von einem Author-Objekt mehrere Instanzen vorhanden sein, die jeweils bestimmten Contents zugeordnet werden können (siehe Content-Container Objekt). Ggf. können die Rollen Author und Originator zusammenfallen - auch in diesem Fall wird zu beiden Rollen eine Instanz gebildet.
- **`Reader`** - aus Sicht eines Clients, der eine Nachricht erzeugt und zustellen will, werden für den jeweiligen Reader lediglich öffentlicher Schlüssel für die Encryption bzw. Verschlüsselungszertifikat benötigt. Diese Attribute sind von einer OSCI-konformen Anwendung entsprechend in des Reader-Objekt einzustellen. Auch die Reader-Klasse kann mehrere Instanzen bilden, die jeweils bestimmten Contents zuzuordnen sind (siehe Content-Container Objekt).

  In der Rollenbesetzung *“Leser”* muss im jeweiligen **`Reader`**-Objekt auch der private Schlüssel für die Decryption verfügbar gemacht werden.

B.3 OSCI-Nachrichtenobjekte

OSCI-Nachrichten sind generell Request-Response Szenarien. Von einer abstrakten Klasse OSCIMessage werden daher zunächst die Klassen **`OSCIRequest`** und **`OSCIresponseTo`** abgeleitet, aus denen wiederum die in der OSCI-Spezifikation definierten konkreten **`Request-`** und **`ResponseTo-Request`**-Nachrichtentypen abgeleitet werden.

Für jeden konkrete OSCI Nachricht **`Request`** und **`ResponseTo`** existiert ein Konstruktor mit dem jeweiligen Namen gem. OSCI-Spezifikation, der die jeweilige Nachrichtenstruktur aufbaut. Die allgemeinen Element- und Attributwerte, die nicht spezifisch in Bezug auf die konkrete Request- bzw. *Response* Ausprägung sind - also vor allem die wesentlichen *SOAP-Header*-Informationen - werden dabei aus den oben geschilderten Objekten in die Nachricht eingestellt.

Das Einstellen der ausprägungsspezifischen Nachrichteninhalte geschieht mittels Methoden, die jeweiligen konkreten Klassen der Nachrichtentypen zugeordnet sind. Für die Nachrichten, die Inhaltsdaten transportieren, werden einzelne ContentContainer-Objekte mit setContent (ContentContainer) eingestellt; diese Objekte müssen zuvor von der Anwendung komplett inkl. Signaturen und Verschlüsselungen (siehe Abschnitt ContentContainer) erstellt worden sein.

Die **OSCI-Request**-Nachrichten haben jeweils eine `send()` Methode, die ein Objekt vom korrespondierenden **ResponseTo-Typ** zurückliefert.

Die **ResponeToRequest**-Objekte beinhalten in jedem Fall die *Feeback*-Informationen einer OSCI-Nachricht. Die *Feedback*-Informationen erstellt der jeweilige Supplier zur Übermittlung der Verarbeitungsinformationen an der *Requestor*. Mit der Methode **responseToRequest.feedBack()** kann die Anwendung ein FeedBack-Objekt aus **responseToRequest** erhalten.

Dabei ist zu beachten, dass schwerwiegende Verarbeitungs- und Übermittlungsfehler (SOAP- oder Transport-Fehler sowie OSCI–Transport-Fehler mit Fehlercode >= 9000) in jedem Fall zum Auslösen einer *Exception* führen, da in diesem Fall ggf. das **ResponseToRequest**-Objekt nicht vollständig aufgebaut werden konnte.

Für die **ResponseToRequest**-Nachrichtypen, die eine `ProcessCard` (*"Laufzettel"* mit Ergebnissen von Zertifikatsprüfungen - InspectionReport -, Zeitstempel zu Nachrichtenbewegungen) beinhalten, kann diese Objekt mit **responseToRequest.fetchProcessCard()** verfügbar gemacht werden.

Sind in einem **ResponseToRequest**-Objekt Inhaltsdaten eingestellt - wie z.B. beim Abholauftrag, wird mit der Methode **responseToRequest.getContents()** ein Array von Objekten des Typs ContentContainer in die Anwendung eingestellt.

Wie beim Erstellen und Versenden von Nachrichten stehen der Anwendung hier Methoden zur Verfügung, die gezieltes Entschlüsseln und die Signaturprüfung auf den einzelnen empfangenen Containern ermöglichen:

- `<responseToRequest>.decryptContent(contentContainer [i], reader)`
- `<responseToRequest>.checkContentSign(contentContainer [i])`
- `String data = contentContainer [i].getXmlData().toString()`

B.4 ContentContainer

Eine Instanz der Klasse **ContentContainer** bildet einen OSCI-*"Inhaltsdatencontainer"* mit allen für die Signatur, Ver- und Entschlüsselung benötigten Attributen, zugeordneten Objekten und Methoden ab. Mit der Methode *setXMLData (String)code* werden die XML-modellierten Inhaltsdaten von der Anwendung eingestellt. Mit der Methode `addAttachment(File)` können zusätzlich beliebige Datencontainer einem `ContentContainer`-Objekt als Attachment zugeordnet werden.

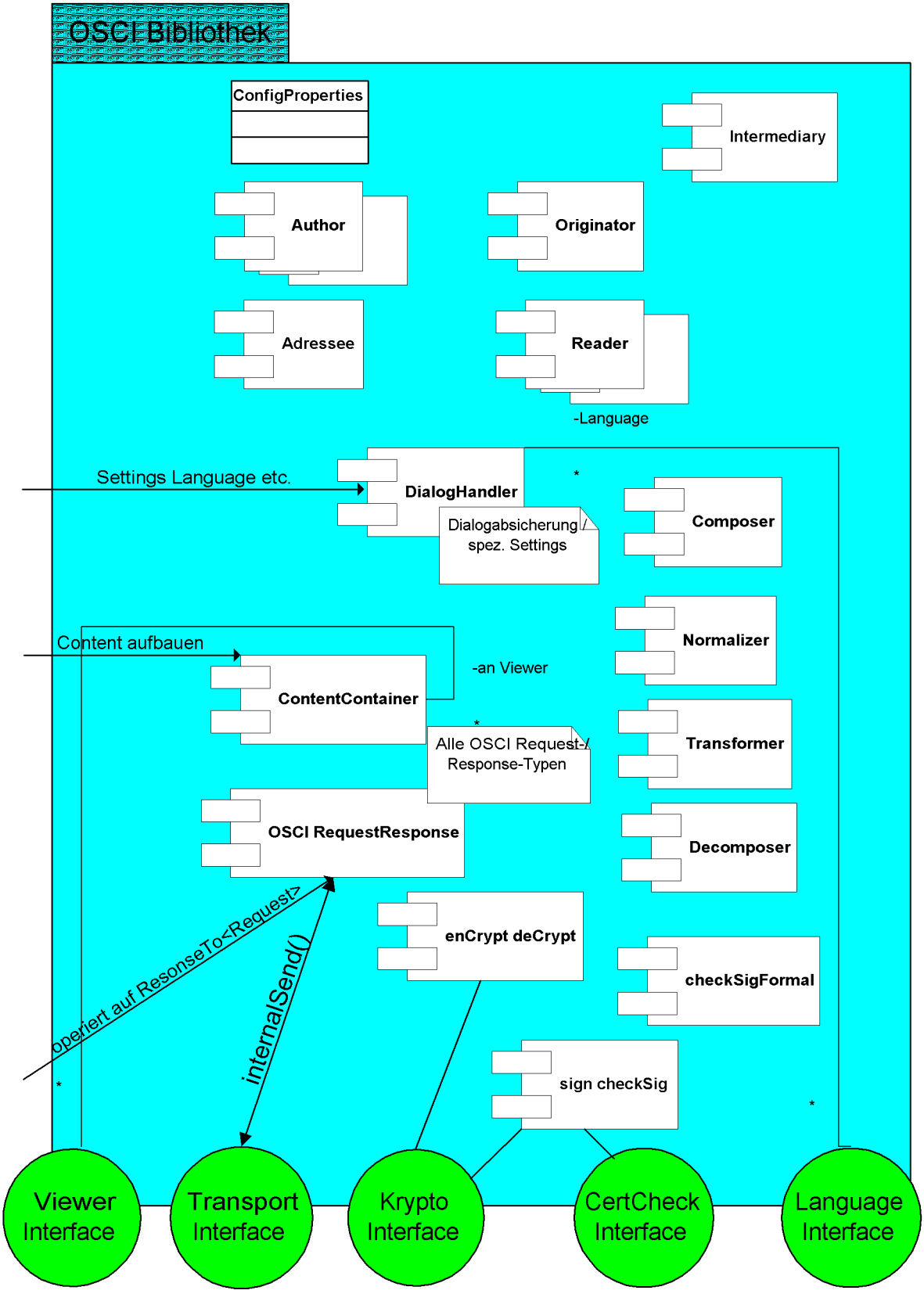
Weiter sind diesem Objekt **Author**-Objekte (Signatur) und **Reader** (Verschlüsselung) zuzuorden.

Ein **Author**-Objekt ist mit der Methode `signContent(Author, TrustedViewer)` bekanntzugeben, das dann mit dem Signaturvorgang in den **ContentContainer** eingestellt wird (weiter muss der zu verwendende **Viewer** bekannt gemacht werden!). Damit ist sichergestellt, das alle Autoren in der von der Anwendung gewünschten Reihenfolge den Inhalt signieren.

Die **Reader** werden mit der Methode `addReader(Reader)` zugeordnet, für die sämtlich mit der Methode `encryptContent()` die Verschlüsselung durchzuführen ist (Überverschlüsselung).

Ein **ContentContainer** beinhaltet weiter ein Attribute wie `stateOfMsg` und `stateOfContent`, welche u.a. den Status des jeweiligen **ContentContainer**s abbildet (Attachments eingestellt, Verschlüsselungsstatus etc.).

Bild 2 Bibliothek im Detail



B.5 Beispielhafte Use-Cases

Use Case Nr.	1.1
Use Case Name	Senden eines Zustellungsauftrag
Geschäftsvorfall	Beispiel: der Versand einer Nachricht in Form eines OSCI Zustellauftrags.
Initiierender Aktor	Sender
Weitere Aktoren	Intermediär
Kurzbeschreibung	Versenden einer OSCI Nachricht mit Inhaltscontainer und Signaturen an den Intermediär
Vorbedingungen	• Verwendete Module müssen konfiguriert sein (Visualisierung, Crypto, Transport und Sprache) • Die Informationen / Zertifikate der beteiligten Personen / Institutionen müssen eingestellt werden (Sender, Empfänger und Intermediär)
Resultate	Zustellungsantwort mit Informationen zu dem Zustellungsauftrag

1. Dialog-Handler-Objekt für die Steuerung des Dialogablaufs anlegen.
   ```
   DialogHandlerClient dh = new DialogHandlerClient(transportModul);
   ```
2. Absender einstellen:
   ```
   dh.setOriginator(new Originator(...));
   ```
3. Intermediär einstellen:
   ```
   dh.setIntermed(new Intermed(URL, Zertifikat));
   ```
4. Erstellen eines OSCI Nachrichtenobjektes (MessageID-Anforderung), Versenden der Nachricht und Einlesen der Rückantwort
   ```
   GetMessageID msgIDReq= new GetMessageID(dh)
   ResponseToGetMessageID msgIDRsp=msgIDReq.send()
   ```
5. Erstellen eines OSCI Nachrichtenobjektes (Zustellungsauftrag)
   ```
   StoreDelivery strDeliReq= new StoreDelivery(dh);
   strDeliReq.setMsgID(msgIDRsp.getMessageID)
   ```
6. Erstellung eines Inhaltscontainers mit Nutzdaten (XML), Hinzufügen der Leser
   ```
   ContentContainer coco=new ContentContainer ();
   coco.setXmlData(String data)
   coco.addReader(new Reader(X509Certificate cert,...))
   ```
7. Signieren der Inhaltsdaten
   ```
   strDeliReq.signContent(coco,new Author(...))
   ```
8. Inhaltsdaten dem Nachrichtenobjekt zuordnen
   ```
   strDeliReq.addContent(coco)
   ```
9. Verschicken der OSCI-Nachricht
   ```
   ResponseToStoreDelivery strDeliRsp=strDeli.send()
   ```
10. Überprüfen der gerade gesendeten Nachricht
    ```
    ProcessCard proCard=strDeliRsp.getProcessCard()
    ```

Alternative Pfade	Keine
Fehlersituationen, Ausnahmen	OSCI Fehlercodes des Typs 9*** lösen Exceptions aus; andere Fehler, Warnungen und Informationen können dem OSCI FeedBack-Objekten der Nachricht entnommen werden

Use Case Nr.	1.2
Use Case Name	Senden eines Zustellungsabholauftrags
Geschäftsvorfall	Ein Empfänger holt eine Nachricht aus seinem Postfach ab.
Initiierender Aktor	Wegzugsmeldebehörde
Weitere Aktoren	Intermediär
Kurzbeschreibung	Abholen einer OSCI-Nachricht vom Intermediär als Empfänger / Leser
Vorbedingungen	• Verwendete Module müssen konfiguriert sein (Visualisierung, Crypto, Transport und Sprache) • Die Informationen / Zertifikate der beteiligten Personen / Institutionen müssen eingestellt werden (Sender und Intermediär) • Der Privatschlüssel des Empfängers (`privateKey`) muß vorhanden sein
Resultate	Zustellungsabholantwort mit dem Inhalt des Zustellungsauftrags

1. Dialog-Handler-Objekt für die Steuerung des Dialogablaufs anlegen.
   ```
   DialogHandlerClient dh = new DialogHandlerClient(transportModul)
   ```
2. Absender einstellen:
   ```
   dh.setOriginator(new Originator(...));
   ```
3. Intermediär einstellen:
   ```
   dh.setIntermed(new Intermed(URL, Zertifikat));
   ```
4. Dialog-Initialisierungsnachricht erzeugen und versenden, Antwortobjekt einlesen:
   ```
   ResponseToInitDialog initDialogRsp initDiaRsp = new InitDialog(dh).send();
   ```
5. Dialog-Parameter prüfen:
   ```
   dh.checkControlBlock(initDiaRsp.getConvID(), initDiaRsp.getSequence(), initDiaRsp.getResp())
   ```
6. Zustellungsabholauftrag anlegen, versenden und Antwortobjekt einlesen:
   ```
   FetchDelivery fetchDev = new FetchDelivery(dh)
   fetchDev.setReceptionOfDelivery(Date)
   ResponseToFetchDelivery fetchDevRsp = fetchDev.send();
   ```
7. Inhaltsdatencontainer extrahieren, ggf. entschlüsseln/Signatur prüfen, Daten auslesen:
   ```
   ContentContainer coco[] = fetchDevRsp.getContents()
   [n-mal]: detchDevRsp.decryptContent(coco[i], privateKey)
   [n-mal]: detchDevRsp.checkContentSign(coco[i])
   [n-mal]: String daten = coco[i].getXmlData().toString()
   ```

Alternative Pfade	Keine
Fehlersituationen, Ausnahmen	Beim Prüfen der Inhaltsdatensignaturen und beim Decrypten des inhaltscontainers können Fehler auftreten, welche zu Exceptions führen. Auch bei dem Überprüfen des DialogContolblcks werden falsche Dialogcontexte durch Fehlermeldungen beantwortet

Use Case Nr.	1.3
Use Case Name	Senden eines Weiterleitungsauftrags
Geschäftsvorfall	
Initiierender Aktor	Sender eine Weiterleitungsauftrags
Weitere Aktoren	Intermediär
Kurzbeschreibung	Versenden einer OSCI Nachricht mit Inhaltscontainer und Signaturen an den Intermediär. Als Ergebnis wird eine Antwort von dem Fachverfahren erwartet ()
Vorbedingungen	• Verwendete Module müssen konfiguriert sein (Visualisierung, Crypto, Transport und Sprache) • Die Informationen / Zertifikate der beteiligten Personen / Institutionen müssen eingestellt werden (Sender, Empfänger und Intermediär)
Resultate	Weiterleitungsantwort mit Informationen zu der Weiterleitung

1. Dialog-Handler-Objekt für die Steuerung des Dialogablaufs anlegen.
   `DialogHandlerClient dh = new DialogHandlerClient(transportModul)`
2. Absender einstellen:
   `dh.setOriginator(new Originator(...));`
3. Intermediär einstellen:
   `dh.setIntermed(new Intermed(URL, Zertifikat));`
4. Erstellen eines OSCI Nachrichtenobjektes (MessageID-Anforderung), Versenden der Nachricht und Einlesen der Rückantwort
   ```
   GetMessageID msgIDReq= new GetMessageID(dh)
   ResponseToGetMessageID msgIDRsp=msgIDReq.send()
   ```
5. Erstellen eines OSCI Nachrichtenobjektes (Weiterleitungsauftrag)
   ```
   ForwardDelivery strForwReq= new ForwardDelivery(dh);
   strForwReq.setMsgID(msgIDRsp.getMessageID)
   ```
6. Erstellung eines Inhaltscontainers mit Nutzdaten (XML), Hinzufügen der Leser
   ```
   ContentContainer coco=new ContentContainer ();
   coco.setXmlData(String data)
   coco.addReader(new Reader(X509Certificate cert,...))
   ```
7. Signieren der Inhaltsdaten
   `strForwReq.signContent(coco,new Author(...))`
8. Inhaltsdaten dem Nachrichtenobjekt zuordnen
   `strForwReq.addContent(coco)`
9. Verschicken der OSCI-Nachricht
   `ResponseToForwardDelivery strForwRsp= strForwReq.send()`
10. Überprüfen der gerade gesendeten Nachricht
    `ProcessCard proCard= strForwRsp.getProcessCard()`

Alternative Pfade	Keine
Fehlersituationen, Ausnahmen	OSCI Fehlercodes des Typs 9*** lösen Exceptions aus; andere Fehler, Warnungen und Informationen können dem OSCI FeedBack-Objekten der Nachricht entnommen werden

Use Case Nr.	1.4
Use Case Name	Annahme eines Annahmeauftrages
Geschäftsvorfall	
Initiierender Aktor	Intermediär
Weitere Aktoren	Sender eines Annahmeauftrages
Kurzbeschreibung	Empfang einer OSCI Nachricht mit Inhaltscontainer und Signaturen vom Intermediär. Als Empfangsquittung wird eine Antwortnachricht zurückgesendet.
Vorbedingungen	• Applicationserver muß die eingehenden Daten entgegennehmen • Verwendete Module müssen konfiguriert sein (Crypto, Transport und Sprache) • Der Privatschlüssel des Empfängers bzw. des Lesers müssen verfügbar sein.
Resultate	Inhaltsdaten des empfangenen Auftrags

1. Dialog-Handler-Objekt für die Steuerung des Dialogablaufs anlegen.
   ```
   DialogHandlerClient dh = new DialogHandlerClient(transportModul)
   ```
2. Dem OSCI Message Builder wird die Nachricht übergeben
   ```
   DialogHandlerClient dh = new DialogHandlerClient(transportModul);
   ```
3. Als Ergebnis wird die verschlüsselte Transportnachricht übergeben
   ```
   SOAPMessageEncrypted enc = (SOAPMessageEncrypted) new OSCIMessage().parse(in);
   ```
4. Einstellen des Empfängerschlüsselpaares
   ```
   Addressee adre= new Addressee(KeyStore key ,"Name des Schlüssels");
   ```
5. Entschlüsseln des Transportumschlages
   ```
   AcceptDelivery req=(AcceptDelivery)enc.decryptMessage(adre);
   ```
6. Erstellen eines Leser Objektes
   ```
   Reader reader= new Reader (KeyStore key,"Name des Schlüssels");
   ```
7. Auswerten der Nutzcontainer
   ```
   ContentContainer[] cocos=req.getContents();
   ReaderAddressed[] adReader= cocos[0].getReaders();
   cocos[0].decryptContent(reader);
   cocos[0].checkContentSign();
   InputStream[] input= coco[0].getAttachements();
   coco[0].getXmlData();
   ```
8. Antwortnachricht erstellen
   ```
   ResponseToAcceptDelivery rsp= new ResponseToAcceptDelivery(req);
   ```
9. Rückgabe der erstellten Nachricht an den Applicationserver

Alternative Pfade	Keine
Fehlersituationen, Ausnahmen	OSCI Fehlercodes des Typs 9*** lösen Exceptions aus; andere Fehler, Warnungen und Informationen können dem OSCI FeedBack-Objekten der Nachricht entnommen werden