OSCI® ist eine registrierte Marke
der Freien Hansestadt Bremen

Entwicklung von OSCI Transport 2.0

Vorlage für die Sitzung des KoopA–ADV im Dezember 2006

JENS DIETRICH, OSCI–Leitstelle
FRANK STEIMKE, OSCI–Leitstelle
Fassung vom 27. November 2006

1 Management Summary

1.1 E-Government braucht Sicherheit

Die Standardisierung im E-Government ermöglicht die Vernetzung von DV-Verfahren in einer heterogenen Welt. Sie dient der Effizienzsteigerung und der Kostensenkung für Dienstleistungen der öffentlichen Verwaltung. Das Ziel der automatisierten, medienbruchfreien Verarbeitung von Prozessketten lässt sich nur erreichen, wenn die Standardisierung die organisatorische, die semantische und auch die technische Ebene umfasst und koordiniert erfolgt.

Für Prozessketten im E-Government wird eine Infrastruktur benötigt, die neben der Vertraulichkeit (Verschlüsselung) auch die Authentisierung (digitale Identität), die Integrität (Schutz vor Verfälschungen) und die Nicht-Abstreitbarkeit unterstützt. Dabei sind neben der sicheren Datenübertragung auch die Archivierung von Dokumenten und die Rechtsverbindlichkeit von Transaktionen über das Internet zu berücksichtigen. Neben der Verschlüsselung muss deshalb auch die elektronische Signatur und die Identifikation anhand der in Deutschland etablierten PKI unterstützt werden. Dies gilt sowohl für die Kommunikationsbeziehungen mit Externen (G2C, G2B, siehe hierzu z. B. das Justizwesen), als auch in der verwaltungsinternen Datenübermittlung (G2G, wie derzeit im Meldewesen).

1.2 E-Government braucht das sichere Internet

E-Government kann nur funktionieren, wenn wir die den Kommunikationspartnern außerhalb der Verwaltung, also der Industrie und den Bürgern, den Zugang über das Internet ermöglichen. Diese für die öffentliche Verwaltung wichtigen Zielgruppen haben keinen Zugang zu verwaltungsinternen Netzen. Darum müssen wir sichere Web-Services anbieten, die das Internet um die Möglichkeiten der Authentisierung, der Vertraulichkeit und der Signatur ergänzen.

Laufende Projekte haben uns gezeigt, dass dies nicht im Widerspruch zu existierenden Infrastrukturen der Verwaltung steht. Verwaltungsinterne *"sichere Netze"* legen oft den Schwerpunkt auf die Vertraulichkeit, sie bedürfen dann der Ergänzung um die Signatur und die Authentisierung.

1.3 Deutschland braucht auch weiterhin OSCI Transport (Version 2)

Weltweit wird derzeit an technischen Möglichkeiten gearbeitet, um auf der Basis von Internettechnologien die Grundlage für sichere, serviceorientierte Architekturen zu schaffen. Von verschiedenen Stellen (W3C, OASIS, Industrie) werden Entwürfe für Standards in diesem Kontext vorgelegt (der so genannten WS-Protokollstapel). Inzwischen wird deutlich, welche Standards sich durchsetzen werden. Außerdem ist festzustellen, dass das Thema der *Sicherheit in Webservices* einen Stellenwert bekommen hat, der einen Einsatz im E-Government realistisch erscheinen lässt.

Besteht angesichts dieser Situation weiterhin Bedarf an OSCI-Transport (Version 2)? Ja, denn:

- WS-Protokolle bieten konfigurierbare Bausteine. Welche man wählt, und wie man konfiguriert, ist festzulegen. Für die geforderte Interoperabilität müssen wir uns der Bausteine bedienen und daraus ein abgestimmtes System konstruieren, welches den Anforderungen Deutschlands entspricht.
- Manche Bausteine (so z. B. *WS-Policy*) standardisieren keine Inhalte, sondern nur die Sprache in der man Inhalte beschreiben kann. Für die geforderte Interoperabilität werden wir die Inhalte entwickeln und diese WS-konform beschreiben müssen.
- OSCI Transport 1.2 bietet Funktionalitäten, die wir in den WS Protokollen nicht finden, die aber von den Anwendern nachgefragt und benötigt werden (z. B *Nachweisbarkeit* im Kontext XJustiz). Wir müssen daher notwendige Erweiterungen abstimmen und umsetzen.

Diese Auffassung wird vertreten durch die Expertengruppe zur Weiterentwicklung von OSCI Transport im Auftrag des KoopA ADV. Sie wurde einhellig bestätigt auf der D21 Tagung am 2./3. November in Berlin. Und wir stellen fest, dass die Regierungen anderer Länder zu der gleichen Auffassung kommen, so z. B. Frankreich mit PRESTO.

Weitere Anforderungen: Flexibilität und Interoperabilität

Die internationale Entwicklung zeigt, dass bei der Gestaltung von Austauschstandards nicht nur Sicherheit, sondern zunehmend auch die Aspekte der Interoperabilität und Konnektivität an Bedeutung gewinnen. Die Fortentwicklung von OSCI Transport 2.0 sollte deshalb auch diese Aspekte miteinbeziehen und damit über (enge) Sicherheitsaspekte hinausweisen.

1.4 OSCI Transport muss Bestandteil der koordinierten Standardisierung bleiben

Es ist international üblich, die Standardisierung der Inhalte (Semantik) und die Standardisierung des Transportes separat zu betrachten. Dieses Vorgehen hat sich auch in Deutschland bewährt und wird nicht in Frage gestellt. Fachstandards (XJustiz, XMeld) stellen funktionale Anforderungen an den Transport, sie erzwingen keine spezielle Technologien oder Produkte.

Dennoch ist die Koordination der Standardisierung auf allen Ebenen unabdingbar. Sichere Webservices sind zielgerichtet so zu entwickeln, dass sie die Anforderungen unserer Fachstandards und der für Deutschland spezifischen Rechtsgrundlagen erfüllen. Die Entwicklung und der Betrieb der Infrastruktur werden durch Fachanwendungen bestimmt. Umgekehrt setzen Infrastrukturkomponenten Grenzen für Fachstandards. Rechtlich-organisatorische Rahmenbedingungen müssen die Möglichkeiten der Infrastruktur berücksichtigen.

Ohne eine enge Koordination besteht die Gefahr von Fehlinvestition und Verzögerungen. Daher muss die Weiterentwicklung der sicheren Infrastruktur inklusive OSCI-Transport 2.0 Bestandteil der koordinierten Standardisierung im Rahmen von Deutschland-Online bleiben und im Auftrag des KoopA ADV durchgeführt werden..

Damit künftig die Daten verlustfrei ausgetauscht und automatisiert weiterverarbeitet werden können, sind gemeinsame Standards für das *Format*, den *Inhalt* und den *Transport* der elektronischen Informationen erforderlich. Daher soll OSCI Transport künftig in Richtung international anerkannter Web Service Standards migrieren. Dies ist eine wichtige Voraussetzung für den internationalen Erfolg deutscher E-Government Lösungen.

1.5 Der Vorschlag zum Vorgehen

Die Entwicklung von OSCI Transport 2.0 erfolgt durch die Gremien, die wertvolle Vorarbeiten im Rahmen der Prüfung der Version 1.3 geleistet habe. Die OSCI Leitstelle finanziert in diesem Projekt aus den Mitteln des KoopA die Aufgabe eines Editors und der Qualitätssicherung. Diese Aufgaben sollen durch *Herrn J. Apitzsch (bremen online services)* und *Herrn T. Schuster (cit GmbH)* wahrgenommen werden.

Wir kalkulieren für diese beiden Aufgaben innerhalb des nächsten Jahres Aufwände in Höhe von 66 PT und 66 Tsd. Euro inkl. MWSt. insgesamt (siehe Tabelle 1 auf Seite 8) Daher sind die vom KoopA ADV im Jahre 2007 für die Weiterentwicklung von OSCI Transport geplanten Mittel ausreichend.

2 Sachstand und Beschlusslage

Anfang 2006 hat sich nach einem offenen Aufruf an alle interessierten Kreise eine Expertengruppe zur Weiterentwicklung von OSCI Transport gebildet. Zunächst wurden von dieser Gruppe Anforderungen an die Weiterentwicklung von OSCI Transport erhoben und abgestimmt. In einem zweiten Schritt wurden zwei alternative Szenarien für eine Umsetzung dieser Anforderungen analysiert und bewertet.

Ergebnis dieser Bewertung war die Empfehlung, dass die zunächst favorisierte Idee einer strikt abwärtskompatiblen Version 1.3 von OSCI Transport nicht weiter verfolgt wird. Die nächste Version von OSCI–Transport (Version 2.0) soll stattdessen auf den mittlerweile aktuellen Standards des sog. Web-Services-Protokollstapel (wie *WS-Security, WS-Reliable-Messaging* etc.) basieren. Die Expertengruppe ist sich sicher, dass auch bei Zugrundelegung dieser internationalen Standards weitere Festlegungen erforderlich sind, um die Interoperabilität der an der Datenübermittlung beteiligten Systeme (Fachverfahren) zu gewährleisten und die Konformität zu den in Europa und Deutschland geltenden Rechtsgrundlagen sicher zu stellen.

Weiterhin wurde empfohlen, bei der Weiterentwicklung eine enge Abstimmung mit gleichartigen Entwicklungen auf der europäischen Ebene (insbesondere mit dem PRESTO-Projekt der französischen Regierung) anzustreben.

Diese Ergebnisse wurden dem KoopA ADV auf seiner Herbstsitzung am 21./22. September vorgetragen. Der KoopA ADV hat daraufhin den Beschluss6–3/2006 gefasst. Darin nimmt er den Bericht des Projekts OSCI–Transport 1.3 (Stand: abgestimmte Version vom 31. August 2006) zur Kenntnis und bittet für die nächste Sitzung um die Vorlage einer Planung und eines Finanzierungskonzeptes zu OSCI Transport 2.0 unter Berücksichtigung der ggf. frei werdenen Mittel für die Version 1.3.

In diesem Papier werden die seit der Herbstsitzung des KoopA–ADV durchgeführten Aktivitäten dargestellt sowie eine Aufwandsabschätzung und ein Finanzierungskonzept für die Entwicklung von OSCI–Transport vorgestellt. Es werden Vorschläge zum Vorgehen in 2007 gemacht.

3 Aktivitäten seit der Herbstsitzung

3.1 Detaillierte Prüfung des Webservice - Protokollstapels

Um eine Abschätzung der erforderlichen Aufwände für die Entwicklung von OSCI Transport 2.0 vornehmen zu können, wurden seit der Herbstsitzung des KoopA–ADV von einzelnen Mitarbeitern der Expertengruppe weitergehende Untersuchungen zur Konzeption von OSCI–Transport auf Basis der vorgeschlagenen aktuellen internationalen Standards durchgeführt. Es handelt sich dabei um den *“Webservice - Protokollstapel”*. Die Prüfung führte zu folgenden Ergebnissen:

- Die empfohlenen internationalen Standards sind mittlerweile stabil genug und bieten notwendige Funktionalitäten, die für den sicheren Nachrichtenaustausch im E-Government benötigt werden. Es gibt eine in der Expertengruppe abgestimmte Einschätzung darüber, welche der Komponenten des *WS Protokollstapels* sich durchsetzen werden.
- Die genannten Standards verstehen sich jedoch als Rahmen bzw. Bausteine, die für konkrete Anforderungsszenarien zu profilieren und zu konkretisieren sind. Dies wird in den jeweiligen Spezifikationen explizit hervorgehoben.

  Manche Bausteine (so z. B. *WS-Policy*) standardisieren keine Inhalte, sondern nur die Sprache in der man Inhalte beschreiben kann. Die Inhalte sind zu entwickeln, dabei sind die Erfahrungen aus laufenden Projekten und die in Deutschland geltenden Rechtsgrundlagen zu Grunde zu legen.
- Nicht alle der in OSCI–Transport 1.2 gebotenen Funktionalitäten werden durch die Webservice-Protokolle abgedeckt. Da wir aus realen Einsatzszenarien den Bedarf an diesen Funktionen kennen[1], werden wir entsprechende Ergänzungen vornehmen müssen.

  Die Anforderungen an den sicheren Nachrichtenaustausch im E-Government erfordern daher weitere Festlegungen und Erweiterungen auf Basis dieser internationalen Standards, die im Rahmen einer OSCI Transport 2.0 Spezifikation festgeschrieben werden müssen.

1.so z. B. im elektronischen Rechtsverkehr die Nachvollziehbarkeit und Nichtabstreitbarkeit der Datenübermittlung

Auch dabei sind die spezifischen Anforderungen deutscher und europäischer Rechtsgrundlagen zu Grunde zu legen.

- In die Entwicklung von OSCI Transport 2.0 werden die Erfahrungen einfließen, die wir in den vergangenen Jahren durch den Einsatz von OSCI Transport 1.2 sammeln konnten. Wir mussten feststellen, dass einige der Annahmen, die im Jahre 2000 den Entwurf des Protokolls OSCI Transport maßgeblich bestimmt haben, nicht eingetroffen sind. Dies betrifft zum Beispiel die Relevanz des Bürgers als Endkunden der E-Government Services (mit der Konsequenz der Adressierung von Nachrichten in *offenen Benutzergruppen*)..

  Wir werden das Design von OSCI Transport 2.0 vornehmlich an den Anforderungen ausrichten, die uns aus laufenden und absehbaren Projekten als besonders wichtig bekannt sind.

- Die Umsetzung der genannten Standards durch die Softwareindustrie ist bereits im Gange. Sowohl in der Java-Welt (Java 6) als auch in der Microsoft-Welt (*.net Framework 3*) sind wesentliche Bestandteile der Webservice-Protokolle enthalten.

  Daher erwarten wir, dass der IT-Markt die Anforderungen des E-Governments an sichere und interoperable elektronische Kommunikation über das Internet kurzfristig wesentlich breiter und wirtschaftlicher bedienen kann als dies bisher der Fall war.

Die obigen Ergebnisse wurde zusätzlich durch einen Workshop im Rahmen der D21 / Media@Komm-Transfer Konferenz am 2./3. November im BMWi bestätigt, auf dem die geplante Entwicklung von OSCI-Transport 2.0 einer breiteren Fachöffentlichkeit vorgestellt und diskutiert wurden (siehe Anlage *“Ergebnisse OSCI-Transport-Workshop D21/Media@KommTransfer-Konferenz 2./3. November 2006”*).

3.2 Kooperationsmöglichkeiten auf europäischer Ebene

Die OSCI–Leitstelle wurde zu einer Vorstellung des PRESTO-Projekts der französischen Regierung am 12. Oktober eingeladen. Auf diesem Treffen wurden der Stand des PRESTO-Projekts und prototypische Implementierungen vorgestellt. Weiterhin fand im Oktober ein Treffen mit der entsprechenden Arbeitsgruppe der europäischen Kommission (IDABC) statt, auf dem die Möglichkeiten einer engen Abstimmung der Weiterentwicklung von OSCI–Transport mit dem PRESTO-Projekt und auf der europäischen Ebene erörtert wurden.

- Das PRESTO-Projekt der französischen Regierung ist an einer Abstimmung der Entwicklungen sehr interessiert und hat die OSCI-Transport-Expertengruppe zu entsprechenden Treffen der PRESTO-Arbeitsgruppe eingeladen.
- Auch weitere EU-Länder (Dänemark, Schweden) setzen aktuell ihre Bemühungen zur Fortschreibung ihrer E-Government-Infrastrukturen auf den genannten internationalen Standards auf und sind an einer engen Abstimmung dieser Entwicklungen interessiert.
- Die europäische Kommission ist an einer abgestimmten Entwicklung auf Basis der vorgeschlagenen internationalen Standards sehr interessiert und wird im Rahmen von IDABC die Abstimmung zwischen der Weiterentwicklung von OSCI–Transport und dem PRESTO-Projekt unterstützen.

4 Vorschlag für das weitere Vorgehen

Wir schlagen vor, die für die Entwicklung von OSCI Transport 1.3 vorgeschlagene Organisation grundsätzlich beizubehalten. Der Projektauftrag ist aber auf die *"Erarbeitung einer Version 2.0 von OSCI Transport auf Basis der WS - Protokolle"* zu ändern, und in der Organisation ist die Zusammenarbeit mit anderen europäischen Ländern stärker zu berücksichtigen. Das bedeutet konkret:

- Der Projektauftrag besteht in der Fortentwicklung des Protokolls OSCI Transport. Er wird mit der Fertigstellung der Spezifikationsdokumente und ergänzender Dokumente wie z. B. XML-Schema für OSCI Transport 2.0 abgeschlossen.
  - Die Erstellung / Anpassung von Software gehört nicht zum Projektauftrag.
  - Die Erstellung einer Referenzimplementierung oder eines Testbed mit staatlicher Finanzierung ist im Rahmen dieses Projektes nicht vorgesehen.
  - Wir verweisen in diesem Zusammenhang auf die Erfahrungen aus Frankreich, wo die Aufgabe der Implementierung und die Erstellung unterstützender Systeme für PRESTO durch die Industrie erfolgt.
- Die Vorgabe der Abwärtskompatibilität auf der Ebene des Standards wird nicht weiter verfolgt. Es sind Migrationsstrategie für einen Umstieg von der Version 1.2 auf die Version 2.0 zu entwickeln, dies wird aber bewusst nicht im Rahmen des hier beschriebenen Projektes erfolgen. Die Begründung dafür ist, dass Migrationsstrategien zu stark von den Rahmenbedingungen in den unterschiedlichen Einsatzbereichen (Meldewesen, Justizwesen, Emmissionshandel …) determiniert werden. Darüber hinaus ist es durchaus möglich, dass Abwärtskompatibilität *auf Produktebene* hergestellt werden kann. Konkrete Aussagen darüber sind aber vermutlich erst nach dem Abschluss der Entwicklung von OSCI Transport 2.0 möglich.
- Die operative Arbeit wird entsprechend weiterhin durch die Expertengruppe durchgeführt. In der Expertengruppe sind Vertreter der Industrie und der öffentlichen Verwaltung zu finden.
- Die Abstimmung der Arbeitsergebnisse erfolgt in der Abstimminstanz des Projekts als einem erweiterten Kreis von Mitgliedern aller an OSCI Transport interessierten Kreise. Dabei wird sich die OSCI-Leitstelle die formal bereits bestehende Beteiligungsmöglichkeiten für die Industrie und andere Akteure, insbesondere aus dem Bereich der *"klassischen Standardisierung"*, also insbesondere dem DIN, durch eine gezielte Ansprache geeigneter Firmen, Institute und einschlägig qualifzierter Fachpersonen aus den Verwaltungen die *"OSCI-Community"* substanziell so zu erweitern, dass die Standardisierungsinitative zu OSCI-Transport noch breiter als bisher in die deutsche *"Verwaltungs-IT-Szene"* integriert werden kann.

  Wegen der zu erwartenden Auswirkungen auf Verzeichnisdienste empfehlen wir, dass technisch versierte Personen, die mit der Entwicklung des DVDV vertraut sind, mindestens auf der Ebene der Abstimminstanz, ggfs. auch in der Expertengruppe vertreten sind.
- Die Abnahme der Ergebnisse obliegt dem KoopA ADV als Auftraggeber des Projektes. Der KoopA ADV ist für die Umsetzung der Projektergebnisse in Bund, Ländern und Kommunen verantwortlich. Er entscheidet uber ggfs. notwendige Folgeaktivitäten, wie z. B. Änderungen an der vom KoopA ADV herausgegebenen OSCI Transport Bibliothek oder ggfs. notwendigen Anpassungen des DVDV.
- Die Organisation des Projektes *"Spezifikation OSCI Transport 2.0"* erfolgt durch die OSCI Leitstelle für den KoopA ADV auf der Basis des mit dem Projektbüro des KoopA ADV abgeschlossenen EVB-IT Vertrages.

  Im Interesse zielgerichteter und zeitnaher Arbeiten im Laufe des Jahres 2007 schlagen wir vor, dass die OSCI Leitstelle zwei Personen mit der Projektdurchführung betraut, die von Beginn an mit der Entwicklung und dem Einsatz von OSCI Transport in Deutschland bestens vertraut sind. Dies sind:
  - Für die Aufgabe des *Editors*, der Arbeitsergebnisse vorbereitet, mit der Expertengruppe abstimmt und die finalen Dokumente erstellt: Herr *Jörg Apitzsch*, Fa. bremen online services.
  - Für die Aufgabe der Qualitätssicherung der Projektergebnisse: Herr *Thilo Schuster*, cit GmbH.
- Die Aktivitäten des Editors und der Qualitätssicherung werden von der OSCI Leitstelle aus den Mitteln des KoopA ADV für die Weiterentwicklung und Pflege von OSCI Transport finanziert. Eine weitere Finanzierung erfolgt nicht.

Die Industrie ist eingeladen, sich auf eigene Kosten an der Entwicklung von OSCI Transport im Rahmen der Expertengruppe oder der Abstimminstanz zu beteiligen.

Interoperabilitätstests des Fraunhofer Institutes *"FOKUS"* haben sich im Rahmen von OSCI Transport 1.2 als hilfreich erwiesen. Wir würden eine Fortführung dieser Aktivitäten für OSCI Transport 2.0 begrüßen, z. B. im Rahmen entwicklungsbegleitender Aktivitäten. Eine Finanzierung aus Projektmitteln ist jedoch nicht vorgesehen.

5 Abschätzung der Aufwände

Der Aufwandsabschätzung liegen folgende Rahmenbedingungen und Annahmen zu Grunde:

- Berücksichtigung der Vorarbeiten und Arbeitsergebnisse der OSCI–Transport Expertengruppe im Rahmen des KoopA ADV Auftrages für OSCI Transport 1.3.
- Neben einer reinen Profilierung werden Erweiterungen erforderlich werden:
  a. für die Rechtsverbindlichkeit und Nachweisbarkeit der Kommunikation gemäß der in Deutschland und der EU geltenden Rechtsgrundlagen
  b. für die Unterstützung der Asynchronität durch *"sichere Postfächer"*
  c. für zentrale Services im Rahmen der der PKI-Anbindung
- Angesichts der flächendeckenden Verfügbarkeit von Authentisierungszertifikaten mit dem neuen Personalausweis / der *European Citizen Card* sind alternative Authentisierungsmechanismen sowie erweiterte Adressierungsmechanismen zu berücksichtigen.

  In diesem Zusammenhang gibt es Querbezüge zu *E-Identity*[1] und zu Diensteverzeichnissen (DVDV).

Die Bausteine des WS-Stack adressieren gezielt jeweils Teilfunktionalitäten des sicheren Nachrichtenaustauschs. Dieses Prinzip soll in OSCI Transport 2.0 aufgenommen werden, indem Empfehlungen zur szenariengerechten Zusammenstellung der Bausteine und Mechanismen ausgesprochen werden[2].

Zur Abstimmung von Teil- und Gesamtergebnissen sind vier Workshops der Experten-Arbeitsgruppe geplant. Darüber hinaus ist vorgesehen:

- die Arbeiten eng mit den parallelen Aktivitäten in anderen EU-Ländern abzustimmen; hier vor allem mit dem *PRESTO*-Projekt in Frankreich. Hierzu sind drei Workshops kalkuliert.
- die Abstimmung mit Aktivitäten zur Weiterentwicklung von DVDV und Konzepten zum Identity Management (die Notwendigkeit der Anbindung von Verzeichnisdiensten für Services und Teilnehmer an der OSCI-Kommunikation wurde schon bei den Arbeiten für die Version OSCI Transport 1.3 sehr deutlich).

Gemäß der detaillierten Darstellung in Abschnitt A kalkulieren wir die in der Tabelle 1 dargelegten Aufwände für die zu finanzierenden Aufgaben des Editors und der Qualitätssicherung: Der geschätzte Gesamtaufwand beträgt 66 PT, davon entfallen ca. 20% (12 PT) auf die Qualitätssicherung.

Tabelle 1: Darlegung der zu finanzierenden Aufwände

Aktivität	**Aufwand in PT**	
	Editor	**QS**
Festlegung aller Anforderungen anhand der Untersuchung von Kommunikationsszenarien und Rollenmodell im Verhältnis zu den WS-Protokollen. Siehe Tabelle 2	16	4
Entwurf und Abstimmung Profillierungen und notwendiger Erweiterungen der WS-Protokolle. Siehe Tabelle 3	28	5
Zusammenführung der Ergebnisse, Erstellung finaler Dokumente inkl. XML Schema. Siehe Tabelle 4	10	3
Summe im Projekt	**54**	**12**

Bei Annahme eines Tagessatzes i. H. v. 1.000 Euro (inkl. MWSt.) werden daher für das Projekt im Jahre 2007 insgesamt 66 Tsd. Euro benötigt. Davon entfallen 80% (52.800 Euro inkl. MWSt.) auf die Aufgabe des Editors, 20% (13.200 Euro inkl. MWSt.) auf die der Qualitätssicherung. Diese Mittel stehen im Rahmen der Beauftragung der OSCI Leitstelle durch den KoopA ADV zur Verfügung (Mittelansatz 2007: 65 Tsd. Euro).

1.Strategisches Ziel auch im Programm E-Government 2.0 des Bundes.

2.Wir erwarten davon eine bessere Skalierbarkeit in den verschiedenen Einsatzszenarien. So kann z. B. in bestimmten Szenarien der *"äußere Umschlag"* durch eine Verschlüsselung auf SSL-Basis ersetzt werden.

Anhang A: Arbeitspakete und Aufwände

Tabelle 2: Kommunikationsszenarien und Rollenmodell

Nr.	Aktivität im Arbeitspaket 1	Aufwand (PT)
1	Überarbeitung des OSCI 1.2-Rollenmodells gemäß praktischen Erfahrungen aus den genutzten Einsatzszenarien, vornehmlich • Meldewesen • Elektronischer Rechtsverkehr • Emissionshandel • Beantragungsverfahren Patent- und Markenwesen Hier sind mit den Arbeiten für OSCI 1.3 schon wesentliche Vorarbeiten bzgl. der Anforderungen und Kommunikationsszenarien geleistet worden	2
2	Aufstellung, differenzierte Bewertung und Zuordnung der benötigten Kommunikations, Sicherheits- und Quittungsmechanismen zu den Funktionalitäten, die die relevanten WS-Standards jeweils als Bausteine für die einzelnen Anforderungsgruppen zur Verfügung stellen. Detaillierung des Profilierungsbedarfs, der sich ergibt aus • den Ergebnissen aus (1.) • Sicherstellung höchstmöglicher Interoperabilität. Entwurf zur Modellierung der OSCI-Funktionalitäten, die durch eine Profilierung der WS-Standards nicht abgedeckt werden können.	2
3	Konzeption alternativer Authentisierungsmechanismen sowie erweiterter Adressierungsmechanismen vor dem Hintergrund: • flächendeckende Verfügbarkeit von Authentisierungszertifikaten mit dem neuen Personalausweis/ *European Citizen Card* (geplantes Rollout ab 2008) • Querbezüge zu *E-Identity* • Verfügbarkeit, mögliche Erweiterungen von Diensteverzeichnissen (*"DVDV"*)	2
4	Abstimmung: 1 WS mit Vor- und Nachbereitung	4
5	Abstimmung EU/PRESTO (ein Meeting, Vor- und Nachbereitung)	2
6	Estellung finales Anforderungsdokument	4
7	Qualitätssicherung für Arbeitspaket 1	4
Summe der PT		**20**

Tabelle 3: Entwurf und Abstimmung Profillierungen

Nr.	Aktivität im Arbeitspaket 2	Aufwand (PT)
8	WS Security, XML Encryption, XML Digital Signature	2
9	WS Addressing; Anbindung DVDV / Teilnehmerverzeichnis	3
10	WS Trust / SAML / XKMS; OSCI-Rolle PKI-Anbindung	3
11	WS Reliable Messaging, WS RM Policy	1
12	WS Secure Conversation	0,5
13	WS Policy, WS-I Basic Profile	2
14	Spezifizierung OSCI-Mechanismen für Rechtsverbindlichkeit und Nachweisbarkeit der Kommunikation, Unterstützung der Asynchronität durch *"Postfächer"*	2
15	Überarbeitung Konzept OSCI-Inhaltsdaten, Attachments (Referenzierung MTOM/XOP)	2,5
16	Abstimmung Rückläufe aus der Expertengruppe	4
17	Zwei Workshops mit Vor- und Nachbereitung	4
18	Abstimmung EU / Presto (zwei Workshops, Vor- und Nachbereitung)	4
19	Qualitätssicherung für Arbeitspaket 2	5
Summe der PT		**33**

Tabelle 4: Zusammenführung der Ergebnisse, Erstellung finaler Dokumente

Nr.	Aktivität im Arbeitspaket 3	Aufwand (PT)
20	Zusammenführung der Teilergebnisse aus AP 2 zur finalen Spezifikation; Erarbeitung von Empfehlung zum szenariengerechten Einsatz der Funktionsbausteine/-Profilvarianten der Spezifikation	5
21	Einarbeitung Kommentierung dazu	2
22	Abschließender Workshop mit Vor- und Nachbereitung	3
23	Finale Qualitätssicherung	3
Summe der PT im Arbeitspaket 3		**13**
Summe der PT insgesamt		**66**

Interoperabilität von OSCI-Implementierungen

Bericht aus dem Fraunhofer FOKUS eGovernment-Labor

Uwe Holzmann-Kaiser

Fraunhofer FOKUS, Berlin

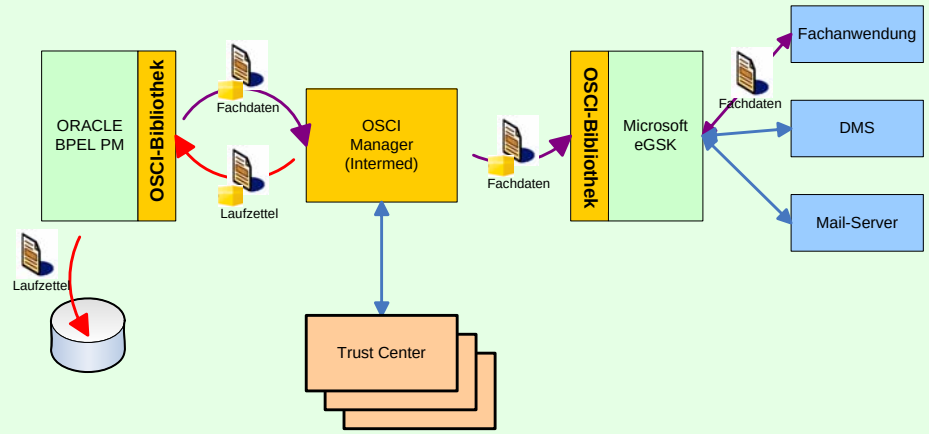
Fraunhofer Institut für Offene Kommunikationssysteme

eGovernment Labor Fraunhofer FOKUS

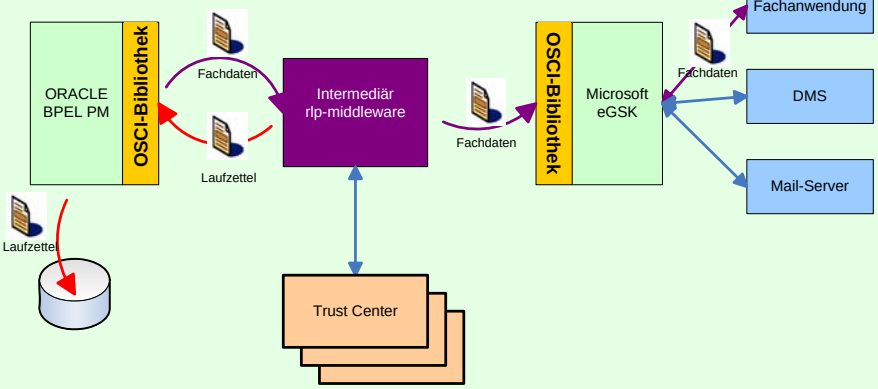
Fraunhofer FOKUS eGovernment-Labor Partner

Fraunhofer Institut für Offene Kommunikationssysteme

Szenario aus den Labor



Szenarien aus den Labor



Ergebnisse

java			transport signature and encryption	KoopA osci lib 1.1.2B / jdk 1.4.2		
				store delivery	fetch process card	fetch delivery
		RLP	no	OK	OK	OK
			sig	NO	NO	NO
			enc	OK	OK	OK
			sig+enc	NO	NO	NO
		Governikus 2.2.0.1	no	OK	OK	OK
			sig	OK	OK	OK
			enc	OK	OK	OK
			sig+enc	OK	OK	OK
		Governikus 2.2.1.1	no	OK	OK	OK
			sig	OK	OK	OK
			enc	OK	OK	OK
			sig+enc	OK	OK	OK

Fraunhofer Institut für Offene Kommunikationssysteme

Ergebnisse

java			transport signature and encryption	KoopA osci lib 1.2.2 / jdk 1.5.0_06		
				store delivery	fetch process card	fetch delivery
		RLP	no	OK	OK	OK
			sig	OK	OK	OK
			enc	OK	OK	OK
			sig+enc	OK	OK	OK
		Governikus 2.2.0.1	no	OK	OK	OK
			sig	OK	OK	OK
			enc	OK	OK	OK
			sig+enc	OK	OK	OK
		Governikus 2.2.1.1	no	OK	OK	OK
			sig	OK	OK	OK
			enc	OK	OK	OK
			sig+enc	OK	OK	OK

Fraunhofer Institut für Offene Kommunikationssysteme

Ergebnisse

.Net			transport signature and encryption	KoopA osci lib 1.1/ .net 1.1 (Visual Studio 2003)		
				store delivery	fetch process card	fetch delivery
		RLP	no	NO	NO	NO
			sig	NO	NO	NO
			enc	NO	NO	NO
			sig+enc	NO	NO	NO
		Governikus 2.2.0.1	no	OK	OK	OK
			sig	OK	OK	OK
			enc	OK	OK	OK
			sig+enc	OK	OK	OK
		Governikus 2.2.1.1	no	OK	OK	OK
			sig	OK	OK	OK
			enc	OK	OK	OK
			sig+enc	OK	OK	OK

Fraunhofer Institut für Offene Kommunikationssysteme

Ergebnisse

.Net			transport signature and encryption	KoopA osci lib 1.2.2/ .net2.0 (Visual Studio 2005)		
				store delivery	fetch process card	fetch delivery
		RLP	no	OK	OK	OK
			sig	OK	OK	OK
			enc	OK	OK	OK
			sig+enc	OK	OK	OK
		Governikus 2.2.0.1	no	OK	OK	OK
			sig	OK	OK	OK
			enc	OK	OK	OK
			sig+enc	OK	OK	OK
		Governikus 2.2.1.1	no	OK	OK	OK
			sig	OK	OK	OK
			enc	OK	OK	OK
			sig+enc	OK	OK	OK

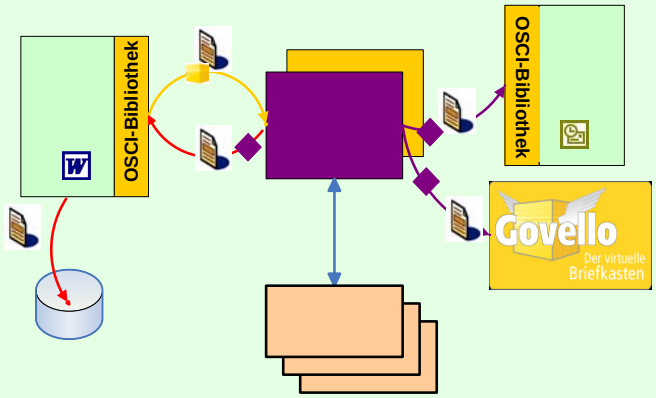
Fraunhofer Institut für Offene Kommunikationssysteme

Ergebnisse

java			transport signature and encryption	Esslingen letzte osci lib impl (jdk 1.4.1_07)		
				store delivery	fetch process card	fetch delivery
		RLP	no			
			sig			
			enc			
			sig+enc			
		Governikus 2.2.0.1	no	OK	OK	OK
			sig	NO	OK	OK
			enc	NO	NO	NO
			sig+enc	NO	NO	NO
		Governikus 2.2.1.1	no	OK	OK	OK
			sig	OK	OK	OK
			enc	NO	NO	NO
			sig+enc	NO	NO	NO

Fraunhofer Institut für Offene Kommunikationssysteme

Szenarien aus den Labor



Fraunhofer Institut für Offene Kommunikationssysteme

Weitere Fallen auf dem Weg

OSCI-Lib 1.2.2
Java 1.5.0_09

Governikus 2.2.1.2
JBOSS 3.2.8 RC 1
Java 1.4.2_03-06

OSCI-Lib

Intermediär

> 2048 bit

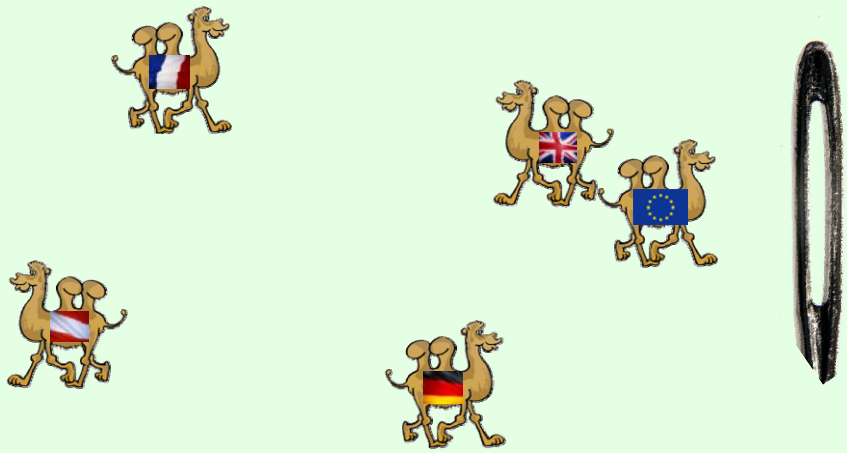
= < 2048 bit

Fraunhofer Institut für Offene Kommunikationssysteme

OSCI Spezifikation und Interoperabilität

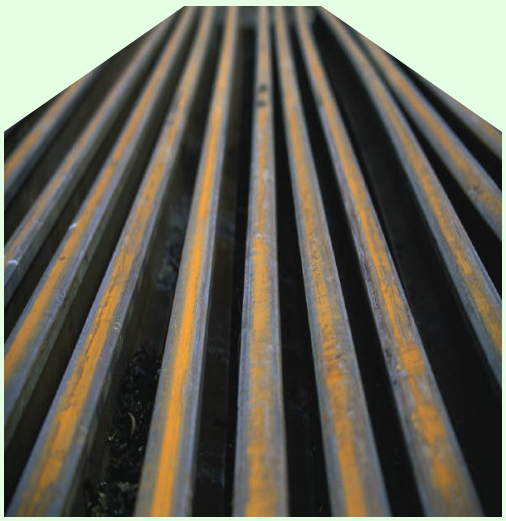
Fraunhofer Institut für Offene Kommunikationssysteme

Sicherer Datenaustausch auf europäischer Ebene



Fraunhofer Institut für Offene Kommunikationssysteme

Konvergenz auf europäischer Ebene (1)



Fraunhofer Institut für Offene Kommunikationssysteme

Konvergenz auf europäischer Ebene (2)

Meinst du, sie werden was *merken?*

Fraunhofer Institut für Offene Kommunikationssysteme

Microsoft Services –

Ihr Partner für Consulting- und Supportleistungen.

OSCI: WS-Profilierung

Microsoft

OSCI: WS-Profilierung

Agenda

- ☑ Überblick über WS-* Spezifikationen
- ☑ Konsequenzen für das OSCI-Kommunikationsmodell
- ☑ Konsequenzen für das OSCI-Rollenmodell
- ☑ Konsequenzen für die Umsetzung von OSCI-Sicherheitsanforderungen
- ☑ Vorteile einer Lösung über WS-*
- ☑ Probleme, offene Punkte bei einer Lösung über WS-*

Microsoft

OSCI: WS-Profilierung

Agenda

- *Überblick über WS-* Spezifikationen*
- Konsequenzen für das OSCI-Kommunikationsmodell
- Konsequenzen für das OSCI-Rollenmodell
- Konsequenzen für die Umsetzung von OSCI-Sicherheitsanforderungen
- Vorteile einer Lösung über WS-*
- Probleme, offene Punkte bei einer Lösung über WS-*

Microsoft

OSCI: WS-Profilierung

Überblick über WS-* Spezifikationen

SOAP 1.1/1.2 (W3C-Standards von 2000, 2003)

- OSCI 1.2 verwendet SOAP 1.1
- SOAP 1.2 seit 06/2003 W3C-Recommendation
- http://www.w3.org/2000/xp/Group/

XOP/MTOM (W3C 2005) vs. DIME vs. SOAP with Attachments (SwA) (W3C 2000)

- Konkurrierende Standards für die Behandlung von Attachments in SOAP-Nachrichten
- XOP/MTOM ist der neueste Standard (2003) und scheint sich gegenüber DIME und SwA durchzusetzen.
- Vorteile von XOP/MTOM: Attachments werden als MIME-Parts abgelegt und aus der SOAP-Nachricht refrenziert. Dadurch entfällt unter Umständen die Base64-Codierung und die eigentliche SOAP-XML-Nachricht wird kleiner.
- XOP/MTOM ähnelt der Behandlung von Attachments in OSCI 1.2
- http://www.w3.org/2000/xp/Group/

Microsoft

OSCI: WS-Profilierung

Überblick über WS-* Spezifikationen

WS-Security (OASIS, v1.0 2004, v1.1, 2006)

- Beschreibt Mechanismen für die Absicherung (Signatur/Verschlüsselung) des Transportweges (z.B. über SSL) und der Nachricht mit einer Ende-zu-Ende Verschlüsselung
- Grundidee ähnelt dem Konzept des „doppelten Umschlags“ in OSCI 1.2. Allerdings wird der äußere Umschlag in der Regel über SSL abgebildet.
- http://www.oasis-open.org/specs/index.php#wssv1.0

Microsoft

OSCI: WS-Profilierung

Überblick über WS-* Spezifikationen

WS-Trust (von IBM und MS 2005 an OASIS zur Standardisierung übergeben)

- Protokoll, über das Security Tokens (X509, Kerberos, SAML, Username/password etc.) ausgestellt oder überprüft werden können.
- Sogenannte Security-Token-Services (STS) übernehmen den Dienst der Überprüfung von Security Tokens anderer Kommunikationspartner und stellen bei entsprechender Vetrauensstellung ein eigenes Token aus. Dadurch kann die Verwaltung der Vertrauensstellungen von den einzelnen Web-Services zu einem zentralen STS deligiert werden.
- Über einen entsprechenden STS könnte beim OSCI-Intermediär die Überprüfung der Zertifikate zur Verfügung gestellt werden. In diesem Fall sind WS-Trust und XKMS konkurrierende Standards.
- ftp://www6.software.ibm.com/software/developer/library/ws-trust.pdf
- http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ws-sx

Microsoft

OSCI: WS-Profilierung

Überblick über WS-* Spezifikationen

WS-MetaDataExchange

- WS-MetadataExchange beschreibt, wie Nutzer die Meta-Informationen (z.B. WSDL Dokumente, XML Schemata und WS-Policies) über Service Endpoints erhalten können.
- http://ifr.sap.com/ws-metadataexchange/WS-MetadataExchange.pdf

WS-Adressing (2004 zur Standardisierung beim W3C eingereicht)

- Spezifikation für Adressinformationen für SOAP-Requests und ggf. Ihre Antworten
- Enthält wie für OSCI 1.3 vorgeschlagen Mechanismen, um festzulegen, wohin Antworten oder Fehler ggf. Auch asynchron geschickt werden sollen.
- http://www.w3.org/Submission/ws-addressing/

Microsoft

OSCI: WS-Profilierung

Überblick über WS-* Spezifikationen

WS-ReliableMessaging (WS-Reliability) (2005 bei OASIS eingereicht)

- Konkurrierende Standards. Mittlerweile sind beide Standards bei OASIS eingereicht und es wird einen konsolidierten Standard (WS-RX Reliable Exchange) aus Basis von WS-ReliableMessaging geben.
- Stellt auf Transportebene sicher, dass Nachrichten in einer Sequenz (Dialog) in der korrekten Reihenfolge und ggf. nur einmal zugestellt werden. Der Empfänger schickt Bestätigungen und fragt ggf. Verlorene Nachrichten erneut ab.
- http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ws-rx

WS-Policy(Attachment) (W3C v1.5 Working Draft, 2006)

- WS-Policy beschreibt Anforderungen, Fähigkeiten und Zusicherungen eines Web Services. Eine Policy kann z.B. Darauf hinweisen, dass ein Web Service nur eingehende Anfragen akzeptiert, wenn diese eine gültige Signatur enthält oder die Nachricht eine bestimmte Größe nicht überschreitet. Die Spezifikationen WS-PolicyAttachment und WS-MetadataExchange spezifizieren, wie eine Policy über SOAP Nachrichten oder eingeschlossen in XML und WSDL Dokumenten zugänglich gemacht werden kann.
- http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-polfram/ws-policy-2006-03-01.pdf
- http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-polatt/ws-polat-2006-03-01.pdf

Microsoft

OSCI: WS-Profilierung

Überblick über WS-* Spezifikationen

WS-SecurityPolicy (2005 an OASIS zur Standardisierung übergeben)

- Beschreibung der domänspezifischen Anforderungen aus WS-Security, WS-Trust und WS-SecureConversation als Ergänzung zu WS-Policy. So können z.B. Anforderungen an zu verwendende Security Tokens definiert werden, es kann festgelegt werden, welche Nachrichtenteile signiert/verschlüsselt sein müssen und ob eine Absicherung der Transportebene erforderlich/möglich ist.
- http://specs.xmlsoap.org/ws/2005/07/securitypolicy/ws-securitypolicy.pdf

WS-RMPolicy (2005 bei OASIS zur Standardisierung eingereicht)

- Beschreibung der Anforderungen für WS-ReliableMessaging als Ergänzung zu WS-Policy. So kann besipielswiese definiert werden, wie lange ein Client warten soll, bis er erneut versucht, eine Nachricht zuzustellen.
- http://msdn.microsoft.com/library/en-us/dnglobspec/html/WS-RMPolicy.pdf

Microsoft

OSCI: WS-Profilierung

Überblick über WS-* Spezifikationen

WS-SecureConversation (2005 an OASIS zur Standardisierung übergeben)

- Beschreibt eine Möglichkeit über einen Security Context rechenaufwändige Operationen wie die Überprüfung eines Security Tokens und die Generation und asymmetrische Verschlüsselung eines symmetrischen Schlüssels nicht für jede Nachricht durchführen zu müssen.
- Würde im Hinblick auf OSCI 1.2 den expliziten Dialog ersetzen
- ftp://www6.software.ibm.com/software/developer/library/ws-secureconversation.pdf

Microsoft

OSCI: WS-Profilierung

Überblick über WS-* Spezifikationen

WS-Federation / Liberty Alliance

- Teilweise konkurrierende Standards für Identitätsmanagement. Clients sollen sich an Webservices in unterschiedlichen Sicherheitsdomänen nur einmal authentifizieren müssen (SSO)
- ftp://www6.software.ibm.com/software/developer/library/ws-fed.pdf
- http://www.projectliberty.org/

WS-Coordination/WS-AtomicTransaction

- In WS-Coordination wird ein allgemeines Protokoll beschrieben, mit dem Transaktionen zwischen Web-Services beschrieben werden können
- In WS-AtomicTransaction werden Erweiterungen zu WS-Coordination für „short running transactions“ definiert. (Two-Phase-Commit mit/ohne Persistenz)
- ftp://www6.software.ibm.com/software/developer/library/WS-Coordination.pdf
- ftp://www6.software.ibm.com/software/developer/library/WS-AtomicTransaction.pdf

Microsoft

OSCI: WS-Profilierung

Agenda

- Überblick über WS-* Spezifikationen
- *Konsequenzen für das OSCI-Kommunikationsmodell*
- Konsequenzen für das OSCI-Rollenmodell
- Konsequenzen für die Umsetzung von OSCI-Sicherheitsanforderungen
- Vorteile einer Lösung über WS-*
- Probleme, offene Punkte bei einer Lösung über WS-*

Microsoft

OSCI: WS-Profilierung

Konsequenzen für das OSCI-Kommunikationsmodell

OSCI 1.2

- Sender ←→ Intermediär (des Empfängers) ←→ Empfänger
  - Der Absender verwendet den Intermediär des Empfängers
  - (Noch) wird im OSCI Protokoll nicht festgeschrieben, dass ein Intermediär die Endpunkte für seine Empfänger kennen muss
  - Der Absender vertraut entweder den Prüfprotokollen des fremden Intermediärs oder muss diese Prüfungen selbst durchführen.

WS-*

- **STS Sender ←→ Sender ←→** x SOAP-Intermediäre **←→Empfänger ←→ STS Empfänger**
- Multihop wird durch WS-Addressing, WS-ReliableMessaging etc. Direkt unterstützt
- Jeder Kommunikationpartner hat seinen eigenen Security-Token-Service (STS), der die Prüfprotokolle erstellt. Ob einem existierenden Prüfprotokoll des Kommunikationspartners vertraut wird, kann konfiguriert werden

Microsoft

OSCI: WS-Profilierung

Konsequenzen für das OSCI-Kommunikationsmodell

OSCI 1.2

- Attachments werden in einem OSCI-spezifischen Format als MIME-Parts transportiert und für XML-Signaturen referenziert.
- Impliziter/expliziter Dialog
- Reliable Messaging: Über die Nachricht GetMessageID und den ControlBlock wird sichergestellt, dass Nachrichten in der richtigen Reihenfolge und nur genau einmal zugestellt werden.

WS-*

- Attachments mit XOP/MTOM als MIME-Parts transportiert und für XML-Signaturen referenziert.
- Der explizite Dialog wird über WS-SecureConversation realisiert. Die Nachrichten Init- und ExitDialog sowie die Referenzen auf die ConversationId entfallen.
- Reliable Messaging: Die oben genannten Anforderungen können durch WS-RX abgedeckt werden. Die Nachricht GetMessageID sowie der ControlBlock können entfallen.

Microsoft

OSCI: WS-Profilierung

Konsequenzen für das OSCI-Kommunikationsmodell

OSCI 1.2

- Laufzettel: Der an der Kommunikation beteiligte Intermediär protokolliert die Zeitpunkte für den Nachrichteneingang, die Weiterleitung und den Empfang und stellt die Informationen zusammen mit den Prüfprotokollen für jede Nachricht zum Abruf bereit.
- Kommunikationsmodelle:
  - Immer genau 1 Intermediär zwischen Sender und Empfänger
  - One Way aktiver/passiver Empfänger, Request-Response mit/ohne Laufzettel

WS-*

- Laufzettel: Die Zusammenstellung von Prüfprotokollen und Zeitpunkten muss auf Anwendungsebene realisiert werden. Entsprechende Vorgaben sind in einer WS-OSCI-Spezifikation vorzugeben.
- Kommunikationsmodelle:
  - Der Intermediär stellt nur noch Dienste für Postfächer (Nachrichten, Persistierung) und Zertifikatsprüfung sowie die Verwaltung der Laufzettel bereit. Er ist bei passiven Szenarien nicht mehr direkt beteiligt.
  - One Way passiver Empfänger sowie Request-Response werden durch WS-ReliableMessaging abgedeckt. Für One Way aktiver Empfänger werden nach wie vor eigene Nachrichten sowie eine Postfach-Komponente benötigt.

Microsoft

OSCI: WS-Profilierung

Agenda

- Überblick über WS-* Spezifikationen
- Konsequenzen für das OSCI-Kommunikationsmodell
- *Konsequenzen für das OSCI-Rollenmodell*
- Konsequenzen für die Umsetzung von OSCI-Sicherheitsanforderungen
- Vorteile einer Lösung über WS-*
- Probleme, offene Punkte bei einer Lösung über WS-*

Microsoft

OSCI: WS-Profilierung

Konsequenzen für das OSCI-Rollenmodell

- Bis auf Intermediär unverändert.
  - Sender und Empfänger verwenden für die zentralen Intermediärs-Dienste jeweils einen Intermediär Ihres Vertrauens.
- Dadurch bedingt:
  - Laufzettel müssen auf jedem beteiligten Intermediär gepflegt werden und die zu synchronisierenden Informationen müssen mit übertragen werden.
  - Zertifikatsprüfungen können von anderem Intermediär übernommen werden, wenn Vertrauensstellung vorhanden. Ansonsten müssen sie mehrfach überprüft werden.

Microsoft

OSCI: WS-Profilierung

Sicherheitsanforderungen

Transportsignatur/-verschlüsselung:

- Das Verschlüsselungsmodell in WS-Security sieht vor, dass eine Verschlüsselung auf Transportebene in der Regel auf Protokollebene per SSL erfolgt.
- In diesem Fall wäre für die Transportebene nur noch ein „Allround-Zertifikate“ sinnvoll.

Inhaltssignatur/- verschlüsselung:

- Das Verschlüsselungsmodell in WS-Security sieht vor, dass für eine Verschlüsselung auf Inhaltsebene der gesamte SOAP-Body nur für den Empfänger verschlüsselt und signiert wird. Es wäre nicht mehr möglich, in einer OSCI-Nachricht ContentContainer für unterschiedliche Leser oder von unterschiedlichen Autoren zu verpacken.

Microsoft

OSCI: WS-Profilierung

Sicherheitsanforderungen

Laufzettel:

- Die Zeitpunkte müssten auf jedem Intermediär geführt werden. Ein Weg zur Synchronisation ist vorzusehen.
- Zeitpunkte und Prüfprotokolle können als signierte SOAP-Header verschickt werden
- Überprüfte Zertifikate werden nach wie vor als eigene SOAP-Header geführt in den Prüfprotokollen nur referenziert, so dass bei Vertrauensstellung das Prüfergebnis eines anderen Intermediärs übernommen werden kann?
- Evtl. Prüfprotokolle für Zertifikate als custom Security-Token über WS-Trust?

Kryptografische Zeitstempel

- Sollten in den Signaturcontainer aufgenommen werden

Benutzerauthentifizierung für Zugriff auf das Postfach

- WS-SecureConversation

Microsoft

OSCI: WS-Profilierung

Agenda

- Überblick über WS-* Spezifikationen
- Konsequenzen für das OSCI-Kommunikationsmodell
- Konsequenzen für das OSCI-Rollenmodell
- Konsequenzen für die Umsetzung von OSCI-Sicherheitsanforderungen
- *Vorteile einer Lösung über WS-**
- Probleme, offene Punkte bei einer Lösung über WS-*

Microsoft

OSCI: WS-Profilierung

Vorteile einer Lösung über WS-*

Standard-Komponenten:

- Mittlerweile sind (fast) alle aufgeführten Standards stabil
- Ein breites Angebot an Standard-Produkten wird diese Standards unterstützen
- Interoperabilität zwischen Produkten verschiedener Hersteller sollte durch die Standard-Produkte sichergestellt werden

Effizienz:

- Das WS-* Framework sieht die Möglichkeit vor, insbesondere die Kommunikation mit passiven Empfängern deutlich effizienter zu gestalten
- FV-spzifische Bindings könnten deutlich flexibler und effizienter sein. (z.B. DVDV-Abfrage)

Internationale Verwendung:

- Es ist damit zu rechnen, dass evtl. anstehende elektronische Datenverarbeitung innerhalb der EU oder international auf den WS-* Standards aufsetzen wird. Deshalb ist eine Evaluation der zusätzlichen Anforderungen durch deutsche Gesetzgebung (z.B. SigG) sicherlich sinnvoll.

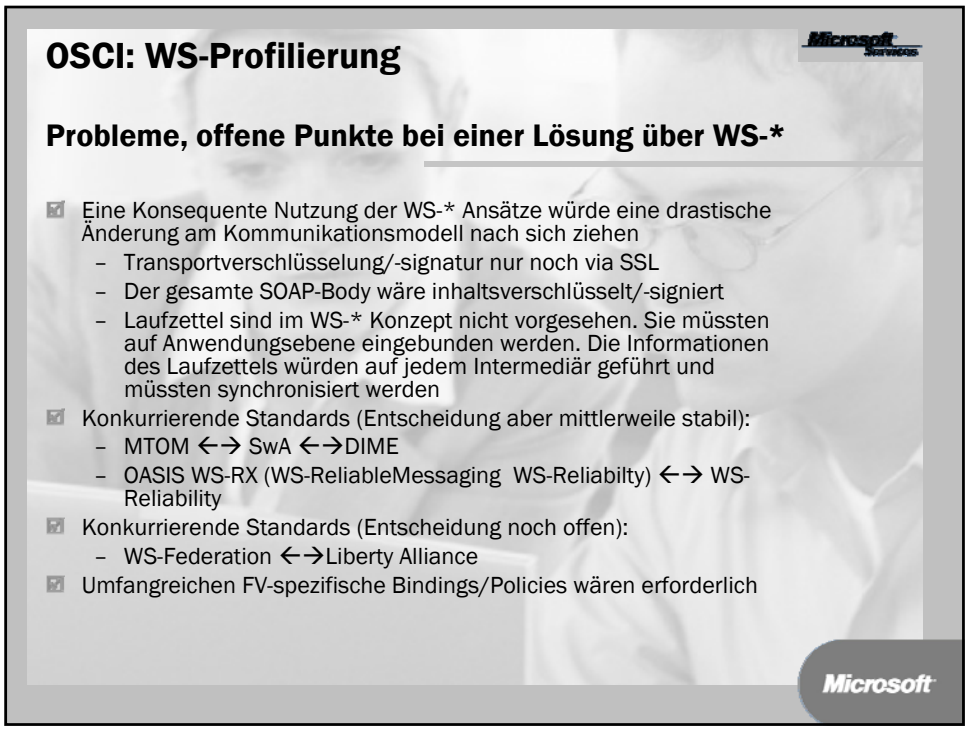
Microsoft

OSCI: WS-Profilierung

Agenda

- Überblick über WS-* Spezifikationen
- Konsequenzen für das OSCI-Kommunikationsmodell
- Konsequenzen für das OSCI-Rollenmodell
- Konsequenzen für die Umsetzung von OSCI-Sicherheitsanforderungen
- Vorteile einer Lösung über WS-*
- *Probleme, offene Punkte bei einer Lösung über WS-**

Microsoft

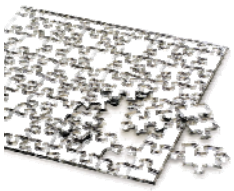

OSCI: WS-Profilierung
Probleme, offene Punkte bei einer Lösung über WS-*
Eine Konsequente Nutzung der WS-* Ansätze würde eine drastische Änderung am Kommunikationsmodell nach sich ziehen
– Transportverschlüsselung/-signatur nur noch via SSL
– Der gesamte SOAP-Body wäre inhaltsverschlüsselt/-signiert
– Laufzettel sind im WS-* Konzept nicht vorgesehen. Sie müssten auf Anwendungsebene eingebunden werden. Die Informationen des Laufzettels würden auf jedem Intermediär geführt und müssten synchronisiert werden
Konkurrierende Standards (Entscheidung aber mittlerweile stabil):
– MTOM ←→ SwA ←→DIME
– OASIS WS-RX (WS-ReliableMessaging WS-Reliabilty) ←→ WS-Reliability
Konkurrierende Standards (Entscheidung noch offen):
– WS-Federation ←→Liberty Alliance
Umfangreichen FV-spezifische Bindings/Policies wären erforderlich
Microsoft

Weiterentwicklung von OSCi auf Basis aktueller Sicherheitsstandards für Web-Services

Marc Horstmann, Leiter Research and Developement

bremen online services

Ansprüche an zukunftssichere E-Government-Software und -Lösungen



Kompatibilität

- zu vorhandenen IT-Infrastrukturen
- zu bereits eingesetzten E-Government-Lösungen
- zu relevanten Produkten auf dem Markt.

Standard- und Gesetzkonformität

- Signaturgesetz-Konformität
- Offenheit für internationale Standards
- Konformität zu Vorgaben SAGA

Wirtschaftlichkeit

- dienen als Infrastruktur für alle Spielarten elektronischer Kommunikation dienen
- dabei möglichst viele Funktionalitäten „vor die Klammer“ ziehen und damit den Aufwand bei der Realisierung einzelner Anwendungen minimieren

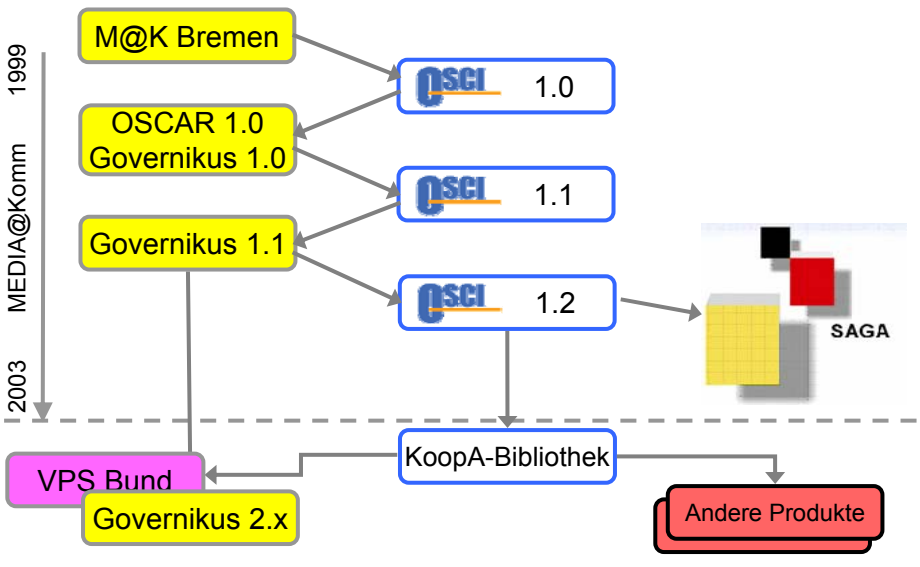
16.11.2006 2

Entwurfsziele von OSCI

- Interoperabilität und Plattformunabhängigkeit
  - Nutzung etablierter XML – Standards
  - Web Services – Paradigma; Absicherung dieser
  - 2002 „stabil“: SOAP; XML Dig. Signature / Encryption; Cryptographic Messaging Syntax, PKCS#*, PKI/X509v3….
  - ➢ Standardisierung auf Inhaltsdatenebene (►„XÖV“)
- Skalierbarkeit
  - optionale Sicherheitsmechanismen verschiedener Niveaus
- Anwendungsunabhängigkeit
  - strikte Trennung der Inhalts- und Transportebene
- Unterstützung offener Benutzergruppen
- Bidirektionale Kommunikation
- Weitgehende Sicherheitsmechanismen auf Protokollebene

16.11.2006 3

OSCI-Transport Spezifikation u. Implementierung: zyklische Entwicklung



Herausforderungen für OSCI Transport

- OSCI wird zunehmend im E-Government genutzt, u.a. „Massenszenarien“ wie z.B. Meldewesen und erv-d führen zu neuen Anforderungen
- Interessierte Expertenrunde aus Verwaltung und Industrie beschäftigte sich in 2006 mit neuen Anforderungen an OSCI Transport (Auszug):
  - Anpassung an den aktuellen Stand der intl. Standardisierung
  - Verbesserte / alternative Authentisierungsmechanismen (Einsatz von Authentisierungszertifikaten -> Personalausweis 2008)
  - Einsatz von Organisations- und Attributzertifikaten
  - Adressierung auf Basis föderierter Dienste- und Nutzerverzeichnisse („Web Identity“ auf Basis SAML und/oder WS Trust)
  - Erweiterung der Protokollierung: Zustellungsnachweise mit Beweiswert, differenzierte Zertifikatsstatus
  - Technische Optimierung des Messaging; in Teilen Aufnahme der Prinzipien von ebXML; Attachment-Handling
  - Differenzierung des Rollenmodells

16.11.2006 5

OSCI 1.3 oder 2.0?

- Ergebnis: Alle Anforderungen lassen sich auf Basis eines „OSCI 1.3“ bei Beibehaltung der 1.2-Strukturen nur sehr unsauber umsetzen
- Die Prinzipien von OSCI müssen im WS-Stack abgebildet werden – eben wie schon 1.0 muss eine Fortschreibung aktuell anerkannte Standards referenzieren
- OSCI soll ein Profiling dieser Industriestandards werden
- Damit Verbesserung der Voraussetzungen für
  - Kompatibilität auf EU-Ebene (zumindest Konvergenz der Protokolle)
  - Kompatibilität mit in der Wirtschaft genutzten Verfahren
- Weiter ist geboten: Abgleich mit entsprechenden Aktivitäten in anderen EU-Ländern („IDABC“)
  - Vorhaben „eLink“ wird eingestellt
  - Andere EU-Länder arbeiten an Adoption der WS-Standards

16.11.2006 6

Ziel: Spezifikation „OSCI 2.0“ in 2007

- Frameworks und Web-/Applikationsserver werden in naher Zukunft Sicherheitsmechanismen zur Verfügung stellen auf Basis jetzt (fast) stabiler relevanter Standards:
  - WS-Security, WS-Trust, WS Addressing, WS Reliable Messaging, WS Secure Conversation, SAML…
- Aktuell begonnen: Kooperation mit anderen EU-Ländern, insbesondere Projekt „PRESTO“ (Protocole d‘Echange Standard et Ouverte de l‘Administration) in Frankreich
  - Präsentation und Abgleich der Anforderungen, Szenarien und Rollenmodelle noch im November 2006
  - Vergleichbare Aktivitäten in Dänemark und Schweden
  - Spezifikation – mit ggf. nationalem Profiling – soll bis Ende 2007 erarbeitet werden
  - Fokus auch: Investitionssicherung; Rollout und Interoperabilität mit genutzten Infrastrukturen soll über Registries gelöst werden

16.11.2006 7