# Bericht der Projektgruppe „Meldewesen“

Teil 1: Die Rückmeldung

**Anlagen:**

1. Länderumfrage NRW
2. OSCI-Projektbeschreibung
3. Sicherheitsbeurteilung des BSI

---

Stand: 24.10.2002
Version: 1.1
Status: Endfassung, verabschiedet

. . .

## Inhaltsverzeichnis

## 1. Der Auftrag

1.1 Der AK I richtete in seiner 102. Sitzung am 29./30.04.2002 in Bremerhaven mit folgendem Beschluss die Projektgruppe ein:

**Beschluss:**

1. *Der AK I beauftragt eine Projektgruppe, bestehend aus Vertretern der Länder Baden-Württemberg, Bayern, Bremen, Hamburg, Nordrhein-Westfalen und Schleswig-Holstein, zu untersuchen,*

   - *welche rechtlichen und technischen Voraussetzungen geschaffen werden müssen, damit Meldedaten mittels automatisierter Datenübertragung reibungslos zwischen den Meldebehörden ausgetauscht werden können; hierbei sind die bereits bekannten technischen Verfahren zu berücksichtigen und zu bewerten;*

   - *in welcher Form es möglich ist, die elektronische Anmeldung und die Melderegisterauskunft über das Internet bei den Meldebehörden weitgehend einheitlich zu gestalten.*

   *Bayern wird gebeten, zu der ersten Sitzung der Projektgruppe einzuladen.*

2. *Der AK I bittet den BMI, einen Vertreter in die Projektgruppe zu entsenden.*

3. *Dem AK I ist zu seiner nächsten Sitzung zu berichten.*

1.2 Auf ihrer 170. Sitzung beschloss die Ständige Konferenz der Innenminister und -senatoren der Länder am 06.06.2002 in Bremerhaven:

„ ...

3. *Die IMK beauftragt die vom AK I in seiner Sitzung vom 29./30. April 2002 zur Umsetzung des Gesetzes zur Änderung des Melderechtsrahmengesetzes und anderer Gesetze vom 25. März 2002 eingesetzte Projektgruppe, das vom KoopA ADV befürwortete Projekt XMeld auf der Basis von OSCI mit in die Prüfung und Bewertung einzubeziehen."*

Die Projektgruppe hat den unter 1.1, Nr.1, 1.Tiret wiedergegebenen Auftrag so verstanden, dass sie nur die Probleme des länderübergreifenden Datenaustausches bearbeitet. Für den landesinternen Datenaustausch können nach § 17 Abs. 1, letzter Satz Melderechtsrahmengesetz –MRRG- in der Fassung der Bekanntmachung v. 25.03.2002 (*alle im Folgenden zitierten Rechtsvorschriften ohne Fundstelle sind solche des MRRG*) weitergehende Regelungen getroffen werden, die sich einer bundesweiten Durchnormierung entziehen.

## 2. Zusammensetzung der Projektgruppe und Vorgehen

Die Projektgruppe aus den in Ziffer 1 des Beschlusses des AK I genannten Ländern wurde ergänzt um einen Vertreter des Bundesministeriums des Innern und des Landes Sachsen sowie eines Vertreters der OSCI-Leitstelle, des Bundesamtes für Sicherheit in der Informationstechnik – BSI-, der Datenzentrale Baden-Württemberg und der Bundesvereinigung der Kommunalen Spitzenverbände.

Die Projektgruppe hat in zwei Sitzungen (20.06. und 24.09.2002) zunächst die Probleme der Rückmeldung behandelt, die nach ihrer Einschätzung die höchste Priorität haben[1]. In einem zweiten Teil dieses Berichtes werden die vom Arbeitsauftrag ebenfalls umfassten Problembereiche der Anmeldung und der Melderegisterauskunft behandelt. Dieser kann aus Zeitgründen dem AK I erst in der ersten Sitzung 2003 vorgelegt werden.

Die Projektgruppe hat eine bundesweite Umfrage unter den Innenministerien/-senatoren durchgeführt zur augenblicklichen Organisation des Datenaustau-

[1] Begründung unter 3.1 des Berichtes

sches der Meldebehörden untereinander sowie über die Planungsabsichten in diesem Bereich. Wortlaut der Umfrage und eine Zusammenfassung des Ergebnisses finden sich als **Anlage 1** dieses Berichtes.

## 3. Die rechtlichen und tatsächlichen Rahmenbedingungen

3.1 Nach § 11 Abs. 2 wird die Pflicht zur Abmeldung für den Fall, dass der betreffende Bürger eine neue Wohnung im Inland bezieht, entfallen[2]. Dadurch kommt der so genannten Rückmeldung (§ 17 Abs. 1, das ist die Unterrichtung der Wegzugsmeldebehörde durch die Zuzugsmeldebehörde über eine erfolgte Anmeldung) für die Richtigkeit der Melderegister eine ganz wesentliche Bedeutung zu. Nicht umsonst hat der Gesetzgeber die Verpflichtung ausgesprochen, diese Kommunikation spätestens drei Tage nach erfolgter Anmeldung aufzunehmen und sobald als möglich abzuschließen.

3.2 Bei den ca. 6.000 Meldebehörden in Deutschland fallen ca. 8 Mio. [3] Rückmeldungen pro Jahr an. Davon sind etwa die Hälfte solche zwischen Meldebehörden verschiedener Länder.

Die Arbeitsgruppe ist sich einig darüber, dass das in § 17 Abs. 1 genannte Zeitziel angesichts einer solch großen Menge an abzuarbeitenden Rückmeldungen letztlich nur erreicht werden kann, wenn die Kommunikation zwischen den Meldebehörden mittels elektronischer Datenverarbeitung erfolgt. Wenn dabei auch noch Medienbrüche (Umsetzung von Meldungen auf Papier in elektronische Form und umgekehrt) vermieden werden können, sind erhebliche Rationalisierungspotentiale zu erschließen, die sich in Kosteneinsparungen niederschlagen.

3.3 Bei den Meldebehörden im Bundesgebiet sind etwa 20 elektronische Verfahren zum Einwohnermeldewesen (im Folgenden: EWO-Verfahren) unterschiedlichster

[2] § 11 Abs.2 gilt nicht unmittelbar, sondern erst nach entsprechender Anpassung der Ländermeldegesetze, vgl. § 23 Abs. 1 und 2 MRRG

[3] Diese Zahl ist aus den Angaben hochgerechnet, die für Bayern vorliegen (ca. 1,1 Mio. Rückmeldungen pro Jahr).

Struktur im Einsatz. Es gibt auch Meldebehörden, die noch auf herkömmliche Weise die Meldedaten per Karteikarte verwalten. Darüber hinaus sind nur ein Teil der Meldebehörden wirklich Online-fähig, d. h. an sichere Datennetze (wie Behördennetze o. ä.) oder an das Internet angeschlossen. Diese tatsächlichen Rahmenbedingungen sind bei den folgenden Überlegungen zu berücksichtigen.

**Eine Vision und ein realistisches Ziel**

Die Projektgruppe hält es für erstrebenswert, Anmeldung und die durch sie ausgelöste Rückmeldung, d. h. die Verständigung der Wegzugs-Meldebehörde von der Anmeldung, in einem Akt und so zu vollziehen, dass Unstimmigkeiten zwischen den bei der Anmeldung abgegebenen Daten und dem Datensatz bei der Wegzugs-Meldebehörde im Beisein des Bürgers am Bildschirm in der Zuzugsmeldebehörde abgeklärt werden können. Das ist jedoch nur dann möglich, wenn die betroffenen Meldebehörden untereinander Online und in Echtzeit kommunizieren können. Wegen der oben genannten tatsächlichen Rahmenbedingungen wird das flächendeckend erst mittel- bis langfristig möglich sein, so dass die Projektgruppe diese Vorstellung als Vision bezeichnet.

Damit die Vision von den innovationswilligen bzw. innovationsfähigen Meldebehörden zügig erreicht werden kann, sollte die Umsetzung der Vorschläge nicht erst erfolgen können, wenn alle Meldebehörden in Deutschland die Voraussetzungen erfüllen. Ebenso sollte auf die Finanzkraft der einzelnen Meldebehörden Rücksicht genommen werden.

Als jedoch realistisches Ziel gibt die Projektgruppe folgende

**Empfehlung Nr.1:**

**Die länderübergreifende Kommunikation zwischen den Meldebehörden sollte ab zwei Jahren nach Inkrafttreten der entsprechenden rechtlichen Vorschriften[4] nur noch mittels elektronischer Datenübertragung erfolgen.**

Die Maßgaben, nach denen diese Empfehlung erreicht werden kann, werden im Folgenden behandelt.

## 4. Die Standards „OSCI-XMeld“ und „OSCI-Transport“

Die Projektgruppe ist davon ausgegangen, dass eine Kommunikation zwischen Meldebehörden mit unterschiedlichen EWO-Verfahren nur dann erfolgreich sein kann, wenn folgende Voraussetzungen erfüllt sind:

- Der Inhalt der Meldung, die die empfangende Behörde erreicht, muss von dieser verstanden werden; daraus folgt, dass durch eine Konvention (einen Standard) dieser Meldeinhalt vollständig beschrieben und in einer Sprache abgefasst ist, die auch das fremde System verstehen kann; die Formatierung der Nachricht muss standardisiert sein;

- der Empfänger muss „die Verpackung“ der Meldung öffnen können; er muss über einen vorher vereinbarten Transportweg erreicht werden können;

- der Empfänger muss sichergestellt sehen, dass die Meldung tatsächlich von der absendenden Behörde stammt (Authentizität), sowie, dass die Meldung von Dritten auf dem Transportweg nicht gelesen und nicht verändert wurde.

Die letzteren Bedingungen werden in der Regel durch kryptologische Verfahren sichergestellt. Über Art und Weise von Verpackung und Transport müssen deshalb ebenfalls Standards entwickelt sein. Die Verschlüsselung muss vom Emp-

[4] 1. Bundesmeldedatenübermittlungsverordnung -BMeldeDÜV

fänger auch aufgehoben werden können. Auch deshalb müssen für diese Fragen zwischen Absender und Empfänger einheitliche Verfahren vereinbart sein.

4.1 Entsprechend dem Auftrag der IMK (vgl. unter 1.2) hat die Projektgruppe überprüft, ob die im Rahmen des MEDIA@Komm – Projektes[5] entwickelten Standards „OSCI-XMeld“ und „OSCI-Transport“ die oben genannten Bedingungen erfüllen können. Sie hat zu diesem Zweck die OSCI-Leitstelle[6], die die entsprechenden Entwicklungsprojekte betreut hat, gebeten, die Projektziele und -inhalte zu beschreiben (vgl. dazu Anlage 2); deren Leiter hat diese der Projektgruppe erläutert.

Die Untersuchungen der Projektgruppe haben Folgendes ergeben:

4.1.1 Im Rahmen des Projektes „XMeld“ hat die dafür verantwortliche Projektgruppe etwa 50 Geschäftsprozesse im Meldewesen, darunter auch die im Vordergrund stehenden Prozesse im Zusammenhang mit der Rückmeldung, untersucht und in einer dem Stand der Technik entsprechenden Maschinensprache (XML) beschrieben. Eine ausführliche Dokumentation dazu liegt vor. Diese Beschreibungen liefern einen Standard, der nicht selbst ein im Einwohnerwesen unmittelbar einzusetzendes Produkt ist, sondern der von den Herstellern von EWO-Verfahren in ihre Software eingearbeitet werden muss. Ist das geschehen, können unterschiedliche EWO-Verfahren miteinander kommunizieren, weil sie die ausgetauschten Meldungsinhalte gegenseitig verstehen können.

4.1.2 Der Standard „OSCI-Transport“ ist ein standardisiertes Nachrichtenprotokoll, welches die digitale Signatur und die Verschlüsselung von auszutauschenden Meldungen erlaubt. Auch dieses ist herstellerunabhängig wie der XMeld konstruiert, muss allerdings, weil es ebenfalls kein Produkt ist, erst in den EWO-Verfahren implantiert werden.

[5] vgl. dazu Ziff. 2 der Anlage 2

[6] siehe Anm. 4

Bezüglich des Standards OSCI-Transport wurden während der Arbeit der Projektgruppe folgende Bedenken geltend gemacht:

- Der Standard habe erhebliche Defizite und Mängel
- er funktioniere nicht
- er müsse weiterentwickelt werden (unklar sei, wer die Kosten trage) sowie
- er sei zu kompliziert und damit auch zu teuer.

Auf einer Konferenz des Städtetages mit Anwendern der Standards und Softwareherstellern am 16.09.2002 konnten diese Bedenken ausgeräumt werden. Es konnten nicht nur keine Mängel aufgezeigt werden, sondern Anwender bestätigten, dass der Standard auch funktionsfähig ist, zumal er angewendet wird. Der „bremer online service“ bietet unter der Adresse http://www.bremer-online-service.de insgesamt 100 Online-Dienste an, die OSCI nutzen. Die OSCI-basierten Verfahren Optimahn und Profimahn werden von Amtgerichten für die Mahnverfahren in insgesamt acht Bundesländern produktiv eingesetzt. Hochschulen und Universitäten in Bremen ermöglichen die Prüfungsanmeldung und weitere Geschäftsvorfälle mittels OSCI. Es wurde auch festgestellt, dass der Standard durchaus in verschiedenen Aufgabenbereichen der öffentlichen Hand mit unterschiedlichen Anforderungen an die Verschlüsselung angewendet werden kann, weil er insoweit skalierbar ist.

Die Ergebnisse dieser Konferenz hat der Vertreter der Bundesvereinigung der Kommunalen Spitzenverbände, der an der Besprechung teilgenommen hat, der Projektgruppe gegenüber bestätigt.

Inzwischen hat das BSI die Sicherheit von OSCI-Transport 1.2 bewertet und zwar mit positivem Ergebnis. Die ausführliche Sicherheitsbewertung liegt diesem Bericht als Anlage 3 bei.

**Empfehlung Nr. 2**

**Für die länderübergreifende elektronische Kommunikation der Meldebehörden untereinander sind die Standards OSCI-XMeld und OSCI-Transport 1.2 verbindlich vorzuschreiben. Dazu sind die Standards und ihre Dokumentation für jedermann zugänglich zu hinterlegen.**

Die Projektgruppe gibt diese Empfehlung aus folgenden Gründen:

- Die Standards sind herstellerneutral und von jedem EWO-Verfahren-Hersteller auch einzubauen;
- sie bieten die Möglichkeit, den Meldeverkehr unter unterschiedlichen EWO-Verfahren reibungslos abzuwickeln;
- OSCI-Transport 1.2 gewährleistet hinreichend die Sicherheit des Kommunikationsverkehrs zwischen den Meldebehörden;
- die Standards sind auf dem Stand der Technik;
- die o.a. Umfrage hat ergeben, dass kein Land gegen die Anwendung dieser Standards Bedenken hat; auch der Deutsche Städtetag vertritt die Auffassung, dass beide Standards so schnell wie möglich verbindlich vorgeschrieben werden sollten, da es außer einer kosten- und zeitaufwendigen Neuentwicklung keine Alternative dazu gäbe.

4.2 Die Projektgruppe hält es für unabdingbar, dass beide Standards unverzüglich weiterentwickelt bzw. für dauernd gepflegt werden müssen.

Im Rahmen des Pilotprojekts XMeld sind bisher zwar 50 Geschäftsprozesse entsprechend beschrieben, es stehen aber noch weitere Bereiche wie die Anmeldung, die Datenübermittlung an andere Behörden nach § 18 und andere Themen an, die standardisiert werden müssen. Andererseits entwickeln sich die Technik der Transporte und die der Verschlüsselung so schnell, dass auch der Standard OSCI-Transport unverzüglich zu pflegen und weiter zu entwickeln ist. Daher

**Empfehlung Nr. 3:**

**Es sind unverzüglich Strukturen zu definieren, die es erlauben beide Standards nachhaltig zu pflegen und weiter zu entwickeln.**

Dabei ist zu unterscheiden:

4.2.1 Die Standardisierung von Inhalten der Kommunikation zwischen Fachbehörden untereinander ist eine Frage des jeweiligen Fachbereichs. Deshalb sollte, was das Melderecht angeht, auf die in diesem Aufgabenbereich bestehenden Strukturen zurückgegriffen werden. So könnten

- die Pflege von XMeld (Anpassungen an gesetzliche Änderungen, Fehlerbereinigungen u. a.) als Daueraufgabe der Arbeitsgruppe unter Leitung des BMI anvertraut werden, die sich bisher um die Fortentwicklung des einheitlichen Datensatzes für das Meldewesen (DSMeld) gekümmert hat[7], während

- für die Erweiterung der Funktionalitäten (Standardisierung weiterer Geschäftsprozesse, der Kommunikation mit anderen Behördenbereichen wie Finanzamt, Kreiswehrersatzamt, Justiz u. ä.) jeweils abgrenzbare Projekte definiert werden können, denen unter Umständen auch Projektmittel (z. B. für eine Begleitung durch externe Firmen) zugewiesen werden könnten. Auftraggeber dieser Projekte sollte der AK I sein. [8]

**Empfehlung Nr. 4:**

[7] Die Arbeitsgruppe "DSMeld" gibt es eigentlich nicht mehr. Sie war von dem damaligen Unterausschuss "Melde-, Pass- und Ausweiswesen" des AK I der IMK eingerichtet worden, der inzwischen aufgelöst wurde. Damit ist formal auch die AG "DSMeld" untergegangen. Um sie unter Vorsitz des BMI wieder auferstehen zu lassen, bedarf es eines neuen Beschlusses des AK I oder der IMK.

[8] Für den XMeld hat bereits ein Folgeprojekt (XMeld 1.1) begonnen, das noch im Rahmen des MEDI-A@Komm-Projektes abgewickelt und auch finanziert werden kann. Nach Ende dieses Projektes allerdings ist sowohl die weitere Finanzierung der Projektarbeit zu klären, als auch die dafür erforderliche Struktur.

. . .

**Der Standard XMeld sollte durch eine fachlich und technisch qualifizierte Arbeitsgruppe gepflegt werden (z. B. die AG „DSMeld“ unter Leitung des BMI und unter der fachlichen Einbeziehung der OSCI Leitstelle). Für die Erweiterung der Funktionalitäten sollten jeweils abgrenzbare Projekte definiert werden, die vom AK I als Auftraggeber beschlossen werden. Den Projekten sind gegebenenfalls die notwendigen Projektmittel zur Verfügung zu stellen.**

4.2.2 Der Standard OSCI-Transport ist nicht ein Problem des Meldewesens (er kann für alle Zwecke der öffentlichen Verwaltung in Anspruch genommen werden), sondern ein Stück Infrastruktur der elektronischen Kommunikationstechnik für den öffentlichen Bereich. Die Projektgruppe sieht sich deshalb nicht in der Lage, vorzuschlagen, in welchen Strukturen dieser Standard gepflegt und fortgeschrieben werden kann.

**Empfehlung Nr. 5:**

**Der KoopA-ADV sollte gebeten werden, Vorschläge für nachhaltige Pflege und funktionale Erweiterungen des Standards OSCI-Transport 1.2 zu machen.**

4.3 Es wurde bereits oben darauf hingewiesen, dass die OSCI-Standards keine Produkte für das Einwohnermeldeverfahren sind, sondern in die entsprechende Software umgesetzt werden müssen. Dabei kann es technische Probleme geben, die sich nicht nur, wie es häufig der Fall ist, im eigenen Bereich der Behörde auswirken, sondern vor allem die Kommunikationsfähigkeit mit anderen Meldebehörden massiv beeinträchtigen mit der Folge, dass das zeitliche Ziel des § 17 Abs.1 nicht erreicht wird.

Die Projektgruppe hält es deshalb für unerlässlich, dass EWO-Verfahren nicht zum Einsatz kommen, solange die Behauptung des Herstellers, sie seien an die Standards angepasst, nicht von einer Stelle überprüft wurde. Nur so ist gewähr-

. . .

leistet, dass es beim Betrieb der Software zu keinen technischen Problemen kommt.

**Empfehlung Nr. 6:**

**Die Arbeitsgruppe empfiehlt, für die mit den neuen Standards versehenen EWO-Verfahren ein Zertifizierungsverfahren entwickeln zu lassen und vorzuschreiben[9].**

Entsprechende Tests sind aufwendig und mit hohen Kosten verbunden. Die Projektgruppe ist deshalb der Meinung, dass es den Herstellern von EWO-Verfahren wesentlich erleichtern würde, die Standards ohne großen Aufwand in ihre Software zu integrieren, wenn zumindest hinsichtlich des Standards OSCI-Transport 1.2 eine „Bibliothek“ entwickelt würde. Konkret bedeutet das, dass ein Softwareprodukt mit allgemein benötigten Grundfunktionen für OSCI-Transport entwickelt und in einer Form verteilt wird, die den Herstellern von EWO-Verfahren eine einfache Einbringung in deren EDV-Systeme ermöglicht. Zumindest würde der notwendige Aufwand für einen Test drastisch sinken oder sogar gegen Null gehen.

**Empfehlung Nr. 7:**

**Zu dem Standard OSCI-Transport 1.2 sollte eine Bibliothek programmiert oder angekauft werden, die es den Softwareherstellern (nicht nur von EWO-Verfahren, sondern auch von allen anderen im öffentlichen Bereich verwendeten Programmen) ermöglicht, den Standard ohne großen Aufwand in ihre Software zu implantieren. Ein entsprechender Auftrag sollte dem KoopA-ADV erteilt werden[10, 11].**

[9] z.B. in der 1. BMeldDÜV

[10] Dieses Gremium ist bisher keiner Fachministerkonferenz zugeordnet. Wer ihm den Auftrag erteilen kann, ist damit unklar. Die Projektgruppe schlägt vor, die IMK als Auftraggeber fungieren zu lassen.

[11] Es existiert bereits ein Produkt, das sich dafür eignet, als Tool den Softwareherstellern angeboten zu werden. Erforderlich wäre wohl, diese Bibliothek auszuschreiben. Nachdem die Standards möglichst

. . .

Die Tauglichkeit von OSCI-Xmeld und von OSCI-Transport wird augenblicklich in einem Großversuch erprobt. Beteiligt sind die Datenzentrale Baden-Württemberg und die Bayer. Anstalt für Kommunale Datenverarbeitung. Ergebnisse dieses Versuches, der sich auf den Austausch von Rückmeldungen bezieht, werden im Spätherbst 2003 vorliegen. Bisher bestehen keine Anhaltspunkte dafür, dass der Test negativ ausgehen wird.

Sobald jedoch OSCI-XMeld erweitert oder fortgeschrieben wird, werden neue Tests erforderlich.

**Empfehlung Nr. 8:**

**Die Organisation künftiger Tests von Folgeversionen des XMeld-Standards sollten dem Gremium übertragen werden, das auch für die Pflege dieses Standards zuständig ist (vgl. oben Empfehlung Nr. 4). Die einzelnen Tests sind zu koordinieren, damit Doppelarbeit vermieden wird.**

## 5. Die Organisation des Datenaustausches unter den Meldebehörden

5.1 Grundsätzlich gäbe es drei Modelle für eine solche Kommunikationsstruktur:

5.1.1 Jede Meldebehörde kann über das Netz mit Hilfe der oben genannten Standards mit jeder Meldebehörde elektronisch Daten austauschen.

Dieser Zustand wird wohl nur mittel- bis langfristig erreichbar sein. Für eine nicht absehbare Zahl von Jahren wird es immer noch Meldebehörden geben, die nicht entsprechend technisch ausgestattet sind.

In diesem Zusammenhang muss auch geklärt werden, wie die Erreichbarkeit der

---

schnell in die Verfahren eingebracht werden sollen, wären mit den Arbeiten zur Ausschreibung unverzüglich zu beginnen.

jeweiligen anderen Meldebehörde gewährleistet werden kann (z. B. wegen unterschiedlicher Dienstzeiten, landesunterschiedliche Feiertage).

Deshalb scheidet für die Projektgruppe ein solches Modell zunächst aus.

5.1.2 Eine einzige Stelle (z. B. eine Bundesbehörde) bildet eine Datendrehscheibe. Sie nimmt bundesweit alle Rückmeldungen gleich welcher Form (per Post, per Fax oder elektronisch entgegen, setzt sie elektronisch um und steuert sie dann weiter an den richtigen Adressaten.

Dieses Modell hält die Projektgruppe für nicht verfassungsgemäß, da damit eine nicht vorgesehene Mischverwaltung zwischen einer Bundesbehörde und den Länderverwaltungen entstünde. Aus diesem Grunde scheidet auch dieses Modell aus.

5.1.3 Die Projektgruppe hält es für den allein gangbaren Weg, die Einrichtung so genannter Clearingstellen in einzelnen Bundesländern vorzusehen, die als Datendrehscheibe fungieren und Medienbrüche organisieren, die aus ökonomischen Gründen und mit Rücksicht auf bestehende technische Infrastrukturen während einer Übergangszeit sinnvoll sind. Das gibt auf der einen Seite jedem Land die Möglichkeit, diese Clearingstelle nach eigenen Vorstellungen und angepasst an die eigene Struktur zu gestalten, auf der anderen Seite ist nur auf diese Art und Weise das oben genannte Ziel erreichbar, den länderübergreifenden Kommunikationsverkehr innerhalb von zwei Jahren zu elektronisieren.

Die Projektgruppe legt Wert darauf, dass die Organisation des Datenaustausches zwischen den Meldebehörden so gelöst werden muss, dass ein fließender Übergang von dem in der Empfehlung Nr. 1 genannten „realistischen Ziel“ hin zur Vision der „interaktiven länderübergreifenden Anmeldung“ möglich ist. Die Projektgruppe ist der Auffassung, dass die unter 6.1.3 genannte Lösung mit Clearingstellen einen solchen Übergang ermöglicht.

**Empfehlung Nr. 9:**

**Die Projektgruppe empfiehlt, in den Bundesländern die Einrichtung von Clearingstellen vorzusehen, die in der Lage sind, bei den ankommenden und abgehenden Rückmeldungen über die Landesgrenze hinweg unter Bewältigung von Medienbrüchen den elektronischen Verkehr zu gewährleisten. Hierfür sollten bei Bedarf eine oder mehrere Clearingstellen eingerichtet werden.**

Die Projektgruppe hat versucht abzuschätzen, wie lange solche Clearingstellen erforderlich sind. Letztlich lässt sich diese Frage nicht hinreichend konkret beantworten. Wie die o.g. Länderumfrage ergab, bestehen gegen die Einrichtung einer solchen Stelle keine grundsätzlichen Bedenken; allerdings sind in einigen Bundesländern derartige Überlegungen noch nicht diskutiert worden. Die Projektgruppe erwartet aber, dass mittel- bis langfristig die Rationalisierungsvorteile, die ein elektronisch abgewickelter Geschäftsverkehr der Meldebehörden unter Verwendung der OSCI-Standards bringen werden, die Träger der Meldebehörden veranlassen, so schnell wie möglich online-fähig zu werden und sich diesem automatisierten Austausch anzuschließen. Deshalb hält die Projektgruppe es für denkbar, dass eines Tages die Clearingstellen als Organisationseinheiten mit Personal- und Sachmitteln aufgelöst werden können.

5.2 Neben den Clearingstellen, in denen Datenformate umgesetzt werden, wird zusätzlich eine „public key Infrastruktur“ (PKI) mit einem Verzeichnisdienst benötigt. Deren Einrichtung ist aus folgenden Gründen erforderlich:

- Die gegenseitige Authentisierung der Meldebehörden muss gewährleistet sein. Das bedeutet, dass zum Beispiel überprüfbar ist, ob der Absender einer Rückmeldenachricht auch wirklich eine Meldebehörde ist. Solche Nachweise („Zertifikate“) erhält man von einer PKI.

- Die Vertraulichkeit der übermittelten Nachrichten ist sicherzustellen. Man muss den öffentlichen Schlüssel einer Meldebehörde kennen, um zielgerichtet

. . .

so zu verschlüsseln, dass nur diese Meldebehörde als berechtigter Empfänger Nachrichten dechiffrieren kann. Solche öffentlichen Schlüssel erhält man von einer PKI.

- Eine sendende Meldebehörde ist in der Regel über den Adressaten der Rückmeldung nur auf der fachlichen Ebene informiert: sie kennt den amtlichen Gemeindeschlüssel der zuständigen Fortzugsgemeinde. Dies muss in die technische Erreichbarkeit der Meldebehörde oder der Clearingstelle übersetzt werden, an die man die Daten zu übermitteln hat. Die notwendigen technischen Adressen erhält man von einem Verzeichnisdienst.

  Sinnvollerweise werden PKI und Verzeichnisdienst zusammengefasst und gemeinsam aufgebaut und gepflegt. Bei der Konzeption dieser Dienste ist darauf zu achten, dass sowohl das „realistische Ziel“ der elektronischen Datenübertragung binnen zwei Jahren, als auch die Vision der interaktiven länderübergreifenden Anmeldung unterstützt wird.

  **Empfehlung Nr. 9a:**

  **Die Projektgruppe empfiehlt die Einrichtung einer PKI und eines Verzeichnisdienstes mit dem Ziel, die technische Erreichbarkeit von Meldebehörden und Clearingstellen sicherzustellen, sowie die Authentizität der Kommunikationspartner und die Vertraulichkeit der Datenübermittlung zu gewährleisten[12].**

5.3 Die Projektgruppe hat ebenfalls diskutiert, ob der Verkehr der Meldebehörden untereinander (gleichgültig, ob länderübergreifend oder landesintern) über so genannte sichere Netze (Behördennetze, sonstige wide-area-networks (WAN)) erfolgen muss oder ob diese Kommunikation auch über das Internet möglich ist. „Sicher“ war hier sowohl im kryptografischen Sinne („authentisch, integer, vertrau-

[12] Im Rahmen des in Anm. 7 erwähnten Projektes „Xmeld 1.1“ wird eine Vorstudie erstellt, die Aussagen zur Struktur und Organisation einer solchen PKI enthalten wird.

lich“), als auch im technischen Sinne („zuverlässig, performant, robust“) verstanden. Das BSI hat diese Frage eindeutig im Sinne der letztgenannten Alternative beantwortet, d. h., aufgrund der OSCI-Transport-Standards lässt sich auch eine Nachricht hinreichend sicher über das Internet verschicken. Damit erweist es sich als nicht erforderlich, eine teuere IT-Infrastruktur für Verkehr der Meldebehörden untereinander aufzubauen.

5.4 § 17 Abs. 1 schreibt für den Geschäftsprozess „Rückmeldung“ vor, dass die Zuzugsmeldebehörde den vollständigen Datensatz erfasst, die Daten nach § 2 Abs. 1 Nr. 1 bis 18 der Wegzugsmeldebehörde übermittelt, diese die Daten auf Widersprüchlichkeiten mit dem Datensatz, den sie selbst gespeichert hat, überprüft und als Rückantwort der Zuzugsmeldebehörde gegebenenfalls die Widersprüche sowie zusätzliche Informationen (Ausschluss des Wahlrechts o. ä.) mitteilt. Dieser Geschäftsprozess erscheint aus zwei Gründen überdenkenswert:

- Die Wegzugsmeldebehörde, die daran eigentlich am wenigsten Interesse hat, überprüft, ob der ihr im Wege der Rückmeldung zugeschickte Datensatz mit dem ihren übereinstimmt. Vielmehr hätte vorrangig die Zuzugsmeldebehörde das Interesse, dass ihr Melderegister richtig ist, und von daher läge es nahe, dass sie die Datensätze auf Stimmigkeit überprüft;

- Aufgrund der Rechtslage ist die Zuzugsmeldebehörde gezwungen, den gesamten Datensatz aufzunehmen, und das, obwohl eine Vielzahl der Angaben bereits im öffentlichen Bereich, nämlich bei der Wegzugsmeldebehörde, vorhanden sind.

Insbesondere aus letzterem Grund hat die Projektgruppe eine Modifizierung des Geschäftsprozesses in folgender Weise diskutiert:

Die Zuzugsmeldebehörde nimmt nur einen identifizierenden Teildatensatz des neu Angemeldeten auf, übermittelt diesen der Wegzugsmeldebehörde, die daraufhin die nach § 2 Abs. 1 Nr. 1 bis 18 genannten Daten des Betroffenen der Zuzugsmeldebehörde überstellt. Sollten sich die (noch nicht aufgenommenen) Da-

tensätze des Anmelders mit dem bei der Wegzugsbehörde gespeicherten Datensatz als kongruent erweisen, so kann die Zuzugsmeldebehörde diesen Datensatz übernehmen, ohne dass der Erfassungsaufwand nochmals anfällt. Berichtigungsmitteilungen zur Rückmeldung, wie sie heute erfolgen, würden entfallen. Ebenso wäre bei mehreren Wohnungen des Betroffenen sichergestellt, dass die Eintragungen zum Wohnungsstatus in allen betroffenen Melderegistern plausibel sind (keine zwei Hauptwohnungen). Hier wären erhebliche Rationalisierungspotentiale zu erschließen.

Zusätzlich ist festzulegen, wie Familienverbände (Ehegatten und minderjährige Kinder) zu übermitteln sind. Dabei ist wichtig, dass der Begriff „Familienverband“ bundeseinheitlich definiert wird. Bei der Übermittlung muss deutlich werden, ob nur ein Familienangehöriger oder der gesamte Familienverband zugezogen ist.

Der BMI hat darauf aufmerksam gemacht, dass eine solche Gestaltung, wenn man landesintern in den Meldegesetzen eine entsprechende Regelung schafft, als Teil der Anmeldung durchaus möglich wäre; im Übrigen lässt ja § 17 Abs. 1 letzter Satz zumindest was die landesinternen Rückmeldungen angeht, eine derartige Gestaltung ohnehin schon zu[13].

**Empfehlung Nr. 10:**

**Der Geschäftsprozess der Rückmeldung sollte im Sinne der aufgezeigten Rationalisierungsmöglichkeiten gegebenenfalls neu modelliert werden.**

[13] § 14 Abs.4 S.2 schleswig-holsteinisches Meldegesetz ermöglicht es, die bei der Wegzugsmeldebehörde gespeicherten Daten im Wege des automatisierten Abrufs der Zuzugsmeldebehörde zu übermitteln. Das könnte ein Modell für eine Regelung in den Ländergesetzen sein.

## 6. Die sonstigen Randbedingungen

6.1 **Empfehlung Nr. 11**:

**Die Standards OSCI-XMeld und OSCI-Transport sollten in der Ersten Bundesmeldedatenübermittlungsverordnung für die elektronische Übermittlung so schnell wie möglich verbindlich festgeschrieben werden, damit sich die Länder und die Hersteller von EWO-Verfahren darauf einrichten können.**

6.2 Die Projektgruppe weist darauf hin, dass mit der Umsetzung des Dritten Änderungsgesetzes zum MRRG durch ein einziges Land alle anderen Länder unter Zugzwang geraten, da dann sofort die Frist für die Rückmeldung auf drei Tage verkürzt wird und damit die technischen und organisatorischen Probleme auftreten, wie sie in diesem Bericht geschildert wurden.

**Empfehlung Nr. 12:**

**Die jeweiligen Landesmeldegesetze sollten vorsehen, dass die Vorschrift über den Wegfall der Abmeldung erst zu dem Zeitpunkt in Kraft tritt, zu dem das letzte (novellierte) Landesmeldegesetz in Kraft gesetzt wird. Alternativ könnte auch schon vorher die Abmeldepflicht entfallen, wenn für eine solche „Vorgriffsregelung“ das Einverständnis aller Länder erreicht wird.**

## 7. Weiteres Vorgehen der Projektgruppe

Auf ihrer nächsten Sitzung am 25./26.11.2002 wird sich die Projektgruppe mit folgenden Fragen zu befassen haben:

- Welcher Sicherheitsstandard soll durch OSCI für das Protokoll festgelegt werden ?
- Wie soll die Authentisierung der Meldung erfolgen ?
- Wie können die Probleme des Datenaustausches mit dem Ausland gelöst werden ?

. . .

- Welche Fragen werfen die elektronische Anmeldung und die einfache Melderegisterauskunft auf.

Ein weiterer Teilbericht wird dem AK I zu seiner Frühjahrssitzung 2003 zugehen.

Schirmeyer
Ministerialrat
Leiter der Projektgruppe „Meldewesen“

Anlage 1

Die Projektgruppe hat zur Ermittlung der derzeitigen organisatorischen/technischen Gegebenheiten des Datenaustausches zwischen den Meldebehörden und im Hinblick auf die Umsetzung der Änderungen des MRRG beabsichtigter Maßnahmen eine Länderumfrage durchgeführt. In diese Umfrage einbezogen wurde die Frage nach der Beurteilung der Produkte X-Meld-Datensatz und OSCI-Transportprotokoll und dazu eventuell erkennbaren Alternativen.

Diese Umfrage hat folgende für die weiteren Überlegungen relevanten Ergebnisse erbracht:

- Lediglich in den Ländern Berlin, Hamburg und derzeit noch Rheinland-Pfalz erfolgt die Verarbeitung von Meldedaten für die einzelnen Meldebehörden in einem zentralen Rechenzentrum.

  In den übrigen Ländern ergibt sich ein völlig uneinheitliches Bild. Zwar existieren in den Ländern - größtenteils als Zweckverbände organisierte - kommunale Datenverarbeitungszentralen, die für die angeschlossenen Kommunen die Meldedaten im Wege der Auftragsdatenverarbeitung verarbeiten. Die Anzahl solcher Datenverarbeitungszentralen je Land und der Anteil der angeschlossenen Kommunen variiert jedoch stark.

- Die Einrichtung einer zentralen Stelle als mögliche „Vermittlungsstelle“ im Zuge des bundesweiten Datenaustausches zwischen den Meldebehörden wird zwar überwiegend als sinnvoll angesehen; abgesehen von den Ländern, in denen die Verarbeitung der Meldedaten bereits zentral erfolgt, bestehen jedoch insoweit allenfalls Überlegungen, aber keine konkreten Planungen.

- Auch hinsichtlich der Nutzung besonderer Netze (nicht Internet) ergeben sich erhebliche Unterschiede. Lediglich in den Ländern Baden-Württemberg, Berlin, Hamburg und Thüringen sind sämtliche Meldebehörden durch ein besonderes Netz miteinander verbunden. In den anderen Ländern existieren zwar solche Netze, ein flächendeckender Anschluss der Kommunen wird als wünschenswert bezeichnet, erscheint aber auf

absehbare Zeit nicht realisierbar, zumal eine Anschlussverpflichtung für die Kommunen überwiegend als problematisch angesehen wird.

- Soweit die Verarbeitung der Meldedaten dezentral erfolgt, bedienen sich die Kommunen zur Verarbeitung unterschiedlichster Software-Produkte überwiegend privater Anbieter.

- Die in die Überlegungen der Projektgruppe einbezogenen Produkte X-Meld-Datensatz und OSCI-Transportprotokoll wurden durchweg positiv beurteilt. Alternativen waren nicht ersichtlich.

# Das Projekt OSCI–XMeld

## Übersicht

FRANK STEIMKE, OSCI LEITSTELLE

16. August 2002

Das novellierte Melderechtsrahmengesetz bietet weit reichende Möglichkeiten, wichtige Geschäftsvorfälle zukünftig schneller, bürgerfreundlicher und kostengünstiger umzusetzen. Um dieses optimal nutzen zu können, ist eine Änderung der 1. BMeldDÜV mit Vorgaben für ein einheitliches Datenformat sowie der Technik der Datenübermittlung notwendig. Die bereits jetzt vorhandene Möglichkeit der bilateralen Einigung ist nicht ausreichend, ohne verbindliche Vorgaben für diese beiden Fragestellungen wird man die erhofften Ziele nicht erreichen können.

Die OSCI–Leitstelle erarbeitet im Auftrag der öffentlichen Verwaltung Lösungen für solche Fragestellungen. Sie kann für beide oben genannten Aufgaben fertige Antworten anbieten: für die Technik der Datenübermittlung das Transportprotokoll OSCI–Transport, für das einheitliche Nachrichtenformat die Ergebnisse des Projektes OSCI–XMeld. Da beide Projektergebnisse im Auftrag der öffentlichen Verwaltung erstellt worden sind, stehen sie zur unentgeltlichen Nutzung zur Verfügung.

Die Ergebnisse wurden durch Fachleute erarbeitet, durch einen anderen Personenkreis qualitätsgesichert, und durch den Auftraggeber KoopA–ADV abgenommen. Sie sind vollständig und umfangreich dokumenttiert.

Dieses Papier beschreibt unsere Projektergebnisse in einer nicht-technischen Form. In dem Abschnitt 1 wird erklärt, weshalb es *trotz eines bundeseitlichen DSMeld* überhaupt Handlungsbedarf gibt. Abschnitt 2 auf Seite 5 stellt die Aufgabe der OSCI–Leitstelle dar, unter deren Leitung die Ergebnisse erarbeitet wurden.

Der Abschnitt 3 beschreibt das Projekt OSCI–XMeld 1.0 An drei kleinen Beispielen wird dargestellt, welche Ergebnisse erarbeitet wurden, und in welcher Form diese dokumentiert sind.

Für die Technik der Datenübermittlung schlagen wir das MEDIA@Komm Projektergebnis OSCI–Transport vor. Im Abschnitt 4 auf Seite 12 wird dieses Protokoll kurz dargestellt.

Auf der Seite 14 werden diese beiden Ergebnisse zusammengeführt. Daraus resultiert ein konkreter Formulierungsvorschlag für die Novellierung der 1. BMeldDÜV, den Sie auf der Seite 15 finden.

Schließlich sind ab Seite 16 die Gremienbesetzung des Projektes OSCI–XMeld 1.0 sowie Auszüge aus den XML-Dateien angegeben. XML hat sich weltweit durchgesetzt und löst frei formulierte Beschreibungen, wie man Sie zum Beispiel als Anlage der 2. BMeldDÜV findet, zunehmend ab. In diesem Papier dienen diese Auszüge lediglich als zusätzliche Erläuterung zu den Beispielen, die wir im Abschnitt 3 geben. Die vollständige Fassung, in der alle Nachrichten zur Rückmeldung, zur Fortschreibung der Melderegister sowie zur einfachen Melderegisterauskunft exakt beschrieben werden, kann von der OSCI–Leitstelle bezogen werden.

# 1 Handlungsbedarf durch das novellierte Melderechtsrahmengesetz

Durch die Novellierung des Melderechtsrahmengesetz sind die gesetzlichen Grundlagen geschaffen worden, um Geschäftsvorfälle des Meldewesens zukünftig effizienter, schneller und bürgerfreundlicher gestalten zu können. Neben qualitativen Verbesserungen erwartet man sich dadurch auch erhebliche Kostensenkungen.

Dem automatisierten und schnellen Rückmeldeverfahren kommt dabei eine Schlüsselrolle zu. Folgerichtig ist eine Novellierung der 1. BMeldDÜV im Jahr 2003 geplant.

Gleichzeitig planen schon jetzt viele Betreiber von EWO-Verfahren eine Verbesserung ihres Dienstleitstungsangebotes auf Basis des novellierten Melderechtsrahmengesetzes. Wegen des hohen wirtschaftlichen Potenzials werden die einfache Melderegisterauskunft nach §21 Abs. 1a sowie die Datenübermittlung an andere Behörden nach §18 Abs. 4 häufig als erstes realisiert.

## Auswirkungen auf Meldeämter

Für die DV-Verfahren in den Meldeämtern sind erhebliche Auswirkungen offensichtlich. Während bisher die Rückmeldungen per Briefpost vorgenommen werden, erzwingt das novellierte Melderechtsrahmengesetz die länderübergreifende Vernetzung der Meldeverfahren. Bei der hohen Zahl von Meldeämtern, dem großen Kommunikationsvolumen, und schließlich der inhomogenen DV-Ausstattung in den Kommunen ist diese Vernetzung eine große Herausforderung.

Den zu erwartenden Einsparungen in den Meldeämtern steht ein Investitionsbedarf in bisher unbekannter Höhe für DV-Verfahren gegenüber. Das Interesse des Bundes, der Länder und der Kommunen muss es sein, gemeinsam ein optimales Kosten- / Nutzenverhältnis zu ermitteln und die technische Umsetzung der Vernetzung an diesem Ziel auszurichten.

Dabei sind unterschiedliche Voraussetzungen in verschiedenen Kommunen zu berücksichtigen. In großen Datenverarbeitungszentralen wird man andere Anforderungen an Verfügbarkeit und Performanz erfüllen können, als in kleinen Meldebehörden.

## Verbindliche Festlegungen sind erforderlich

Für einen reibungslosen Datenaustausch zwischen Meldebehörden und ihren Kunden (bzw. den anderen Meldebehörden) sind verbindliche Festlegungen bezüglich der zu übermittelnden Daten und der technischen Infrastruktur unerläßlich. Die Hersteller der EWO-Verfahren benötigen klare Vorgaben, unter welchen Umständen sie welche Daten in welcher Form an den Empfänger zu senden haben.

### Der DSMeld reicht nicht aus

Dieser Klärungsbedarf besteht, obwohl mit dem DSMeld ein bundeseinheitlicher Datensatz existiert. Doch der DSMeld ist hauptsächlich für die Zwecke der *Erfassung* und *Speicherung* nützlich, also für die Anwendung *in* den Meldeämtern. Für die Übermittlung *zwischen* Meldeämtern und anderen benötigt man weitergehende Festlegungen.

Welcher Regelungsbedarf über den DSMeld hinaus noch besteht, zeigt ein Vergleich mit der 2. BMeldDÜV, in der die automatisierte Daten-

übermittlung an öffentliche Stellen (Kreiswehrersatzämter, Bundesanstalt für Arbeit etc.) beschrieben wird:

**Festlegung der Nachrichtenformate**

Es bedarf verbindlicher Vorgaben, wie die zu übertragenen Daten zu formatieren und darzustellen sind. Wie kennzeichnet man Beginn und Ende von Datenfeldern? Wie werden Wiederholungen dargestellt? Wie differenziert man zwischen Pflichtfelder und optionale Feldern? Wo stehen Angaben über *Absender* und *Empfänger* der Nachricht?

In der 2. BMeldDÜV wird pro Empfänger das Datenformat exakt und verbindlich in den Anlagen zu §6 (2) festgeschrieben. In der 1. BMeldDÜV fehlen solche Festlegungen.

Darüber hinaus ist auch der Datenumfang festzulegen. Unter welchen Umständen müssen (und dürfen) welche Daten an wen übermittelt werden? In der 2. BMeldDÜV ist dies pro Empfänger exakt und abschließend festgelegt. In der 1. BMeldDÜV ist dies ebenfalls für die Rückmeldung erfolgt (in §2 und §3). Diese verbindliche Festlegung fehlt jedoch im Falle der Fortschreibung des Melderegisters nach §4, denn es gibt *diverse Anlässe,* das Melderegister fortzuschreiben (zum Beispiel: *Wegzug aus einer Gemeinde, Aufhebung einer bestehenden Lebenspartnerschaft, Änderung des Geburtsnamens auf Grund einer Adoption*) und so weiter. Aus Gründen des Datenschutzes dürfen nur solche Daten übermittelt werden, die für die Erfüllung der Aufgabe unterläßlich sind. Es gibt in der 1. BMeldDÜV oder anderen Verordnungen jedoch keine abschließende Aufzählung der Datenfelder pro Anlaß.

**Technik der Nachrichtenübermittlung**

Das technische Übertragungsprotokoll muss den Kommunikationspartnern vorgegeben werden. In dem sensiblen Bereich der Meldedaten haben Fragen des Datenschutzes und der Datensicherheit eine besonders hohe Bedeutung. Darüber hinaus muss es möglich sein, den Nachrichtenversand mit Sende- und Empfangszeitpunkten sicher nachvollziehen zu können, um gegebenenfalls den Nachweis der Fristwahrung führen zu können.

Das Melderechtsrahmengesetz erzwingt bei vielen Geschäftsvorfällen, die Privatkunden betreffen, den Einsatz der qualifizierten elektronischen Signatur. Für die Übertragung zwischen Meldebehörden ist dies nicht der Fall, dort wird die fortgeschrittene Signatur lediglich nahegelegt (in der Begründung zu §17).

In der 2. BMeldDÜV werden ab §7 verschiedene Verfahren der Datenübermittlung mittels automatisierter Verfahren beschrieben, inklusive der Vorkehrungen zur Sicherung der Integrität, Authentizität und Vertraulichkeit.

In der 1. BMeldDÜV wird von der schriftlichen Form der Datenübermittlung ausgegangen. Eine automatisierte Datenübermittlung setzt voraus, dass sich Sender und Empfänger jeweils bilateral bezüglich der Modalitäten geeinigt haben. Vorgaben des Gesetzgebers fehlen. Genau das ist der Grund für den hohen Aufwand, der bei der manuellen Bearbeitung schriftlich übermittelter Rückmeldungen anfällt.

In der Tabelle auf Seite 14 werden die Regelungen der 2. BMeldDÜV dem aktuellen Stand und unserem Vorschlage bezüglich der 1. BMeldDÜV gegenübergestellt.

**Festlegung von *Standards*, nicht Produkten**

Die verbindliche Vorgabe für die oben angesprochenen Fragestellungen darf nicht auf der Ebene von zu nutzenden Produkten stattfinden. Dadurch würde sich automatisch eine Herstellerabhängigkeit ergeben, dies kann nicht im Interesse der öffentlichen Verwaltung sein. Vielmehr sind Standards festzuschreiben, die von allen potenziellen Kommunika-

tionspartnern zu erfüllen sind. Mit welchen Produkten sie dies tun, ist unerheblich.

In der 2. BMeldDÜV werden beispielsweise in den Anlagen zum §6 nur die Datenformate beschrieben. Es werden keine Produkte für deren Verarbeitung vorgeschrieben. Die Hersteller von EWO-Verfahren werden lediglich beauftragt, Daten in diesen Formaten zu verarbeiten.

## Es müssen *beide* Fragen verbindlich geregelt werden

Um eine Infrastruktur für den Datenaustausch zwischen Meldebehörden zu etablieren, ist es zwingend erforderlich, dass *beide* oben genannten Fragestellungen für die Kommunikationsbeteiligten verbindlich vereinbart werden.

Eine einvernehmliche Festlegung auf ein Nachrichtenformat nützt überhaupt nichts, wenn die Übermittlung der Nachrichten zwischen den Meldebehörden auf Grund nicht kompatibler Übermittlungsverfahren oder unterschiedlicher Sicherheitssoftware scheitert.

Ebensowenig hilfreich wäre eine Einigung auf eine einheitliche Technik der Datenübermittlung inklusive elektronischer Signaturen und Quittungsmechanismen, wenn der Nachrichteninhalt vom Empfänger nicht verstanden oder nicht automatisiert verarbeitet werden kann.

Wenn es nicht gelingt, auf *beiden* Ebenen zu praktikablen Lösungen zu kommen, wird man das Ziel der Kostenreduktion durch die automatisierte Übermittlung von Rückmeldungen nicht erreichen.

**Regelungsbereich: der *länderübergreifende* Datenaustausch**

Da die Realisierung der Rückmeldung mittels automatisierter Datenübermittlung ein hohes wirtschaftliches Potenzial bietet, sind in einzelnen Bundesländern bereits Lösungsansätze entstanden. Diese sind untereinander nicht kompatibel, außerdem in der Regel integraler Bestandteile bestimmter EWO-Produkte.

Die 1. BMeldDÜV regelt nur den Datenaustausch *"zwischen Meldebehörden verschiedener Länder"*. Daher läßt eine Vorgabe der zu nutzenden Technik solche, bereits in den Ländern existierenden Lösungen, unberührt. Innerhalb der Bundesländer wäre eine Übernahme technischer Vorgaben aus der 1. BMeldDÜV ebenso möglich, wie die Weiterentwicklung bestehender Techniken. Es könnten *Clearingstellen* eingerichtet werden, welche für die Umsetzung eines landesspezifischen Datenformats in die von der 1. BMeldDÜV vorgeschriebenen Formate zuständig sind. In dem Bild 1 auf Seite 4 sind mögliche Realisierungsformen mit und ohne Clearingstelle dargestellt.

## Für beide Fragestellungen gibt es fertige Lösungen

Die OSCI–Leitstelle koordiniert im Auftrag der öffentlichen Verwaltung die Entwicklung von Standards für den Bereich des E–Government. Nach der Novellierung des Melderechtsrahmengesetzes ist das Meldewesen der erste große Bereich, in dem E–Government flächendeckend eingeführt werden kann. Die OSCI–Leitstelle kann fertige Lösungen für beide Bereiche anbieten:

- Für die *Festlegung der Nachrichtenformate* die Ergebnisse des Projektes OSCI–XMeld 1.0

  In der 1. BMeldDÜV sollte - analog zu den Anlagen des §6 der 2. BMeldDÜV - auf die XML-Schema-Dateien verwiesen werden, die als Projektergebnis entstanden sind. In diesen werden die Nachrichtenformate für die verschiedenen Geschäftsvorfälle des Meldewesens exakt und eindeutig definiert.

  XML hat sich als eine Beschreibungssprache für Datenaustauschformate inzwischen weltweit durchgesetzt. Da XML für die automa-

tisierte Verarbeitung optimiert, aber für Menschen schwer lesbar ist, hat die OSCI–XMeld Projektgruppe zusätzlich eine umfangreiche Dokumentation erstellt.

- Für die *Technik der Nachrichtenübermittlung* das Protokoll OSCI–Transport.

  OSCI–Transport wurde speziell für die sichere und nachvollziehbare Abwicklung von Geschäftsvorfällen des E–Government entwikkelt. Über elektronische Signaturen und Verschlüsselungsmechanismen hinaus bietet OSCI–Transport auch Quittungen und Zeitstempel, um den Nachweis der Fristwahrung führen zu können.

  Die Eignung von OSCI–Transport für das E–Government aus sicherheitstechnischer Sicht ist durch das BSI bestätigt worden. OSCI–Transport ist ein *empfohlener Standard* in der *SAGA*-Architektur des Bundes.

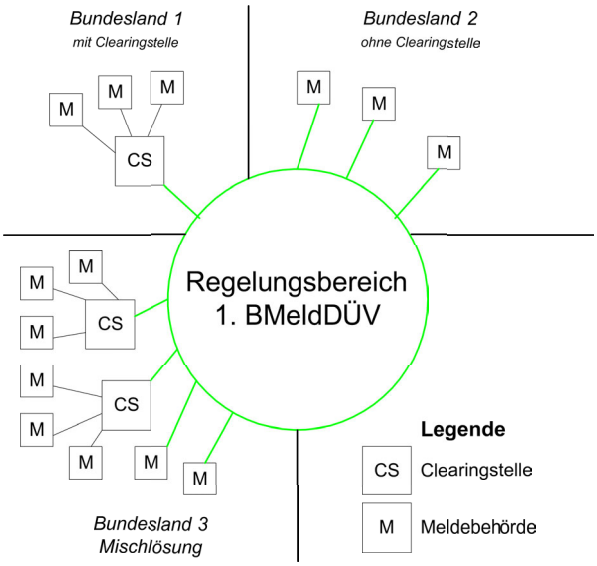
  Daher sollte die 1. BMeldDÜV - analog zu den §§7 ff. der 2. BMeldDÜV - das Protokoll OSCI–Transport zur verbindlichen Vorgabe für die Technik der Datenübermittlung zwischen Meldebehörden verschiedener Bundesländern machen.

**Übernahme von Lösungen ohne Produktabhängigkeit**

In beiden Fällen handelt es sich um Standards, *nicht um Produkte*, die im Auftrag der öffentlichen Verwaltung entwickelt wurden. Die Ergebnisse wurden jeweils durch Fachleute (des Meldewesens bzw. der Sicherheitstechnik) erarbeitet. Sie stehen der öffentlichen Verwaltung unentgeltlich zur Verfügung. Der KoopA–ADV hat die Ergebnisse abgenommen und ihre Verwendung in E–Government-Projekten empfohlen (Beschlüsse 1-12-09 und 1-12-10 des KoopA–ADV).

Die Aufgaben der OSCI–Leitstelle, unter deren Leitung beide Ergebnisse erarbeitet wurden, sowie die Ergebnisse OSCI–XMeld sowie OSCI–Transport werden auf den folgenden Seiten genauer beschrieben.

**Bild 1: Realisierungsvarianten in den Bundesländern**



# 2 Festlegung von Standards für die öffentliche Verwaltung

Der Bedarf an einer stärkeren Vernetzung von Organisationseinheiten der öffentlichen Verwaltung mit dem Ziel, Geschäftsprozesse schneller, effizienter, kostengünstiger und bürgerfreundlicher zu gestalten, ist nicht auf das Meldewesen beschränkt. Das Internet hat im Bereich des *E-Business* bereits zu einer drastischen Veränderung geführt. Lange Zeit konnte dies in der öffentlichen Verwaltung nicht nachvollzogen werden, weil hier besondere Anforderungen an die Sicherheit und die Nachvollziehbarkeit der Kommunikation gestellt werden.

Erst mit der Verfügbarkeit neuester Sicherheitstechniken, insbesondere der elektronischen Signatur, können besonders sensible Geschäftsprozesse der öffentlichen Verwaltung umgesetzt werden. Seitdem diese Techniken zur Verfügung stehen, werden Projekte initiiert, um die Vernetzung in der Praxis nutzbringend anzuwenden. An vielen Stellen finden Pilotprojekte statt.

## Die Aufgabe der OSCI–Leitstelle

Im Rahmen des Bundesprojektes MEDIA@Komm finanziert die Bundesregierung anteilig die OSCI–Leitstelle. Deren Aufgabe ist es, für die öffentliche Verwaltung Standards in den Bereichen der sicheren Datenübermittlung sowie der Datenformate und -repräsentation zu entwikkeln. Die Leitstelle befindet sich in Bremen und ist derzeit mit zwei Personen besetzt.

**Auftraggeber: KoopA–ADV**

Die Leitstelle ist nicht kommerziell orientiert. Der Auftraggeber für die Standardisierungsprojekte ist der KoopA–ADV, denn in der Regel sind von E–Government-Projekten Bund, Land und der kommunale Bereich betroffen. Die genaue Beschreibung der Aufgaben der OSCI–Leitstelle und ihrer Vorgehensweise sind in einem Organisationskonzept festgelegt, welches gemeinsam mit dem BMWi, dem BMI, den MEDIA@Komm-Städten, dem Deutschen Städtetag und weiteren Beteiligten entwickelt wurde.

**Sicherheit und Datenformate müssen gemeinsam betrachtet werden**

Bei der Umstellung der Geschäftsprozesse auf einen neuen *Vertriebskanal Internet* kann die Frage der Sicherheit nicht separat betrachtet werden. Am Beispiel des Meldewesens wird deutlich, dass die Vorgaben des Gesetzgebers die Nachrichteninhalte ebenso bestimmen wie die Sicherheitsmechanismen.

Prozesse müssen so modelliert werden, dass die *richtigen Inhalte* den Empfänger *sicher* erreichen. Ob rechtsverbindliche Zeitstempel und Quittungen benötigt werden, ergibt sich aus den Rechtsnormen.

Aus diesem Grunde ist es Auftrag der OSCI–Leitstelle, sich sowohl um die Inhalte, als auch um die Technik der Datenübermittlung zu kümmern.

**Ergebnisse sind unentgeltlich**

Die von der OSCI–Leitstelle erarbeiteten Ergebnisse werden im Auftrag der öffentlichen Verwaltung erarbeitet. Sie sollen dort möglichst breitflächig eingesetzt werden. Sie stehen der öffentlichen Verwaltung unentgeltlich zur Verfügung.

Dies gilt selbstverständlich auch für OSCI–XMeld 1.0 und OSCI–Transport.

**Die OSCI–Leitstelle vertreibt keine Produkte**

Die Aufgabe der OSCI–Leitstelle endet dort, wo für die Verwaltung und gegebenenfalls gemeinsam mit Software-Herstellern Spezifikationen für Standards erarbeitet worden sind. Bevor diese Ergebnisse konkret genutzt werden können, müssen sie in Produkten implementiert werden.

Die Erstellung und der Vertrieb von Produkten, die Spezifikationen in Technik umsetzen, ist nicht mehr die Aufgabe der Leitstelle. Hier kann es ganz unterschiedliche Situationen geben. Kommerzielle Firmen können die frei verfügbaren Spezifikationen ebenso implementieren und anschließend auf dem Markt anbieten, wie dies Kommunal- oder Landesrechenzentren möglich ist.

Die technische Umsetzung der Ergebnisse von OSCI–XMeld kann beispielsweise durch die Anpassung bestehender Schnittstellen, oder auch durch den Zukauf von Standardkomponenten erfolgen. Welche dieser Alternativen kostengünstiger ist, muss im Einzellfall durch den jeweiligen Auftraggeber entschieden werden.

Aus Sicht der Verwaltung ist es sicher wünscheswert, wenn es mehrere Produkte gibt, welche die Standards der öffentlichen Verwaltung erfüllen. Die Wettbewerbssituation führt in der Regel zu geringeren Kosten und eröffnet Wahlmöglichkeiten.

**Die Ergebnisse sind Hersteller- und Produktneutral**

Die Erarbeitung unserer Ergebnisse erfolgt gemeinsam mit Fachleuten der Verwaltung aus unterschiedlichen Bundesländern. In der Regel werden fachlich versierte Mitarbeiter von DV-Herstellern und aus Landes- oder Kommunalrechenzentren ebenfalls im Projekt beteiligt. Dies war sowohl bei OSCI–XMeld, als auch bei OSCI–Transport der Fall. Dadurch wird sichergestellt, daß es keine versteckten Produkt- oder Herstellerabhängigkeiten in den jeweiligen Projektergebnissen gibt.

Für die erste Version von OSCI–Transport wurde zu Recht der Vorwurf erhoben, dass es Abhängigkeiten von Produkten der Firma *bremen online services* gäbe. In der aktuellen Version 1.2 von OSCI–Transport wurde die Produktneutralität durch ein QS-Gremium bestätigt, zu dem unter anderem die drei MEDIA@Komm-Städte, die AKDB und die Firma SAP gehören.

# 3 Das Projekt OSCI–XMeld 1.0

## Pilotprojekt *Online-Ummeldung* in Bremen

Die Stadt Bremen hat im Rahmen des MEDIA@Komm Projektes die *Online Ummeldung* umgesetzt (also Umzug *innerhalb der Gemeinde*). Vor dem Hintergrund der anstehenden Novellierung des Melderechtsrahmengesetzes hat die OSCI–Leitstelle Frühjahr 2001 mit den Planungen für ein bundesweites Projekt begonnen, in denen die in diesem Pilotprojekt gemachten Erfahrungen zu einem bundesweit abgestimmten Datenaustauschformat führen sollten.

## Die Projektorganisation

In dem Projekt wurden drei Gremien eingerichtet:

**Die Arbeitsgruppe**

In der *Arbeitsgruppe* haben Fachleute aus Meldeämtern sowie kommunaler Rechenzentren, Datenzentralen und Herstellern kommunaler Software gemeinsam die Fachinhalte erarbeitet.

**Die Abstimminstanz**

Vorliegende Ergebnisse wurde in einer *Abstimminstanz* qualitätsgesichert. Dieses Gremium war besetzt durch Melderechtsreferenten, den Bundesbeauftragten für den Datenschutz, einen Vertreter des Deutschen Städtetages sowie die drei MEDIA@Komm Städte. Darüber hinaus waren auch hier Vertreter von Datenzentralen, Rechenzentren und Herstellern vertreten.

**Die Entscheidungsinstanz**

In der *Entscheidungsinstanz* wurden die strategischen Ziele festgelegt und die qualitätsgesicherten Ergebnisse abgenommen. Die Entscheidungsinstanz war besetzt durch Vertreter des KoopA–ADV.

Die Gremienbesetzung finden Sie auf Seite 16.

**Die Projektleitung**

Die Projektleitung lag bei der OSCI–Leitstelle. Wir wurden durch externe Methodenberater von der Firma MSI unterstützt.

Das Projekt wurde in drei Phasen durchgeführt und dauerte von August 2001 bis März 2002. Der Aufwand betrug rund 150 MT (ohne den Aufwand der Projektleitung).

## Ergebnis: Exakte Vorgaben für Nachrichtenformate

Die Projektergebnisse bestehen in einer Beschreibung der Nachrichtenformate für die wichtige Geschäftsvorfälle des novellierten Melderechtsrahmengesetzes. Es handelt sich somit um genaue Vorgaben für ein Datenaustauschformat, so wie es in der 2. BMeldDÜV durch die Anlagen zum §6 geregelt wird. Allerdings bedienen wir uns im Projekt OSCI–XMeld der wesentlich moderneren Beschreibungssprache XML, um Nachrichtenformate exakt und unmissverständlich festzulegen.

**Die Beschreibung erfolgt in XML**

Bei XML handelt es sich um eine moderne Methode, um genau zu definieren, welche Struktur Nachrichten haben müssen, wenn sie zwischen Sendern und Empfängern auszutauschen sind. Unter anderem wird festgelegt:

- Welche Datenfelder Nachrichtenbestandteil sein können;
- In welcher Reihenfolge sie zu senden sind;
- Ob Felder zwingend, optional oder wiederholbar sind;
- Welches Format die Felder haben dürfen (Zeichensatz, ggfs. Feldlänge etc.)

XML hat sich als Beschreibungssprache weltweit durchgesetzt.

**XML ist automatisiert zu verarbeiten ...**

Ein wesentlicher Vorteil von XML gegenüber frei erstellen Vereinbarungen (wie sie als Anlagen der 2. BMeldDÜV genutzt werden) ist, dass

XML automatisiert verarbeitet werden kann. Man kann mit sehr geringem Aufwand eine Software erstellen, die automatisch prüft, ob eine Nachricht zwischen zwei Meldeämtern den Formatvorgaben der OSCI–XMeld-Gruppe entspricht.

**... aber für Menschen schwer lesbar**

Dieser große und ökonomisch wichtige Vorteil wird jedoch mit dem Nachteil erkauft, dass eine in XML vorliegende Beschreibung erlaubter Nachrichtenformate (eine so genannte *Schema-Datei)* für Menschen schwer lesbar ist.

Aus diesem Grunde wurde im OSCI–XMeld-Projekt neben dem eigentlichen Arbeitsergebnis (drei XML Schema-Dateien) eine sehr umfangreiche Dokumentation erstellt. Sie hat vor allem das Ziel, dem Leser den Inhalt der Schema-Dateien nahezubringen. Darüber hinaus werden in dieser Dokumentation Entwurfsprinzipien erläutert und das Verhältnis zwischen jedem DSMeld-Feld und den OSCI–XMeld-Nachrichten dargestellt.

In diesem Papier beschreiben wir zwei Beispiele der OSCI–XMeld Projektergebnisse in Form von Bildern, wie Sie sie auch in der von uns erstellten Dokumentation finden. Für den technisch interessierten Leser haben wir ab Seite 18 auch den zugehörigen Auszug aus der verbindlichen XML Schema-Datei beigefügt.

**Drei Bereiche wurden erfogreich abgeschlossen**

In der oben dargestellten Projektlaufzeit konnten drei Bereiche vollständig abgeschlossen werden. Es liegen abgestimmte und qualitätsgesicherte XML Schema-Definitionen vor für:

- Die Rückmeldung nach Zuzug oder nach Statuswechsel inklusive der Auswertung einer Rückmeldung, entsprechend §§2,3 der 1. BMeldDÜV.
- Insgesamt rund 50 Nachrichtenformate für Ereignisse, die zu einer Fortschreibung des Melderegisters entsprechend §4 der 1. BMeldDÜV führen..
- Die einfache Melderegisterauskunft an private (Einzelauskunft) oder gewerbliche (Sammelauskünfte) Kunden nach §21 Abs. 1a des novellierten Melderechtsrahmengesetz

## Ein Beispiel: Tod des Ehegatten

Am Beispiel der Nachricht *Tod des Ehegatten* wird das Arbeitsergebnis des OSCI–XMeld Projektes dargestellt.

Verstirbt der Ehegatte des Betroffenen, so ist dies den Meldeämtern aller Gemeinden, in denen der Betroffene (Neben-) Wohnungen unterhält, im Rahmen der Fortschreibung des Melderegisters nach §4 Abs. 1 der 1. BMeldDÜV mitzuteilen.

**Welche Daten werden übermittelt?**

Da die Einzelfälle der Fortschreibung in der 1. BMeldDÜV nicht geregelt sind, wurden die erforderlichen Daten zunächst durch die Fachleute des Meldewesens in der Projektgruppe ermittelt. Die für diesen Spezialfall erforderlichen Datenfelder wurden in ein allgemein anwendbares Schema eingefügt, welches generell bei der Fortschreibung des Melderegisters anzuwenden ist.

**Daten für jede Fortschreibung ...**

So muss bei jeder Fortschreibung des Melderegisters sichergestellt werden, dass eine eindeutige Identifikation des Betroffenen in der empfangenden Gemeinde gewährleistet wird.

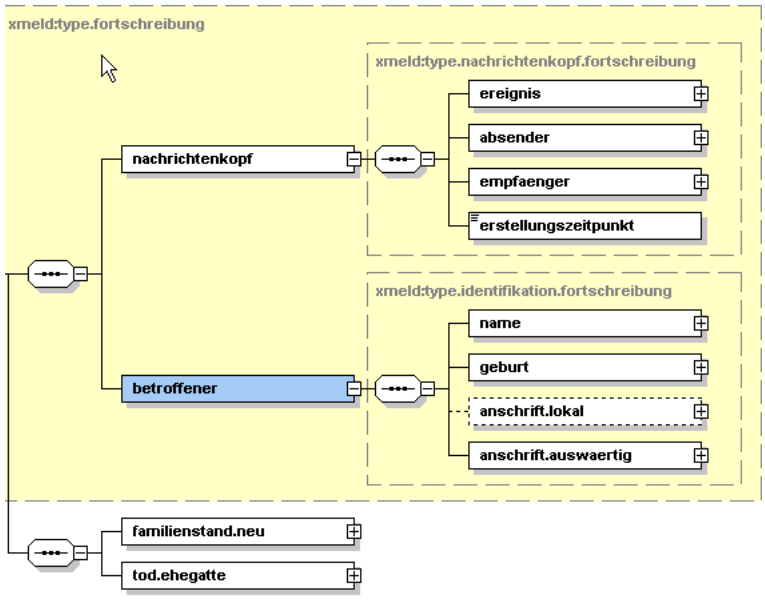
**... und spezifische Daten pro Anlaß**

Für den speziellen Fall der Fortschreibung des Melderegisters aus Anlaß des *Todes des Ehegatten* kommt hinzu, dass Angaben zum neuen

Familienstand des Betroffenen benötigt werden, außerdem nähere Angaben zum Sterbefall.

Das Ergebnis ist im Bild 2 auf Seite 9 dargestellt.

**Bild 2: Nachrichtenstruktur im Falle des Todes eines Ehegatten**




Diese grafische Darstellung wurde für den menschlichen Leser erstellt. Die verbindliche Beschreibung selbst ist in XML formuliert und Bestandteil der mit OSCI–XMeld 1.0 ausgelieferten XML Schema-Dateien. Der entsprechende Ausschnitt aus der XML Schema-Datei ist in dem Beispiel auf der Seite 18 dargestellt.

## Einfache Nachrichtenerstellung durch *Bausteine*

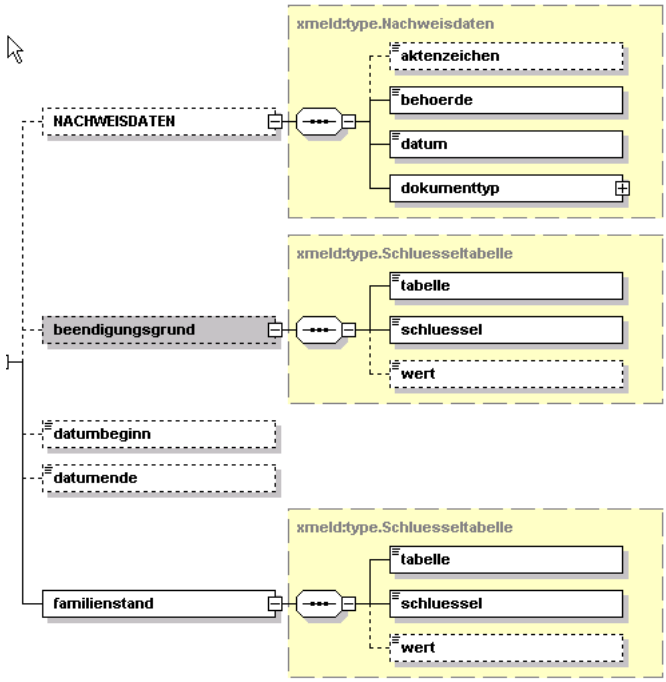
Alle Nachrichten des Meldewesens beziehen sich auf stets wiederkehrende Strukturelemente wie zum Beispiel *Anschrift, Meldebehörde, Familienstand, Nachweisdaten* und so weiter. Tatsächlich bildete die Erarbeitung dieser *"Bausteine"* auf Basis eines formal beschriebenen Informationsmodells die Hauptarbeit der OSCI–XMeld-Arbeitsgruppe. Die Komposition neuer Nachrichtenformate, etwa für die Datenübermittlung zwischen Behörden nach §18 Melderechtsrahmengesetz, gestaltet sich durch den Rückgriff auf diesen Baukasten relativ einfach.

### Ein Beispiel: der Familienstand

Einer der Bausteine, auf die bei der Nachricht zum Tod des Ehegatten zurückgegriffen wird, ist der *Familienstand*. Die Projektgruppe hat gemeinsam festgelegt, welche Datenfelder des DSMeld im Zusammenhang mit der Übermittlung eines Familienstandes (des Betroffenen oder eines Familienangehörigen) übermittelt werden können. Das Ergebnis der Überlegungen mündete in eine Datenstruktur, die ebenfalls in den XML-Schema-Dateien zu finden ist. Die verbindliche, in XML formulierte Beschreibung ist in dem Ausschnitt aus der Schema-Datei auf Seite 19 zu finden. Da aber dieser XML-Code schwer lesbar ist, finden Sie in dem Bild 3 auf Seite 10 die entsprechende grafische Beschreibung.

Die von der Projektgruppe erstellte Dokumentation besteht zu einem überwiegenden Anteil aus der Beschreibung der gemeinsam entwickelten Bausteine.

**Bild 3: Der Nachrichtenbaustein *"Familienstand"***




**Ein Baukasten für das Meldewesen**

Die XML Schema Datei `xmeld-baukasten.xsd` umfasst derzeit rund 30 solcher Bausteine für Nachrichten des Meldewesens. Neben dem oben als Beispiel dargestellten *Familienstand* haben die Fachleute des Meldewesens unter anderem folgende Strukturen erarbeitet: *Anschrift, Auskunftssperre, Ausweisdokument, Einwohnerschaft, Unionsbürgerschaft* und weitere. So ist durch eine gründliche Erarbeitung des Informationsmodells die Fortführung des Projektes mit dem Ziel, weitere Nachrichtenstrukturen zu erarbeiten, gut vorbereitet worden.

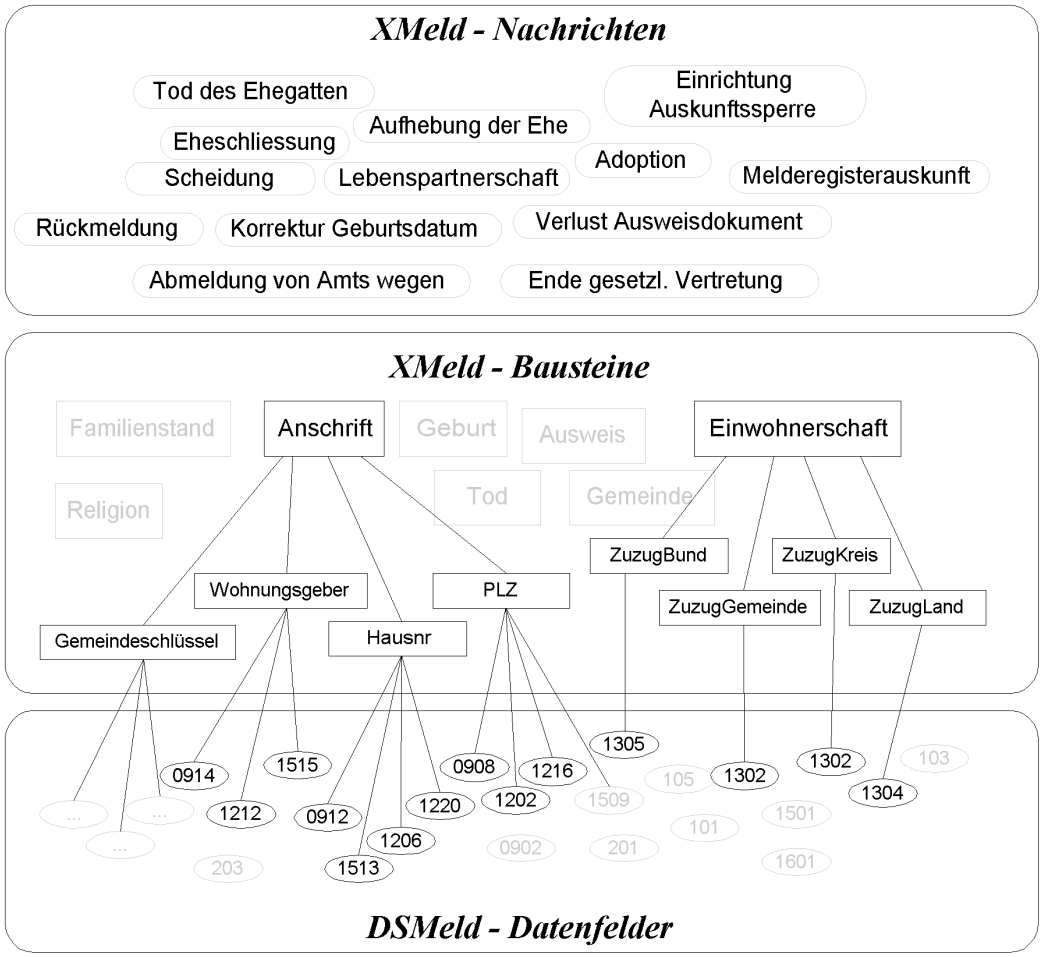
**Der DSMeld bildet das Fundament von OSCI–XMeld**

Letztendlich werden nahezu alle Bestandteile der OSCI–XMeld - Strukturen auf den DSMeld zurückgeführt. Die inhaltlichen Definitionen des DSMeld werden durch OSCI–XMeld nicht angetastet. In OSCI–XMeld hat lediglich eine Erweiterung für solche Datenfelder stattgefunden, die spezifisch sind für die *Übermittlung* von Nachrichten. Dazu gehören zum Beispiel Angaben zur adressierten Meldebehörde im Rahmen der Rückmeldung, aber auch Angaben zum Kunden im Rahmen der einfachen Melderegisterauskunft nach §21 Abs. 1a.

In dem Bild 4: ist dargestellt, dass OSCI–XMeld-Nachrichten aus OSCI–XMeld-Bausteinen zusammengesetzt sind. Diese werden durch den DSMeld definiert.

So bildet der DSMeld als *Vorgabe für die Erfassung und Speicherung* von Daten in Melderegistern auch die Basis für die OSCI–XMeld-Nachrichten. Die dazwischen liegende Hierarchiestufe der *"Bausteine"* sichert die leichte Erweiterbarkeit und Wartbarkeit der OSCI–XMeld Nachrichtenstrukturen.

**Bild 4: Nachrichten, Bausteine und der DSMeld**




## Projektende im März 2002

Das Projekt OSCI–XMeld 1.0 wurde im März 2002 mit der Abnahme aller Ergebnisse durch die Entscheidungsinstanz termingerecht abgeschlossen. Die Entscheidungsinstanz hat dabei die OSCI–Leitstelle aufgefordert, mit den Planungen für ein Folgeprojekt OSCI–XMeld 1.1 zu beginnen, in dem weitere Geschäftsvorfälle des Meldewesens abzudekken sind.

Die Projektergebnisse (also die XML Schema-Dateien und die zugehörige Dokumentation) stehen - wie alle Spezifikationen der OSCI–Leitstelle - unentgeltlich zur Verfügung.

# 4 OSCI–Transport für die sichere Nachrichtenübermittlung

Für den automatisierten Nachrichtenaustausch zwischen Meldebehörden ist die verbindliche Festlegung von Nachrichtenformaten nicht ausreichend. Es wird außerdem verbindliche Vorgaben über die Technik der Nachrichtenübermittlung geben müssen, ansonsten ist der reibungslose Nachrichtenaustausch trotz einer Einigung über die Inhalte nicht gewährleistet.

## Sichere Nachrichtenübermittlung als Querschnittsaufgabe

Die Frage nach einer Methode für den sicheren und nachvollziehbaren Datenaustausch wird sich in sehr vielen Projekten des E–Government stellen. Die meisten Geschäftsvorfälle stellen hohe Anforderungen:

- an den Datenschutz (weil personenbezogene Daten übermittelt werden),
- an die elektronische Signatur (als Ersatz der eigenhändigen Unterschrift),
- und an die Nachvollziehbarkeit der Datenübermittlung (zum Nachweis der Fristwahrung).

Anders als im *E-Business* hat die öffentliche Verwaltung nicht die Möglichkeit, ihre Sicherheitsmechanismen anhand einer Risikoanalyse und anschließenden Wirtschaftlichkeitsbetrachtungen selbst festzulegen. Die Entwicklung eines Transportprotokolls, welches speziell für diese besonderen Anforderungen geeignet ist, ist somit eine *Querschnittsaufgabe* im Rahmen des E–Government.

## OSCI–Transport: ein MEDIA@Komm-Ergebnis

Der Bedarf an einem solchen Protokoll ist von der Verwaltung früh erkannt worden. Deshalb ist die OSCI–Leitstelle im Rahmen des MEDIA@Komm-Projektes damit beauftragt worden, hier einen Entwurf vorzulegen und diesen innerhalb der öffentlichen Verwaltung abzustimmen.

**Ende 2000: Version 1.0**

Die OSCI–Leitstelle hat Ende 2000 die erste Version von OSCI–Transport vorgelegt. Seitdem wird OSCI–Transport in vielen E–Government-Projekten produktiv eingesetzt

**Aktuell: Version 1.2**

Die Erfahrungen aus der Praxis führten zu neuen Anforderungen. Diese wurden durch die OSCI–Leitstelle gesammelt und priorisiert. Im März diesen Jahres wurde das Projekt *"OSCI–Transport 1.2"* begonnen. Unter der Projektleitung der OSCI–Leitstelle erarbeiteten Fachleute der Verwaltung (drei MEDIA@Komm-Städte und Stadt Hagen) und der Wirtschaft (Firmen ppi, SAP, *bremen online services*, datenschutz nord) gemeinsam die neue Version. Die Anforderungen wurden vor dem Projektbeginn mit dem Bundesamt für Sicherheit in der Informationstechnik abgeglichen.

Aufgrund des hohen Engagements aller Beteiligten konnte die neue Version 1.2 bereits im Juni diesen Jahres vom Auftraggeber KoopA–ADV abgenommen werden. Seitdem steht OSCI–Transport in der neuen Version der öffentlichen Verwaltung unentgeltlich zur Verfügung.

**Bestandteil des BSI-Handlungsleitfadens ...**

Die Eignung von OSCI–Transport für die Anforderungen des E–Government wurde mit Fachleuten aus der Verwaltung immer wieder diskutiert. Mit der Arbeitsgruppe *"Kommunikation und Sicherheit"* des KoopA–ADV wurde das Einsatzszenario für OSCI–Transport beschrie-

ben. Als Ergebnis dieses Diskussionsprozesses wurde OSCI–Transport in den *"Handlungsleitfaden für die Einführung der elektronischen Signatur und Verschlüsselung in der Verwaltung"* aufgenommen.

**... und *"empfohlener Standard in SAGA"***

In dem Dokument *"SAGA: Standards und Architekturen für E–Government Anwendungen"* bewertet der Bund verschiedene Techniken und Methoden, die im E–Government zur Anwendung kommen können.. OSCI–Transport hat dort die Einstufung als *empfohlener Standard* erhalten. Es wird darauf hingewiesen, dass *"nach sicherheitstechnischer Bewertung durch das BSI und der Unterstützung durch geeignete Produkte ... diese Standards den Status obligatorisch erlangen [können]"*. In diesem Fall würde OSCI ein verbindlicher Standard im Rahmen von *Bund Online 2005*. Die entsprechende sicherheitstechnische Bewertung nimmt das BSI auf Grund eines Erlasses des BMI derzeit vor.

## OSCI–Transport schafft eine einheitliche Transportbasis

Die Technologien für den Umgang mit elektronisch unterschriebenen Dokumenten und Nachrichten sind noch recht jung. Mit den auf dem Markt vorhandenen Produkten kann man elektronisch signieren und Zeitstempel erzeugen, aber es mangelt oft an der Interoperabilität. Das bedeutet, man kann sich nicht darauf verlassen, dass der Empfänger einer unterschrieben und verschlüsselten Nachricht diese auch öffnen und lesen kann - wenn Sender und Empfänger unterschiedliche Sicherheitsprodukte (Signaturkarten, Kartenleser oder Software) einsetzen, sind Probleme zu befürchten.

**Im Meldewesen muss es einheitliche Lösungen geben**

Für den Regelungsbereich der 1. BMeldDÜV ist eine verbindliche Vorgabe von Übertragungsverfahren nicht akzeptabel, wenn dies faktisch den Zwang zur Nutzung eines einzigen Produktes als Konsequenz hat. Aus diesem Grunde haben alle Projektbeteiligten stets betont:

- Eine Einigung auf einheitliche Standards für die Technik der Datenübermittlung ist sinnvoll und notwendig.

  Eine Wettbewerbssituation *auf der Ebene der Standards* ist unsinnig und verhindert effiziente, flächendeckende Lösungen.
- Die alternativen Umsetzungsmöglichkeiten in Ländern und Kommunen müssen erhalten bleiben.

  Eine Wettbewerbssituation *auf Hersteller- und Produktebene* ist sinnvoll und führt in der Regel zu einer ökoomisch günstigeren Situation für die Verwaltung.

**OSCI–Transport ist Hersteller- und Produktneutral**

Die Spezifikation von OSCI–Transport ist überall dort, wo es möglich war, an international anerkannten Standards und Projekten ausgerichtet. Die in der Version 1.0 noch vorhandenen Abhängigkeiten von konkreten Implementierungen (also Produkten) der Firma *bremen online services* wurden in der Version 1.2 vollständig entfernt. Dies wurde durch das QS-Gremium bestätigt (Arbeitsgruppe *Transport und Verpackung* des DIN im Rahmen der MEDIA@Komm-Begleitforschung).

# 5 OSCI–XMeld und OSCI–Transport sind Lösungen für den Einsatz im Meldewesen

Durch den gemeinsamen Einsatz von OSCI–XMeld und OSCI–Transport kann ein hersteller- und produktneutraler Informationsverbund zwischen den Meldeämtern der Bundesrepublik aufgeaut werden. Dann regelt:

- OSCI–XMeld das verbindliche Nachrichtenformat, so wie es in der 2. BMeldDÜV durch die Anlagen zum §6 geschieht; und
- OSCI–Transport bestimmt die Technik der Nachrichtenübermittlung, so wie es in der 2. BMeldDÜV in §7 ff gemacht wird. Dabei sichert OSCI–Transport die Einhaltung der hohen Anforderungen an Datenschutz und Datensicherheit ebenso zu, wie die Nachvollziehbarkeit der Datenübermittlung.

Bei beiden Spezifikationen handelt es sich um Arbeitsergebnisse, die im Auftrag der öffentlichen Verwaltung erstellt wurden und unentgeltlich genutzt werden können.

**Tabelle 1: Vergleich mit der 2. BMeldDÜV**

| **Regelungsbedarf** | **2. BMeldDÜV** | **1. BMeldDÜV** | |
|---|---|---|---|
| | | **aktuell** | **zukünftig** |
| Technik der Datenübermittlung | §7 ff | In der Regel Briefpost, bilaterale Einigung ist möglich | OSCI–Transport |
| Nachrichtenformat | Spezifisch pro Empfänger in den Anlagen zu §6 | Ohne Vorgabe | OSCI–XMeld |

## Zustimmung durch Bürger- und Meldeamtsleiter

Nach dem Abschluß des Projektes OSCI–XMeld 1.0 wurden die Ergebnisse dem *Arbeitskreis der Bürger und Meldeamtsleiter im Deutschen Städtetag*vorgestellt. Diese Gruppe von Fachleuten schloss sich der Argumentation zu Gunsten von OSCI–XMeld sowie OSCI–Transport an und fordert, die Novellierung der 1. BMeldDÜV auf dieser Basis zu betreiben.

## Die Verwaltung bestimmt ihre Standard selbst

Von besonderer Bedeutung für diese Entscheidung der Fachleute des Meldewesens war dabei die Tatsache, dass die Entwicklung sowohl von OSCI–XMeld, als auch von OSCI–Transport, im Auftrag der öffentlichen Verwaltung erfolgt und auch durch diese kontrolliert wird. Einer Herstellerabhängigkeit müsse bei dem Aufbau eines Informationsverbundes im Meldewesen unbedingt entgegengewirkt werden, dies war die übereinstimmende Auffassung aller Teilnehmer.

## Ein konkreter Formulierungsvorschlag

Bezüglich der Novellierung der 1. BMeldDÜV schlagen wir daher folgende Änderungen vor:

> Die Datenübermittlungen sind in automatisierter Form vorzunehmen. Eine Übermittlung der Daten hat unter Beachtung der Satzbeschreibung OSCI-XMeld 1.0 und des Übermittlungsprotokolls OSCI-Transport 1.2 zu erfolgen. OSCI-XMeld 1.0 und OSCI-Transport 1.2 sind vom Bundesministerium des Innern am (...) herausgegeben worden und im Internet unter *www.bmi.bund.de/...* sowie bei dem Bundesarchiv, Potsdamer Straße 1, 56075 Koblenz, jedermann zugänglich niedergelegt.

An den genannten Stellen würden die als Projektergebnis erstellten XML-Schema Dateien hinterlegt werden. Diese sind die verbindliche Beschreibung der Nachrichtenformate. Die von der Projektgruppe erstellte ergänzende Information, in der die Inhalte der XML-Schema Dateien erläutert und (teilweise mit Beispielen) dargestellt werden, sollte an diesen Bezugsquellen (zumindest im Internet) ebenfalls hinterlegt werden.

# 6 Die Gremienbesetzung im Projekt OSCI–XMeld 1.0

**Tabelle 2: Besetzung der Arbeitsgruppe**

| Name | Institution |
|---|---|
| Bielmeier-Seidl | AKDB |
| Klein - Uebbing | IfI, Duisburg |
| Kuschnereit | Meldeamt Hamburg |
| Kötter | IDB, Bremen |
| Rabenstein | LEA Berlin |
| Riekenberg | HIT Hannover |
| Singer | Datenzentrale Baden-Württenberg |

**Tabelle 3: Besetzung der Abstimminstanz**

| Name | Institution |
|---|---|
| Brümmel | Bundesdruckerei |
| Eichhorn | AKDB |
| Hauber | HSH GmbH |
| Hellenkamp | Bundesbeauftragter für den Datenschutz |
| Klüttermann | IfI, Duisburg |
| Kraft | Stadt Esslingen |
| Langenfeld | LEA Berlin |
| Ley | KGRZ Kassel |
| Luckow | Kreis Segeberg |
| Maas | KOMFIT |
| Marx | Senator für Inneres, Bremen |
| Müller-Vollmer | bremen online services |
| Steinl | Deutscher Städtetag |
| Thede | Landeskoordinierungsstelle IT, Mecklen-burg-Vorpommern |
| Wedler | LfD, Bremen |
| Wessel-Niepel | Melderechtsreferentin, Bremen |

**Tabelle 4: Besetzung der Entscheidungsinstanz**

| Name | Institution |
|---|---|
| Arnold | Innenministerium Baden-Württenberg |
| Franßen | Staatsministerium des Inneren, Bayern |
| Löper | Senatsverwaltung für Inneres, Berlin |
| Samsel | Bundesministerium des Innern |
| Schramm | Innenministerium Schleswig Holstein |
| Schwellach | Senator für Finanzen, Bremen |
| te Reh | Deutscher Städtetag |

# 7 Beispiele für OSCI–XMeld

In diesem letzten Abschnitt haben wir für interessierte Leser XML-Quelltexte beigefügt. Dies dient lediglich der Illustration der Sachverhalte, die auf den vorhergehenden Seiten erläutert wurden.

Sie finden hier zwei Auszüge aus den XML-Schema Dateien, in denen das Datenaustauschformat OSCI–XMeld verbindlich geregelt wird. Zur Beschreibung nutzen wir die Sprache XML, die sich seit 1999 weltweit für solche Zwecke durchgesetzt hat.

Eine Beschreibung eines Austauschformats in *XML Schemata* ist in der Regel präziser, eindeutiger und mächtiger als die früher üblichen Datensatzbeschreibungen, wie man sie beispielsweise noch als Anlagen der 2. BMeldDÜV findet. Der wesentliche Vorteil von XML ist die automatisierte Interpretation durch handelsübliche Softwareprodukte *(XML Parser, XML Editoren)*, die allerdings zu Lasten der Lesbarkeit durch Menschen geht.

Jede Software, die in der Lage ist XML zu verarbeiten, kann prüfen, ob eine OSCI–XMeld-Nachricht korrekt bezüglich unserer Vorgaben ist. Es ist keine spezifische EWO-Software dafür erforderlich.

**XML Definition der Nachricht *"Tod des Ehegatten"***

```
<--
*******************************************************************************
*                                                                             *
*                fortschreibung.beziehung.011                                 *
*                ============================                                 *
*                                                                             *
* Hier wird die Nachrichtenstruktur für die Fortschreibung des Melderegisters  *
* wegen des Todes des Ehegatten in XML definiert                              *
*******************************************************************************
-->
<xs:element name="fortschreibung.beziehung.011">
 <xs:annotation>
   <xs:documentation>
   Der Ehegatte des Betroffenen ist verstorben.
   Übermittelt werden der neue Familienstand und nähere Angaben zum Tod des Ehegatten.
   Nähere Angaben zum Dokument, mit dem der Tod des Ehegatten belegt wird (Sterbeurkunde)
   sind im Element tod.ehegatte/nachweisdaten
   (und nicht in familienstand.neu/nachweisdaten) zu übermitteln.
   </xs:documentation>
 </xs:annotation>
 <xs:complexType>
   <xs:complexContent>
     <xs:extension base="xmeld:type.fortschreibung">
       <xs:sequence>
         <xs:element name="familienstand.neu" type="xmeld:type.Familienstand">
           <xs:annotation>
             <xs:documentation>
             Der neue Familienstand des Betroffenen, wie er sich nach dem Tod
             des Ehegatten ergibt.
             </xs:documentation>
           </xs:annotation>
         </xs:element>
         <xs:element name="tod.ehegatte" type="xmeld:type.Tod">
           <xs:annotation>
             <xs:documentation>
             Nähere Angaben zum Tod des Ehegatten des Betroffenen.
             </xs:documentation>
           </xs:annotation>
         </xs:element>
       </xs:sequence>
     </xs:extension>
   </xs:complexContent>
 </xs:complexType>
</xs:element>
```

```
<--
*******************************************************************************
*                                                                             *
*                         Familienstand                                       *
*                         =============                                       *
*                                                                             *
* Dies ist die Beschreibung des "Bausteins" FAMILIENSTAND in XM. In diversen   *
* Nachrichten wird darauf Bezug genommen                                      *
*******************************************************************************
-->
<xs:complexType name="type.Familienstand">
   <xs:annotation>
     <xs:documentation>
     Angaben zum familienstand einer Person.
     </xs:documentation>
   </xs:annotation>
   <xs:sequence>
     <xs:element name="NACHWEISDATEN" type="xmeld:type.Nachweisdaten" minOccurs="0">
       <xs:annotation>
         <xs:documentation>
         Weitere Nachweisdaten zum Familienstand.
         </xs:documentation>
       </xs:annotation>
     </xs:element>
     <xs:element name="beendigungsgrund" type="xmeld:type.Schluesseltabelle" minOccurs="0">
       <xs:annotation>
         <xs:documentation>
         Schlüsseltabelle 8: Beendigungsgrund Ehestand
         Es ist der rechtliche Grund der Beendigung der letzten Ehe
         oder der letzten Lebenspartnerschaft anzugeben.</xs:documentation>
       </xs:annotation>
     </xs:element>
     <xs:element name="datumbeginn" type="xs:date" minOccurs="0">
       <xs:annotation>
         <xs:documentation>
        Es ist das Datum der letzten Eheschließung oder der Begründung
        der letzten Lebenspartnerschaft anzugeben.</xs:documentation>
       </xs:annotation>
     </xs:element>
     <xs:element name="datumende" type="xs:date" minOccurs="0">
       <xs:annotation>
         <xs:documentation>
         Es ist das Datum der letzten Ehe oder
         der letzten Lebenspartnerschaft anzugeben.</xs:documentation>
       </xs:annotation>
     </xs:element>
     <xs:element name="familienstand" type="xmeld:type.Schluesseltabelle">
       <xs:annotation>
         <xs:documentation>
         Schlüsseltabelle 7: Familienstand
         Es ist der personenstandsrechtliche Familienstand anzugeben.
         </xs:documentation>
       </xs:annotation>
     </xs:element>
   </xs:sequence>
   <xs:attribute name="id" type="xs:ID" use="optional"/>
 </xs:complexType>
```

Abschließend sehen Sie hier ein Beispiel für eine OSCI–XMeld-Nachricht, und zwar für eine einfache Melderegisterauskunft. In diesem fiktiven Beispiel hat die Meldebehörde Bremens eine Anfrage erhalten bezüglich einer Person mit dem *Familiennamen: Hinz* und dem *Gebräuchlichen Vornamen: Uwe*. An weiteren Daten waren das *Geburtsdatum: 17. Januar 1962*, der *Geburtsort: Bremen* sowie das *Geschlecht: männlich* bekannt. Die Anforderungen an eine Melderegisterauskunft nach §21 Abs. 1a MRRG sind somit erfüllt.

Die Meldebehörde antwortet mit der aktuellen Anschrift des Betroffenen: *Streesemannstraße 55 in Bremen*.

**Beispiel: Melderegisterauskunft**

```
<?xml version="1.0" encoding="ISO-8859-2"?>
<xmeld xmlns:xdsig="http://www.w3.org/2000/09/xmldsig#"
 version="1.0" xmlns="http://www.osci.de/xmeld"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.osci.de/xmeld xmeld-nachrichten.xsd">
  <melderegisterauskunft.einfach.600>
    <nachrichtenkopf>
      <ereignis>
        <tabelle>0</tabelle>
        <schluessel>melderegisterauskunft.einfach.600</schluessel>
      </ereignis>
      <kunde/>
      <meldebehoerde>
        <GEMEINDE>
          <amtlichergemeindename>Bremen</amtlichergemeindename>
          <amtlichergemeindeschluessel>
            <tabelle>36</tabelle>
            <schluessel>04011000</schluessel>
          </amtlichergemeindeschluessel>
        </GEMEINDE>
      </meldebehoerde>
      <erstellungszeitpunkt/>
    </nachrichtenkopf>
    <melderegisterauskunft.einfach>
      <suchprofil>
        <name>
          <NACHNAME>
            <nachname>Hinz</nachname>
            <rolle>
              <tabelle>28</tabelle>
              <schluessel>FN</schluessel>
            </rolle>
          </NACHNAME>
          <VORNAME>
            <gebraeuchlich>
              <tabelle>22</tabelle>
              <schluessel>GV</schluessel>
            </gebraeuchlich>
            <laufendenr>1</laufendenr>
            <rolle>
              <tabelle>21</tabelle>
              <schluessel>AV</schluessel>
            </rolle>
            <vorname>Uwe</vorname>
          </VORNAME>
        </name>
        <geburt>
          <geburtsort>Bremen</geburtsort>
          <tagdergeburt>1962-01-17</tagdergeburt>
        </geburt>
        <geschlecht>
          <tabelle>1</tabelle>
          <schluessel>m</schluessel>
          <wert>männlich</wert>
        </geschlecht>
      </suchprofil>
      <anschrift.aktuell>
        <hausnummer>55</hausnummer>
        <strasse>Streesemannstraße</strasse>
        <wohnort>Bremen</wohnort>
      </anschrift.aktuell>
    </melderegisterauskunft.einfach>
  </melderegisterauskunft.einfach.600>
</xmeld>
```

Bundesamt für Sicherheit in der Informationstechnik


# Sicherheitsbewertung

# zur Spezifikation OSCI – Transport 1.2

**Stand: 30.07.2002**

**Bundesamt für Sicherheit in der Informationstechnik**

# Inhaltsverzeichnis

# 1. Sicherheitsbewertung OSCI-Transport 1.2

## 1.1 Gegenstand der Sicherheitsbewertung und Einordnung von OSCI-Transport 1.2

Gegenstand dieser Stellungnahme ist eine sicherheitstechnische Bewertung des Protokolls OSCI auf Grundlage der finalen Version der Spezifikation „OSCI-Transport 1.2“. In der Spezifikation wird ein technischer Standard für eine „automatisiert nutzbare Schnittstelle für die Abwicklung von Geschäftsprozessen zwischen Bürgern und Kommunen“ dargestellt. Dieser Standard wurde im Auftrag der OSCI-Leitstelle als Herausgeber im Rahmen des Projektes Media@Komm entwickelt.
Die Zielgruppe des Standards bilden Software-Ersteller, die Produkte für die Abwicklung von web-basierten Kommunikations- und Transaktionsszenarien entwickeln.
Technische Basis von OSCI-Transport 1.2 stellen der Kommunikationsstandard SOAP (Simple Object Access Protocol) sowie der Standard zur Datenbeschreibung XML dar, die durch das World Wide Web Consortium (W3C) verabschiedet wurden und inzwischen international Anerkennung gefunden haben. Mit OSCI-Transport 1.2 liegt ein Standard vor, „mit dem prinzipiell beliebige Informationen [zwischen Benutzern] automatisiert übertragen werden können“.

In Ausführung des Erlasses vom 28.05.02 (Geschäftszeichen IT 2 - 195 950/29) wurde der vorliegende Standard hinsichtlich folgender Kriterien untersucht:

1. Erfüllung der Anforderungen aus Sicht der Kommunikationssicherheit im E-Government und
2. Erfüllung der Anforderungen hinsichtlich der kryptographischen Sicherheit der eingesetzten Algorithmen und Verfahren

## 1.2 Abgrenzung der Sicherheitsbewertung

In dieser Stellungnahme wird ausschließlich der Standard OSCI-Transport 1.2 im Status -final- mit Stand vom 06. Juni 2002 bewertet. Datenmodellierungen im Teil B der OSCI-Spezifikation sind nicht Gegenstand der Sicherheitsbewertung, da sie keinen direkten Bezug zur Bewertung der Kommunikations- und kryptographischen Sicherheit besitzen.

Der Prüfungsumfang ergibt sich aus dem o.g. Erlass vom 28.05.2002. Die ursprünglichen Anforderungsdokumente für die Erstellung der aktuellen Spezifikation wurden nur insoweit berücksichtigt, als sie einschlägig für die Kommunikationssicherheit in OSCI-Transport 1.2 eingegangen sind.

Alle Feststellungen zur Sicherheitseignung einer auf OSCI basierenden Architektur betreffen entweder die Erfüllung der Anforderungen aus Sicht der Kommunikation im E-Government oder deren Erfüllung hinsichtlich der verwendeten kryptographischen Mechanismen. Sie beziehen sich ausschließlich auf die in der Spezifikation abstrakt konzipierten logischen und technischen Funktionalitäten des Protokolls.
Die Sicherheitsbewertung umfasst keine konkreten Implementierungen der Spezifikation. Aussagen über Konformität und Interoperabilität Standard-konformer Produkte können somit nicht gegeben werden.

Weiterhin werden folgende Annahmen bezüglich der Sicherheit des Standards vorausgesetzt:

(1) Korrektheit der Implementation

Die in XML-Notation angegebenen Datenschemata stellen funktionierende Quellcodes dar und sind problemlos zu implementieren. Eine auf dem Standard beruhende Implementation, hin zu einem konkreten Produkt, erfolgt korrekt und schafft damit keine neuen Sicherheitsrisiken für eines der Sicherheitsziele.

(2) Korrektheit der referenzierten Dokumente
Die in der Spezifikation angegebenen Links zu Web-Adressen bzw. Verweise auf referenzierte Dokumente funktionieren einwandfrei und sind inhaltlich korrekt.

Damit die abstrakten Aussagen über die Sicherheit auf eine konkrete Realisierung des Standards übertragen werden können, müssen weitere Voraussetzungen erfüllt sein:

(3) sichere Einsatzumgebung
Die für eine Realisierung notwendige Einbettung des Standards erfolgt in eine geeignete Einsatzumgebung, die insbesondere den sicheren Betrieb des entstehenden Produkts ermöglicht.

(4) sicherer Betrieb
Die in der Sicherheitsbewertung getroffenen Aussagen über die Einhaltung bestimmter Sicherheitsziele setzen insbesondere den korrekten Betrieb Standard-konformer Produkte innerhalb einer OSCI-Infrastruktur voraus. Derartige Kriterien sind aber nicht Bestandteil des Standards und sollen in einem ‚Betriebshandbuch' (siehe www.osci.de) ausgeführt werden. Dieses liegt derzeit noch nicht vor und kann daher nicht bewertet werden. Entsprechend findet die folgende Sicherheitsbewertung lediglich auf einer abstrakten Ebene unabhängig konkreter Implementierungen statt.

(5) Schutzbedarf der IT-Anwendung
Anforderungen, die durch den Schutzbedarfs der Fachverfahren gestellt werden, müssen auch bezüglich ihrer Unterstützung durch den unterliegenden Transportmechanismus betrachtet werden. Da dies aber nur im Zusammenspiel der Fachverfahren mit den (OSCI-) Produkten und deren Einsatzumgebung hinreichend aussagekräftig ist, wird dieser Aspekt hier nicht berücksichtigt.

Eine Bewertung bezüglich der Erfüllung der Vorschriften des Signaturgesetzes (SigG) für das Erstellen und Verifizieren qualifizierter elektronischer Signaturen wird nicht gegeben, da eine solche Bestätigung nur durch die Regulierungsbehörde für Telekommunikation und Post (RegTP), als zuständige Behörde, erfolgen kann.

## 2. Funktionsweise von OSCI-Transport 1.2

OSCI ermöglicht als Anwendungsprotokoll die sichere (d.h. vertrauliche und authentische) elektronische Abwicklung von Geschäftsprozessen zwischen zwei Kommunikationsparteien. Der Standard beinhaltet keine eigene Benutzerverwaltung und bietet neben den Funktionen Signieren und Verschlüsseln weitere Sicherheitsmechanismen (siehe Kap. 3).
Zur Realisierung der internen Adressierung (Ebene der Fachverfahren) besitzt jeder Benutzer (Person, Gruppe oder Prozess) ein Chiffrierzertifikat. Angaben über dessen Herkunft und Qualität werden in OSCI nicht gemacht (wobei dies auch keine Aufgabe eines derartigen

Protokolls darstellt). Ein Benutzer darf nur dann als Diensteanbieter auftreten, wenn er dauerhaft über eine URL (Uniform Resource Locator) erreichbar ist.

Sämtliche Kommunikation erfolgt ausschließlich vermittelt durch einen „Intermediär“. Dieser erfüllt die Aufgaben der Protokollierung des Datenflusses, der Prüfung der Zertifikate sowie der Erbringung weiterer Mehrwertdienste.

Obwohl andere Transportmedien für OSCI grundsätzlich möglich sind, ist in aller Regel das WWW als zu Grunde liegendes Transportmedium anzusehen, in diesem Sinne ist OSCI http-basiert.

## 2.1 Architektonischer Aufbau des Protokolls

In OSCI-Transport 1.2 werden Nachrichten auf drei logischen Ebenen ausgetauscht. Je nach Ebene treten dabei die beteiligten Instanzen (Benutzer bzw. Intermediär) in verschiedenen Rollen auf:

a) Geschäftsvorfallebene
Auf dieser Ebene wird die reflexive n:m - Beziehung zwischen *Autoren* und *Lesern* bezüglich der Inhaltsdaten beschrieben (Zustellung). Die Inhaltsdaten können beliebiger Natur sein und den Anforderungen einer Ende-zu-Ende-Verschlüsselung unterliegen. In der Zustellung werden die Inhaltsdaten vom Sender zum Empfänger (jeweils als OSCI-Benutzer) transportiert. Der Intermediär tritt auf Geschäftsvorfallsebene nicht in Erscheinung.

b) Auftragsebene
Die Auftragsebene skizziert den Weg eines *Auftrags* bzw. einer *Auftragsantwort* zwischen *Client* und *Supplier*. OSCI-Transport unterscheidet *implizite* und *explizite* Dialoge. Bei ersteren besteht der gesamte Dialog lediglich aus einem Auftrag und der zugehörigen Antwort. Im expliziten Fall wird der Dialog durch einen *Dialoginitialisierungsauftrag* vom Client an den Supplier gestartet und besteht bis der Supplier eine Antwort auf einen *Dialogendeauftrag* abschickt oder einen Fehler meldet. Im Regelfall treten die OSCI-Benutzer als Clients und der Intermediär als Supplier auf.

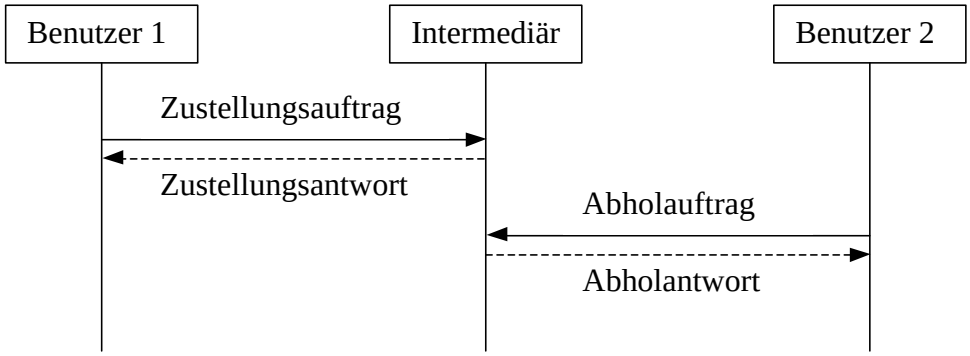
c) Nachrichtenebene
OSCI-Nachrichten werden zwischen Benutzer und Intermediär (bei Bedarf verschlüsselt) verschickt. Beide können als Sender oder Empfänger auftreten. Die OSCI-Nachrichten bestehen aus einem Auftrag, einer Auftragsantwort oder einer Fehlermeldung.

## 2.2 Kommunikations - Szenarien

Es werden 4 Kommunikationsszenarien unterschieden. Die Abwicklung jeglicher Kommunikation von Benutzer 1 zu Benutzer 2 erfolgt über einen Intermediär.

a) One-way-message bei aktivem Empfänger mit Protokollierung
Bei diesem protokollierten Szenario erfolgt die Übertragung der Inhaltsdaten von Benutzer 1 zum Benutzer 2. Dabei muss sich Benutzer 2 selbst (aktiv) um die an ihn gerichtete Zustellung bemühen.

Dieser Ablauf kann Anwendung finden, wenn Benutzer 2 nicht permanent erreichbar ist. Weiterhin ist hier eine URL zur Adressierung nicht zwingend erforderlich, so dass Benutzer 2 keinen Diensteanbieter darstellen muss.
Zur Verdeutlichung sei folgendes Schema aus der Spezifikation zitiert:




b) One-way-message bei passivem Empfänger mit Protokollierung
Bei diesem protokollierten Szenario erfolgt die Übertragung der Inhaltsdaten von Benutzer 1 zum Benutzer 2. Die Zustellung erfolgt hier ohne Zutun des Benutzers 2.
Ein solcher Ablauf eignet sich für Diensteanbieter, die permanent unter einer URL erreichbar sind und die Zustellung ohne Verzögerung erhalten sollen.

c) Request-response bei passivem Empfänger mit Protokollierung
Bei diesem protokollierten Szenario erfolgt zuerst eine Zustellung von Benutzer 1 an Benutzer 2 und anschließend eine zweite Zustellung von Benutzer 2 an Benutzer 1.
Ein derartiger Ablauf kann dann Verwendung finden, wenn der Benutzer 2 unmittelbar auf die erste Zustellung reagieren soll. Auch hier ist der Benutzer 2 Diensteanbieter und permanent unter einer URL erreichbar.

d) Request-response bei passivem Empfänger ohne Protokollierung
Bei diesem nicht protokollierten Szenario findet wie unter c) die erste Zustellung von Benutzer 1 zu Benutzer 2 und anschließend eine zweite Zustellung in umgekehrter Reihung statt.
Aufgrund der fehlenden Protokollierung dient ein solcher Ablauf einfacher Kommunikation, die auf einen späteren Nachweis verzichten kann.

## 3. Sicherheitsfunktionen und -mechanismen

### 3.1 Digitale Signaturen

Soweit die Zertifikate für digitale Signaturen von einem qualifizierten Zertifizierungsdiensteanbieter (ZDA) herausgegeben wurden, kann man von einem definierten, zugesicherten (und darüber hinaus gesetzlich garantiertem) Sicherheitsniveau ausgehen. Hierdurch wird neben der Daten-Integrität auch die Authentizität des Signaturschlüsselinhabers sowie die Nicht-Abstreitbarkeit des Ursprungs der signierten Daten sichergestellt (unter der Annahme, dass „digitale Signaturen“ im Sinne der ISO 7498-2 verstanden werden) und darauf aufbauend auch die Erfüllung des Schriftformerfordernisses gewährleistet.

Stammt das Zertifikat nicht von einem qualifizierten ZDA im Sinne des SigG, so hängen Authentizität der Herkunft und Nicht-Abstreitbarkeit des Ursprungs von der zugrunde liegenden PKI ab.

Insbesondere wird im folgenden davon ausgegangen, dass die zugrunde liegende PKI (für Signaturschlüssel) als Sicherheitsinfrastruktur betrieben wird.

### 3.1.1 Signieren und Verifizieren von Inhaltsdaten

Folgende Sicherheitsziele werden durch die o.g. Funktion realisiert:

Integrität der Inhaltsdaten, Authentizität der Herkunft und Nicht-Abstreitbarkeit des Ursprungs

Autoren können auf Geschäftsvorfallebene Signaturen erzeugen, die dann von Lesern verifiziert werden können. Somit kann der Leser die mathematische Korrektheit der Signatur von (signierten) Inhaltsdaten und bei Bedarf auch die Gültigkeit des Zertifikatpfades überprüfen.

Hiermit wird im Falle qualifiziert signierter Inhaltsdaten erreicht, dass in Abhängigkeit der Anforderungen des jeweiligen Fachverfahrens eine komplette Überprüfung aller korrespondieren Zertifikate (einschließlich Attribut-Zertifikate, Verzeichnisdienstauskünfte, Sperrlisten) in der Verantwortung des Lesers liegt.

### 3.1.2 Signieren und Verifizieren von Nutzungsdaten (Aufträge und Auftragsantworten)

Folgende Sicherheitsziele werden durch die o.g. Funktion realisiert:

Integrität der Nutzungsdaten und Authentizität des Senders

Signierte Aufträge müssen verifiziert werden. Hierbei prüft der Supplier (Intermediär) obligatorisch die mathematische Korrektheit der vom Client signierten Aufträge und ob der verwendete Signaturschlüssel auch zum Signieren vorgesehen war.
Nicht signierte Aufträge oder Aufträge mit fehlerhaften Signaturen werden vom Supplier abgelehnt.
Signierte Auftragsantworten müssen bzw. können verifiziert werden. Der Intermediär als Client muss obligatorisch die mathematische Korrektheit der vom Supplier signierten Auftragsantworten prüfen und ob der verwendete Signaturschlüssel auch zum Signieren vorgesehen war. Ein Benutzer als Client kann diese Prüfung durchführen (muss aber nicht).

Die KeyUsage des verwendeten Schlüssels wird explizit beim Verifizieren gecheckt. Es wird also eine „falsche“ Schlüsselanwendung erkannt. Die Korrespondenz von privatem zu öffentlichem Schlüssel wird implizit beim Verifizieren gecheckt.
Somit werden Fälschungen bzw. Verfälschungen von Nutzungsdaten erkannt; hiermit ist insbesondere die Authentizität des Clients als Sender von Aufträgen sowie die Authentizität des Suppliers als Sender von Auftragsantworten sichergestellt. Durch diese Funktion wird eine Sender-Maskerade verhindert, indem das (absichtliche) Vortäuschen einer falschen Identität erkannt wird.

### 3.1.3 Zertifikatsprüfungen

Folgende Sicherheitsziele werden durch die o.g. Funktion realisiert:
Integrität und Authentizität der öffentlichen (Verifizier-) Schlüssel

Geprüft wird vom Intermediär

a) die mathematische Korrektheit der Signatur des Zertifikates,
b) dass der Prüfzeitpunkt innerhalb des Gültigkeitszeitraums des Zertifikates liegt sowie
c) dass das Zertifikat zum Prüfzeitpunkt nicht gesperrt war!

Ist das Ergebnis einer dieser Prüfungen negativ, so liegt die Reaktion im Ermessen des Empfängers.

Bei Signaturzertifikaten erfolgt die Zertifikatsprüfung bei Anwendung des öffentlichen Schlüssels. Es ist allerdings aus der Spezifikation NICHT ersichtlich, was unter „mindestens die offline möglichen Prüfungen“ zu verstehen ist.

Vor dem Hintergrund einer Validierung anhand des Kettenmodells kann dies nicht korrekt oder problematisch sein. Hier sollte in Abhängigkeit der Anforderungen des jeweiligen Fachverfahrens eine separate Restrisikoanalyse der folgenden Fälle erfolgen:

1) Das Zertifikat wurde nach der Signaturerstellung aber vor dem Prüfzeitpunkt gesperrt.
2) Der Gültigkeitszeitraum des Zertifikates ist nach der Signaturerstellung aber vor dem Prüfzeitpunkt abgelaufen.
3) Die Zertifikatsprüfung erfolgt nur gegen die Sperrliste und nicht gegen den Verzeichnisdienst.
4) Der Signaturerstellungszeitpunkt ist nur näherungsweise bekannt.

## 3.2 Verschlüsselung

Die Authentizität des Chiffierschlüsselinhabers hängt von der zugrunde liegenden PKI ab.

Insbesondere wird im folgenden davon ausgegangen, dass die zugrunde liegende PKI (für Chiffrierschlüssel) als Sicherheitsinfrastruktur betrieben wird.

### 3.2.1 Ver- und Entschlüsseln von Inhaltsdaten

Folgendes Sicherheitsziel wird durch die o.g. Funktion realisiert:
Vertraulichkeit der Inhaltsdaten

Autoren können auf Geschäftsvorfallebene Chiffrate erzeugen, die dann von Lesern dechiffriert werden können. Hiermit kann vom Autor in Abhängigkeit der Anforderungen des jeweiligen Fachverfahrens eine Ende-zu-Ende-Verschlüsselung zum Leser erzwungen werden.

Somit wird verhindert, dass ein anderer außer dem Leser Kenntnis der Inhaltsdaten erlangt.

### 3.2.2 Ver- und Entschlüsseln von Nutzungsdaten (Aufträge und Auftragsantworten)

Folgendes Sicherheitsziel wird durch die o.g. Funktion realisiert:
Vertraulichkeit der Nutzungsdaten

Der Supplier prüft, ob sich der Auftrag entschlüsseln lässt und ob der verwendete Chiffrierschlüssel auch zum Verschlüsseln vorgesehen war.
Der Client prüft, ob sich die Auftragsantwort entschlüsseln lässt und ob der verwendete Chiffrierschlüssel auch zum Verschlüsseln vorgesehen war.

Die KeyUsage des verwendeten Schlüssels wird explizit beim Entschlüsseln gecheckt. Es wird also nur eine „falsche“ Schlüsselanwendung erkannt, diese jedoch nicht verhindert. Die Korrespondenz von privatem zu öffentlichem Schlüssel wird implizit beim Entschlüsseln gecheckt.

Somit wird verhindert, dass Unbefugte Kenntnis von den Nutzungsdaten erhalten können.

### 3.2.3 Zertifikatsprüfungen

Folgende Sicherheitsziele werden durch die o.g. Funktion realisiert:
Integrität und Authentizität der öffentlichen (Chiffrier-) Schlüssel

Geprüft wird vom Intermediär:
a) die mathematische Korrektheit der Signatur des Zertifikates,
b) dass der Prüfzeitpunkt innerhalb des Gültigkeitszeitraums des Zertifikates liegt sowie
c) dass das Zertifikat zum Prüfzeitpunkt nicht gesperrt war!

Ist das Ergebnis einer dieser Prüfungen negativ, darf der Sender das Zertifikat nicht zum Verschlüsseln verwenden.

Bei Chiffrierzertifikaten erfolgt die Zertifikatsprüfung bei Anwendung des öffentlichen Schlüssels. Es ist allerdings aus der Spezifikation NICHT ersichtlich, was unter „mindestens die offline möglichen Prüfungen“ zu verstehen ist.

Vor dem Hintergrund einer Validierung anhand des Schalenmodells ist dies korrekt und unproblematisch.
Der Intermediär als Supplier muss einen Auftrag ablehnen, wenn das Chiffrierzertifikat des Benutzer2 gesperrt ist und unterrichtet hierüber den Benutzer1. Der Intermediär als Supplier darf eine Auftragsantwort nicht an den Client senden, wenn das Chiffrierzertifikat des Clients gesperrt ist.

## 3.3 Beweissicherung

### 3.3.1 Protokollierung der Ergebnisse von Zertifikatsprüfungen

Ergebnisse von (Signatur- und Chiffrier-) Zertifikatsprüfungen werden vom Intermediär in einem Prüfprotokoll protokolliert. Dass es sich dabei um den Laufzettel handelt (was sinnvoll wäre) ist aus der Spezifikation NICHT ersichtlich.

Folgendes Sicherheitsziel wird durch die o.g. Funktion realisiert:

Nicht-Abstreitbarkeit des Ursprungs

Unter der Annahme, dass es sich beim Protokoll-Medium um den Laufzettel handelt, werden auf diesem die Ergebnisse der mathematischen Zertifikatsprüfung, der Offline-Gültigkeitsprüfungen und der Online-Gültigkeitsprüfungen für jede Zustellung durch den Intermediär vermerkt.
Der Intermediär lehnt einen Auftrag ab, falls das Chiffrierzertifikat des Lesers oder Benutzers (hier als Supplier) als widerrufen verifiziert wurde. Dann sendet der Supplier lediglich eine entsprechende Antwort an den Client. Ist das Client-Zertifikat widerrufen, so wird die Auftragsantwort nicht mit diesem Zertifikat verschlüsselt, sondern der Client erhält lediglich eine unverschlüsselte Information darüber durch den Supplier.

Somit kann der Client erkennen, dass die vom Intermediär erwarteten Sicherheits-Mehrwertdienste erbracht wurden und kann eigene zusätzliche Prüfungen basierend auf den gelieferten Ergebnissen aufsetzen.

### 3.3.2 Protokollierung von Zeitpunkten

Die Qualität des Zeitpunktes hängt von dem verwendeten Zeitstempel-Mechanismus ab.

Insbesondere wird im folgenden davon ausgegangen, dass die „kryptographischen Zeitstempel“ einen hinreichend genauen Zeitpunkt erkennen lassen (z. B. gesetzlich gültige Zeit). Es ist allerdings in der Spezifikation NICHT festgelegt, was unter „kryptographischen Zeitstempeln“ zu verstehen ist. Die Verwendung ISIS-MTT-konformer Zeitstempel wird lediglich als eine Möglichkeit erwähnt.

Folgende Sicherheitsziele werden durch die o.g. Funktion realisiert:

Zurechenbarkeit von (bestimmten) Aktionen zu Zeitpunkten sowie ggf. Nicht-Abstreitbarkeit des Empfangs(-Zeitpunktes)

Der Intermediär hält folgende Zeitpunkte fest:

a) den Zeitpunkt des Empfangs von Zustellungs-, Weiterleitungs- und Abwicklungsaufträgen
b) den Zeitpunkt der Weiterleitung an den Empfänger
c) den Zeitpunkt der Empfangsbestätigung durch den Empfänger (der vom Eingang der Quittung abhängt)

Im Fall c) ist zwischen einem Annahme- oder Bearbeitungsauftrag sowie einem Zustellungsauftrag zu unterscheiden. Durch die positive Rückmeldung in Form einer Annahme- oder Bearbeitungsantwort, bestätigt der Benutzer2 (indirekt) den Empfang eines Annahme- oder Bearbeitungsauftrags. Hierbei wird der Zeitpunkt protokolliert, zu dem der Intermediär diese positive Rückmeldung erhält und zwar mit dem (zusätzlichen) Ziel der Nicht-Abstreitbarkeit des Empfangs des Auftrags.
Durch den Eingang eines Folgeauftrags oder durch den Eingang eines Dialogendeauftrags (im Rahmen eines expliziten Dialogs) bestätigt der Benutzer1 (indirekt) den Empfang einer Zustellungsantwort; hierbei wird der Zeitpunkt protokolliert, zu dem beim Intermediär ein weiterer Auftrag eingeht und zwar mit dem Ziel der Nicht-Abstreitbarkeit des Empfangs der Auftragsantwort.

Somit können die Benutzer die Zeitpunkte erkennen, zu denen bestimmte Aktionen vom Intermediär durchgeführt wurden.

## 3.4 Challenge-Response

Folgendes Sicherheitsziel wird durch die o.g. Funktion realisiert:

Zurechenbarkeit von Aktionen

Somit wird erkannt, dass Nachrichten von unberechtigten Dritten (auf Auftragsebene) wiedereingespielt wurden und der aktuelle Dialog noch in korrekter Aufeinanderfolge der Nachrichten stattfindet.

### 3.4.1 Vergeben und Prüfen von Challenge-Response-Werten

Durch das Mitschicken eines (frei gewählten) Challenge-Wertes im Auftrag durch den Client und das Wiederholen dieses als Response-Wert in der Antwort durch den Supplier – wobei zu jeder Nachricht ein „neuer" Challenge-Wert gebildet wird – erreicht man, dass jeweils 2 aufeinanderfolgende Nachrichten auch „frisch" sind.
Zusätzlich zum Response-Wert werden auch ConversationID sowie SequenceNumber durch den Supplier geprüft.

### 3.4.2 Dialogende

Bei unerwarteten oder ungültigen Challenge-Werten in der Antwort wird der Dialog – falls es sich um einen expliziten handelt – vom Client dadurch beendet, dass er keinen (Folge-) Auftrag sendet.
Bei unerwarteten oder ungültigen ConversationID- sowie SequenceNumber-Werten im (Folge-)Auftrag wird der Dialog – falls es sich um einen expliziten handelt – vom Supplier beendet.

Bei Überschreiten einer (bestimmten) Zeitspanne, innerhalb der kein Folgeauftrag oder Dialogendeauftrag beim Supplier eingeht, wird der Dialog – falls es sich um einen expliziten handelt – vom Supplier beendet.

## 3.5 Client-Authentisierung

Folgendes Sicherheitsziel wird durch die o.g. Funktion realisiert:

Authentizität des Empfängers

Somit wird sichergestellt, dass der Client während eines expliziten Dialogs auch als Empfänger von Auftragsantworten „authentisch" bleibt.

### 3.5.1 Authentisieren mittels eines Chiffrierzertifikats

Im Rahmen eines expliziten Dialogs wird festgestellt, dass derjenige Client, der den Dialoginitialisierungsauftrag an den Supplier geschickt hat, auch tatsächlich im Besitz des privaten Chiffrierschlüssels ist.

Die Dialoginitialisierungsantwort (und auch jede weitere Antwort) wird vom Supplier für den Client mit dem Chiffrierzertifikat verschlüsselt, das der Supplier mit dem Dialoginitialisierungsauftrag erhalten hat.

### 3.5.2 Dialogende

Ist der Empfänger der verschlüsselten Auftragsantwort nicht im Besitz des privaten Schlüssels, so kann der Client diese auch nicht entschlüsseln. Eine Fortsetzung des Dialogs ist nicht möglich, weil 1. der Supplier – wenn er nicht innerhalb einer gewissen Zeitspanne einen (Folge-)Auftrag des Clients erhält – den (expliziten) Dialog schliesst und 2. der Supplier – wenn der Client den vom Supplier in seiner Dialoginitialsierungsantwort (frei gewählten) Challenge-Wert nicht in seinem Folgeauftrag als Response mitschickt – den Auftrag aufgrund eines ungültigen Response-Wertes ablehnt.

## 3.6 MessageID

Folgendes Sicherheitsziel wird durch die o.g. Funktion realisiert:
Zurechenbarkeit von Aktionen

Somit wird erkannt, dass Zustellungen (auf Geschäftsvorfallsebene) doppelt eingereicht wurden. Durch diese Funktion wird ein Sender-Replay verhindert, indem das Wiedereinspielen einer alten Nachricht erkannt wird.

### 3.6.1 Vergeben und Prüfen einer MessageID

Bevor der Intermediär einen Zustellungs- bzw. Weiterleitungsauftrag bearbeitet, muss er dem Client eine MessageID zusenden. Durch das Mitschicken dieser MessageID in einem Zustellungs- bzw. Weiterleitungsauftrag (beim Abwicklunsauftrag ist dies optional, da hier die gleiche Wirkung durch den Challenge-Response-Wert erzielt wird) durch den Client, kann der Intermediär als Supplier prüfen, ob diese MessageID von ihm erzeugt und schon einmal verwendet worden ist.

### 3.6.2 Dialogende

Ist das Ergebnis einer der vorgenannten Prüfungen negativ, so muss der Intermediär den Auftrag ablehnen (und beendet damit den Dialog).

## 3.7 Quittierung von Aufträgen und Auftragsantworten

Folgendes Sicherheitsziel wird durch die o.g. Funktion realisiert:
Nicht-Abstreitbarkeit des Empfangs

Sender und Empfänger können auf Dialogebene durch Erhalt einer Auftragsantwort bzw. eines (Folge-)Auftrags auf die Durchführung der vorangegangenen Aktion schließen.
Bei einer OneWay-Message wird durch das Senden einer Auftragsantwort (mit positivem Rückmeldecode) vom Supplier der Erhalt des Auftrags implizit bestätigt. Bei einer Request-Response-Message wird durch das Senden eines Response-Wertes, der mit dem Challenge-

Wert aus der vorangegangenen Auftragsantwort übereinstimmt, in einem (Folge-)Auftrag vom Client der Erhalt der Auftragsantwort bestätigt.

Somit wird verhindert, dass der Empfänger den Erhalt eines Auftrages bzw. einer Auftragsantwort erfolgreich abstreiten kann.

### 3.8 Protokollauswertung des Laufzettels

Folgendes Sicherheitsziel wird durch die o.g. Funktion realisiert:
Zurechenbarkeit von (bestimmten, zu protokollierenden) Aktionen

Sender und Empfänger können auf Geschäftsvorfallsebene eine Kopie des Laufzettels anfordern und diesen hinsichtlich durchgeführter Aktionen auswerten.

Es ist allerdings aus der Spezifikation NICHT ersichtlich, wozu das Wiederholen der Selektionskriterien (Seite 25 in Verbindung mit Seite 81) dient.

Somit können die Benutzer erkennen, dass der Intermediär bestimmte Aktionen durchgeführt hat.

### 3.9 Zusammenfassung der Sicherheitsfunktionen und -mechanismen

Mit den Funktionen

- Digitale Signatur
- Verschlüsselung
- Beweissicherung
- Challenge-Response
- Client-Authentisierung
- Quittierung von Aufträgen und Auftragsantworten
- Protokollauswertung des Laufzettels

werden die Sicherheitsziele

- Integrität von Inhaltsdaten und Nutzungsdaten (im Sinne von Daten-Integrität)
- Vertraulichkeit von Inhaltsdaten und Nutzungsdaten (im Sinne von Daten-Vertraulichkeit)
- Authentizität der Herkunft der Inhaltsdaten (im Sinne von Authentisierung)
- Authentizität des Senders von Nutzungsdaten (im Sinne von Authentisierung)
- Authentizität des Empfängers von Nutzungsdaten (im Sinne von Zugriffskontrolle)
- Authentizität (und Integrität) der öffentlichen Schlüssel
- Zurechenbarkeit von Aktionen
- Zurechenbarkeiten von Aktionen zu Zeitpunkten
- Nicht-Abstreitbarkeit des Ursprungs der Inhaltsdaten (im Sinne von Sendenachweis)
- Nicht-Abstreitbarkeit des Empfangs von Nutzungsdaten (im Sinne von Empfangsnachweis)

durchgesetzt.

Somit wird insbesondere der „Schutz der Daten während der Übertragung über Kommunikationskanäle“ (Übertragungssicherung im Sinne der ITSEC) sichergestellt. Grundsätzlich liegen derzeit keine speziellen Sicherheitsanforderungen an Kommunikation im E-Government im Kontext von BundOnline 2005 vor. Aber es kann davon ausgegangen werden, dass Übertragungssicherung eine Anforderung an „sicherere“ Kommunikation im allgemeinen und Kommunikation im E-Government im besonderen ist. Demnach erfüllt die zu bewertende Spezifikation diejenigen Sicherheitsziele, die bzgl. Kommunikationssicherheit (im engeren Sinne) als relevant zu erachten sind.

## 4. Kryptographische Verfahren in OSCI

### 4.1. XML Signature und XML Encryption

Wie bereits erwähnt, benutzt OSCI grundsätzlich Daten im XML-Format. Es sei daran erinnert, dass XML eine Metasprache (Daten für Daten) ist, d.h. eine Beschreibungssprache für Daten, die es erlaubt eine Datenmenge bzw. ein Dokument -durch „Markierung“ verschiedener Teile - zu strukturieren. (Anders als z.B. in HTML wird dabei die Präsentation der Daten strikt von deren Inhalt und Struktur getrennt).

XML-Signature bzw. XML-Encryption sind XML-basierte Datenformate bzw. (Vorschläge für) XML-Erweiterungen, die einerseits die Erstellung/Verifizierung von digitalen Signaturen bzw. von Verschlüsselung von XML-Dokumenten regeln, andererseits allgemein verbindlich XML-Elemente und Syntax für die Repräsentation von digitalen Signaturen bzw. verschlüsselten Daten in XML festlegen.

[Anmerkung zum Verständnis:
Das Wort „Erstellung“ bezieht sich hier auf die Fragen, welcher kryptographische Algorithmus, mit welchem Schlüssel angewendet wird, und insbesondere auf die Art und Weise der Umsetzung auf Byte-Ebene. Signiert, bzw. verschlüsselt werden können nur Bytefolgen. Will man ein XML-Dokument signieren bzw. verschlüsseln, so muss es daher dazu in einer vorgeschriebenen Reihenfolge, und unter Berücksichtigung etwaiger Transformationen, in eindeutiger Weise in eine „kanonische“ Bytefolge umgesetzt werden.]

Es handelt sich also nicht etwa um eine „neue“ Art von Signatur- bzw. Verschlüsselungsverfahren (es werden bekannte kryptographische Algorithmen verwendet), die Begriffe XML Signature bzw. XML Encryption bezeichnen lediglich die Teile der XML-Spezifikation, die die „Verarbeitung“ von XML-Dokumenten (bei Anwendung von Signatur/Verschlüsselung) und die XML-Codierung von digitalen Signaturen und verschlüsselten Daten (nebst zugehörigen Parametern) regeln. Der Regelfall ist dabei, dass XML Dokumente selbst signiert bzw. verschlüsselt werden, es können jedoch auch beliebige andere Binärdaten mit einer XML-Signatur bzw. XML-Verschlüsselung versehen werden.

Die Verwendung von XML-Signature und XML-Encryption bietet also eine XML-interne Möglichkeit, diese Sicherheitsdienste zu nutzen und zu beschreiben - eine nahtlose Integration dieser Dienste in XML-, es ist daher nahezu selbstverständlich, dass diese XML-Erweiterungen von OSCI ebenfalls genutzt werden.
Von besonderem Interesse für OSCI-Zwecke ist die Flexibilität von XML-Signature bzw. XML-Encryption. Dabei bietet insbesondere XML-Signature mehr Freiheitsgrade als herkömmliche Systeme: z.B. kann eine XML-Signatur im signierten XML-Dokument enthalten („enveloped“) sein, (was problemlos Mehrfach-Signaturen („Workflow“) möglich

macht), und es können ohne weiteres auch nur kleine Teile von XML-Dokumenten signiert werden.
Gerade dieser (in der Spezifikation von XML-Signature schon enthaltene und nicht erst umständlich zu schaffende) große Gestaltungsspielraum beim Einsatz von Signaturen macht den Einsatz von XML-Signature in den Szenarien, die OSCI abdecken will, sinnvoll.

Das W3C (WorldWideWeb-Consortium) betreibt Aktivitäten zur Standardisierung von XML Signature bzw. XML Encryption, beides ist „Work in Progress", wobei XML-Signature seit Februar 2002 den Status einer W3C-„Recommendation" besitzt, XML-Encryption hat derzeit den Status einer „Candidate Recommendation". Diese Standardisierungsaktivitäten haben „Open Source"-Charakter. Die OSCI-Entwickler streben zukünftig ausdrücklich Konformität zur konsolidierten Version von XML Encryption an.

Für die aktuellen Fassungen von XML-Signature bzw. XML-Encryption gilt:
derzeit sind weder kryptographische noch andere gravierende Schwächen entdeckt worden.

## 4.2 Kryptographische Algorithmen

### 4.2.1 Signaturalgorithmen

Als Signaturalgorithmen unterstützt OSCI-Transport derzeit die RSA-Signaturen RSA/SHA-1 und RSA/RIPEMD-160, wobei die Modullänge des RSA-Moduls mindestens 1024 Bit betragen muss. Die Signaturschemen folgen der W3C-Recommendation „XML Signature: Syntax and Processing".

Dabei erfolgt die bitgenaue Realisierung der RSA /SHA-1 Signatur exakt nach dem Signaturschema RSASSA-1-PKCS1-v1_5 gemäß RFC2437 (PKCS1v1_5 , Sektion 8.1.1), wobei eine Kodierung nach EMSA-PKCS1-v1_5 (PKCS1v1_5, Sektion 9.2.1) erfolgt (d.h. es wird aus dem SHA-1 Object Identifier und dem Hashwert ein ASN1-Objekt vom Typ MessageDigest gebildet, und dieses Objekt dann „gepaddet"). Die bitgenaue Realisierung der RSA/RIPEMD160 Signatur erfolgt völlig analog, wobei anstelle von SHA-1 RIPEMD160 als Hashfunktion, und dazu dann der RIPEMD160 Object Identifier verwendet wird. Die zugehörigen SignatureValue Elemente enthalten diese Signaturen in (gemäß MIME) base64-codierter Form.

Diese Signaturschemen gelten derzeit als kryptographisch stark, und werden u.a. auch in der derzeit gültigen Veröffentlichung der RegTP „Geeignete Kryptoalgorithmen" (in Erfüllung von §17 (1) SigG vom 16. Mai 2001 in Verbindung mit §17 (2) SigV vom 22.Oktober 1997) aufgeführt (siehe http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/39.pdf).

### 4.2.2 Verschlüsselungsalgorithmen

Zur Verschlüsselung werden in OSCI hybride Verfahren eingesetzt, d.h. die Massendaten werden mittels eines symmetrischen Algorithmus verschlüsselt, wobei der zugehörige „Sitzungsschlüssel" zuvor -mittels eines asymmetrischen Verfahrens für den Empfänger verschlüsselt – übertragen wird.
Die hybriden Verfahren folgen der W3C-Recommendation „XML Encryption: Syntax and Processing".

Als asymmetrisches Verfahren zum Schlüsseltransport ist in OSCI-Transport 1.2 ausschließlich RSA-Verschlüsselung vorgesehen, wobei die zugehörige RSA-Modullänge mindestens 1024 Bit betragen muss.
Die bitgenaue Realisierung der Verschlüsselung erfolgt dabei

(1) - für Triple-DES-Schlüssel (oder 192 Bit AES-Schlüssel) nach dem Schema RSAES-PKCS1-v1_5 gemäß RFC 2437 (PKCS1v1_5, Sektion 7.2.1), wobei gemäß EME-PKCS1-v1_5 (Sektion 9.2.1.1) gepaddet wird (mit mindestens 8 Zufallsbytes ungleich 0).

Anmerkung:
Gegen dieses Paddingformat gab es einige kryptographische Attacken, (insbesondere eine Implementierungsattacke (Bleichenbeicher), und Angriffe auf „low exponent“ RSA (Coppersmith)) aber die beschriebene Version gilt bei Beachtung der in RFC 2437 dazu gegebenen Empfehlungen noch als sicher. Dies (veraltende) Format wird in XML-Encryption unterstützt, um zu den vielen bestehenden „alten“ RSA/Triple-DES Anwendungen abwärtskompatibel zu sein.

(2) - für AES-Schlüssel nach RSAOAEP-PKCS1-v1_5 gemäß RFC 2437 (PKCS1v1_5, Sektion 7.1.1), wobei gemäß EME-OAEP-PKCS1-v1_5 (Sektion 9.1.1.1) gepaddet wird. Die entsprechenden CipherValue Elemente werden durch (gemäß MIME) base64-Codierung der Verschlüsselungsergebnisse erhalten.

Diese Schlüssel-Verschlüsselungsverfahren gelten derzeit als kryptographisch stark, wobei allerdings das alte Padding EME-PKCS-v1_5 nur noch in Verbindung mit zusätzlich unterstützenden Sicherheitsmaßnahmen verwendet, und langfristig abgelöst werden sollte.
Für eine konkrete Implementierung des alten Paddings ist insbesondere zu prüfen, ob die in RFC 2437 gegebenen Empfehlungen umgesetzt sind. Auch für das neue OAEP-Padding sollte eine konkrete Implementierung insbesondere die aktuellen Hinweise aus PKCS1-v2.1 zur Durchführung von Fehlerbehandlung beachten.

Symmetrische Verfahren:
Von den symmetrischen Verfahren unterstützt OSCI die Blockchiffrierer Three-Key-TripleDES, sowie die drei AES-Versionen AES-128, AES-192 und AES-256. Sie werden ausschließlich im CBC-Modus eingesetzt, wobei die Initialisierungsvektoren zufällig gewählt werden.
Falls ein Klartext einer Bytelänge $l$ verschlüsselt wird, wird mit einem String aus Zufallsbytes, gefolgt von dem Byte „Anzahl der insgesamt zu ergänzenden Bytes“ (zwischen 1 und b, wobei b die Blockbreite in Bytes darstellt) auf das nächstgrößere ganzzahlige Vielfache der Blockbreite „gepaddet“, die Länge des ergänzten Stücks wird beim Entschlüsseln zunächst auf Plausibilität geprüft, dann die ergänzten Bytes entfernt.

Diese Blockchiffrierer gelten mit den angegebenen Schlüssellängen, der gewählten Betriebsart und dem gewählten Padding derzeit als kryptographisch sicher. In einer konkreten Implementierung ist hier die Qualität der verwendeten Zufallszahlen ein Gesichtspunkt, der besondere Aufmerksamkeit verdient. Weiter ist in einer konkreten Implementierung zu prüfen, ob die CBC-Seitenkanal-Attacke (Vaudenay, Eurocrypt 2002) unter den gegebenen Umständen möglich ist, und ggf. zu unterbinden.

## 4.3 Schlüsselmanagement

### 4.3.1 Asymmetrische Verfahren

Das OSCI-Schlüsselmanagement verwendet grundsätzlich Public-Key-Zertifikate, dabei werden ausschließlich Zertifikate im Format X509v3 in der ISIS-MTT konformen Ausprägung verwendet.

Für die Zwecke Verschlüsselung bzw. digitale Signatur eines Benutzers werden dabei unterschiedliche Schlüsselpaare eingesetzt. Der Besitz eines Chiffrierzertifikates ist Voraussetzung, um als Benutzer an OSCI teilnehmen zu können – ohne Chiffrierzertifikat kann ein Benutzer keine für ihn bestimmten, vertraulichen OSCI-Nachrichten erhalten.

Entschlüsselt werden kann eine OSCI-Nachricht nur durch den Besitzer des privaten Schlüssels eines Chiffrierzertifikates, signiert werden kann eine OSCI-Nachricht nur durch den Besitzer des privaten Schlüssels eines Signierzertifikates. Verschlüsselt wird eine OSCI-Nachricht für einen bestimmten Addressaten mit Hilfe des öffentlichen Schlüssels seines Chiffrierzertifikates, die Verifikation der Signatur eines OSCI-Benutzers geschieht mit Hilfe des öffentlichen Schlüssels seines Signierzertifikates.

Anmerkung:
Implizit setzt **OSCI–Transport 1.2** voraus, dass die „generischen“ Anforderungen für die vertrauenswürdige Benutzung von Public-Key Kryptographie erfüllt sind. D.h., wie stets bei Benutzung von Public-Key-Kryptographie ist die Existenz einer vertrauenswürdigen „Zertifizierungsautorität“ nötig, die die verschiedenen Nutzer registriert, und die Zugehörigkeit (Identität des Nutzers, öffentlicher Schlüssel des Nutzers) beglaubigt, und die dabei angemessen starke Registrierungs- und Zertifizierungsrichtlinien einhält. In diesem Sinne wird der wesentliche Teil des OSCI-Schlüsselmanagements von der zugrunde liegenden PKI geleistet. Vorausgesetzt ist hier ebenfalls der Einsatz von vertrauenswürdiger Technik zur Speicherung von privaten Schlüsseln, Verteilung von Zertifikaten und Durchführung von relevanten kryptographischen Prozessen.

Kurz: es muss dafür gesorgt sein, dass (1) ein bestimmtes Public-Key-Paar vertrauenswürdig einem Nutzer zuzuordnen ist, dass (2) diese Zuordnung authentisch geprüft werden kann, und dass (3) der zugehörige private Schlüssel ausschließlich durch den zugehörigen Nutzer verwendet werden kann.

Anmerkung:
In OSCI-Transport 1.2 finden sowohl Verschlüsselungszertifikate als auch Signaturzertifikate Verwendung. Wir gehen davon aus, dass ein Zertifikat nur für den ihm zugedachten Bestimmungszweck verwendet werden kann, d.h. Verschlüsselungszertifikate dürfen ausschließlich für Verschlüsselungszwecke, Signaturzertifikate ausschließlich für Signaturzwecke verwendet werden. Das ist bei einer konkreten Implementierung durch geeignete Maßnahmen sicherzustellen. Somit werden Gefährdungen oder Fehlfunktionen, die durch die bestimmungsfremde Benutzung von Zertifikaten entstehen, im weiteren nicht betrachtet.

**Zertifikatsprüfungen in OSCI-Transport 1.2:**

Anmerkung:

Da die für eine Zweckbestimmung der Verschlüsselungs- und Signaturzertifikate erforderlichen technischen Maßnahmen bisher nicht in OSCI-Transport 1.2 integriert sind, sollte vor einem Einsatz des Zertifikats eine Prüfung des Bestimmungszwecks möglich sein und zwingend erfolgen.

Weiterhin sollen Sender und Autoren vor dem Verschlüsseln mindestens die offline möglichen Zertifikatsprüfungen vornehmen.

Anmerkung:
Der Umfang der offline durchzuführenden Zertifikatsprüfung geht aus der Spezifikation nicht klar hervor. Grundsätzlich sind offline möglich: (1) eine Prüfung, ob der im Zertifikat genannte DNS-Name der Name des Empfängers ist, (2) eine Prüfung, dass der Gültigkeitszeitraum nicht überschritten ist, sowie (3) eine Prüfung der Signatur auf dem Zertifikat. Lediglich (2) und (3) werden in der Spezifikation als mögliche Prüfungen aufgeführt.

Empfänger und Leser sollen nach dem Empfang signierter Daten ebenfalls mindestens die offline möglichen Zertifikatsprüfungen durchführen.

Anmerkung:
Besser wäre es, wenn alle Parteien ebenfalls Online-Prüfungen auf Sperrung von Zertifikaten durchführen könnten – hier orientiert sich OSCI 1.2 an den gegenwärtigen technischen Möglichkeiten: die Parteien nehmen i.d.R. über ihre WWW-Browser an OSCI teil, und die gegenwärtigen Browser unterstützen i.d.R. keinen Zugriff auf Sperrlisten von Zertifizierungsstellen. Sobald Sperrlistenzugriff problemlos zu haben ist, sollten die Parteien in OSCI verpflichtet werden, Online-Prüfungen auf Sperrung von Zertifikaten durchzuführen.

Der Intermediär hat alle Zertifikate, die sich in einer Nachricht auf Auftragsebene befinden, im vollen Umfang zu prüfen, er prüft die Zertifikate auf Ablauf und Sperrung, und er prüft ggf. alle Signaturen einer Zertifikatskette.

### 4.3.2. Symmetrische Verfahren

Symmetrische Chiffrierverfahren finden in OSCI ausschließlich als Teil eines hybriden Verfahrens Verwendung, die zugehörigen Schlüssel sind „Einmal“-Schlüssel, die zu jeder Verwendung neu zufällig erzeugt, und nach Verwendung vernichtet werden.
Vertrauliche Aufbewahrung/Speicherung von Dokumenten sind nicht Gegenstand der Spezifikation **OSCI-Transport 1.2.**

## 5. Weitere Sicherheitsaspekte

### 5.1 Einsatz von SOAP

OSCI verwendet grundsätzlich das SOAP (Simple Object Access Protocol) zur Strukturierung von Nachrichten („Bildung von Umschlägen“). Die OSCI-Entwickler streben für die Zukunft die Konformität zur konsolidierten Version von SOAP 1.2 an.

SOAP ist ein (ursprünglich von der amerikanischen Firma Microsoft entworfenes) XML-basiertes „Lightweight“ Protokoll zur (plattformunabhängigen) Übertragung von

strukturierten Informationen zwischen Rechnern eines verteilten Rechnersystems; SOAP-Nachrichten sind grundsätzlich XML-codiert.
SOAP kann als ein Vorschlag für einen allgemeinen „Nachrichtenübertragungsstandard“ in der entstehenden Welt der WebServices aufgefasst werden, es ist Plattform-, Programmiersprachen- und CPU -neutral.
Das W3C betreibt seit ca. 2 Jahren Open-Source-Aktivitäten zur Standardisierung von SOAP.

SOAP erweitert die Möglichkeiten von XML i.w. in zwei Richtungen:

(1) SOAP erlaubt die Bildung von „Umschlägen“ (wobei der Header Information für durchlaufene Netzknoten (in OSCI der „Intermediär“) darüber enthalten kann, wie die Nachricht im Rumpf zu bearbeiten ist) und die Bildung von benutzerdefinierten, applikationsspezifischen Datentypen

(2) SOAP kann für „Remote Procedure Calls“ (RPC) verwendet werden. RPC ist ein Protokoll, das die Implementierung verteilter Anwendungen erleichtern soll: dabei wird einem Programm eines Rechners die Nutzung eines Programms, das auf einem anderen Rechner läuft, ermöglicht.

Bei der Verwendung von SOAP sind folgende sicherheitstechnischen Eigenschaften dieses Protokolls zu beachten:

(1) SOAP verfügt (derzeit) über keinerlei „eigene“ Sicherheitsmechanismen:
In der Tat besteht ein wesentlicher Teil von OSCI darin, für die Einsatzszenarien geeignete Sicherheitsmechanismen zu definieren.
(Es sei bemerkt, dass im April 2002 (gemeinsam von IBM, Microsoft und VeriSign) die Spezifikation „Web Services Security“ vorgelegt wurde, ein Vorschlag, wie SOAP um umfassende Sicherheitsdienste erweitert werden kann.)

(2) SOAP kann zum „HTTP-Tunneling“ benutzt werden:
Darunter ist folgendes zu verstehen: SOAP benutzt üblicherweise HTTP als zugrunde liegendes Transportprotokoll, und findet deshalb über den HTTP-Port Eingang zum Rechner. Üblicherweise ist der HTTP-Port von Firewalls „offen“ (die meisten Firewalls gehen davon aus, dass über diesen Port „reines HTTP“ hereinkommt, und Filterregeln etwa für SOAP-spezifische HTTP header sind i.d.R. kaum verfügbar). Über diesen „Eingang“ kann dann z.B. ein SOAP-RPC eine Anwendung hinter der Firewall initiieren bzw. benutzen, dadurch wird die Firewallfunktionalität unterlaufen. (Es ist gerade ein Sinn von Firewalls, RPCs und ähnliches allenfalls von vertrauenswürdigen Kommunikationsparteien zuzulassen).

Die Sicherheitsmechanismen für OSCI-Nachrichten werden in der Spezifikation OSCI-Transport 1.2 definiert.
In einer konkreten Implementierung von OSCI ist darauf zu achten, dass die Tunnelingfunktionalität von SOAP bzw. SOAP-RPCs nur strikt kontrolliert eingesetzt wird.

Anmerkung:
Diese Ausführungen beinhalteten keine Trendaussage. Wie grundsätzlich bei „avantgardistischen“ Technologien, ist auch im Falle SOAP eine Vorhersage, ob sich SOAP schließlich im Umfeld „WebServices“ unter den existierenden Server-zu-Server Technologien auf breiter Front durchsetzen wird (konkurrierend sind etwa CORBA, DCOM, RMI und andere), nicht möglich.

## 5.2 Einordnung von OSCI-Transport 1.2 in das ISO/OSI - Referenzmodell

Ein grundlegendes Ziel von OSCI-Transport 1.2 besteht darin, plattformunabhängig Ende-zu-Ende Sicherheitsdienste (d.h. von der Eingabe der Information am Endgerät A bis zur Ausgabe/Bearbeitung am Endgerät B) für OSCI-Nachrichten anzubieten. Im OSI Schichtenmodell ist OSCI auf der obersten Schicht - der Anwendungsschicht 7 – anzusiedeln (im Grunde definiert OSCI eine eigene Anwendungsschicht darüber).
Die zugrunde liegenden Designüberlegungen begründen, dass die Anwendungsdaten möglichst nahe der Anwendung geschützt bzw. unsichere Wege möglichst kurz gehalten werden – nur so ist Ende-zu-Ende Sicherheit möglich.
Die Sicherheitsmechanismen von OSCI sind ausschließlich auf der Anwendungsschicht verwirklicht, insofern darf der Name OSCI-Transport 1.2 nicht fehlgedeutet werden: OSCI dient zum „secure messaging“, „transport security“ d.h. Umsetzung von Sicherheitsmaßnahmen in den unteren, transportorientierten Schichten des Referenzmodells ist NICHT Ziel von OSCI-Transport 1.2.

Ein konkreter, üblicherweise web-basierter Einsatz von OSCI-Transport 1.2. setzt das fehlerfreie Funktionieren der unterliegenden Dienste auf Transportebene (z.B. Domain Name Service, IP-Routing) voraus.

## 5.3 Einhaltung datenschutzrechtlicher Vorschriften

Mit der Vorgabe einer Client-Intermediär-Architektur in OSCI-Transport 1.2 und dem damit verbundenen Angebot von Mehrwertdienstleitungen durch den Intermediär verbinden sich weit reichende Fragen bezüglich der Einhaltung datenschutzrechtlicher Vorschriften. Dazu liegt eine Position des Arbeitskreises Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vor, die dieser Sicherheitsbewertung als Anlage beiliegt.

## 5.4 Weiterentwicklung von OSCI-Transport

Mit OSCI-Transport 1.2 liegt die Spezifikation eines Protokolls für einen Transportmechanismus im E-Government vor, mit dem auf technischer Basis des SOAP-Protokolls sichere web-basierte Transaktionen ermöglicht werden sollen. Hierbei handelt es sich allerdings nicht um einen Standard oder gar um eine Norm im engeren Sinne. Dazu bedürfte es zumindest einer Referenzimplementierung oder eines Schutzprofils, mit deren Hilfe die Prüfung auf korrekte Umsetzung in konkrete Produkte möglich würde. Somit bleiben dem Softwareentwickler Interpretationsspielräume, die zur Verfehlung der Ziele Standard-Konformität sowie Interoperabilität der Produkte führen können.

Im Hinblick auf einen sicheren Betrieb der auf der Spezifikation basierenden Produkte sei hier noch einmal auf das fehlende Betriebshandbuch verwiesen. Nur wenn dieses eine sichere Einsatzumgebung skizziert, kann ein auf OSCI basierendes Produkt auch sicher betrieben werden.

Abschließend sei die Bemerkung gestattet, dass ein Standard (und seine Verbreitung) von der dynamischen Fortschreibung der Spezifikation lebt. Dies gilt um so dringlicher, da es sich bei den Basistechnologien von OSCI um relativ junge Standardisierungen handelt, die sich noch nicht ausreichend bewähren konnten. Hier gilt es, einen dauerhaften Prozess zu initiieren, der die permanente Einarbeitung der aus den Implementierungen gewonnenen Erfahrungen sowie der Änderungen im Bereich internationaler Standardisierungen garantiert.

## 6. Zusammenfassung

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 unter Annahme der unter 1.2 beschriebenen Voraussetzungen 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 $2^{80}$ Operationen.