

F OSCI-Transport-Profil für OSCI-XMeld



OSCI® ist eine registrierte Marke
der Freien Hansestadt Bremen

F.1 Regelungsgegenstand und Geltungsbereich

F.1.1 Die Übermittlungsstandards OSCI-Transport und OSCI-XMeld

Für die elektronische Datenübermittlung im Meldewesen wird der Standard OSCI-XMeld durch die OSCI Leitstelle entwickelt. OSCI-XMeld ist die am 23. Juli 2003 von der Bundesvereinigung der kommunalen Spitzenverbände auf der Grundlage des Datensatzes für das Meldewesen - Einheitlicher Bundes-/Länderteil - (DSMeld) herausgegebene Beschreibung des Datensatzes für Datenübermittlungen im Bereich des Meldewesens. OSCI-XMeld trifft Aussagen über die zwischen den Verfahren zu übermittelnden *Inhaltsdaten*, macht aber keine Aussagen über den sicheren Transport der zu übermittelnden Nachrichten, sondern überlässt dies einer sicheren Transportschicht.

Für den sicheren Transport von Nachrichten wurde ebenfalls durch die OSCI Leitstelle der Standard OSCI-Transport entwickelt. OSCI-Transport ist der am 6. Juni 2002 vom Kooperationsausschuss ADV Bund/Länder/Kommunaler Bereich herausgegebene Standard für ein Datenübermittlungsprotokoll, welches eine sichere Datenübermittlung sowohl über öffentliche Netze (zum Beispiel das Internet), als auch über verwaltungseigene Kommunikationsnetze erlaubt.

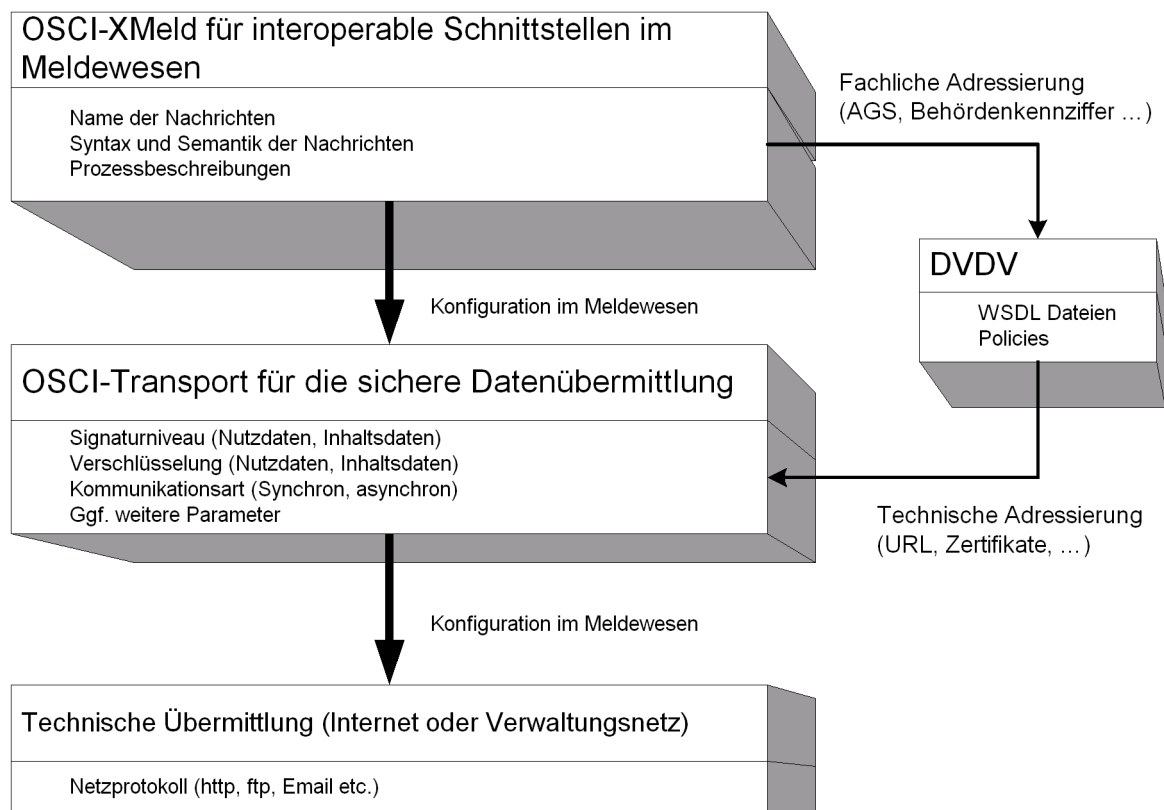
Die Standards OSCI-XMeld und OSCI-Transport sind beim Bundesverwaltungsamt, Barbarastr. 1, 50735 Köln, der DSMeld ist beim Verlag W. Kohlhammer GmbH, Heßbrühlstr. 69, 70565 Stuttgart, zu beziehen. Beide Standards sowie der DSMeld sind bei dem Bundesarchiv, Potsdamer Str. 1, 56075 Koblenz, jedermann zugänglich und archivmäßig gesichert niedergelegt.

OSCI-Transport ist als generische Infrastrukturkomponente entworfen. Sein Einsatz ist nicht auf das Meldewesen beschränkt. Deshalb ist OSCI-Transport hochgradig konfigurierbar. So kann zum Beispiel durch den Sender einer Nachricht festgelegt werden:

- ob und wie die *Inhaltsdaten* (also der eigentliche Nachrichteninhalt, zum Beispiel eine Rückmeldung gemäß § 17 MRRG) signiert und / oder verschlüsselt werden;
- ob und wie die *Nutzungsdaten*¹ (also Daten zur Steuerung und zum Nachvollzug einer Datenübermittlung, mit Angaben über Sender und Empfänger, Übermittlungszeitpunkten etc.) signiert und / oder verschlüsselt werden;
- ob die Daten *synchron* (also mit unmittelbarer Antwort des Senders) oder *asynchron* (also analog der klassischen EMail) ausgetauscht werden .
- welches technische Transportprotokoll auf der Nachrichtenebene zwischen den jeweiligen OSCI-Transport Instanzen genutzt werden soll (zum Beispiel *http* oder *ftp*).

Details zu diesen Konfigurationsmöglichkeiten sind in [OSCI-Transport 2002] ausgeführt. Die verschiedenen Ebenen der Konfiguration und die Komponenten im Meldewesen sind in dem [Bild F-1](#) dargestellt.

1.Nutzungsdaten sind gemäß [TDDSG 2001] Daten, die zusätzlich zu den Inhaltsdaten ausgetauscht werden und dazu dienen, die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen oder den Datenfluss zu kontrollieren und zu steuern.

Bild F-1 Der Zusammenhang zwischen OSCI-XMeld und OSCI-Transport

Um eine vollständige Interoperabilität zu gewährleisten und somit die vollautomatische und medienbruchfreie Datenübermittlung im Meldewesen zu ermöglichen, müssen sich alle im Meldewesen beteiligten Stellen auf eine bestimmte Art der Nutzung von OSCI-Transport einigen. Insbesondere müssen *Diensteanbieter*, also zum Beispiel Meldebehörden, die den Service der "elektronischen Rückmeldung" anbieten, sich mit den potenziellen Klienten absprechen. So wird in dem Abschnitt „Konformitätskatalog“ von [OSCI Transport 2002] ausgeführt:

Softwaresysteme für Intermediäre müssen alle in dieser Spezifikation definierten Auftragstypen in der angegebenen Version unterstützen. Softwaresysteme für Benutzer und Dienstanbieter brauchen nur Unterstützung für diejenigen Auftragstypen zu bieten, die sie für ihren speziellen Einsatzzweck benötigen.

Dieses Dokument beschreibt, auf welche Weise OSCI-Transport im Meldewesen zu nutzen ist.

F.1.2 Bezug zum Deutschen Verwaltungsdienstverzeichnis (DVDV)

Das Deutsche Verwaltungsdienstverzeichnis (DVDV) wurde vom KoopA-ADV als wichtige Komponente einer E-Government Infrastruktur beauftragt. Es ist generisch entworfen und steht in einer ersten Ausbaustufe seit dem 01.01.2007 zunächst für die Dienste "Rückmeldung" und "Fortschreibung" im Meldewesen zur Verfügung. Ein schrittweiser Ausbau ist geplant. Es werden im Folgenden Festlegungen getroffen, die auf den jetzigen Status des DVDV und die derzeit vorhandenen technischen Möglichkeiten abgestimmt sind.

Das DVDV ist ein Verzeichnis der öffentlichen Verwaltung, in dem Behörden Informationen zu angebotenen Dienstimplementierungen publizieren können. Die Publikation für OSCI-XMeld Dienste ist für Meldebehörden verbindlich. Die Informationen zu den Diensten beinhalten primär technische Parameter, die zur Nutzung der Dienste zwingend erforderlich sind wie Netzwerkadressen und zu verwendende

öffentliche Zertifikate. Darüber hinaus sind im DVDV mit Hilfe einer XML-basierten Spezifikationssprache für Netzwerkdienste — Web Service Description Language (WSDL) — aber auch Festlegungen zu Signaturniveau, Erfordernis der Verschlüsselung oder Struktur der Inhaltsdaten formal beschrieben.

Mit Hilfe der WSDL werden alle veröffentlichten Dienste hinsichtlich ihrer Protokollsyntax formal und präzise spezifiziert. Für OSCI-Transport sind Spracherweiterungen der WSDL definiert, die den besonderen Belangen des Protokolls wie z.B. die Struktur der Transport-Inhaltsdatencontainern Rechnung tragen. Sämtliche in diesem Dokument festgelegten Regelungen (siehe [Tabelle F-2 auf Seite 915](#)) sind in der WSDL-Beschreibung abbildbar. Im XMeld-Kontext relevante Beschreibungselemente sind:

1. URL (Protokoll, IP-Adresse/Domainname, Port-Nummer, Pfad) des Intermediärs
2. ggf. URL des Empfängers (bei passiven Empfänger-Szenarien)
3. Verschlüsselungs- und Signatur-Zertifikat des Intermediärs
4. Erfordernis und Niveau der Signatur auf Transportebene
5. Erfordernis der Verschlüsselung auf Transportebene
6. Angabe der OSCI-Transport-Kommunikationstypen (one-way-passive, request/response etc.)
7. Schemata der Inhaltsdaten
8. Struktur der Inhaltsdatencontainer
9. Erfordernis und Niveau von Signaturen der Inhaltsdaten(-Teile)
10. Erfordernis von Verschlüsselung der Inhaltsdaten(-Teile)
11. zur Verschlüsselung von Inhaltsdaten (innerhalb von Aufträgen) benötigte Zertifikate
12. zur Prüfung von Signaturen von Inhaltsdaten in Auftragsantworten benötigte Zertifikate

WSDL folgt dem allgemeinen informationstechnologischen Verständnis von Diensten (Services); d.h. ein Dienst ist eine Sammlung von fachlich zusammenhängenden Operationen eines Kommunikationsobjektes. Im Kontext OSCI-XMeld entspricht eine Operation der Entgegennahme einer konkreten OSCI-XMeld Nachricht. Ein Dienst resp. dessen Dienstbeschreibung gruppiert demzufolge fachlich zusammenhängende Nachrichten (z.B. XMeld-Rückmeldung die Nachrichten 0200 ... 0205). Eine Strukturierung der Nachrichten/Operationen analog den in OSCI-XMeld spezifizierten Situationen (Anmeldung, Rückmeldung, Fortschreibung etc.) ist gerade vor dem Hintergrund nicht zeitgleicher Einführung und unterschiedlicher Kommunikationspartner sinnvoll.

F.1.3 Grundlegende Festlegungen

Zur Gewährleistung einer verlässlichen Datenübertragung werden grundsätzliche Festlegungen gemäß Tabelle F-1 getroffen. Dabei wird in der Regelung Nr. 2 der Begriff der *“DVDV-unterstützte Dienste”* eingeführt. Dieser Begriff bedarf einer Erläuterung: Die Aufnahme neuer elektronischer Dienste in das DVDV erfolgt in einem kontrollierten Prozess durch Abstimmung zwischen Fachministerkonferenzen und dem KoopA-ADV. Als *“DVDV-unterstützten Dienst”* bezeichnen wir im Folgenden einen elektronischen Dienst, dessen Aufnahme in das DVDV im Rahmen dieses kontrollierten Prozesses positiv entschieden worden ist. Für das Meldewesen wurden als erstes die Dienste *“Rückmeldung”* und *“Fortschreibung”* in das DVDV aufgenommen.

Tabelle F-1: Grundlegende Festlegungen für die Datenübermittlung im Meldewesen

Nr.	Mechanismus	Regelung
1	Nutzung von Zertifikaten	Bei jeglicher, auf OSCI-Transport basierenden Datenübermittlung im Meldewesen <i>müssen</i> alle beteiligten Kommunikationspartner Zertifikate nutzen, die von der TESTA-CA herausgegebenen worden und zum Zeitpunkt ihrer Anwendung gültig – also speziell nicht abgelaufen und nicht gesperrt – sind ¹ .
	Durch diese Regelung wird sichergestellt, dass sämtliche Zertifikate einer <i>public key infrastructure</i> entstammen, die durch die öffentliche Verwaltung organisiert, betrieben und kontrolliert wird. Die explizite Erwähnung <i>aller</i> Kommunikationspartner macht deutlich, dass sich obige Anforderung nicht nur auf die beteiligten DV Fachverfahren, sondern auch auf die OSCI-Transport Intermediäre bezieht.	

Nr.	Mechanismus	Regelung
2	Bezug von Daten aus dem DVDV	Die an der Datenübermittlung im Meldewesen beteiligten Stellen müssen gewährleisten, dass für alle <i>DVDV-unterstützten Dienste</i> die für eine Datenübermittlung benötigten, technischen Kommunikationsparameter <i>unmittelbar</i> aus dem Deutschen Verwaltungsdienstverzeichnis (DVDV) entstammen.
	Für die Sicherheit und Funktionalität der Datenübermittlung ist es zwingend erforderlich, dass die technischen Kommunikationsparameter, die für den Aufbau einer auf OSCI-Transport basierenden Verbindung benötigt werden, weder verfälscht noch veraltet sind. Diese Anforderung könnte nicht gewährleistet werden, wenn die Daten aus Systemen Dritter bezogen würden, deren Organisation und Betrieb nicht der Kontrolle der öffentlichen Verwaltung unterliegen.	
3	OSCI-Transport	Es ist OSCI-Transport in der Version 1.2 zu nutzen.
	Die OSCI-Leitstelle hat im Auftrag der öffentlichen Verwaltung „OSCI-Transport 2.0“ entwickelt. Während einer Übergangs- und Migrationsphase könne beide Versionen parallel existieren. Durch diese Regelung soll sichergestellt werden, dass im Meldewesen die Umstellung geplant und unter Bezug auf dieses Transportprofil erfolgt.	

1. Nähere Informationen sind im Internet erhältlich unter <http://www.bsi.de/fachthem/verwpki/index.htm>

F.2 Datenübermittlung für Nachrichten gemäß § 17 MRRG

Datenübermittlungen im Zusammenhang mit § 17 MRRG sind die *Rückmeldung* inklusive der *Auswertung der Rückmeldung* sowie die *Fortschreibungen der Melderegister*. Sie werden in OSCI-XMeld durch Nachrichten der 02xx und 00xx Gruppen realisiert.

Für alle Nachrichten gemäß § 17 MRRG gilt:

- Datenübertragungen erfolgen zwischen den Meldebehörden unmittelbar oder über Vermittlungsstellen. Es handelt sich also um einen Geschäftsvorfall mit *geschlossener Benutzergruppe*, der eine Authentisierung erforderlich macht.
- § 17 Abs. 1 Satz 2 macht eine Datenübermittlung *„unverzüglich, spätestens jedoch drei Werktage nach der Anmeldung durch Datenübertragung“* erforderlich. Es wird auf § 8 Abs. 2 Satz 2 verwiesen: *„Dabei ist zu gewährleisten, dass dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit getroffen werden, die insbesondere die Vertraulichkeit und die Unversehrtheit der im Melderegister gespeicherten und an den Betroffenen übermittelten Daten gewährleisten“*.
- Die 1. BMeldDÜV schreibt in § 2 Abs. 2 Satz 2 vor: *„Die zu übermittelnden Daten sind mit einer fortgeschrittenen elektronischen Signatur nach § 2 Nr. 2 des Signaturgesetzes zu versehen und zu verschlüsseln“*.

Daher wird für alle OSCI-XMeld Nachrichten gemäß § 17 MRRG verbindlich festgelegt:

Tabelle F-2: Festlegungen für Datenübermittlungen gemäß § 17 MRRG

Nr.	Mechanismus	Regelung
1	Signatur der Inhaltsdaten	Die Inhaltsdaten müssen signiert werden. Als Hash-Algorithmus ist ausschließlich SHA-256 zu verwenden. Das Signaturzertifikat muss von der TESTA-CA ausgestellt und zum Zeitpunkt der Signaturerstellung gültig sein.

Nr.	Mechanismus	Regelung
	<p><i>Erläuterung:</i> Die Signatur der Inhaltsdaten dient der Authentisierung des Autors (nur Meldebehörden bzw. Vermittlungsstellen sind berechtigt, Nachrichten gemäß § 17 MRRG zu versenden). Gleichzeitig wird die Integrität der Nachrichten (Schutz vor unberechtigter Manipulation) sichergestellt. Es ist die Signatur der Organisationseinheit zu nutzen, welche die Inhaltsdaten erstellt (keine Signatur einer Person). Unter Bezug auf § 2 Abs. 2 Satz 1 der 1. BMeldDÜV dürfen Vermittlungsstellen im Auftrag ihrer Mandanten (Meldebehörden) mit dem Zertifikat der Vermittlungsstelle signieren. Die ausschließliche Verwendung von SHA-256 als Hashalgorithmus dient einer einheitlichen Regelung aller auf OSCI-Transport basierenden Kommunikation.</p>	
2	Verschlüsselung der Inhaltsdaten	Die Inhaltsdaten der Nachricht müssen verschlüsselt werden. Der hierzu zu verwendende öffentliche Schlüssel des Empfängers ist dem im DVDV hinterlegten Zertifikat der TESTA-CA zu entnehmen. Ist ein solches Zertifikat nicht vorhanden oder nicht gültig, dann darf keine Datenübermittlung stattfinden, da die geforderte Sicherheit der Datenübermittlung nicht gewährleistet werden kann.
	<p><i>Erläuterung:</i> Die <i>Vertraulichkeit</i> der Inhaltsdaten ist durch Ende-zu-Ende Verschlüsselung sicherzustellen. Unter Bezug auf § 2 Abs. 2 Satz 1 der 1. BMeldDÜV bezieht sich die <i>Ende-zu-Ende Verschlüsselung</i> ggfs. nur auf die OSCI-Transport Verbindung von / zu Vermittlungsstellen. In diesen Fällen sind die geforderten Sicherheitsmechanismen zwischen Vermittlungsstelle und Meldebehörde durch andere Maßnahmen sicherzustellen.</p>	
3	Signatur der Nutzungsdaten	Die Nutzungsdaten können signiert werden.
	Hinsichtlich des zu nutzenden Zertifikates und des zu nutzenden Hash-Algorithmus gelten die Regelungen der Nummer 1 entsprechend.	
4	Verschlüsselung der Nutzungsdaten	Die Nutzungsdaten müssen verschlüsselt werden.
	Hinsichtlich des zu nutzenden öffentlichen Schlüssels gelten die Regelungen der Nummer 2 entsprechend.	
5	Kommunikationsszenario	Jeder Diensteanbieter im Bereich des § 17 MRRG (also jede Meldebehörde bzw. die von ihr beauftragte Vermittlungsstelle) muss alle hier relevanten Operationen eines Dienstes <i>one-way-active</i> im Sinne von [OSCI-Transport 2002] anbieten.
	<p><i>Erläuterung:</i> Nachrichten an eine Meldebehörde werden in dem Postfach der adressierten Meldebehörde auf einen OSCI Intermediär zwischengespeichert. Sie müssen von der adressierten Meldebehörde <i>aktiv</i> abgeholt werden. Dadurch werden insbesondere die Meldebehörden entlastet, die mit der derzeitigen DV-Ausstattung keinen 24h / 365 Tage Betrieb gewährleisten können. Die Beschränkung auf genau einen Kommunikationstyp soll die Komplexität des Gesamtsystems insbesondere in der Einführungsphase reduzieren. Denn alternative Kommunikationstypen bei der Dienstimplementierung setzen eine höhere Flexibilität bei den Dienstnutzern voraus, die dann eine weitergehende Interpretation der DVDV-Informationen (WSDL-Dokumente) vornehmen und abhängig davon unterschiedliche Auftragsnachrichten konstruieren müssten. Zu späteren Zeitpunkten und für andere OSCI-XMeld-Situationen ist die Erweiterung auf andere und ggf. auch optionale Kommunikationstypen zu prüfen.</p>	
6	Technische Übertragung auf Netzebene	Jeder Diensteanbieter im Bereich des § 17 MRRG muss für alle hier relevanten Dienste das Protokoll " <i>http</i> " unterstützen. Als Port-Nummer muss 80 oder 8080 verwendet werden.

Nr.	Mechanismus	Regelung
		<p><i>Erläuterung:</i> Die "OSCI-Transport Bibliothek" des KoopA-ADV unterstützt <i>http</i> in der zum Download bereitstehenden Versionen. Andere Protokolle wären (über das definierte Interface) erst zu programmieren. Alle uns bekannten Intermediärs-Produkte unterstützen <i>http</i>.</p> <p><i>http</i> kann problemlos sowohl über das Internet, als auch über die sicheren Verwaltungsnetze genutzt werden.</p> <p>Um die Verträglichkeit zu bestehenden Netzwerk-Policies bei Dienstnutzern und -anbietern zu erleichtern, wird eine Beschränkung auf die alternativen IP-Port-Nummern 80 und 8080 verbindlich festgelegt.</p>
7	Transportstruktur	<p>Jede OSCI-XMeld-Nachricht gemäß § 17 MRRG muss als einziger Inhalt (Content) innerhalb eines Inhaltsdatencontainers übertragen werden. Die OSCI-XMeld-Nachricht darf nicht als Anhang (Attachment) oder in Form verschachtelter Inhaltscontainer versandt werden.</p> <p>Dieser XMeld-Container muss zur einfacheren Identifizierung eine definierte Ref. -ID mit dem Text "XMELD_DATA" besitzen.</p> <p>Der XMeld-Container muss im obersten ContentContainer liegen. Es gibt innerhalb der Nachricht keine weiteren Container mit einer OSCI-XMeld Nachricht als Inhalt.</p> <p>Es kann aber weitere Container geben innerhalb der Nachricht geben, die andere Inhalte transportieren.</p> <p><i>Erläuterung:</i> Um eine problemlose automatisierte Verarbeitung auf Seiten des Empfängers zu gewährleisten, muss die Transportstruktur zur Übermittlung der OSCI-XMeld-Nachricht einheitlich und eindeutig sein.</p> <p>Im Interesse einer möglichst einfachen Transportstruktur wird festgelegt, dass es pro OSCI-Transport Nachricht genau einen <i>ContentContainer</i> mit einer einzigen OSCI-XMeld Nachricht geben darf. Es dürfen aber weitere <i>ContentContainer</i> als Bestandteil der Nachricht mittransportiert werden.</p> <p>Darüber hinaus wird festgelegt, dass die OSCI-XMeld-Nachricht als Inhalt innerhalb des Inhaltscontainers, nicht aber als Attachment oder in Form geschachtelter Container zu übermitteln ist.</p>
8	Verschlüsselungsalgorithmus	Für die Verschlüsselung der Inhalts- und Nutzungsdaten ist ausschließlich der Algorithmus AES-256 zu verwenden

F.3 Datenübermittlung an das Bundeszentralamt für Steuern gemäß § 139 AO

Bezüglich der Datenübermittlungen zwischen Meldebehörden und dem Bundeszentralamt für Steuern gemäß §139 AO gelten die Festlegungen gemäß Tabelle F-2.

F.4 Datenübermittlung an die Datenstelle der Rentenversicherungsträger

Bezüglich der Datenübermittlungen zwischen Meldebehörden und der Datenstelle der Rentenversicherungsträger gemäß 2. BMeldDÜV gelten die Festlegungen gemäß Tabelle F-2.

F.5 Datenübermittlung an das Bundesamt für Justiz

Bezüglich der Datenübermittlungen zwischen Meldebehörden und dem Bundesamt für Justiz gemäß der 2. BMeldDÜV gelten die Festlegungen gemäß Tabelle F-2.

F.6 Datenübermittlung an das Bundesverwaltungsamt

Bezüglich der Datenübermittlungen zwischen Meldebehörden und dem Bundesverwaltungsamt gemäß der § 34 StAG in Verbindung mit § 5d 2. BMeldDÜV gelten die Festlegungen gemäß Tabelle F-2.

F.7 Datenübermittlung im Zusammenhang mit dem vorausgefüllten Meldeschein zwischen Meldebeörden

Bei der Datenübermittlung im Zusammenhang mit dem vorausgefüllten Meldeschein zwischen Meldebeörden handelt es sich um eine synchrone Kommunikation. Aus diesem Grund sind die Regelungen in [Abschnitt F.2 auf Seite 915](#) nicht passend, obwohl die Nachrichten im Zusammenhang mit dem vorausgefüllten Meldeschein ebenfalls Nachrichten gemäß § 17 MRRG sind.

Datenbermittlungen in diesem Sinne sind ausschließlich die Nachrichten anmeldung.datenanforderung.0300 und anmeldung.datenbereitstellung.0301.

Datenübermittlung in diesem Sinne sind Nachrichten gemäß § 17 MRRG und daher gilt:

- a. Datenübertragungen erfolgen zwischen den Meldebehörden unmittelbar oder über Vermittlungsstellen. Es handelt sich also um einen Geschäftsvorfall mit *geschlossener Benutzergruppe*, der eine Authentisierung erforderlich macht.
- b. § 17 Abs. 1 Satz 2 macht eine Datenübermittlung *„unverzüglich, spätestens jedoch drei Werktage nach der Anmeldung durch Datenübertragung“* erforderlich. Es wird auf § 8 Abs. 2 Satz 2 verwiesen: *„Dabei ist zu gewährleisten, dass dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit getroffen werden, die insbesondere die Vertraulichkeit und die Unversehrtheit der im Melderegister gespeicherten und an den Betroffenen übermittelten Daten gewährleisten“*.
- c. Die 1. BMeldDÜV schreibt in § 2 Abs. 2 Satz 2 vor: *„Die zu übermittelnden Daten sind mit einer fortgeschrittenen elektronischen Signatur nach § 2 Nr. 2 des Signaturgesetzes zu versehen und zu verschlüsseln“*.

Daher wird für alle OSCI–XMeld Nachrichten gemäß § 17 MRRG verbindlich festgelegt:

Tabelle F-3: Festlegungen für Datenübermittlungen gemäß § 17 MRRG

Nr.	Mechanismus	Regelung
1	Signatur der Inhaltsdaten	Die Inhaltsdaten müssen signiert werden. Als Hash-Algorithmus ist ausschließlich SHA-256 zu verwenden. Das Signaturzertifikat muss von der TESTA-CA ausgestellt und zum Zeitpunkt der Signaturerstellung gültig sein.
	<i>Erläuterung:</i> Die Signatur der Inhaltsdaten dient der Authentisierung des Autors (nur Meldebehörden bzw. Vermittlungsstellen sind berechtigt, Nachrichten gemäß § 17 MRRG zu versenden). Gleichzeitig wird die Integrität der Nachrichten (Schutz vor unberechtigter Manipulation) sichergestellt. Es ist die Signatur der Organisationseinheit zu nutzen, welche die Inhaltsdaten erstellt (keine Signatur einer Person). Unter Bezug auf § 2 Abs. 2 Satz 1 der 1. BMeldDÜV dürfen Vermittlungsstellen im Auftrag ihrer Mandanten (Meldebehörden) mit dem Zertifikat der Vermittlungsstelle signieren. Die ausschließliche Verwendung von SHA-256 als Hashalgorithmus dient einer einheitlichen Regelung aller auf OSCI–Transport basierenden Kommunikation.	
2	Verschlüsselung der Inhaltsdaten	Die Inhaltsdaten der Nachricht müssen verschlüsselt werden. Der hierzu zu verwendende öffentliche Schlüssel des Empfängers ist dem im DVDV hinterlegten Zertifikat der TESTA-CA zu entnehmen. Ist ein solches Zertifikat nicht vorhanden oder nicht gültig, dann darf keine Datenübermittlung stattfinden, da die geforderte Sicherheit der Datenübermittlung nicht gewährleistet werden kann.
	<i>Erläuterung:</i> Die <i>Vertraulichkeit</i> der Inhaltsdaten ist durch Ende-zu-Ende Verschlüsselung sicherzustellen. Unter Bezug auf § 2 Abs. 2 Satz 1 der 1. BMeldDÜV bezieht sich die <i>Ende-zu-Ende Verschlüsselung</i> ggfs. nur auf die OSCI-Transport Verbindung von / zu Vermittlungsstellen. In diesen Fällen sind die geforderten Sicherheitsmechanismen zwischen Vermittlungsstelle und Meldebehörde durch andere Maßnahmen sicherzustellen.	
3	Signatur der Nutzungsdaten	Die Nutzungsdaten können signiert werden.

Nr.	Mechanismus	Regelung
	Hinsichtlich des zu nutzenden Zertifikates und des zu nutzenden Hash-Algorithmus gelten die Regelungen der Nummer 1 entsprechend.	
4	Verschlüsselung der Nutzungsdaten	Die Nutzungsdaten müssen verschlüsselt werden.
	Hinsichtlich des zu nutzenden öffentlichen Schlüssels gelten die Regelungen der Nummer 2 entsprechend.	
5	Kommunikationsszenario	Jeder Diensteanbieter im Bereich des § 17 MRRG (also jede Meldebehörde bzw. die von ihr beauftragte Vermittlungsstelle) muss alle hier relevanten Operationen eines Dienstes <i>Request-Response (ohne Protokollierung)</i> im Sinne von [OSCI-Transport 2002] anbieten.
6	Technische Übertragung auf Netzebene	Jeder Diensteanbieter im Bereich des § 17 MRRG muss für alle hier relevanten Dienste das Protokoll " <i>http</i> " unterstützen. Als Port-Nummer muss 80 oder 8080 verwendet werden.
	<p><i>Erläuterung:</i> Die "<i>OSCI-Transport Bibliothek</i>" des KoopA-ADV unterstützt <i>http</i> in der zum Download bereitstehenden Versionen. Andere Protokolle wären (über das definierte Interface) erst zu programmieren. Alle uns bekannten Intermediärs-Produkte unterstützen <i>http</i>. <i>http</i> kann problemlos sowohl über das Internet, als auch über die sicheren Verwaltungsnetze genutzt werden.</p> <p>Um die Verträglichkeit zu bestehenden Netzwerk-Policies bei Dienstnutzern und -anbietern zu erleichtern, wird eine Beschränkung auf die alternativen IP-Port-Nummern 80 und 8080 verbindlich festgelegt.</p>	
7	Transportstruktur	<p>Jede OSCI-XMeld-Nachricht gemäß § 17 MRRG muss als einziger Inhalt (Content) innerhalb eines Inhaltsdatencontainers übertragen werden. Die OSCI-XMeld-Nachricht darf nicht als Anhang (Attachment) oder in Form verschachtelter Inhaltscontainer versandt werden.</p> <p>Dieser XMeld-Container muss zur einfacheren Identifizierung eine definierte Ref. -ID mit dem Text "<i>XMELD_DATA</i>" besitzen.</p> <p>Der XMeld-Container muss im obersten ContentContainer liegen. Es gibt innerhalb der Nachricht keine weiteren Container mit einer OSCI-XMeld Nachricht als Inhalt.</p> <p>Es kann aber weitere Container geben innerhalb der Nachricht geben, die andere Inhalte transportieren.</p> <p><i>Erläuterung:</i> Um eine problemlose automatisierte Verarbeitung auf Seiten des Empfängers zu gewährleisten, muss die Transportstruktur zur Übermittlung der OSCI-XMeld-Nachricht einheitlich und eindeutig sein.</p> <p>Im Interesse einer möglichst einfachen Transportstruktur wird festgelegt, dass es pro OSCI-Transport Nachricht genau einen <i>ContentContainer</i> mit einer einzigen OSCI-XMeld Nachricht geben darf. Es dürfen aber weitere <i>ContentContainer</i> als Bestandteil der Nachricht mittransportiert werden.</p> <p>Darüber hinaus wird festgelegt, dass die OSCI-XMeld-Nachricht als Inhalt innerhalb des Inhaltscontainers, nicht aber als Attachment oder in Form geschachtelter Container zu übermitteln ist.</p>
8	Verschlüsselungsalgorithmus	Für die Verschlüsselung der Inhalts- und Nutzungsdaten ist ausschließlich der Algorithmus AES-256 zu verwenden

F.8 Versionshistorie

In diesem Abschnitt beschreiben wir die Versionshistorie des Anhangs *OSCI-Transport-Profil für OSCI-XMeld*.

Versionshistorie			
Version vom		Status	Inhalt
	28.02.06	Entwurf	Initiale Version
	22.03.06	Entwurf	In der Tabelle F-2 wurde bezüglich der Verschlüsselung der Inhaltsdaten der Hinweis auf unterschiedliche Rollen der Kommunikationspartner entfernt. (Hinweis Hr. Kremser, BZBW)
1.3.1	23.04.06	Final	Aufgrund der Stellungnahme Niedersachsens wurde in der Tabelle 1 die Ziffer 7 (<i>Transportstruktur</i>) dahingehend geändert, dass zwar weiterhin jede OSCI-Transport Nachricht nur eine OSCI-XMeld Nachricht enthalten darf, die als einziger Inhalt in einem Containers enthalten sein muss. Es darf darüber hinaus aber in der Nachricht weitere Container geben, die andere Daten enthalten können. Dieser Version wurde innerhalb der <i>Projektgruppe Meldewesen</i> im Umlaufverfahren abgestimmt und Bestandteil von OSCI-XMeld 1.3.1.
OSCI-XMeld 1.3.2		Final	In der Tabelle 1 wurde die Ziffer 7 (<i>Transportstruktur</i>) dahingehend ergänzt, dass am Ende des ersten Absatzes der Text <i>“Die OSCI-XMeld-Nachricht darf nicht als Anhang (Attachement) oder in Form verschachtelter Inhaltscontainer versandt werden.”</i> eingefügt worden ist. Die Tabelle F-1 auf Seite 914 mit den grundlegenden Regelungen für den Bezug von Daten aus dem DVDV und der PKI-I Verwaltung wurde neu aufgenommen.

Versionshistorie		
Version vom	Status	Inhalt
OSCI-XMeld 1.4	Final	<p>CR 43-2 Der Hash-Algorithmus SHA-256 wurde verpflichtend für alle Signaturen (Inhalts- und Nutzungsdaten) vorgeschrieben (siehe Tabelle F-2 auf Seite 915 Nr. 1 und Nr. 4).</p> <p>CR 43-3 Gemäß eines Beschlusses der PG Meldewesen vom 18./19.06.08. wurde die alte Festlegung aller Kommunikationspartner auf ein Zertifikat der PKI-1-Verwaltung verschärft: Es sind zukünftig ausschließlich Zertifikate der TESTA-CA zu verwenden (siehe Tabelle F-1 auf Seite 914 Nr. 1 und Tabelle F-2 auf Seite 915 Nr. 1 und Nr. 2).</p> <p>CR 43-4 Für die Verschlüsselung der Inhalts- und Nutzungsdaten wurde der Algorithmus AES-256 verbindlich vorgeschrieben.</p> <p>CR 6-3 Da eine Datenübermittlung zwischen Meldebehörden und der Deutschen Post AG ab dem 01.11.2009 nicht mehr länger erfolgt, wurde der entsprechende Abschnitt aus dem Transportprofil entfernt.</p> <p>CR 33-33 Für die Datenübermittlung im Zusammenhang mit dem vorausgefüllten Meldeschein zwischen Meldebehörden wurde Abschnitt F.7 auf Seite 918 aufgenommen.</p> <p>CR 4-10 Für die Datenübermittlung an das Bundesverwaltungsamt wurde Abschnitt F.6 auf Seite 917 aufgenommen.</p> <p>Bundesamt für Justiz Für die Datenübermittlung an das Bundesamt für Justiz wurde Abschnitt F.5 auf Seite 917 aufgenommen.</p> <p>OSCI-Transport 2.0 Um einen geplanten Umstieg von OSCI-Transport 1.2 auf OSCI-Transport 2.0 zu ermöglichen, wurde eine Regelung aufgenommen, die die Verwendung von OSCI-Transport 1.2 vorschreibt.</p>