OSCI-Transport 1.2

– Entwurfsprinzipien, Sicherheitsziele und -mechanismen –

Status: FINAL

OSCI Leitstelle

Bremen, den 6. Juni 2002

Inhaltsverzeichnis

OSCI-Transport 1.2

– Entwurfsprinzipien, Sicherheitsziele und -mechanismen –

OSCI (Online Service Computer Interface) ist ein Nachrichten-Standard für den E-Government-Bereich, der zurzeit in einem breit getragenen, gemeinsamen Diskussions- und Kooperationsprozess von Bund, Ländern und Kommunen unter Federführung der Bremer „OSCI-Leitstelle“ im Auftrag des KoopA-ADV entwickelt wird.

OSCI wurde mit dem Ziel entworfen, die vollständige und rechtsverbindliche Abwicklung von Transaktionen im Bereich des E-Government über den Betriebsweg Internet und auf Basis der digitalen Signatur zu ermöglichen. Dies erfordert eine umfangreiche Interoperabilität sowohl auf der Ebene der Inhaltsdaten, als auch auf der Ebene der Transport- und Sicherheitsfunktionen. Zusätzlich sind die Regularien und Reglementierungen zu berücksichtigen, denen der Bereich des öffentlichen Handels unterworfen ist. Die hieraus erwachsenden Anforderungen haben die Entwurfsentscheidungen von OSCI bestimmt.

Auf diese Anforderungen wird in diesem Dokument als Teil der Spezifikation, Version 1.2 ausführlich eingegangen. Zunächst werden generelle Entwurfsprinzipien sowie Anforderungen beschrieben, die aus Sicht des E-Government an OSCI gestellt werden. Anschließend werden Sicherheitsrisiken sowohl externer als auch interner Art in Form von Szenarien dargestellt. Hieraus werden Sicherheitsziele abgeleitet, die bei der Konzeption des OSCI-Standards berücksichtigt worden sind. In Anlehnung an die formale OSCI-Spezifikation werden die Komponenten einer OSCI-Nachricht und Sicherheitsmechanismen von OSCI vorgestellt. Es wird ausführlich darauf eingegangen, welche Sicherheitsziele durch die jeweiligen OSCI-Sicherheitsmechanismen unterstützt werden.

Nicht eingegangen wird auf Sicherheitsmechanismen außerhalb von OSCI. Maßnahmen zur Server- und Gebäudesicherheit sowie Firewallsysteme und ihre Filteregeln werden in einem gesonderten OSCI-Betriebskonzept ausführlich dargestellt.

1. Entwurfsprinzipien

Der Geltungsbereich von OSCI umfasst sowohl die fachlich/inhaltliche Ebene als auch die Ebene der Transport- und Sicherheitsfunktionen inklusive der digitalen Signatur.

In dem nunmehr in der Version 1.2 vorliegenden Teil A der OSCI-Spezifikation, auch OSCI-Transport 1.2 genannt, werden weitgehend nur Transport- und Sicherheitsfunktionen von OSCI behandelt, während die fachlich/inhaltlichen Anforderungen an OSCI in einem Teil B der Spezifikation zusammengefasst werden.

Die OSCI-Transportspezifikation liegt seit November 2000 in der Version 1.0 vor. Auf dieser Basis wurden bislang in der Freien Hansestadt Bremen Produkte implementiert und wichtige Erfahrungen im praktischen Einsatz gewonnen. U.a. haben diese Erfahrungen zu weiteren Anforderungen geführt, die sich nunmehr in der vorliegenden Folgeversion 1.2 wiederfinden.

OSCI-Transport 1.2 beschreibt das Datenaustauschformat für eine automatisiert nutzbare Schnittstelle für die sichere Übertragung von Nachrichten auf Basis der digitalen Signatur über das Internet oder andere vergleichbare Kommunikationsmedien.

OSCI dient der sicheren und signaturgesetzkonformen Übertragung von Daten eines Geschäftsvorfalles zwischen zwei Kommunikationspartnern. Diese Kommunikation wird unterstützt durch einen Intermediär, der über den Transport der Nachrichten hinaus zusätzliche Dienstleistungen per OSCI anbietet. Nicht über OSCI-Transport wird die Zahlbarmachung der Dienstleistung abgewickelt.

Der Transport von OSCI-Nachrichten orientiert sich sowohl an dem Vorbild elektronische Post als auch an Online-Transaktionen mit folgenden Gestaltungsprinzipien:

- Interoperabilität:
  OSCI ist für beliebige Geschäftsprozesse einsetzbar und ermöglicht signaturgesetzkonforme elektronische Unterschriften und die sichere Übertragung elektronischer Dokumente zwischen öffentlicher Verwaltung bzw. Unternehmen und ihren Kunden. Durch die Offenlegung des OSCI-Protokolls ist zum einen die Entwicklung OSCI-konformer Produkte sichergestellt, zum anderen wird hierdurch auch eine permanente Fortentwicklung bzw. Verbesserung des Standards garantiert.
- Skalierbarkeit:
  OSCI ermöglicht die Anwendung unterschiedlicher Sicherheitsniveaus. Beispielsweise können zur Unterstützung einfacher Geschäftsvorfälle fortgeschrittene Signaturen eingesetzt werden, während für Vorgänge mit Schriftformerfordernis qualifizierte bzw. akkreditierte elektronische Signaturen zur Anwendung kommen können. OSCI erfordert jedoch nicht zwingend den Einsatz von elektronischen Signaturen.
- Anwendungsunabhängigkeit:
  OSCI ist universell und vollständig unabhängig von der jeweiligen Anwendung einsetzbar, die online unterstützt wird.
- Plattformunabhängigkeit bzw. Portabilität:
  OSCI verwendet XML-Technologie und ist betriebssystemunabhängig.
- Offene Benutzergruppe:
  OSCI verfügt über keine explizite Benutzerverwaltung, sondern arbeitet mit einer offenen Benutzergruppe. Die Benutzer müssen vorab gegenüber der Fachanwendung nicht explizit als Online-Nutzer registriert sein. Da aber die OSCI-interne Adressierung anhand von Chiffrierzertifikaten erfolgt, ist der Besitz eines solchen Zertifikats für die vollständige Nutzung der von OSCI-Transport zur Verfügung gestellten Dienste erforderlich. Insbe-

sondere muss der Empfänger ein Chiffrierzertifikat besitzen. In sehr eingeschränktem Maße kann ein Sender auch ohne Chiffrierzertifikat Nachrichten per OSCI versenden.

- Unabhängigkeit vom Intermediär:
  Durch die strikte Trennung von Inhaltsdaten einerseits und Nutzungsdaten andererseits erhält der Intermediär keinerlei Kenntnis von den Daten des Geschäftsvorfalls. Der Intermediär ist als klassischer Spediteur tätig.
- Signaturgesetzkonformität:
  Die per OSCI übermittelten Dokumente können signaturgesetzkonform elektronisch unterschrieben werden, d.h. der Autor eines Dokuments kann beim Signieren zwischen fortgeschrittener, qualifizierter und akkreditierter elektronischer Signatur gemäß Signaturgesetz wählen (siehe Anlage zu rechtlichen Anforderungen an den elektronischen Geschäftsverkehr).

Entscheidenden Einfluss auf das Sicherheitskonzept von OSCI hat dabei die durchgängig umgesetzte Plattformunabhängigkeit. Hiermit verbunden ist das Ziel, Sicherheit möglichst weitgehend auf OSCI-Ebene umzusetzen, möglichst unabhängig vom Sicherheitsstandard anderer Komponenten, beispielsweise des Trägernetzes sowie der lokal beim Bürger eingesetzten Betriebssysteme und Browser.

Plattformunabhängigkeit bedeutet jedoch nicht, dass keinerlei Anforderungen an die OSCI-Transportarchitektur, insbesondere an den Betrieb der OSCI-Plattform und des Backend-Systems des Anwenders gestellt werden. Ein ordnungsgemäßer Betrieb der jeweiligen Anlagen ist vielmehr Grundvoraussetzung für OSCI und wird daher in einem gesonderten Betriebskonzept dargestellt.

2. OSCI-Kommunikationsmodell

2.1 OSCI-Rollenmodell

OSCI berücksichtigt sowohl die Kommunikation der öffentlichen Verwaltung mit ihren Kunden (Bürger und Unternehmen) durch das Anbieten und die Abwicklung von Verwaltungsdienstleistungen über das Internet als auch die interne Kommunikation zwischen unterschiedlichen Verwaltungen bzw. Verwaltungsbereichen. Aufgrund der vielfältigen Anwendungsszenarien in diesem Umfeld ergeben sich vielfältige funktionale und sicherheitstechnischen Anforderungen, die zu einem sehr spezifischen Kommunikations- bzw. Rollenmodell bei OSCI führen.

Grundlage jeglicher elektronischer Kommunikation ist die Übermittlung von Daten von einem Sender zu einem Empfänger. Dabei ist jedoch zu berücksichtigen, dass im Allgemeinen mehrere Personen durch gemeinschaftliches Verfassen bzw. durch Genehmigung und Abzeichnung für den Inhalt von Nachrichten verantwortlich sind, während der eigentliche Versand einer Nachricht nur von einer Person veranlasst werden kann. Beide Rollen sind mit unterschiedlichen Verantwortlichkeiten verbunden. So liegt die Inhaltsverantwortung bei den Autoren, während der Sender für den fristgerechten Versand an den richtigen Empfänger verantwortlich ist. Analog ist auch auf der Empfangsseite zwischen dem Empfänger als demjenigen, der eine Nachricht entgegennimmt und den Lesern einer Nachricht, die die eigentlichen Inhalte verarbeiten, zu unterscheiden. Für die Unterscheidung dieser Rollen und der damit verbundenen Verantwortlichkeiten differenziert OSCI zwischen den sogenannten Inhaltsdaten (vgl. 3.3) und den Nutzdaten (vgl. 3.2) einer OSCI Nachricht.

Insgesamt wird bei OSCI folgendes Rollenmodell zu Grunde gelegt (vgl. Abb.1):

1. Die Inhaltsdaten können von mehr als einer Instanz erzeugt werden. Jede Instanz, die Inhaltsdaten generiert, wird als Autor einer OSCI-Nachricht bezeichnet. Die Autoren können bei Bedarf die Inhaltsdaten elektronisch signieren und verschlüsseln. Das Signieren und Verschlüsseln der Inhaltsdaten erfolgt damit bei OSCI optional.

   Das Signieren von Inhaltsdaten von mehreren Autoren setzt bei OSCI-Transport 1.2 eine Mehrfachsignatur der Inhaltsdaten voraus.

2. Die Personen, für die die Inhaltsdaten verfasst sind, werden als Leser einer OSCI-Nachricht bezeichnet. Dabei können mehrere Leser pro Nachricht existieren. Die Autoren verschlüsseln bei Bedarf die Inhaltsdaten daher so, dass sie nur durch die Leser entschlüsselt werden können.

   Das optionale Verschlüsseln von Inhaltsdaten für mehrere Leser setzt bei OSCI-Transport 1.2 eine Mehrfachverschlüsselung der Inhaltsdaten voraus.

3. Die Inhaltsdaten werden vor dem Versand um Nutzungsdaten (vgl. Kap. 3.2) ergänzt, die sich u.a. aus Absender- und Empfängerzertifikaten sowie Zeitstempel zusammensetzen. Die Nutzungsdaten können ebenfalls optional elektronisch signiert und verschlüsselt werden. Der Inhaber des Signaturzertifikats der Nutzungsdaten wird als Sender bezeichnet.

   OSCI-Nachrichten haben genau einen Sender; folglich gibt es bei OSCI-Transport 1.2 keine Mehrfachsignatur der Nutzungsdaten.

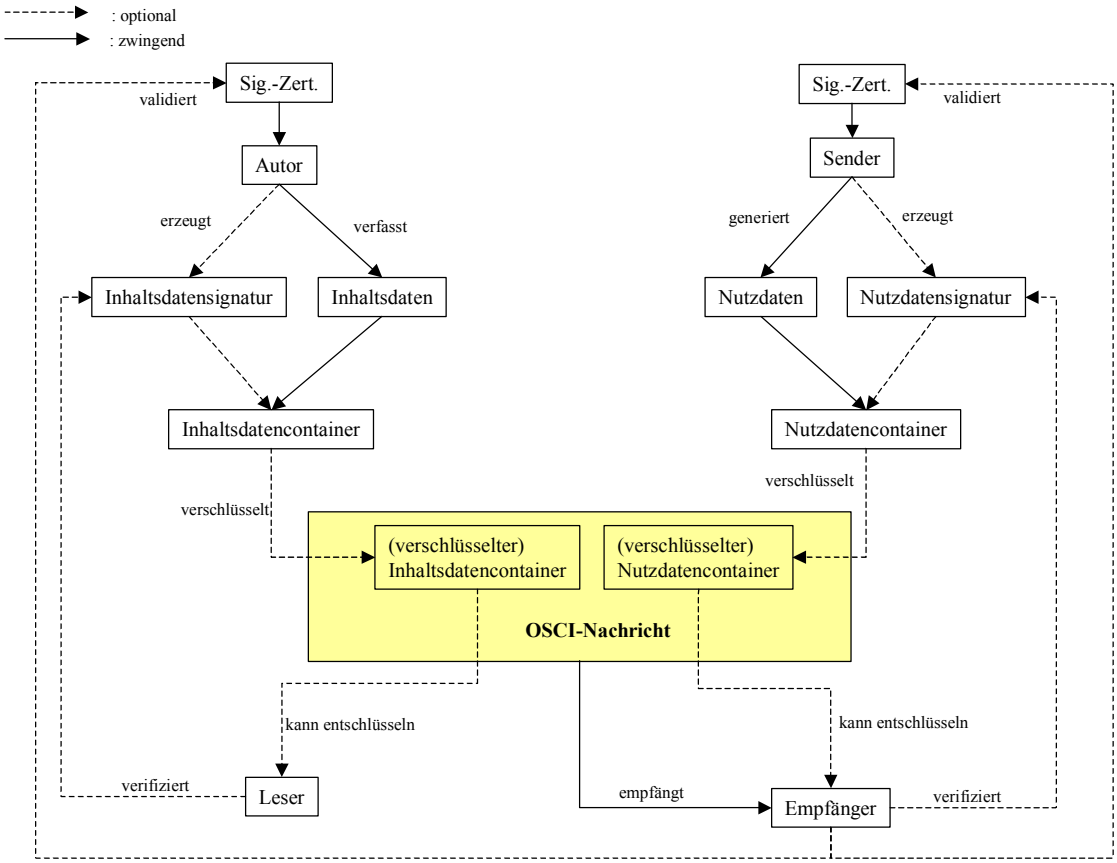


Abb. 1: OSCI-Rollenmodell

4. Die Instanz, an die die OSCI-Nachricht gerichtet ist, wird Empfänger bezeichnet. Jede OSCI-Nachricht ist genau an einen Empfänger gerichtet.

   Folglich gibt es bei OSCI-Transport 1.2 keine Mehrfachverschlüsselung der Nutzungsdaten.

2.2 Synchrone bzw. asynchrone Datenübertragung

Der Kontakt des Bürgers mit der Verwaltung erfolgt im Rahmen des E-Government auf vielfältige Weise. Bürgerfreundlichkeit und eine höhere Effizienz sind in der Regel nur erreichbar, wenn eine synchrone Kommunikationsphase einen Dialog zwischen der Client-Komponente beim Bürger und der Server-Komponente auf Seiten der öffentlichen Verwaltung erlaubt. Durch den Zugriff auf vorhandene Datenbestände in den Fachverfahren der öffentlichen Verwaltung wird die Fehlerrate der Kundennachrichten verringert, die Qualität erhöht und die Attraktivität der angebotenen Dienstleistungen der Verwaltung gesteigert. Am Ende dieses Dialogs steht dann in der Regel ein vom Kunden elektronisch signiertes Formular, dessen strukturierte Inhaltsdaten an die Verwaltung gesendet werden. Die Antwort hierauf ist wiederum Gegenstand eines neuen Dialogs, in dem die Rollen getauscht werden.

Andererseits sind viele Prozesse des E-Government so beschaffen, dass sie durch eine Nachricht des Kunden zwar angestoßen werden, aber nicht vollständig maschinell bearbeitbar sind. Häufig sind manuelle Tätigkeiten von Sachbearbeitern auf Seiten der öffentlichen Verwaltung erforderlich. Dabei muss auch die Rückrichtung von der Verwaltung zum Bürger bedacht werden. In diesem Fall kann aber nicht vorausgesetzt werden, dass der Nachrichtenempfänger stets online erreichbar ist. OSCI unterstützt daher nicht nur den synchronen, sondern auch den asynchronen Austausch von OSCI Nachrichten.

2.3 Der Intermediär

Die Existenz einer zentralen Vermittlungsstelle, dem sogenannten Intermediär, der Mehrwertdienste erbringen kann, ohne die Vertraulichkeit der Inhaltsdaten zu gefährden, ist bei der Kommunikation mittels OSCI charakteristisch und wird u.a. durch den Bedarf an einer asynchronen Kommunikation begründet. Dem Kommunikationspartner wird hierbei eine OSCI-Nachricht zugestellt, ohne vorauszusetzen, dass Sender und Empfänger zeitgleich online sind (vgl. Abb.2).

Für eine asynchrone Kommunikation führt der Intermediär für potentielle Empfänger Postkörbe, in denen OSCI-Nachrichten zwischengespeichert werden. Ein Zugriff auf den Postkorb zwecks Abholung von Nachrichten bedarf der vorherigen Authentisierung im Rahmen eines Abholauftrags. Dieser löst im Falle der positiven Authentisierung einen Zustellauftrag im Rahmen einer synchronen Kommunikation zwischen Intermediär und berechtigten Empfänger aus. Der Besitz eines Postfaches bedarf keiner vorgeschalteten Registrierung gegenüber dem Fachverfahren, sondern ist an den Besitz eines X.509v3 Zertifikats geknüpft und wird durch den Eingang der ersten Nachricht beim Intermediär automatisch eröffnet. Durch die Bindung der Postkörbe an das Zertifikat ist eine eindeutige und zweifelsfreie Authentisierung des berechtigten Empfängers gewährleistet.

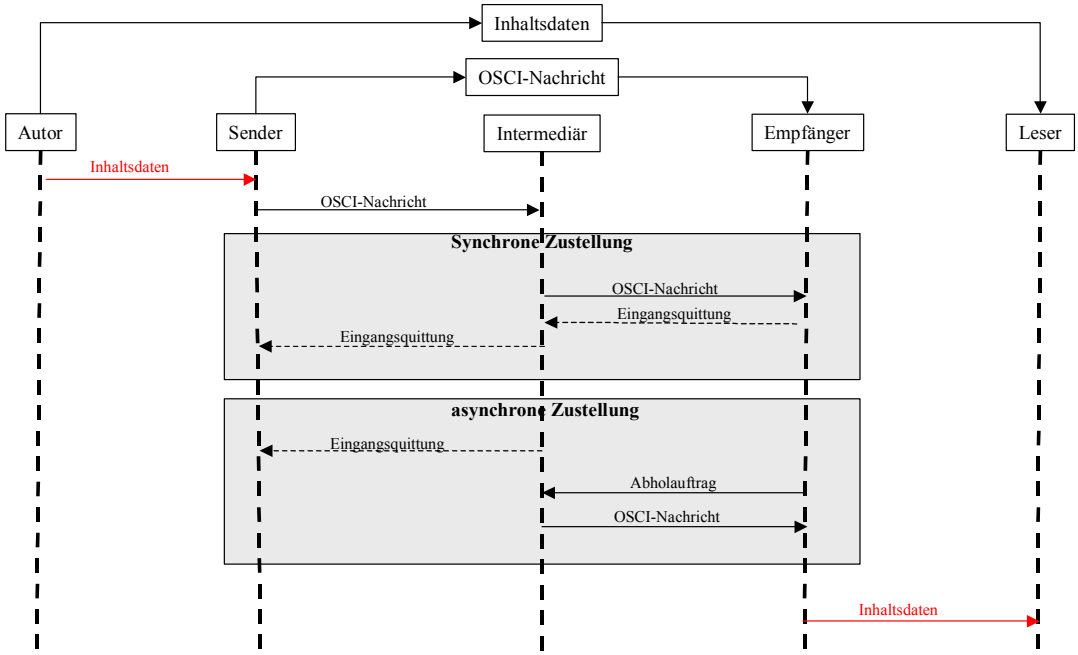


Abb. 2: Synchrone bzw. asynchrone Zustellung

Ein wesentlicher Aspekt bei der Kommunikation mittels OSCI ist die Gewährleistung der Rechtsverbindlichkeit und der Vertraulichkeit. Geschäftsprozesse, deren Abwicklung über den neuen Vertriebsweg Internet zwingend die elektronische Signatur voraussetzt, bilden einen wichtigen Teilbereich des E-Government. Die Erfüllung dieser Anforderungen basiert in OSCI auf den Techniken der Public-Key-Kryptographie. Aus diesem Grund enthalten die Datenstrukturen der Auftragsebene Signatur- und Chiffrierzertifikate. Die Gültigkeit dieser Zertifikate muss verifiziert werden, um Aussagen hinsichtlich der Authentizität treffen zu können. Die PKI nach SigG ermöglicht dem Empfänger einer signierten Nachricht diese Prüfung. Die hierfür erforderlichen Techniken sind jedoch sehr aufwändig, wartungsintensiv und teuer. Der OSCI-Intermediär ist die ideale Stelle, um solche Mechanismen zu zentralisieren. Die Ergebnisse aller vom Intermediär vorgenommenen Prüfungen der Zertifikate werden in einem Prüfprotokoll vermerkt. Es ist Aufgabe des Nachrichtenempfängers, anhand der Prüfergebnisse über den Umgang mit der Nachricht zu entscheiden.

Grundsätzlich sollte jeder potenzielle Empfänger von OSCI Nachrichten in der Lage sein, Zertifikats- und Signaturprüfungen auch selbst vorzunehmen. Die Nutzung einer OSCI Infrastruktur darf nicht dazu führen, dass Empfänger der OSCI-Nachrichten sich auf die Prüfprotokolle des Intermediärs verlassen müssen. Es ist aber ein pragmatischer Ansatz, mit dem Intermediär eine zentrale Stelle vorzusehen, an die solche Prüfaufgaben delegiert werden kann. Aufgrund der in OSCI vorgenommenen Trennung von Inhalts- und Nutzungsdaten ist dies ohne Verletzung der datenschutzrechtlich gebotenen Vertraulichkeit der Inhaltsdaten möglich. Die durch die Zentralisierung dieser Techniken eintretenden ökonomischen Vorteile sind gerade für kleine Kommunen oftmals die Voraussetzung, den Vertriebsweg Internet schrittweise aufbauen zu können.

Als zusätzliche Dienstleistung unterzieht der Intermediär alle eingehenden Nachrichten einer Strukturprüfung gegen die OSCI-Schemadefinition und bietet Mechanismen für die Etablierung und Sicherung eines Dialogkontextes. Aufgrund der von ihm wahrgenommenen Aufgaben tritt der Intermediär sowohl in der Rolle des Empfängers als auch in der Rolle des Senders auf.

Für den Intermediär gelten hinsichtlich dieses Funktionsumfangs folgende Sicherheitsaspekte:

- Vertraulichkeit der Inhaltsdaten gegenüber dem Intermediär:
  Sofern die Inhaltsdaten des jeweiligen Geschäftsvorfalles verschlüsselt werden, ist auch der Intermediär mit detaillierten Kenntnissen über das Verschlüsselungsverfahren nicht in der Lage, die Inhaltsdaten zu entschlüsseln und somit zu lesen.
- Offenbarung der Nutzungsdaten gegenüber dem Intermediär:
  Der Intermediär muss in der Lage sein, die für den Nachrichtentransport benötigten Nutzungsdaten zu identifizieren.

Die Rolle des Intermediärs muss bei OSCI nicht zwingend von einer dritten Instanz wahrgenommen werden; diese Funktionalität kann auch einem Fachverfahren direkt vorgeschaltet werden. In diesem Fall sind zusätzliche Sicherheitsvorkehrungen bei der Stelle umzusetzen, die beide Rollen wahrnimmt (vgl. Abb.3).

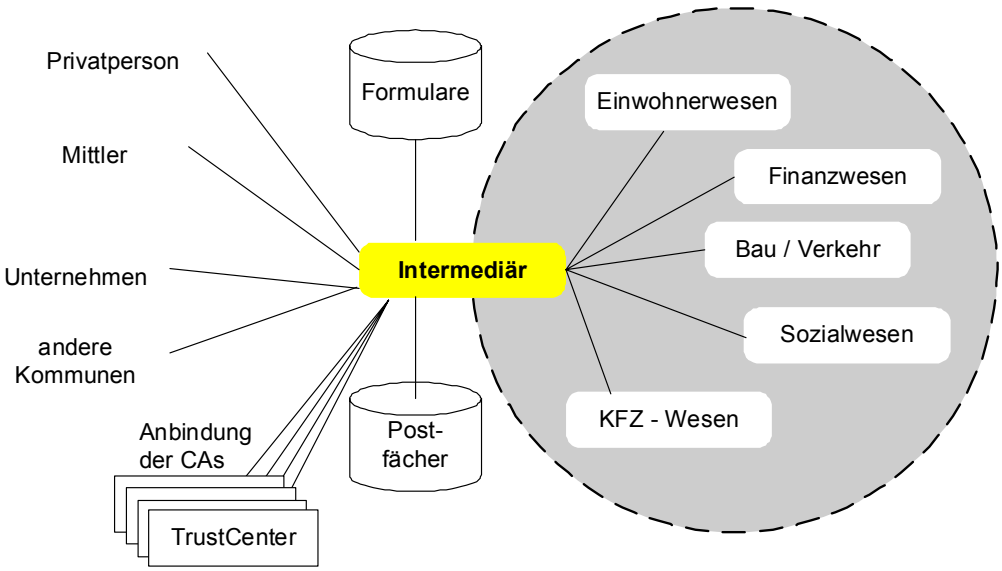


Abb.3: Rolle des Intermediärs

3. Komponenten einer OSCI-Nachricht

Die Kommunikation zwischen Bürger, Intermediär und Verwaltung erfolgt in OSCI über strukturierte Objekte auf drei Ebenen:

- Nachrichtenebene:
  Auf dieser Ebene befinden sich Daten, die den Datentransport zwischen zwei direkt miteinander kommunizierenden OSCI-Teilnehmern steuern. Da diese Daten unverschlüsselt und unsigniert übertragen werden, werden sie in diesem Anforderungsdokument nicht weiter betrachtet.
- Auftragsebene:
  Auf dieser Ebene werden Nutzungsdaten verarbeitet, die für die Adressierung benötigt werden. Die Nutzungsdaten erlauben die Nachvollziehbarkeit der Übermittlung und enthalten Elemente, um einen Dialog steuern und überwachen zu können.
- Geschäftsvorfallebene:
  Auf dieser Ebene werden Inhaltsdaten verarbeitet, die die eigentlichen Geschäftsvorfälle repräsentieren. Der Intermediär greift auf diese Daten nicht zu.

Um diese Trennung insgesamt zu ermöglichen, realisiert OSCI das Prinzip des geschachtelten Umschlags. Ein äußerer Umschlag enthält die Nutzungsdaten, die für die technische Zustellung und die Erbringung der Mehrwertdienste benötigt werden. Die Inhaltsdaten werden separat in einen eigenen Umschlag verpackt, der seinerseits, optional verschlüsselt und signiert, wieder Bestandteil des äußeren Umschlags wird. Dabei ist es durchaus möglich, dass es mehrere Umschläge mit Inhaltsdaten gibt. Der äußere Umschlag kann nun unabhängig von dem inneren Umschlag verschlüsselt und signiert werden, sofern dies erforderlich ist.

Die Strukturierung der Nutzungs- und Inhaltsdaten erfolgt auf Basis der Extensible Markup Language (XML) entsprechend der Spezifikation des W3C. XML ermöglicht als offen zugänglicher und von einzelnen Herstellern unabhängiger Standard den strukturierten Austausch elektronischer Dokumente und schafft dadurch die Grundlage für eine Datenverarbeitung ohne Medienbrüche. Eine gültige OSCI-Nachricht stellt somit ein wohlgeformtes XML Dokument dar. Sowohl Inhaltsdaten als auch Nutzungsdaten werden per XML Encryption bzw. XML Signature verschlüsselt bzw. signiert.

Die Strukturierung der Inhaltsdaten erfolgt anhand einer dem jeweiligen Anwendungsbereich zugrunde liegenden XML-Schema-Datei. Die Definition dieser Schemata erfolgt unabhängig von der Strukturdefinition der Nutzdaten und ist Gegenstand des Teil B der OSCI- Spezifikation.

Neben den Methoden des eigentlichen XML-Standards nutzt OSCI die Mechanismen des auf XML basierenden Transportprotokolls SOAP (Simple Objekt Access Protokoll) für die Strukturierung der Nutzungsdaten; eine OSCI-Nachricht bildet ein sogenanntes SOAP-Message-Package. Bei SOAP handelt es sich um ein leistungsfähiges, leicht zu verwendendes Netzwerkprotokoll für stark verteilte Architekturen. SOAP basiert auf standardisierten und herstellerunabhängigen Technologien von XML und schafft damit die Basis für eine breite Interoperabilität.

Alternativ ist auch die Übermittlung von Inhaltsdaten in Fremdformaten per OSCI möglich; dies erfolgt in den Attachments.

3.1 SOAP-Struktur

SOAP ist ein auf XML basierendes Protokoll, um den Austausch strukturierter Nachrichten zwischen verteilten Systemen zu ermöglichen. Eine OSCI-SOAP-Message besteht aus einem SOAP-Header, einem SOAP-Body und ggf. zugehörigen Attachments. Gemäß der SOAP-Spezifikation enthält der Header der Nachricht diejenigen Angaben, die im Laufe der Zustellung aktualisiert und verarbeitet werden, während der SOAP-Body die in diesem Sinne statischen Elemente der Nachricht enthält.

Der SOAP-Body dient in erster Linie der Aufnahme der XML-strukturierten Inhaltsdaten (vgl. Kap. 3.3). Diese können auf mehrere sogenannte Inhaltsdatencontainer aufgeteilt werden, die optional und unabhängig voneinander verschlüsselt und signiert werden können. Die Signatur ist Bestandteil der jeweiligen unverschlüsselten Inhaltsdatencontainer. Die für eine Entschlüsselung der Inhaltsdatencontainer notwendigen Verschlüsselungsinformationen sind ebenfalls im Body in Form sogenannter Verschlüsselungsköpfe untergebracht.

Die Übermittlung von Inhaltsdaten in Fremdformaten erfolgt in Form von Attachments zur SOAP-Nachricht, die im Body der Nachricht referenziert werden. Die Attachments werden unabhängig verschlüsselt und signiert, wobei der Hashwert der Signatur ebenfalls im Body der SOAP-Nachricht eingestellt wird. Neben den eigentlichen Inhaltsdaten enthält der SOAP-Body die Chiffrier- und Signierzertifikate der Autoren und des Senders, sowie die Chiffrierzertifikate des Empfängers und der Leser.

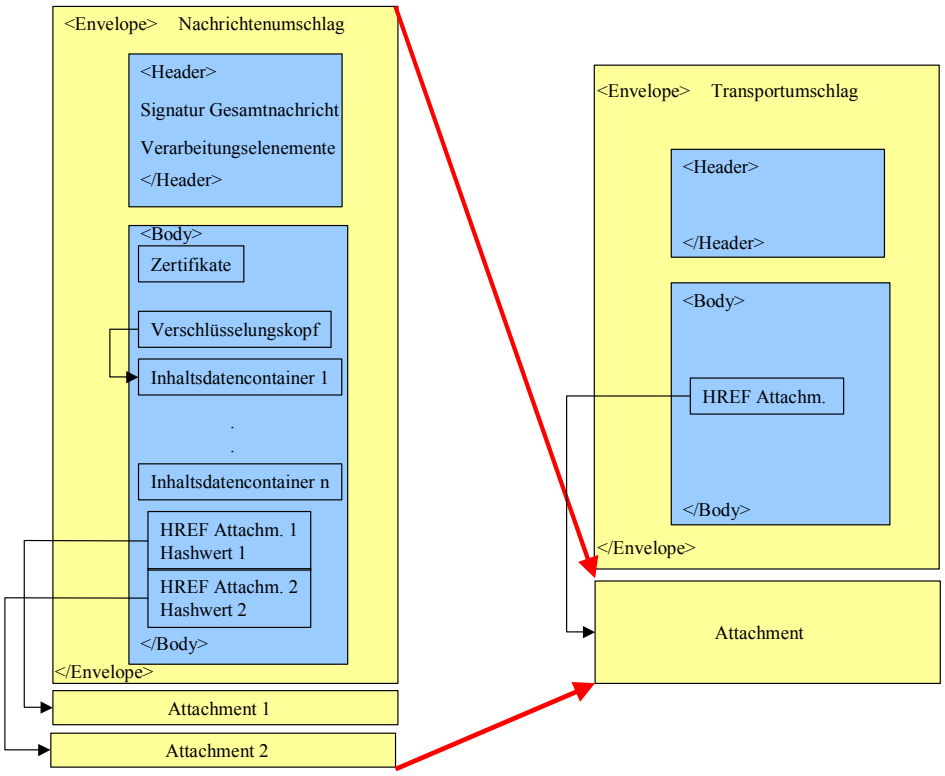


Abb. 4: Aufbau eines OSCI-Pakets

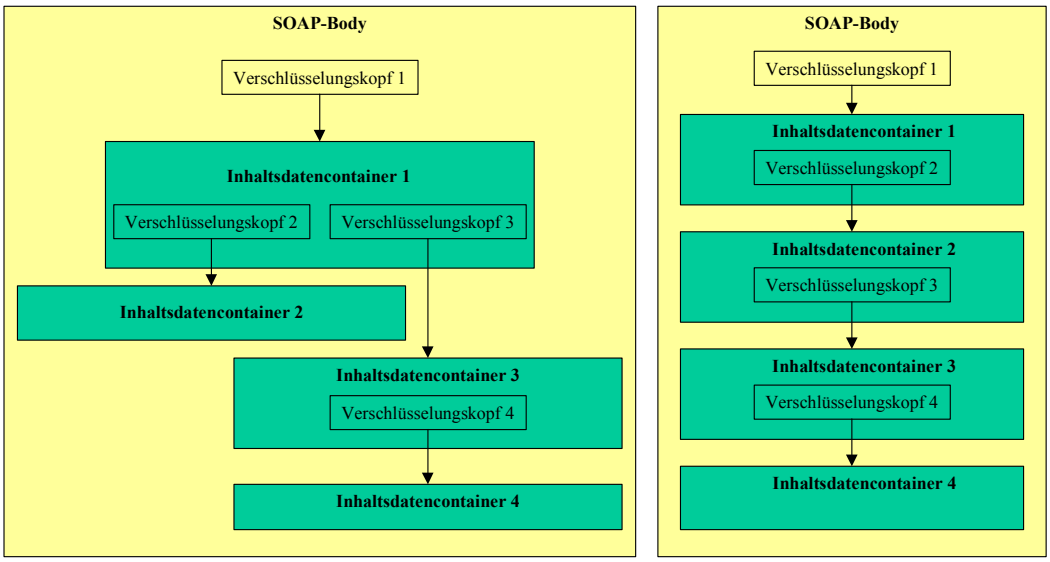
Die Header-Elemente der SOAP-Nachricht beinhalten diejenigen Nutzungsdaten (vgl. Kap. 3.2), die während der Zustellung der Nachricht verarbeitet werden müssen. Neben einer optionalen Signatur über die gesamte Nachricht sind dies ein Laufzettel für die Dokumentation bzw. Steuerung der Zustellung sowie Datenobjekte für die Überwachung des gesamten Dialogkontextes. Weiterhin ist das Signier- und Chiffrierzertifikat des Intermediärs Bestandteil eines Headerelements, da diese erst im Verlauf der Nachrichtenzustellung Bestandteil der Nachricht werden.

Die konkrete Ausprägung der SOAP-Struktur wird durch den jeweiligen Nachrichtentyp bestimmt. Die Übertragung einer auf diese Weise strukturierten OSCI-Nachricht erfolgt als Attachment einer weiteren SOAP-Nachricht, die die ursprüngliche Nachricht in ihrem Body referenziert. Die für eine optionale Verschlüsselung der Nutzungsdaten notwendigen Informationen werden im Header dieser zweiten SOAP-Nachricht aufgeführt.

Durch dieses Prinzip des doppelten Umschlags wird der Zusammenhalt der gesamten OSCI-Nachricht auf dem Transportweg gewährleistet und somit die Möglichkeit ausgeschlossen, unbemerkt Attachments zu entfernen bzw. auszutauschen. Zudem erlaubt diese Vorgehensweise die Transportverschlüsselung auch mit anderen Techniken wie beispielsweise SSL oder S/MIME, anstatt einen doppelten Transportumschlag zu realisieren.

Während es pro OSCI-Nachricht stets nur einen Nutzungsdatencontainer gibt, der im Laufe der Zustellung einer Nachricht durch die Empfänger ergänzt und aktualisiert wird, kann es durchaus mehrere Inhaltsdatencontainer geben, die unabhängig voneinander verschlüsselt und signiert werden können. Auf diese Weise ist es möglich, unterschiedliche Leser zu adressieren, indem ein Inhaltsdatencontainer so verschlüsselt wird, dass nur der berechtigte Leser in der Lage ist, diesen zu entschlüsseln.

Mehrere Inhaltsdatencontainer zu verwenden, hat den weiteren Vorteil, dass die Verarbeitung der übermittelten Inhaltsdaten auf Anwendungsebene regelgesteuert erfolgen kann, d.h. es werden hinsichtlich der Verarbeitung der Inhaltsdaten Regeln verfasst. Ein solcher Regelcontainer enthält dann auch die für die Entschlüsselung der weiteren Container benötigten Verschlüsselungsköpfe. Auf diese Weise ist gewährleistet, dass der Leser die anderen Inhaltsdatencontainer erst nach Kenntnisnahme der Regeln lesen kann. Durch dieses Prinzip lässt sich auch eine Reihenfolge für die Abarbeitung der verschiedenen Inhaltsdatencontainer abbilden.



3.2 Nutzungsdaten

Die Nutzungsdaten bestehen im Wesentlichen aus dem Laufzettel sowie dem mit dem Transport der OSCI-Nachricht verbundenen Auftrag für den Intermediär; sie werden ggf. ergänzt um die Signatur der Nutzungsdaten.

Die Nutzungsdaten können vom Absender mit dem öffentlichen Schlüssel des Intermediärs verschlüsselt werden, so dass die Daten vertraulich transportiert werden, jedoch durch den Intermediär verarbeitet werden können. Die Antwort des Intermediärs (beispielsweise eine Eingangsquittung) auf den Auftrag wird dagegen mit dem öffentlichen Schlüssel des Auftragsabsenders verschlüsselt; der entsprechende Schlüssel befindet sich auf dem Laufzettel des Auftrags und kann vom Intermediär genutzt werden.

Der Laufzettel, der die Verarbeitung der Zustellungsaufträge steuert, ist während der gesamten Verarbeitung durch den Intermediär die zentrale Datenstruktur und präzisiert die Zustellungsmodalitäten und die Inanspruchnahme seiner Mehrwertdienste. Der Laufzettel wird vom Intermediär erstellt und im weiteren Verlauf der Zustellung durch diesen aktualisiert. Der Laufzettel dient als Quittung für die Kommunikationsbeteiligten und kann von diesen beim Intermediär angefordert werden. Die Zustellung eines Laufzettels kann optional vom Intermediär signiert werden.

Die Nutzungsdaten umfassen somit alle für den Transport notwendigen Datenfelder:

- das Signier- und Chiffrier-Zertifikat der Autoren,
- das Signier- und Chiffrier-Zertifikat des Senders,
- das Chiffrier-Zertifikat der Leser,
- das Chiffrier-Zertifikat des Empfängers,
- Betreff-Informationen,
- Zeitstempel,
- Bearbeitungsstatus des Zustellungsauftrags
- Elemente zur Dialogsteuerung.

Die Zertifikate stellen die Zuordnung zwischen Schlüsselpaar und Absender bzw. Empfänger her und basieren auf dem Standard X.509, Version 3. Die Zertifikate bestehen u.a. aus folgenden Elementen:

- Name des Zertifikatinhabers,
- Gültigkeitszeitraum des Zertifikats,
- ausgebende Zertifizierungsstelle einschließlich Verweis auf Signierzertifikat,
- öffentlicher Schlüssel aus dem Schlüsselpaar,
- Zertifikattyp,
- Signatur der Zertifizierungsstelle,
- Seriennummer des Zertifikats.

Durch Anreicherung wird der Laufzettel zum Transportprotokoll. Er kann bei Bedarf sowohl dem Absender als auch dem Empfänger als Quittung ausgehändigt werden. Für den Intermediär dient der Laufzettel als Nachweis des Transports einschließlich Zustellzeitpunkt.

Zeitstempel dienen dem allgemeinen Nachweis, dass bestimmte Daten zu einem bestimmten Zeitpunkt einer Zeitstempeldienststelle vorgelegen haben. Gegenwärtig existiert zu die-

ser Thematik der vorläufige Internet-Standard [PKIX-TSP 00], der ein allgemeines Format für die Anfragen an Zeitstempeldienststellen und deren Antworten definiert[1].

Das Signaturgesetz schreibt zwar nicht vor, dass der Zeitpunkt der Signaturerstellung aus der Signatur ersichtlich sein muss; eine Signatur ist auch ohne Zeitstempel rechtskonform. Dennoch verwendet OSCI Zeitstempel, allerdings nicht im Signaturobjekt selbst, sondern in dem Laufzettel. OSCI stellt sicher, dass der Zeitpunkt der Signierung weitgehend identisch ist mit dem Zeitpunkt des Eintrags auf den Laufzettel durch den Intermediär. Auf dem Laufzettel werden folglich nicht das exakte Erstellungsdatum festgehalten, sondern das hiermit fast identische Eingangsdatum sowie das Übermittlungsdatum. OSCI-Transport 1.2 sieht auch die Verwendung von akkreditierten Zeitstempeln vor - dies sind Zeitstempel von akkreditierten Trust-Centern. Diese werden jedoch nur optional angeboten und sind nicht zwingend vorgeschrieben.

3.3 Inhaltsdaten

Die Inhaltsdaten setzen sich zusammen aus den eigentlichen Daten des Geschäftsvorfalls, ggf. ergänzt um die Signatur der Inhaltsdaten. Geschäftsvorfalldaten sind beispielsweise Aktenzeichen, Passwörter auf Anwendungsebene zur Authentisierung der Benutzer gegenüber dem Fachverfahren sowie der Auslöser des Geschäftsvorfalls.

Die Inhaltsdaten können bei Bedarf mit dem öffentlichen Schlüssel des Lesers bzw. der verschiedenen Leser verschlüsselt werden, so dass der Intermediär keine Kenntnis von diesen Daten erhalten kann. Die Daten können auf diese Weise lediglich von den Lesern entschlüsselt werden.

4. Sicherheitsrisiken

Die gesamte OSCI-Transportarchitektur unterliegt folgenden Grundgefährdungen:

- Verlust der Vertraulichkeit – d.h. die Gefahr, dass Unberechtigte Inhalts- und Nutzungsdaten zur Kenntnis nehmen,
- Verlust der Integrität – d.h. die Gefahr, dass Inhalts- und Nutzungsdaten auf dem Weg vom Autor oder Absender zum Empfänger während ihrer Übertragung verfälscht werden,
- Verlust der Authentizität – d.h. die Gefahr, dass Inhalts- und Nutzungsdaten nicht vom Urheber bzw. Autor oder Absender stammen,
- Abstreitbarkeit der Kommunikation und Autorenschaft – d.h. die Gefahr, dass die Autorenschaft, der Versand oder der Empfang von Inhalts- bzw. Nutzungsdaten bestritten wird,
- Verlust der Verfügbarkeit – d.h. die Gefahr, dass auf Inhalts- und Nutzungsdaten bzw. die OSCI-Plattform nicht, nicht vollständig oder nicht rechtzeitig zugegriffen werden kann.
- Verlust der Zurechenbarkeit – d.h. die Gefahr, dass Aktionen nicht (nachträglich) einer Person und einem Zeitpunkt zugeordnet werden können.

[1] Anfragen an Zeitstempeldienststellen können sowohl unsigniert als auch signiert erfolgen. In beiden Fällen enthalten die Anfragen sowohl den Hashalgorithmus als auch den Hashwert der digitalen Daten, für die ein Zeitstempel generiert werden soll. Signierte Zeitstempeldienstanfragen werden allerdings verschlüsselt übertragen. Antworten der Zeitstempeldienststellen werden stets signiert und verschlüsselt.

Dies sind abstrakte Begriffe, die in ihrer Allgemeinheit nicht ausreichen, die Risiken zu erfassen, der die OSCI-Transportarchitektur ausgesetzt ist. Aus ihnen müssen vielmehr konkrete Einzelrisiken für die jeweils betroffenen Module abgeleitet werden.

Ausführlich analysiert werden im Folgenden die Risiken, denen sowohl die OSCI-Plattform des Intermediärs, das Backend-System des Anwenders als auch die Client-Plattform eines der beiden Kommunikationspartners ausgesetzt sind. Bei allen Szenarien wird von einem unsicheren Transportnetz ausgegangen. Bei allen Szenarien wird jedoch nicht von einer Kompromittierung von Hard- oder Software des Senders oder Empfängers ausgegangen.

Die OSCI-Transportarchitektur ist insgesamt folgenden Sicherheitsrisiken ausgesetzt:

- **Arbeiten unter falscher Identität:**

  Eine falsche Identität kann auf Anwendungsebene durch Benutzung einer fremden Kennung vorgetäuscht werden, auf Netzwerkebene durch Manipulation der Netzadresse.

  Gelingt es, der OSCI-Plattform oder der Fachanwendung eine falsche Identität vorzuspiegeln, besteht die Gefahr, dass auf fremde Daten zugegriffen sowie sämtliche Privilegien des rechtmäßigen Benutzers übernommen werden können. Die falsche Identität kann durch zwei Methoden angenommen werden:

  1. Bereits bei der Benutzerauthentisierung wird – beispielsweise unter Verwendung eines abgelaufenen bzw. ungültigen Zertifikats – dem System ein falscher Benutzer vorgespiegelt. Dies kann beispielsweise auch durch Wiederverwenden von (verschlüsselten) OSCI-Nachrichten zu erreichen versucht werden (Replay-Attacken).
  2. Nach einer erfolgreichen Authentisierung wird die interne Repräsentation eines anderen Benutzers dauerhaft oder zur Durchführung einzelner Tätigkeiten angenommen. (Man-in-the-Middle-Attacken)

  Während die erste Methode die Kenntnis geheimer Information oder den Besitz privater Gegenstände voraussetzt und insofern von der eingesetzten Technik relativ unabhängig ist, beruht die zweite Methode auf der Ausnutzung technischer Schwächen des eingesetzten Systems, Informationen über eine erfolgreiche Authentisierung im Dialog fälschungssicher verwalten zu können.

  Eine Manipulation der Netzwerkadresse, sei es auf der Ebene der Übertragungs-, Netzwerk- oder Transportschicht, ist für den OSCI-Transport nicht relevant, sondern betrifft die Administration der OSCI-Plattform. Hierauf wird im OSCI-Betriebskonzept ausführlich eingegangen.

- **Erweitern von Zugriffsrechten:**

  Gelingt es, die festgelegten Zugriffsrechte zu erweitern, können personenbezogene Daten in unzulässiger Weise verarbeitet oder fremde Daten zur Kenntnis genommen werden. Neben der Möglichkeit, Rechte durch Arbeiten unter falscher Identität zu erweitern, kann versucht werden, unter der eigenen Identität zusätzliche Rechte zu gewinnen und zunächst nur temporär gewährte Rechteerweiterungen dauerhaft zu sichern.

  Dieses Risiko bezieht sich zum einen auf die Gefahr, dass sowohl Bürger mit gültigem Zertifikat als auch Außenstehende versuchen, den allgemein zugänglichen http-Server der OSCI-Plattform zu attackieren und erweiterte Rechte auf der Plattform zu erhalten. Zum anderen können Administratoren versuchen, ihre privilegierten Rechte missbräuchlich zu verwenden.

Bezüglich OSCI-Transport 1.2 sind Ressourcen zu betrachten, die von OSCI für einzelne Kommunikationspartner zur Verfügung gestellt werden, beispielsweise Postfächer.

- **Lesen von Inhaltsdaten:**

  Inhaltsdaten können während ihres Transports oder während ihrer Nutzung von Unbefugten mitgelesen werden. Dadurch können vertrauliche Informationen in unbefugte Hände gelangen. Das Mitlesen von Daten kann auf zweierlei Weise geschehen:

  1. Abhören von Geräten:
     Bildschirme, Tastaturen, Drucker und andere Geräte können aus gewisser Entfernung abgehört werden, wobei ihre kompromittierende Strahlung ausgewertet wird. Auf diese Weise können verarbeitete Daten oder Zugangsinformationen zur Kenntnis genommen werden. Der für ein elektronisches Abhören erforderliche Aufwand ist allerdings in der Regel relativ hoch.
  2. Abhören von Übertragungsmedien:
     Übertragungsmedien bergen das Risiko des unbefugten Mitlesens der Daten. Interne Mitarbeiter können auf broadcastorientierten Medien, die zur Übermittlung von Daten verschiedener Netzteilnehmer dienen, sämtliche übertragenen Daten zur Kenntnis nehmen. Externe können Strecken, die innerhalb von Gebäuden verlaufen oder diese verlassen, an beliebiger Stelle zwischen den Endpunkten abhören. Der dafür erforderliche Aufwand hängt wesentlich vom verwendeten Medium und dessen Verwendung ab. Besonders problematisch sind dabei die Fälle, bei denen das Mitlesen ohne merkliche Eingriffe geschieht und insofern nicht feststellbar ist.

- **Lesen von Nutzungsdaten:**

  Nicht nur Inhaltsdaten können während des Transports oder lokal von Unbefugten mitgelesen werden. Auch besteht die Gefahr, dass Nutzungsdaten ausgekundschaftet und wiederverwendet werden, um hierüber Zugriff auf geschützte Systemressourcen zu erhalten. Nutzungsdaten bestehen bei OSCI-Transport u.a. aus dem Absender- und Empfängerzertifikat, das auch zur Nichtabstreitbarkeit der Kommunikation dienen kann.

  Gelingt es, Nutzungsdaten in größerem Umfang zu ermitteln und zu analysieren, können Benutzerprofile erstellt und gegen die Interessen der Betroffenen ohne deren Kenntnis verwendet werden. Nutzungsdaten stehen dem Intermediär in umfangreicher Weise zur Verfügung.

- **Verändern von Inhaltsdaten:**

  Daten können lokal oder auf dem Transport vom Autor bzw. Absender zum Empfänger verändert werden, wenngleich das Verändern von Daten während des Transports umfangreiche Rechte auf das Transportsystem und entsprechende Kenntnisse hiervon voraussetzt.

- **Verändern von Nutzungsdaten:**

  Gelingt es, Nutzungsdaten zu verändern, können Kommunikationsvorgänge sowohl vom Autor bzw. Absender einer Nachricht als auch vom Empfänger abgestritten werden. Der Streitgegenstand kann sich auch auf den Zeitpunkt des Absendens einer Nachricht oder auf deren Zustellzeitpunkt beziehen.

  Rechte zum Verändern von Nutzungsdaten können auch dazu benutzt werden, die Spuren einer Manipulation der Inhaltsdaten zu verwischen, so dass diese unentdeckt bleibt.

- **Stören der Plattform:**

  Gelingt es, die OSCI-Plattform zu stören, kann die Dienstleitung nicht mehr in dem geforderten Umfang zur Verfügung gestellt werden. Dies kann bei termingebundenen Zustellaufträgen ein gravierendes Problem darstellen.

  Die OSCI-Plattform kann durch sogenannte Denial-of-Service-Attacken lahmgelegt werden. Dabei werden eine Vielzahl von Nachrichtenpaketen an einen Server geschickt, der unter der Überlast seine Arbeit einstellt bzw. keine Rückmeldungen mehr in der gewünschten Form abgeben kann.

Hinsichtlich der skizzierten Risiken wird im Folgenden zwischen Bürger mit gültigem Zertifikat, Verwaltung und Intermediär sowie allgemeinen Internetnutzern differenziert, wobei sich Bürger mit gültigem Zertifikat und allgemeine Internetnutzer durch die Art des Systemzugangs unterscheiden. Während allgemeine Internetnutzer in der Regel anonym versuchen können, ohne Zugriffsrechte Sicherheitslücken zu erkunden, sind Bürger zumindest im Besitz einer fortgeschrittenen Signatur und greifen hierüber nachträglich identifizierbar und rechtmäßig auf Teilmodule der OSCI-Plattform oder des Backendsystems zu.

Stellen Bürger mit Zertifikat bzw. allgemeine Internetnutzer bereits bei kleineren Sicherheitslücken ein ernstzunehmendes Risiko dar, da in diesem Fall jeder Zugriff auf fremde Daten einen gravierenden datenschutzrechtlichen Verstoß bedeuten würde, ist dies bei Mitarbeitern der Verwaltung und des Intermediärs nur bei sensiblen personenbezogenen Daten der Fall. Andererseits haben Betreiber eines Intermediärs in der Regel weit mehr Möglichkeiten, bestehende technische oder organisatorische Schwachstellen auszunutzen. Von welchen Personengruppen die jeweiligen Risiken ausgehen, beschreibt folgende Tabelle.

Personengruppe **Sicherheitsrisiken**	Bürger	Intermediär	Verwaltung	Internet-nutzer
Arbeiten unter falscher Identität	X	X	X	X
Erweitern von Rechten	X	X	X	
Lesen von Inhaltsdaten		X		X
Lesen von Nutzungsdaten				X
Verändern von Inhaltsdaten		X		X
Verändern von Nutzungsdaten				X
Stören der Plattform				X

5. Sicherheitsziele

Zur Reduzierung bzw. Vermeidung der in Kap. 4 formulierten Sicherheitsrisiken verfolgt OSCI zahlreiche Sicherheitsziele. Von OSCI-Transport 1.2 werden jedoch nicht alle der Risiken abgedeckt. Einige der Risiken erfordern einen sicheren Betrieb der OSCI-Plattform sowie einen sicheren Client-Kernel; die entsprechenden Maßnahmen hierzu werden im OSCI-Betriebskonzept beschrieben.

Die von OSCI-Transport 1.2 verfolgten Sicherheitsziele werden in Kap. 5.1 dargestellt; Kapitel 5.2 erörtert die von OSCI nicht betrachteten Ziele.

5.1 OSCI-Sicherheitsziele

Von OSCI-Transport 1.2 werden insgesamt fünf Sicherheitsziele verfolgt.

5.1.1 Vertraulichkeit

OSCI ermöglicht sowohl eine vertrauliche Übertragung der Inhaltsdaten als auch der Nutzungsdaten.

- Vertraulichkeit der Inhaltsdaten:
  OSCI stellt eine Verschlüsselung der Inhaltsdaten vom Absender zum Empfänger zur Verfügung und kann somit die Vertraulichkeit der Inhaltsdaten während der Übertragung sowie gegenüber dem Intermediär garantieren.
- Vertraulichkeit der Nutzungsdaten:
  Die Nutzungsdaten können auf der Strecke zwischen Sender und Intermediär sowie zwischen Intermediär und Empfänger verschlüsselt übertragen werden. Die Nutzungsdaten werden vom Intermediär gelesen und entsprechend ergänzt.

In Bezug auf die Vertraulichkeit der Inhalts- und Nutzungsdaten wird von OSCI die Schutzbedarfsklasse *gering* (keine Verschlüsselung) sowie *hoch bis sehr hoch* (Triple-DES/AES-Verschlüsselung) unterstützt, d. h. die Auswirkungen im Falle eines Verlustes der Vertraulichkeit können entweder vernachlässigt werden oder beträchtlich sein bzw. ein existentielles bedrohliches, katastrophales Ausmaß annehmen; der Ansehensverlust für die Verwaltung ist beträchtlich. Ein möglicher Missbrauch personenbezogener Daten hat ebenfalls erhebliche Auswirkungen auf die gesellschaftliche Stellung oder wirtschaftlichen Verhältnisse des Bürgers, ggf. bedeutet dies für den Betroffenen sogar den gesellschaftlichen oder wirtschaftlichen Ruin.

5.1.2 Integrität

OSCI garantiert sowohl eine integre bzw. manipulationssichere Übertragung der Inhaltsdaten als auch der Nutzungsdaten.

- Integrität der Inhaltsdaten:
  Die Inhaltsdaten werden von dem Autor bzw. den Autoren mit dessen bzw. deren Zertifikaten signiert. Verfälschungen werden ausschließlich vom Empfänger erkannt.
- Integrität der Nutzungsdaten:
  Die Nutzungsdaten werden von dem Sender mit dessen Zertifikat signiert. Verfälschungen werden vom Intermediär bzw. vom Empfänger erkannt.

In Bezug auf die Integrität der Inhalts- und Nutzungsdaten wird von OSCI die Schutzbedarfsklasse *gering* (keine Signatur), *mittel* (fortgeschrittene Signatur) sowie *hoch bis sehr hoch*

(qualifizierte/akkreditierte Signatur) unterstützt, d.h. die zu erwartenden Schäden nach Integritätsverlust der Daten sind gering, mittel bzw. hoch bis sehr hoch einzuschätzen.

5.1.3 Authentizität

OSCI garantiert sowohl eine Authentisierung der Benutzer, sofern diese auf Postfächer zugreifen bzw. eine Quittung ausgestellt bekommen wollen, sowie eine Authentizität der Inhalts- bzw. Nutzungsdaten. Die Authentisierung der Benutzer erfolgt im Rahmen der expliziten Dialoginitialisierung. Dabei wird geprüft, ob der Benutzer im Besitz desjenigen privaten Schlüssels ist, der dem Chiffrier-Zertifikat zugeordnet ist.

Sofern eine Authentisierung der Benutzer benötigt wird, um beispielsweise den Zugriff auf Postfächer zu ermöglichen, wird von OSCI die Schutzbedarfsklasse *hoch bis sehr hoch* (Triple-DES/AES) unterstützt, d.h. die zu erwartenden Schäden nach fehlerhafter Authentisierung der Benutzer sind hoch bis sehr hoch einzuschätzen.

Die Authentizität der Daten bezieht sich auf die Authentizität sowohl der Inhalts- als auch der Nutzungsdaten.

- Authentizität der Inhaltsdaten:
  Die Inhaltsdaten können von dem Autor bzw. den Autoren mit dessen bzw. deren Zertifikaten signiert werden. Die Signatur wird von dem Leser bzw. den Lesern einer Verifikationsprüfung unterzogen; ob das Zertifikat gültig ist, wird vom Intermediär geprüft. Die übertragenen Inhaltsdaten sind authentisch, d.h. können einer Person zugeordnet werden, die im Besitz eines zum Zeitpunkt des Absendens gültigen Zertifikats ist. Dies sind im Falle der Inhaltsdaten die Autoren. Die Authentizität wird ausschließlich vom Leser erkannt.
- Authentizität der Nutzungsdaten:
  Die Nutzungsdaten können vom Absender mit dessen Zertifikat signiert werden und in diesem Fall vom Empfänger einer Signaturprüfung unterzogen werden. Die übertragenen Nutzungsdaten sind authentisch, d.h. können einer Person zugeordnet werden, die im Besitz eines zum Zeitpunkt des Absendens gültigen Zertifikats ist. Dies sind im Falle der Nutzungsdaten der Absender. Die Authentizität wird vom Intermediär bzw. vom Empfänger erkannt.

In Bezug auf die Authentizität der Inhalts- und Nutzungsdaten wird von OSCI die Schutzbedarfsklasse *gering* (keine Signatur), *mittel* (fortgeschrittene Signatur) sowie *hoch bis sehr hoch* (qualifizierte/akkreditierte Signatur) unterstützt, d.h. die zu erwartenden Schäden nach Authentizitätsverlust der Daten sind gering, mittel bzw. hoch bis sehr hoch einzuschätzen.

5.1.4 Nichtabstreitbarkeit

Nichtabstreitbarkeit bezieht sich sowohl auf die Autorenschaft einer Nachricht als auch auf den Kommunikationsvorgang.

- Nichtabstreitbarkeit der Autorenschaft:
  Die Nichtabstreitbarkeit der Autorenschaft unterliegt den Anforderungen des Signaturgesetzes. Das Signaturgesetz legt u.a. fest, dass qualifizierte Signaturen dort zum Einsatz kommen müssen, wo gemäß Verwaltungsrecht Schriftformerfordernis vorgeschrieben ist (vgl. Anlage). Die Nichtabstreitbarkeit der Kenntnisnahme wird nicht durch Mittel von OSCI gesichert.

  Die Nichtabstreitbarkeit der Autorenschaft wird durch Signierung der Inhaltsdaten realisiert und der Archivierung der Inhaltsdaten einschließlich der Signatur beim Empfänger.

Sofern mehrere Autoren existieren, sollten diese auch das Dokument gemeinsam signieren können. Dies setzt Mehrfachsignaturen voraus.

In Bezug auf die Nichtabstreitbarkeit der Autorenschaft wird von OSCI die Schutzbedarfsklasse *gering* (keine Signatur), *mittel* (fortgeschrittene Signatur) sowie *hoch bis sehr hoch* (qualifizierte/akkreditierte Signatur) unterstützt, d.h. die zu erwartenden Schäden nach Verlust der Nichtabstreitbarkeit der Autorenschaft sind gering, mittel bzw. hoch bis sehr hoch einzuschätzen.

- Nichtabstreitbarkeit des Kommunikationsvorgangs:
  Die Nichtabstreitbarkeit des Kommunikationsvorgangs unterteilt sich wiederum in zwei Unterziele:
  - Nichtabstreitbarkeit des Absendens:
    Die Nichtabstreitbarkeit des Absendens stellt sicher, dass der Absender nicht erfolgreich bestreiten kann, eine bestimmte Nachricht verschickt zu haben.
  - Nichtabstreitbarkeit des Empfangs:
    Die Nichtabstreitbarkeit des Empfangs stellt sicher, dass der Empfänger den Erhalt einer Nachricht nicht erfolgreich abstreiten kann. Mit dem Erhalt einer Nachricht ist allerdings nicht automatisch auch deren Kenntnisnahme verbunden.

  Die Nichtabstreitbarkeit des Kommunikationsvorgangs wird realisiert durch Signierung der Nutzungsdaten und der Archivierung der Nutzungsdaten einschließlich Signatur (Laufzettel) beim Intermediär. Dieser kann den Kommunikationspartnern auf Wunsch Quittungen über das Zustellen bzw. das Absenden einer Nachricht ausstellen.

  Die Nichtabstreitbarkeit des Empfangs bezieht sich in der Version 1.2 auch auf Attachments, nicht nur auf die eigentlichen Inhaltsdaten.

  In Bezug auf die Nichtabstreitbarkeit des Kommunikationsvorgangs wird von OSCI die Schutzbedarfsklasse *gering* (keine Signatur), *mittel* (fortgeschrittene Signatur) sowie *hoch/sehr hoch* (qualifizierte/akkreditierte Signatur) unterstützt, d.h. die zu erwartenden Schäden nach Verlust der Nichtabstreitbarkeit des Kommunikationsvorgangs sind gering, mittel bzw. hoch bis sehr hoch einzuschätzen.

5.1.5 Zurechenbarkeit

Die Zurechenbarkeit setzt sich aus der Zugriffskontrolle, der Beweissicherung bzw. Protokollierung sowie aus der zeitlichen Bestimmtheit zusammen.

- Zugriffskontrolle:
  Die Zugriffskontrolle hindert Benutzer und Prozesse, die für diese Benutzer tätig sind, lesenden oder schreibenden Zugriff auf Informationen oder Betriebsmittel zu erhalten, für die sie kein Zugriffsrecht haben, beispielsweise Postfächer oder Laufzettel.

  In Bezug auf die Zugriffskontrolle wird von OSCI ausschließlich die Schutzbedarfsklasse *hoch bis sehr hoch* unterstützt, d.h. die zu erwartenden Schäden nach Verlust der Zugriffskontrolle sind hoch bis sehr hoch einzuschätzen.

- Beweissicherung/Protokollierung:
  Die Beweissicherung erkennt, dass Aktionen, ggf. auch von Unbefugten, ausgeführt worden sind.

  In Bezug auf die Beweissicherung wird von OSCI ausschließlich die Schutzbedarfsklasse *hoch bis sehr hoch* unterstützt, d.h. die zu erwartenden Schäden nach Verlust der Beweissicherung sind hoch bis sehr hoch einzuschätzen.

- Zeitliche Bestimmtheit:
  Hierdurch wird erkannt, wann (Datum, Uhrzeit) eine Aktion stattgefunden hat.

  In Bezug auf die zeitliche Bestimmtheit wird von OSCI die Schutzbedarfsklasse *gering* sowie *hoch bis sehr hoch* unterstützt, d.h. die zu erwartenden Schäden nach Verlust der zeitlichen Bestimmtheit sind als *gering* (keine Bestimmung des Zeitpunkts erforderlich), *mittel* (nicht fälschungssichere Bestimmung des Zeitpunkts erforderlich) bzw. *hoch bis sehr hoch* (fälschungssichere Bestimmung des Zeitpunkts erforderlich) einzuschätzen.

Eine Übersicht über die Schutzbedarfsklassen, die bezüglich der jeweiligen Sicherheitsziele unterstützt werden, gibt folgende Tabelle:

Vertraulichkeit der Inhaltsdaten	gering		hoch bis sehr hoch
Vertraulichkeit der Nutzungsdaten	gering		hoch bis sehr hoch
Integrität der Inhaltsdaten	gering	mittel	hoch bis sehr hoch
Integrität der Verbindungsdaten	gering	mittel	
Authentizität der Benutzer			hoch bis sehr hoch
Authentizität der Inhaltsdaten	gering	mittel	hoch bis sehr hoch
Authentizität der Nutzungsdaten	gering	mittel	
Nichtabstreitbarkeit der Autorenschaft	gering	mittel	hoch bis sehr hoch
Nichtabstreitbarkeit des Absendens	gering	mittel	
Nichtabstreitbarkeit des Empfangs	gering	mittel	
Zugriffskontrolle			hoch bis sehr hoch
Beweissicherung			hoch bis sehr hoch
Zeitliche Bestimmtheit	gering	mittel	hoch bis sehr hoch

5.2 Nicht durch OSCI abgedeckte Sicherheitsziele

Nicht durch OSCI abgedeckt werden die Kriterien Identifizierung der Benutzer und Verfügbarkeit. Ebenfalls nicht abgedeckt sind einige andere der in Abschnitt 4 genannten Sicherheitsrisiken, z.B. Abhören von Geräten.

5.2.1 Verfügbarkeit

Die Verfügbarkeit der Inhalts- und Nutzungsdaten sowie die Verfügbarkeit des Systems insgesamt wird im Wesentlichen durch Maßnahmen außerhalb von OSCI garantiert. Diese sind Bestandteil des Betriebskonzepts.

5.2.2 Identifizierung des Benutzers

Die elektronische Signatur ist unmittelbar mit dem Begriff des Signaturzertifikats verbunden. Es handelt sich dabei um eine Datenstruktur, die die Zugehörigkeit eines öffentlichen Schlüssels zu dem Zertifikatsinhaber bescheinigt. Ein Zertifikat wird nur solchen Personen ausgestellt, die ihre Identität durch Vorlage eines Personalausweises belegen können.

Aus dem sorgsamen Prozess der Zertifikatsausstellung kann jedoch nicht geschlossen werden, dass Zertifikate eine Art elektronischer Personalausweis bilden, mit dem sich der Inha-

ber auch in offenen Systemen ohne Medienbruch zweifelsfrei identifizieren kann. Zertifikate nach dem SigG enthalten neben Informationen über das Zertifikat (Zertifikats-Nr., Gültigkeitszeitraum) höchstens den Vornamen und den Nachnamen des Antragstellers. Mit diesen Merkmalen lässt sich jedoch keine Person eindeutig identifizieren. Es besteht das Risiko, dass Personen die Identität eines Namensvettern vortäuschen und sich auf diese Weise missbräuchlich Zugang zu Fachverfahren erschleichen. Zwar lassen sich solche Identitätstäuschungen nachträglich nachweisen, da Vor- und Nachname mit einem eindeutigen Zertifikat signiert werden. Dies hat jedoch nur noch Auswirkungen auf mögliche Schadensersatzansprüche; der missbräuchliche Zugriff bleibt zunächst unerkannt.

Um eine eindeutige Identifizierung per OSCI-Transport 1.2 zu ermöglichen, wäre es erforderlich, zusätzliche Attributzertifikate gemäß § 7 Abs. 2 Signaturgesetz (SigG) auszustellen, die weitere Informationen über den Zertifikatsinhaber wie beispielsweise Geburtsdatum, Geburtsort enthalten. Solche Attribute sind jedoch zur Zeit nicht auf der Chipkarte vorhanden sind, so dass diese vom Intermediär – sofern er sie noch nicht lokal gespeichert hat – beim zuständigen Trust-Center jederzeit abgerufen werden müssten. Vorab müsste der Bürger bzw. Anwender die Attributzertifikate jedoch beim Trust-Center beantragen. Eine flächendeckende Nutzung von Attributzertifikaten, die beim Zertifikatherausgeber gespeichert und zum Abruf bereit gehalten werden, existiert zurzeit jedoch nicht.

Da OSCI-Transport folglich auf keine flächendeckend einsetzbaren Attributzertifikate zurückgreifen kann, ist OSCI-Transport in der Version 1.2 so ausgelegt, dass Informationen transportiert werden, ohne den Absender vorab zu identifizieren. Die einzige Voraussetzung für den Weitertransport besteht darin, dass der Empfänger im Besitz eines nicht widerrufenen Chiffrier-Zertifikats ist, da die Adressierung anhand dieses Zertifikats erfolgt. Setzt der betrachtete Geschäftsvorfall voraus, dass die Nachricht signiert bzw. verschlüsselt werden muss, so muss auch der Sender über die entsprechenden Zertifikate verfügen.

Der Intermediär unterzieht die Zertifikate allerdings einer Zertifikatsprüfung. Erweist sich dabei das Chiffrierzertifikat des Empfängers als widerrufen, so wird die Zustellung der Nachricht verweigert. Im Falle eines abgelaufenen Zertifikats wird die Nachricht zwar zugestellt, aber der Empfänger wird über das Prüfergebnis in Form eines Prüfprotokolls informiert (vgl. Kap. 6.7).

OSCI-Transport 1.2 kennt außer den beteiligten Intermediären, deren Zertifikat auch dem Client-Kernel bekannt ist, gar keine Benutzer. OSCI-Transport identifiziert in diesem Sinne keine Benutzer, sondern ordnet die übertragenen Daten einem Zertifikat eindeutig zu. In diesem Sinne sind die übertragenen Informationen authentisch. Die Identifizierung der Kommunikationspartner erfolgt stattdessen durch das Anwendungssystem.

6. OSCI-Sicherheitsmechanismen

OSCI-Transport 1.2 stellt zahlreiche Mechanismen zur Verfügung. Bevor auf die einzelnen OSCI-Mechanismen genauer eingegangen wird, werden in der folgenden Tabelle zunächst die einzelnen Mechanismen den jeweiligen Sicherheitszielen einschließlich deren Ausprägung zugeordnet.

Sicherheitsziele **OSCI-Mechanismus**		Vertraulichkeit	Integrität	Authentizität	Nichtab-streitbarkeit	Zurechen-barkeit
A	Verschlüsselung der Inhaltsdaten	hoch/sehr hoch				
B	Verschlüsselung der Nutzungsdaten	hoch/sehr hoch				
C	Entschlüsselung der Inhaltsdaten	hoch/sehr hoch				
D	Entschlüsselung der Nutzungsdaten	hoch/sehr hoch				
E	Signierung der Inhaltsdaten		mittel hoch/sehr hoch	mittel hoch/sehr hoch	mittel hoch/sehr hoch	
F	Signierung der Nutzungsdaten		mittel hoch/sehr hoch	mittel hoch/sehr hoch	mittel hoch/sehr hoch	
G	Signaturprüfung der Inhaltsdaten		mittel hoch/sehr hoch	mittel hoch/sehr hoch	mittel hoch/sehr hoch	
H	Signaturprüfung der Nutzungsdaten		mittel hoch/sehr hoch	mittel hoch/sehr hoch	mittel hoch/sehr hoch	
I	Zertifikatsprüfung		hoch/sehr hoch	hoch/sehr hoch	hoch/sehr hoch	
K	Protokollierung des Zeitpunkts					mittel hoch/sehr hoch
L	Quittungs-mechanismus				hoch/sehr hoch	
M	Benutzer-authentisierung per Dialoginitialisierung			hoch/sehr hoch		
N	Challenge-Response			hoch/sehr hoch		
O	Vergabe und Prü-fung Message-ID			hoch/sehr hoch		

6.1 Verschlüsselung bzw. Entschlüsselung der Inhaltsdaten

Inhaltsdaten können auf Geschäftsvorfallebene mit einem hybriden Verfahren verschlüsselt bzw. entschlüsselt werden. Hierbei werden die Nachrichten mit einem symmetrischen Triple-DES-bzw.AES-Verfahren verschlüsselt; der jeweilige Sitzungsschlüssel wird mit dem öffentlichen Teil des RSA-Schlüssels des Lesers codiert. Der übertragene Sitzungsschlüssel wird vom Leser mit dem privaten Teil seines RSA-Schlüssels entschlüsselt; der entschlüsselte Sitzungsschlüssel dient anschließend zum Entschlüsseln der eigentlichen Nachricht.

Benutzer benennen in dem Verschlüsselungsheader den verwendeten Algorithmus und geben hierüber das Verfahren vor, das der Intermediär bei der Auftragsantwort anzuwenden hat. Falls der Intermediär ein vom Benutzer gewähltes Verfahren nicht unterstützt, wird dem Benutzer eine entsprechende Rückmeldung gegeben und der Dialog wird beendet.

Das Hybrid-Verfahren ermöglicht es, Dokumente an einen Stellvertreter oder mehrere Empfänger verschlüsselt zu versenden (z.B. bei Verteilerlisten). Hierbei werden die zu versendenden Dokumente mit einem Sitzungsschlüssel codiert. Dieser Sitzungsschlüssel wird an jeden Empfänger RSA-verschlüsselt verschickt. Dabei ist es unerheblich, dass sämtliche Empfänger auch diejenigen RSA-codierten Sitzungsschlüssel mitlesen können, die nicht für sie bestimmt sind.

Sofern verschlüsselt wird, wird durch die Verschlüsselung bzw. Entschlüsselung der Inhaltsdaten hinsichtlich der Vertraulichkeit der Inhaltsdaten die Schutzbedarfsklasse *hoch bis sehr hoch* unterstützt.

6.2 Verschlüsselung bzw. Entschlüsselung der Nutzungsdaten

Die Nutzungsdaten der Auftragsebene können ebenso wie die Inhaltsdaten mit einem Hybrid-Verfahren verschlüsselt werden (vgl. 6.1). Die Nutzungsdaten werden zunächst vom Absender auf dem Weg zum Intermediär verschlüsselt und von diesem nach Erhalt der Nachricht entschlüsselt, da der Intermediär für die Zustellung der Nachricht und die Erbringung seiner Mehrwertdienste lesenden Zugriff hierauf benötigt. Für die Zustellung der Nachricht an den eigentlichen Empfänger werden die Nutzungsdaten durch den Intermediär wieder verschlüsselt.

Durch die Verschlüsselung bzw. Entschlüsselung der Nutzungsdaten wird hinsichtlich der Vertraulichkeit der Nutzungsdaten die Schutzbedarfsklasse *hoch bis sehr hoch* unterstützt.

6.3 Signieren der Inhaltsdaten

Ebenso wie die Verschlüsselung erfolgt auch das Signieren von Dokumenten mit einem Hybridverfahren. Zunächst werden die Hashwerte aller zu signierenden Dokumente zu einem Element zusammengeführt. Anschließend wird dieses Element mittels RSA signiert.

Benutzer benennen in dem Signierheader den verwendeten Signieralgorithmus und geben hierüber den Algorithmus an, den der Intermediär bei der Auftragsantwort anzuwenden hat. Kein OSCI-Teilnehmer – weder der Benutzer noch der Intermediär – darf das Verfahren innerhalb eines Dialogs ändern.

Die signierten Daten werden zeitgleich mit der Signierung geeignet visualisiert, sofern es sich um XML-strukturierte Inhaltsdaten handelt. Inhaltsdaten in Fremdformaten, die in Form von Attachments zur eigentlichen Nachricht versendet werden, werden nicht mitvisualisiert; es wird lediglich der Dateiname und das Dateiformat des Attachment angegeben

Daten können per OSCI mit folgenden Signaturen versehen werden (vgl. Anlage, Kap.2):
- fortgeschrittene Signatur,
- qualifizierte Signatur,
- akkreditierte Signatur.

Durch die Signierung der Inhaltsdaten wird hinsichtlich der Integrität, der Authentizität und der Nichtabstreitbarkeit der Inhaltsdaten die Schutzbedarfsklasse *mittel* (fortgeschrittene Signatur) sowie *hoch bis sehr hoch* (qualifizierte/akkreditierte Signatur) unterstützt.

6.4 Signieren der Nutzungsdaten

Nicht nur die Inhaltsdaten, auch die Nutzungsdaten können signiert werden, um die Authentizität und Integrität dieses Dokuments zu gewährleisten. Das Signieren der Nutzungsdaten erfolgt mit dem Signierzertifikat des Absenders.

Die Nutzungsdaten werden vom Intermediär lediglich mit einer fortgeschrittenen Signatur signiert. Die Signatur des Senders einer Nachricht erfolgt wahlweise fortgeschritten oder qualifiziert bzw. akkreditiert. Nutzungsdaten müssen während des Signierens nicht explizit visualisiert werden.

Durch die Signierung der Nutzungsdaten wird hinsichtlich der Integrität, der Authentizität und der Nichtabstreitbarkeit der Nutzungsdaten die Schutzbedarfsklasse *mittel* (fortgeschrittene Signatur) sowie *hoch bis sehr hoch* (qualifizierte/akkreditierte Signatur) unterstützt.

6.5 Signaturprüfung der Inhaltsdaten

Nach erfolgter Zustellung der OSCI-Nachricht kann der Leser im eigenen Interesse die Signaturprüfung der Inhaltsdaten selbst vornehmen. Dies ist vom Intermediär nicht durchführbar, da die Inhaltsdaten des Geschäftsvorfalls für ihn aufgrund der Verschlüsselung nicht sichtbar sind. Die Verifikation der Signatur verläuft im Wesentlichen analog zur Signierung: Es wird aus dem übertragenen Dokument der Hashwert gebildet. Darüber hinaus wird die im Signaturkopf der übermittelten Nachricht enthaltene elektronische Signatur mit Hilfe des öffentlichen Schlüssels des Absenders decodiert. Stimmen dieser Wert und der ermittelte Hashwert überein, gilt das übermittelte Dokument als authentisch und unverändert.

6.6 Signaturprüfung der Nutzungsdaten

Die Signatur der Nutzungsdaten wird zunächst vom Intermediär geprüft, wenn eine Nachricht bei diesem eingeht. Der Intermediär ergänzt die Nutzungsdaten um den Laufzettel, der auch ein Prüfprotokoll enthält, in dem das Ergebnis der Signaturprüfung vermerkt wird. Im Falle eines negativen Prüfergebnisses wird die Nachricht nicht zugestellt, sondern an den Sender zusammen mit dem negativen Prüfergebnis zurückgeschickt. Die aktualisierten Nutzungsdaten werden ggf. vom Intermediär signiert. Die Signaturprüfung der vom Intermediär angebrachten Signatur der Nutzungsdaten erfolgt durch den endgültigen Empfänger der Nachricht. Die Verifikation der Signatur basiert auf dem in Kap. 6.5 beschriebenen Verfahren.

6.7 Zertifikatsprüfung

§ 2 Ziff. 3 SigG definiert eine qualifizierte Signatur als solche, die auf einem zum Zeitpunkt ihrer Erzeugung gültigen Zertifikat beruht. Hieraus ergibt sich neben der Notwendigkeit, die Signatur auf mathematische Korrektheit zu prüfen (vgl. Kap. 6.5), die Prüfung, ob das jeweilige Zertifikat zum Zeitpunkt der Signaturerstellung gültig war. Für die Zertifikatsprüfung sind folgende Tätigkeiten durchzuführen:

- Mathematische Prüfung der Signatur des Zertifikats: Der Hashwert über das Zertifikat wird erneut berechnet und muss mit der entschlüsselten Signatur übereinstimmen.
- Offline-Gültigkeitsprüfung: Der Zeitpunkt der Prüfung befindet sich innerhalb des Gültigkeitszeitraums, der im Zertifikat angegeben ist.
- Online-Gültigkeitsprüfung: Das Zertifikat ist zum Zeitpunkt der Prüfung nicht widerrufen.

Da die Zertifikate Teil der Nutzungsdaten und somit für den Intermediär zugänglich sind, kann eine Zertifikatsprüfung sowohl für die Inhaltsdaten als auch für die Nutzungsdaten durch diesen erfolgen. Die Signierung der Nutzungsdaten und der Inhaltsdaten kann ggf. mit dem selben Zertifikat erfolgen, wenn die Rollen des Autors und des Senders von einer Person wahrgenommen werden.

Die Zeitpunkte der Erzeugung dieser beiden Signaturen können zwar im Einzelfall durchaus voneinander abweichen, dies ist jedoch unproblematisch, falls die Nutzungsdaten-Signatur auf einem zum Zeitpunkt ihrer Erzeugung gültigen Zertifikat beruhte. Da die Signatur der Inhaltsdaten zeitlich immer vor der Signatur der Nutzungsdaten erfolgt, kann hieraus auch auf ein zum Zeitpunkt der Inhaltsdaten-Signatur gültigen Zertifikat geschlossen werden.

Nicht eindeutig ist es vielmehr im Falle eines negativen Prüfergebnisses. Wenn die Nutzungsdaten-Signatur auf einem zum Zeitpunkt ihrer Erzeugung ungültigen Zertifikat beruht, so folgt daraus nicht zwingend, dass das Zertifikat auch schon zum Zeitpunkt der Erzeugung der Inhaltsdaten-Signatur ungültig war. Zwar könnte das Zertifikat theoretisch zwischen der Erzeugung der Inhaltsdaten-Signatur und der Erzeugung der Nutzungsdaten-Signatur ungültig geworden sein. Dennoch wird in jedem Fall der Empfänger darüber informiert, dass es sich um ein Zertifikat handelt, das zum Zeitpunkt der Nutzungsdaten-Signatur ungültig war. Wie er mit einem negativen Prüfergebnis umgeht, ob er seinerseits eine eigene Prüfung der Signatur der Inhaltsdaten-Daten vornimmt oder die Annahme der OSCI-Nachricht verweigert, bleibt ihm überlassen und dürfte auch von der Art des Geschäftsvorfalls abhängen.

Ist das Zertifikat gültig, wird dem Backendsystem die Qualität des Zertifikats mitgeteilt (fortgeschrittene Signatur, qualifizierte bzw. akkreditierte Signatur). Das Prüfergebnis für die einzelnen Zertifikate wird in einem Prüfprotokoll vermerkt. Im Fall eines widerrufenen Empfänger-Chiffrier-Zertifikats wird die OSCI-Nachricht nicht zugestellt, sondern zusammen mit dem negativen Prüfergebnis an den Sender zurückgeschickt.

6.8 Protokollierung von Zeitpunkten

Auf dem Laufzettel werden vom Intermediär Absende- und Zustellzeitpunkt vermerkt. Optional kann der Zustellzeitpunkt mit Hilfe eines signierten Zeitstempels festgehalten werden. Dabei kann wiederum zwischen folgenden Zeitstempeln differenziert werden:

- fortgeschrittener Zeitstempel:
  Dieser wird vom Intermediär ausgestellt und von diesem per fortgeschrittener elektronischer Signatur signiert.
- qualifizierter Zeitstempel:
  Dieser wird von einem Trust-Center im Auftrag des Intermediärs erstellt bzw. signiert und diesem zur Verfügung gestellt.
- akkreditierter Zeitstempel:
  Dieser wird von einem akkreditierten Trust-Center im Auftrag des Intermediärs erstellt bzw. signiert und diesem zur Verfügung gestellt.

Zwar schreibt das Signaturgesetz nicht vor, dass der Zeitpunkt der Signaturerstellung aus einer qualifizierten elektronischen Signatur zweifelsfrei ersichtlich sein muss. Eine Signatur ist daher auch ohne Zeitstempel rechtskonform. Eine sichere Bestimmung des Zeitpunkts ist allerdings nur dann möglich, wenn eine Signatur mit einem qualifizierten Zeitstempel im Sinne des § 2 Ziff. 14 SigG versehen wurde. Soweit eine qualifizierte elektronische Signatur nicht mit einem qualifizierten Zeitstempel versehen wurde, basiert das angezeigte Datum – wenn überhaupt – nur auf der Systemzeit der Anwendungsumgebung des Absenders. Diese Systemzeit ist jedoch leicht zu manipulieren.

Durch das Eintragen des Zeitstempels wird hinsichtlich der Nichtabstreitbarkeit der Kommunikation die Schutzbedarfsklasse *mittel* (fortgeschrittener Zeitstempel) sowie *hoch bis sehr hoch* (qualifizierter/akkreditierter Zeitstempel) unterstützt.

6.9 Quittungsmechanismus

Der Laufzettel gilt auch als Quittung für Absender, Empfänger und Intermediär und kann vom Intermediär angefordert werden, um das Absenden bzw. den Erhalt einer Nachricht nachweisen zu können. Für den Intermediär dient der Laufzettel ebenfalls als Zustellnachweis.

Ebenfalls als Quittung können folgende Aufträge bzw. Auftragsantworten angesehen werden:

Durch das Senden einer Auftragsantwort mit einem erfolgreichen Rückmeldecode bestätigt ein Empfänger, dass er den zugehörigen Auftrag empfangen hat und ausführen konnte.

Durch das Senden eines Auftrags mit einem Response-Wert, der mit dem Challenge-Wert aus der vorangegangenen Auftragsantwort übereinstimmt, und einer Auftragsnummer, die um 1 größer als die Nummer des vorangegangenen Auftrags ist, quittiert ein Client, dass er die Antwort auf den vorangegangenen Auftrag erhalten hat.

In den Antworten zu Abholaufträgen werden die jeweiligen Selektionskriterien wiederholt; dies kann ebenfalls als Quittung benutzt werden.

6.10 Benutzerauthentisierung durch explizite Dialoginitialisierung

Im Rahmen der expliziten Dialoginitialisierung wird geprüft, ob ein Benutzer im Besitz desjenigen privaten Schlüssels ist, der einem Chiffrier-Zertifikat zugeordnet ist. Hierbei wird zunächst ein Zufallswert mit dem öffentlichen Schlüssel des Benutzers chiffriert und an den zu authentisierenden Benutzer geschickt. Ist dieser in der Lage, den chiffrierten Wert korrekt mit seinem privaten Schlüssel zu entschlüsseln und zurückzuschicken, ist er erfolgreich authentisiert. Diese Form der Authentisierung wird benötigt, um sowohl den autorisierten Zugriff auf das Postfach als auch auf den Laufzettel zu ermöglichen. Die Berechtigung zum Zugriff auf Postfach und Laufzettel erfolgt nämlich über das Chiffrier-Zertifikat des Inhabers.

6.11 Challenge-Response-Verfahren

Wie bereits erwähnt bietet OSCI keinen Mechanismus für die Identifizierung der Kommunikationsteilnehmer, da dies mit Hinblick auf die offene Benutzergruppe nicht möglich ist. Innerhalb eines Dialogs erfolgt jedoch eine Authentisierung auf Basis eines Challenge/Response-Verfahrens.

6.12 Vergabe und Prüfung der Message-ID

Jeder Zustellung eines OSCI-Pakets kann eine Message-ID zugeordnet werden, die weltweit und zeitlich unbegrenzt eindeutig ist. Damit gilt die Message-ID für genau eine Zustellung auf dem Weg vom Sender über den Intermediär zum Empfänger.

Die Message-ID wird auf Anforderung des Senders vom Intermediär erzeugt. Der Intermediär prüft, ob

- er die Message-ID erzeugt hat,
- die Message-ID schon einmal verwendet worden ist.

Liefert eine dieser Prüfungen ein negatives Ergebnis, so lehnt der Intermediär den Auftrag ab, mit dem der Sender die Zustellung eingereicht hat. Die Vergabe und Prüfung einer Message-ID dient dazu, Replay-Attacken bzw. die Doppeleinreichung von Zustellungen zu vermeiden.

Anlage: Rechtliche Anforderungen an den elektronischen Geschäftsverkehr

1. Das neue Signaturgesetz

Das seit 22. Mai 2001 in Kraft getretene neue Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG) verfolgt zwei Ziele: Zum einen dient es der Umsetzung der seit 19. Januar 2000 in Kraft getretenen EU-Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen. Zum anderen greift das neue Gesetz die Ergebnisse der Evaluierung des alten Signaturgesetzes auf, wie es im IuKDG-Bericht der Bundesregierung vom 18. Juni 1999 niedergelegt ist.

Das neue Signaturgesetz zeichnet sich im Wesentliche durch folgende Neuerungen aus:

- Regelungen zur Haftung der Zertifizierungsdiensteanbieter
- Regelungen zur Anerkennung von Prüfstellen,
- Regelungen bezüglich der Verwendung von Pseudonymen,
- Bestandsschutzregelungen für Unternehmen, die Produkte und Dienstleistungen nach dem Signaturgesetz anbieten,
- Differenzierte Signaturbegriffe,
- Anforderungen an Zeitstempel,
- Erweiterung der Unterrichtungspflicht für Zertifizierungsdiensteanbieter.

2. Differenzierte Signaturbegriffe

Wesentlicher Bestandteil des neuen Signaturgesetzes ist die bereits in der EU-Richtlinie enthaltene Differenzierung zwischen

- einfacher Signatur,
- fortgeschrittener Signatur und
- qualifizierter Signatur.

Elektronische Signaturen sind Daten in elektronischer Form, die der Authentisierung dienen; dies können auch Namenskürzel oder eingescannte Unterschriften sein.

Fortgeschrittene elektronische Signaturen müssen darüber hinaus

- ausschließlich dem Inhaber des Signaturschlüssels zugeordnet sein,
- die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
- mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann,
- mit den Daten, auf die sie sich beziehen, so verknüpft sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Qualifizierte elektronische Signaturen werden gegenüber fortgeschrittenen Signaturen zudem noch mit einer sicheren Signaturerstellungseinheit erzeugt und beruhen auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat, das seinerseits nur für natürliche Personen und von Zertifizierungsdiensteanbietern (Trust-Centern) ausgesellt wird.

Sofern die qualifizierte Signatur von akkreditierten Zertifizierungsdiensteanbietern ausgestellt wird, kann zusätzlich noch von **akkreditierten elektronischen Signaturen** gesprochen werden.

Die akkreditierte Signatur ist charakterisiert durch

- die Garantie einer 30-jährigen Überprüfbarkeit (§15 Abs. 7 SigG),

- die umfassende Evaluation aller gesetzlich geforderten technischen Produkte nach dem Stand von Wissenschaft und Technik (§15 Abs.8 SigG),
- die staatliche Überprüfung der Zertifizierungsanbieter vor Aufnahme der Tätigkeit (§15 Abs.1 und 3 SigG).

Bei der qualifizierten Signatur, bei der es sich um die europäische Standardsignatur gemäß EU-Richtlinie handelt, ist hingegen

- eine dauerhafte Überprüfbarkeit nicht garantiert (§13 Abs.1 und 2 SigG),
- werden die eingesetzten technischen Komponenten nur eingeschränkt evaluiert (§17 Abs. 4 SigG),
- müssen die Zertifizierungsanbieter die Aufnahme der Tätigkeit der staatlichen Aufsicht lediglich anzeigen (§ 4 Abs. 1 und 3 SigG).

Das Signaturgesetz schreibt nicht vor, dass der Zeitpunkt der Signaturerstellung aus der Signatur ersichtlich sein muss. Eine Signatur ist daher auch ohne Zeitstempel rechtskonform. Eine sichere Bestimmung des Zeitpunkts ist nur dann möglich, wenn eine Signatur mit einem qualifizierten Zeitstempel im Sinne des § 2 Ziff. 14 SigG versehen wurde.

3. Rechtsgültigkeit der elektronischen Unterschrift

An behördliche Schreiben werden formelle Anforderungen gerichtet. Dazu gehört ein amtlicher Briefkopf sowie die Angabe der ausfertigenden Stelle bzw. des Sachbearbeiters, abgeschlossen i.a. mit einer Unterschrift (Ausnahme automatisierte Bescheide) sowie ggf. versehen mit einem Stempel oder Dienstsiegel. Die äußere Form macht deutlich, dass es sich nicht um eine Person für sich handelt, sondern um einen im Auftrag der Organisation handelnden Mitarbeiter.

Im Rahmen des elektronischen Geschäfts- und Rechtsverkehrs kann dieser Anforderung mit Hilfe geeigneter Attribute Rechnung getragen werden. Es kann nicht nur die ausstellende Person, sondern auch ihre Handlungsvollmacht für die Organisation/Behörde an dem übermittelten Text selbst erkennbar und möglichst prüfbar sein.

Wann welche Signaturqualität erforderlich ist, ist Gegenstand des *Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Formvorschriften an den modernen Rechtsgeschäftsverkehr*. Ausdrücklich abgelehnt wird eine Regelung, die elektronische Dokumente den Vorschriften über den Beweis durch Urkunden unterstellt, weil dies nicht dem hohen Beweiswert elektronischer Dokumente, die mit qualifizierten Signaturen versehen seien, gerecht werde. Das Gesetz sieht die Schaffung eines § 126a für das BGB vor, der die Ersetzung der Schriftform durch die elektronische Form ermöglicht, sofern das elektronische Dokument mit einer qualifizierten Signatur versehen ist. Qualifizierte Signaturen müssen demnach dort zum Einsatz kommen, wo bislang Schriftformerfordernis vorlag.

Eine vergleichbare Regelung gibt es auch im Verwaltungsrecht. Sofern jedoch Verwaltungsakte nicht mehr schriftlich dokumentiert werden sollen, müssen die qualifizierten Signaturen noch durch akkreditierte Trust-Center ausgestellt worden sein (akkreditierte Signatur). Der nach Artikel 5 der EU-Richtlinie geforderte Zulassung elektronischer Signaturen vor Gericht wird dagegen bereits durch den geltenden Rechtsgrundsatz der freien Beweiswürdigung der Gerichte entsprochen.

Im Streitfall ist die Qualität einer Signatur durch einen oder mehrere vom Gericht bestellte Gutachter zu bewerten. Ein neuer § 292a ZPO soll den Verwendern qualifizierter elektronischer Signaturen (mit oder ohne Anbieter-Akkreditierung) durch Normierung eines vorgezogenen Anscheinsbeweises die Beweisführung erleichtern: *„Der Anschein der Echtheit einer*

in elektronischer Form (§ 126a BGB) vorliegenden Willenserklärung, der sich auf Grund einer Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die es ernsthaft als möglich erscheinen lassen, dass die Erklärung nicht mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist.“ Dass auch qualifizierte elektronische Signaturen ohne Anbieter-Akkreditierung von § 292a ZPO profitieren sollen, wird allerdings vielfach kritisiert.