Bundesamt für Sicherheit in der Informationstechnik

Sicherheitsbewertung

zur Spezifikation OSCI – Transport 1.2

Stand: 30.07.2002

Bundesamt für Sicherheit in der Informationstechnik

Inhaltsverzeichnis

1. Sicherheitsbewertung OSCI-Transport 1.2

1.1 Gegenstand der Sicherheitsbewertung und Einordnung von OSCI-Transport 1.2

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

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

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

1.2 Abgrenzung der Sicherheitsbewertung

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

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

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

Weiterhin werden folgende Annahmen bezüglich der Sicherheit des Standards vorausgesetzt:

(1) Korrektheit der Implementation

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

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

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

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

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

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

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

2. Funktionsweise von OSCI-Transport 1.2

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

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

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

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

2.1 Architektonischer Aufbau des Protokolls

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

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

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

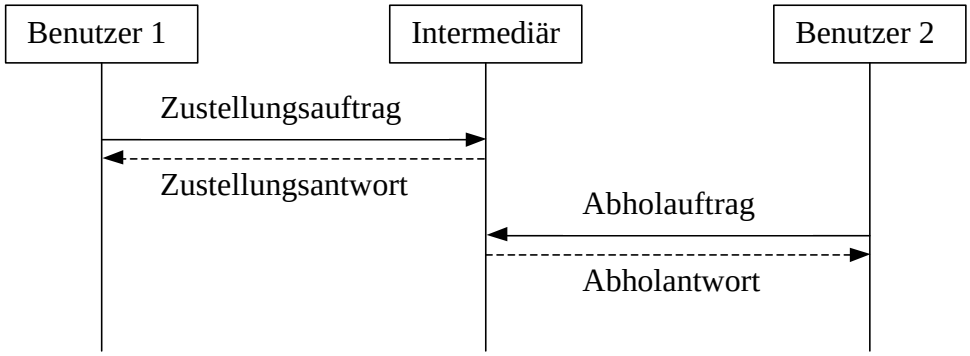
c) Nachrichtenebene
OSCI-Nachrichten werden zwischen Benutzer und Intermediär (bei Bedarf verschlüsselt) verschickt. Beide können als Sender oder Empfänger auftreten. Die OSCI-Nachrichten bestehen aus einem Auftrag, einer Auftragsantwort oder einer Fehlermeldung.

2.2 Kommunikations - Szenarien

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

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

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



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

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

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

3. Sicherheitsfunktionen und -mechanismen

3.1 Digitale Signaturen

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

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

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

3.1.1 Signieren und Verifizieren von Inhaltsdaten

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

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

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

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

3.1.2 Signieren und Verifizieren von Nutzungsdaten (Aufträge und Auftragsantworten)

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

Integrität der Nutzungsdaten und Authentizität des Senders

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

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

3.1.3 Zertifikatsprüfungen

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

Geprüft wird vom Intermediär

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

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

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

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

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

3.2 Verschlüsselung

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

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

3.2.1 Ver- und Entschlüsseln von Inhaltsdaten

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

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

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

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

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

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

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

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

3.2.3 Zertifikatsprüfungen

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

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

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

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

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

3.3 Beweissicherung

3.3.1 Protokollierung der Ergebnisse von Zertifikatsprüfungen

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

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

Nicht-Abstreitbarkeit des Ursprungs

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

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

3.3.2 Protokollierung von Zeitpunkten

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

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

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

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

Der Intermediär hält folgende Zeitpunkte fest:

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

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

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

3.4 Challenge-Response

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

Zurechenbarkeit von Aktionen

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

3.4.1 Vergeben und Prüfen von Challenge-Response-Werten

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

3.4.2 Dialogende

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

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

3.5 Client-Authentisierung

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

Authentizität des Empfängers

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

3.5.1 Authentisieren mittels eines Chiffrierzertifikats

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

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

3.5.2 Dialogende

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

3.6 MessageID

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

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

3.6.1 Vergeben und Prüfen einer MessageID

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

3.6.2 Dialogende

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

3.7 Quittierung von Aufträgen und Auftragsantworten

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

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

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

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

3.8 Protokollauswertung des Laufzettels

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

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

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

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

3.9 Zusammenfassung der Sicherheitsfunktionen und -mechanismen

Mit den Funktionen

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

werden die Sicherheitsziele

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

durchgesetzt.

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

4. Kryptographische Verfahren in OSCI

4.1. XML Signature und XML Encryption

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

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

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

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

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

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

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

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

4.2 Kryptographische Algorithmen

4.2.1 Signaturalgorithmen

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

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

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

4.2.2 Verschlüsselungsalgorithmen

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

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

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

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

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

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

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

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

4.3 Schlüsselmanagement

4.3.1 Asymmetrische Verfahren

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

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

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

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

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

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

Zertifikatsprüfungen in OSCI-Transport 1.2:

Anmerkung:

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

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

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

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

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

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

4.3.2. Symmetrische Verfahren

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

5. Weitere Sicherheitsaspekte

5.1 Einsatz von SOAP

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.3 Einhaltung datenschutzrechtlicher Vorschriften

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

5.4 Weiterentwicklung von OSCI-Transport

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

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

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

6. Zusammenfassung

Im gegeben Prüfungsumfang des Erlasses vom 28.05.02 kann für die Frage nach der Erfüllung der Anforderungen aus Sicht der Kommunikationssicherheit im E-Government festgestellt werden:

Eine Übertragungssicherung im Sinne der ITSEC (Schutz der Daten während der Übertragung über Kommunikationskanäle) ist sichergestellt. Damit kann davon ausgegangen werden, dass die Anforderungen aus Sicht der Kommunikationssicherheit im E-Government abgedeckt werden. Produkte, die auf der Basis der vorliegenden Spezifikation implementiert wurden, können somit unter Annahme der unter 1.2 beschriebenen Voraussetzungen die Anforderungen der Kommunikationssicherheit im E-Government erfüllen.

Bezüglich der ebenfalls im Erlass beauftragten Frage nach der Erfüllung der Anforderungen hinsichtlich der kryptographischen Sicherheit der eingesetzten Algorithmen und Verfahren ist festzustellen:
OSCI-Transport 1.2 sieht ohne Ausnahme die Verwendung von der Fachwelt anerkannter, nach derzeitigem Kenntnisstand kryptographisch starker Algorithmen (für die Zwecke „digitale Signatur“ bzw. Ver-/Entschlüsselung) vor, wobei die verwendeten Schlüssellängen ebenfalls derzeit nicht zu beanstanden sind. Zudem orientieren sich die Vorschläge für die konkrete Realisierung der verwendeten Verfahren an bewährten, weithin eingesetzten Standards.
Bei Einhaltung der im Text gegebenen Empfehlungen zur Implementierung kann davon ausgegangen werden, dass das von einem entsprechenden Produkt erzielbare kryptographische Sicherheitsniveau durchgängig angemessen hoch ist.
„Angemessen hoch“ heißt hier: nach aktuellem Stand der Algorithmik und der Rechentechnik liegt der vermutliche Minimalaufwand für die Erlangung der zugrundeliegenden kryptographischen Schlüssel durch Kryptoanalyse oberhalb der derzeit akzeptierten Schwelle von 2^{80} Operationen.