Koordinierungsstelle
für IT-Standards

Ende-zu-Ende-Verschlüsselung in einer XTA-OSCI-Infrastruktur

Dokumentenversion Entwurf 0.8

veröffentlicht unter https://www.xoev.de/sixcms/media.php/13/OSCI_E2E_Verschluesselung.pdf

Änderungshistorie

Version	Datum	Autor	Kapitel	Änderungen
0.8	16.12.2021	SevenPrinciples, Bundesdruckerei, Governikus, KoSIT	Alle	Erstellung

Status dieses Dokumentes

Das vorliegende Dokument ist ein nicht-normativ Hilfsmittel zur Arbeit mit OSCI-Transport 1.2 und XTA 2 Version 3. Es beschreibt die grundlegenden Schritte zur Umsetzung einer Ende-zu-Ende-Verschlüsselung in einer XTA-OSCI-Infrastruktur. Das Dokument wird in unregelmäßigen Abständen durch die KoSIT aktualisiert.

Ausblick

Eine generelle Klärung der Definition des Four-Corner-Modells mit grundlegender Verantwortungs- und Aufgabenteilung, u.a. im Rahmen einer Ende-zu-Ende Verschlüsselung, soll in einer weiteren Handreichung erstellt werden. Mit Verweis auf diese Klärung könnte dieses Hilfsmittel überarbeitet werden.

Die im Kapitel „2.1 Autor“ skizzierten Abläufe bzgl. mit und ohne Einsatz der OSCI-Bibliothek sollten noch ihre Praxistauglichkeit in Form einer Proof-of-Concept-Implementierung auf Interoperabilität zwischen Unterschiedlichen bestehenden Softwaresystemen geprüft werden. Hierfür sollen nach Veröffentlichung dieses Dokumentes Tester geworben werden.

Inhaltsverzeichnis

1 Zielgruppe und Voraussetzungen

In diesem Kapitel soll kurz angerissen werden für Wen dieses Dokument erstellt wurde und welches Wissen beim Lesen des Dokumentes vorausgesetzt wird.

1.1. Zielgruppe

Die Zielgruppe des Dokumentes sind Verantwortliche und Entwickler von Verfahren die über OSCI kommunizieren und ggf. auch XTA verwenden. Es werden mindestens grundlegende Kenntnisse von OSCI und XTA vorausgesetzt.

1.2. Kommunikationsmodel auf Basis von OSCI und XTA

Im Kontext einer Ende-zu-Ende-Verschlüsselung auf der Basis von OSCI und XTA gibt es die in der Abbildung 1 dargestellten Rollen, welche die in der folgenden Tabelle aufgeführten Aufgaben haben. Im Rahmen der Nutzung von XTA können einige dieser Aufgaben auf andere Rollen delegiert werden; diese Rollen-Delegation verändert dann möglicherweise die Eigenschaften der Ende-zu-Ende-Verschlüsselung.

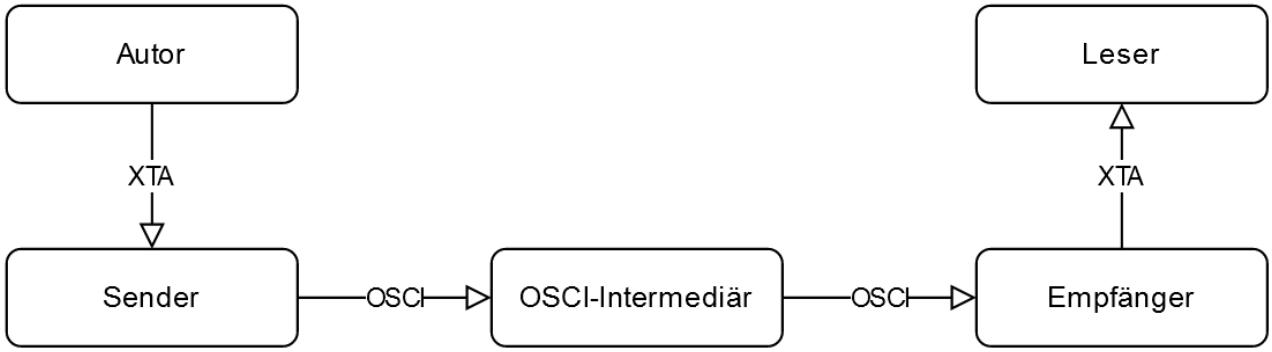

Abbildung 1 Kommunikationsmodel auf der Basis von OSCI und XTA

Hinweise für eine OSCI-Datenübertragung ohne XTA-Nutzung: Die Nutzung von XTA zwischen Autor und Sender sowie zwischen Empfänger und Leser kann durch andere Übermittlungswege ersetzt werden oder die jeweiligen Rollen von Autor und Sender sowie von Empfänger und Leser verschmelzen jeweils sogar zu einer Applikation. Weiterhin können auf jeweils einer Seite des Intermediärs unterschiedliche Übermittlungen zwischen den Rollen eingesetzt werden und trotzdem wird eine vom Autor bis zum Leser verschlüsselte Nachricht übertragen.

Tabelle 1: Definition der Aufgaben der einzelnen Rollen

ID	Rolle	Aufgabe
A1	Autor	Erstellen der Inhaltsdaten, die an den Leser übermittelt werden
A2	Autor	Ggf. Signieren der Inhaltsdaten, um Authentizität und Integrität sicher zu stellen, wenn zum Beispiel ein von OSCI unabhängig signiertes PDF versendet wird
A3	Autor	Ggf. Verschlüsseln der Inhaltsdaten für den Leser, wenn es eine Vereinbarung oder Vorgabe gibt, die Daten vor der Verwendung von OSCI zu verschlüsseln (bspw. bei XHD angewendet)
A4	Autor	Aufbau der Nachrichten-Struktur, die mit dem Leser vereinbart wurde. Dies ist eine OSCI-ContentContainer-Struktur, in die ein oder mehrere Contents (XML-Strukturierte Inhaltsdaten und ggf. zusätzliche Attachments) verpackt werden. Dabei wird jeder Bestanteil (Content oder Attachment) mit einer ID versehen, so dass der Leser die übermittelten Inhalte im fachlichen Prozess weiter verarbeiten kann

ID	Rolle	Aufgabe
A5	Autor	Ggf. signieren der OSCI-ContentContainer-Struktur, um Authentizität und Integrität sicher zu stellen.
A6	Autor	Ggf. Verschlüsseln der OSCI-ContentContainer-Struktur für den Leser. Dies beinhaltet ggf. auch eine DVDV-Abfrage, um das Leser-Zertifikat zu ermitteln. Dies kann über die XTA-Methode `lookupService()` erfolgen, so dass der Autor keine Kenntnis vom verwendeten Verzeichnisdienst (bspw. DVDV oder SAFE) haben muss.
A7	Autor	Übergabe der verschlüsselten OSCI-ContentContainer-Struktur an den Sender. Dies erfolgt beim Einsatz von XTA in Form eines XTA-Sendeauftrags, der einen MessageMetaData-Header enthält.
S1	Sender	Aufbau des OSCI-Sendeauftrags inkl. ggf. Signatur des Sendeauftrags und ggf. Verschlüsselung für den OSCI-Intermediär. Der Sendeauftrag enthält die für den Leser verschlüsselten Inhaltsdaten in der vom Leser erwarteten Nachrichtenstruktur. Der Aufbau beinhaltet das Ermitteln der OSCI-Parameter für die Übergabe des Auftrags an den OSCI-Intermediär. Die OSCI-Parameter umfassen die URL des OSCI-Intermediärs und die vom Intermediär verwendeten Signatur- und Verschlüsselungszertifikate, sowie das Zertifikat des Empfängers. Diese OSCI-Parameter werden ggf. aus dem DVDV oder SAFE abgerufen. Bei der Nutzung von XTA wird der MessageMetaData-Header vom XTA-Auftrag in den OSCI-Sendeauftrag als Custom-OSCI-Header übernommen.
S2	Sender	Übermittlung des OSCI-Sendeauftrags an den OSCI-Intermediär inkl. Übernahme der OSCI-ProcessCard vom OSCI-Intermediär im Erfolgsfall. Inhalte der OSCI-ProcessCard werden ggf. über den XTA-TransportReport für den Autor aufbereitet.
I1	OSCI-Intermediär	Übernahme des OSCI-Sendeauftrags inkl. ggf. Entschlüsselung des Sendeauftrags und ggf. Signaturprüfung des Sendeauftrags. Gemäß dem Sendeauftrag wird OSCI-ContentContainer-Struktur in der Datenbank abgelegt (asynchrone Kommunikation) oder für die Übermittlung zum Empfänger aufbereitet (synchrone Kommunikation). Falls im OSCI-Sendeauftrag ein MessageMetaData-Header enthalten ist, wird dieser zusammen mit der OSCI-ContentContainer Struktur weiter gegeben.
I2	OSCI-Intermediär	Übermittlung an den Empfänger inkl. Signatur und Verschlüsselung für den Empfänger. o Bei asynchroner Zustellung erfolgt die Übermittlung als Antwort auf einen Abholauftrag. o Bei synchroner Zustellung wird eine Verbindung zur URL des Empfängers aufgebaut und die Nachricht übermittelt und ggf. eine fachliche Antwort entgegengenommen, die dem Sender übermittelt wird. Der Zeitpunkt der Abholung / Übermittlung durch / an den Empfänger wird auf der OSCI-ProcessCard dokumentiert. Die OSCI-ProcessCard kann auch vom Sender im Nachhinein abgeholt werden, um den Abholzeitpunkt abzufragen.
E1	Empfänger	Abholung der Nachricht vom Intermediär (asynchrone Kommunikation) oder Übermittlung der Nachricht durch den Intermediär an die URL des Empfängers (synchrone Kommunikation).
E2	Empfänger	Entschlüsselung der abgeholten Nachricht auf Transport-Ebene. Die Nachricht enthält die ggf. für den Leser verschlüsselte OSCI-ContentContainer-Struktur und ggf. den XTA MessageMetaData Header, falls dieser vom Sender beigelegt wurde.
E3	Empfänger	Validierung der Transport-Signatur, die der OSCI-Intermediär angebracht hat.

ID	Rolle	Aufgabe
E4	Empfänger	Übergabe der ggf. verschlüsselten OSCI-ContentContainer-Struktur an den Leser. Dies erfolgt ggf. per XTA.
L1	Leser	Ggf. Entschlüsselung der verschlüsselten OSCI-ContentContainer-Struktur.
L2	Leser	Ggf. Signatur-Validierung der signierten OSCI-ContentContainer-Struktur
L3	Leser	Entnehmen der Inhaltsdaten (Content(s) und ggf. Attachments) aus der OSCI-ContentContainer-Struktur für die Weiterverarbeitung.
L4	Leser	Ggf. Entschlüsselung der Inhaltsdaten, falls diese außerhalb von OSCI verschlüsselt wurden (bspw. bei XHD)
L5	Leser	Ggf. Signatur-Validierung falls Attachments außerhalb von OSCI direkt am Dokument signiert wurden.

Für eine Ende-zu-Ende Verschlüsselung muss der Autor mindestens eine der Aufgaben A3 und A6 durchführen.

1.3. Voraussetzungen

Folgende Punkte gelten als grundsätzliche Voraussetzungen:

1. Autor und Leser haben sich auf ein Transportprofil geeinigt; dieses Transportprofil verwenden Sender und Empfänger im Auftrag von Autor und Leser; das Transportprofil sollte als Teil des Fachstandards der zu übertragenen Daten definiert werden, weil der Schutzbedarf der Daten von den fachlichen Anforderungen abhängt. Die OSCI-Spezifikation kann hier immer nur einen Rahmen und Mindestanforderungen an die kryptographischen Algorithmen festlegen. Aber ob signiert (Integritätssicherung oder Authentizität oder Nicht-Abstreitbarkeit) oder verschlüsselt (Vertraulichkeit) werden muss, kann nur von der Fachlichkeit festgestellt werden.
2. Fachnachricht liegt vor (ggf. ist diese mehrteilig und vorzugsweise im XML-Format)
3. Schlüsselmaterial liegt dem Autor vor (es kann bspw. aus dem DVDV abgerufen werden), d.h.
   - Zertifikat mit öffentlichem Schlüssel des Lesers für Fachnachricht (Inhaltsdaten)
   - Signatur-Schlüssel zum Signieren der Fachnachricht (Inhaltsdaten)
4. Schlüsselmaterial liegt dem Sender vor (es kann bspw. aus dem DVDV abgerufen werden), d.h.
   - Zertifikat mit öffentlichem Schlüssel des Empfängers für die Adressierung des Empfängers
   - Signatur-Schlüssel zum Signieren der OSCI-Auftragsdaten
   - Zertifikat mit öffentlichem Schlüssel des Intermediärs für die Verschlüsselung der OSCI-Auftragsdaten

Ein Transportprofil muss für die Nutzung einer Ende-zu-Ende Verschlüsselung mindestens folgende Festlegungen machen:

- Die Qualität, der zu nutzenden Zertifikaten (bspw. fortgeschrittene Zertifikate aus einer bestimmten PKI)
- die Quelle der für die Datenübermittlung benötigten, technischen Kommunikationsparameter (z.B. DVDV, SAFE)
- die Signatur von Inhaltsdaten
- die Verschlüsselung von Inhaltsdaten
- die Signatur von Nutzungsdaten
- die Verschlüsselung von Nutzungsdaten
- die zu verwendenden kryptographischen Algorithmen

2 Beispielhafte asynchrone OSCI-Übermittlung

Für die in Abschnitt 2 beschriebene asynchrone Übermittlung wird folgendes zur Vereinfachung festgelegt:

- genau ein `ContentContainer` mit 1 Content und 0..n Attachments wird verwendet. Dies entspricht einer Fachnachricht mit 0..n Anlagen / Anhängen.
- Es wird das Vorgehen für eine asynchrone OSCI-Nachrichtenübermittlung beschrieben.

Bei einer synchronen OSCI-Nachrichtenübermittlung kann ähnlich vorgegangen werden.
Der nachfolgend beschriebene Ablauf verwendet OSCI-Transport 1.2 und XTA 2 Version 3 als etablierte Standards zur sicheren Datenübermittlung in Infrastrukturen der IT-PLR-Mitglieder. Ferner wird in den Beispielen auf die OSCI-1.2-Bibliothek aus der IT-PLR Anwendung Governikus referenziert.
Bezeichner die mit `xta:` anfangen beziehen sich auf den XTA 2 Version 3 Standard.
Beim Ablauf ist die Aufgaben-Nr. aus der Tabelle in Abschnitt 1.2 dem Vorgehen voran gestellt.

2.1. Autor

Voraussetzungen:

a) Dem Autor liegt die aus n Teilen bestehende Fachnachricht vor
b) Autor kennt die Struktur der Inhaltsdaten aus dem verwendeten Transportprofil
c) Autor hat das Zertifikat mit dem öffentlichen Schlüssel des Lesers (dies kann für viele Szenarien vom DVDV abgerufen werden)
d) Der Autor verwendet die OSCI-Bibliothek aus der Anwendung Governikus des IT-PLR

Mögliche alternative Abläufe[1]:

I. Nutzung der OSCI-Bibliothek beim Autor für die Verschlüsselung der Inhaltsdaten
   - [A1, A4, A5, A6] Autor baut verschlüsselte Nachrichtenstruktur auf und verpackt diese mit der Java-Klasse `StoredMessage` für die Übermittlung zum Sender. (siehe Beispiel-Code in den Methoden `createContentContainer()` in `SendEncryptedContent.java` in der OSCI-1.2-Bibliothek Version 2.1 verfügbar seit 22.03.2021)
   - [A7] Die serialisierte `osci:StoredMessage` wird mit den für den Transport erforderlichen Informationen als Auftragsdaten dem Sender übergeben. [A7]
   - Beim Einsatz von `xta:sendMessage` wird die serialisierte `osci:StoredMessage` als `xta:GenericContentContainer/xta:ContentContainer/xta:Message` übertragen. Dabei werden automatisch die in XTA vorgesehenen MTOM Effizienzsteigerungen angewendet.

II. Verschlüsselung der Inhaltsdaten ohne OSCI-Bibliothek
   - [A4] Aufbau einer OSCI-ContentContainer-XML-Struktur basierend auf XML-Content und base64-codierten eingebetteten Attachments. [A4]
   - [A6] Mittels XML-Encryption wird die OSCI-ContentContainer-XML-Struktur verschlüsselt. Hierbei sind die Kryptographischen Vorgaben der OSCI-Spezifikation zu befolgen, da nicht alle in XML-Encryption verwendbaren Algorithmen erlaubt sind.
   - [A7] Der verschlüsselte OSCI-ContentContainer wird dem Sender übergeben

[1] Die aufgezeigten Abläufe sollten, wie im Kapitel Ausblick angedeutet, noch auf Interoperabilität zwischen unterschiedlichen, bestehenden Softwaresystemen untersucht/ getestet werden.

Ergebnis:
Der Autor hat die für den Leser verschlüsselte Fachnachricht in einem Sendeauftrag an den Sender übergeben.

2.2. Sender

Voraussetzungen:

- Dem Sender liegen die Zertifikate des Empfängers und des Intermediärs vor
- Der Sender kennt die Adresse des Empfänger-Intermediärs
- (diese Daten können für viele Szenarien vom DVDV abgerufen werden)

Ablauf:

- Sender ergänzt Nachrichtenstruktur aus `StoredMessage` soweit, dass er eine OSCI-Übertragung zum Intermediär durchführen kann. [S1] (s. Beispiel-Code in der Methode sendStoreDelivery() in der Datei `SendEncryptedContent.java` in der OSCI-1.2-Bibliothek Version 2.1 verfügbar seit 22.03.2021 // EncryptedData von OSCI enthält keine Infos zum Reader, diese Info wird anders transportiert)
- [S2] Sender übermittelt den OSCI-Auftrag inkl. der verschlüsselten Inhaltsdaten-Struktur zum Intermediär

Ergebnis:
Der Sender hat die verschlüsselte Fachnachricht an den Intermediär des Empfängers gemäß dem Sendeauftrag des Autors übermittelt.

2.3. Intermediär

- [I1] empfängt die Nachricht vom Sender
- [I1] entschlüsselt die Nachricht auf Transport-Ebene und führt ggf. die Prüfung der Transport-Signatur durch
- [I1] Speichert die Nachricht für die Abholung durch den Empfänger
- [I2] Die Antwort auf den Abholauftrag durch den Empfänger wird signiert und für den Empfänger verschlüsselt; in der Antwort ist die verschlüsselte Inhaltsdaten-Struktur des Autors enthalten.

2.4. Empfänger

Voraussetzungen:

- Der Empfänger hat den privaten Schlüssel zum Abholen der OSCI-Nachricht vom Intermediär
- Dem Empfänger liegt das Zertifikat des Intermediärs vor
- Der Empfänger kennt die Adresse des Empfänger-Intermediärs
- (die letzten beiden Parameter können für viele Szenarien vom DVDV abgerufen werden)

Ablauf:

- [E1] Der Empfänger holt die gesamte Nachrichtenstruktur vom Intermediär ab; die Nachricht wird hierbei in einer Antwort auf einen Abholauftrag übermittelt
- [E2, E3] Der Empfänger führt alle Schritte zur Entschlüsselung und Signatur-Prüfung auf Transport-Ebene gemäß OSCI-Spezifikation durch
- Die entschlüsselte `ResponseToFetchDelivery` (enthält verschlüsselte `ContentContainer`-Struktur, wie vom Autor erstellt) wird durch den Empfänger mittels `StoredMessage` serialisiert; das Ergebnis der Serialisierung ist eine MIME-Struktur, die den SOAP-Envelope und alle referenzierten Attachments enthält.
- [E4] Die `StoredMessage` wird dem Leser übergeben.

Sofern bei der Übermittlung zwischen Empfänger und Leser XTA eingesetzt wird, wird die serialisierte `StoredMessage` als `xta:GenericContentContainer/xta:ContentContainer/xta:Message` übertragen. Dabei werden automatisch die in XTA vorgesehenen MTOM Effizienzsteigerungen angewendet.

Ergebnis:
Der Empfänger hat die für den Leser verschlüsselte Fachnachricht an den Leser übergeben.

2.5. Leser

Voraussetzungen:

- Der Leser hat den privaten Schlüssel zum Zertifikat, das der Autor unter 2.1 zum Verschlüsseln verwendet hat
- Der Leser kennt insbesondere die Inhaltsdatenstruktur (im Sinne von OSCI-ContentContainer) gemäß dem verwendeten OSCI-Transportprofil.

Ablauf:

- Holt die Nachricht per XTA (`xta:getMessage`) ab oder bekommt die `StoredMessage` anders übermittelt.
  Die verschlüsselten ContentContainer (`EncryptedDataOSCI`) können mit der Methode `encryptedData` aus der Klasse `StoredMessage` ausgelesen werden
- [L1] Der ContentContainer und seine Attachments werden entschlüsselt
- [L2] ggf. wird die Signatur des entschlüsselten ContentContainer validiert (ein Beispiel-Code für die Analyse des Lesers ist in der OSCI-1.2-Bibliothek in `OneWayMessage_ActiveRecipient.java` ab Zeile 324 zu finden)
- [L3] Die Fachnachricht wird mit den n Bestandteilen aus dem entschlüsselten `osci:ContenContainer` entnommen

Ergebnis:
Dem Leser liegt die vom Autor verschlüsselte und vom Sender übermittelte Fachnachricht im Klartext zur Weiterverarbeitung vor.

3 Bespiel für synchrone OSCI-Übermittlung: XHD

Bei der Übertragung von Anträgen für hoheitliche Dokumente wird synchrone OSCI-Übermittlung gemäß der XhD TR-03123[2] des BSI verwendet. Die XhD-Fachnachricht enthält einen verschlüsselten Teil für eine Ende-zu-Ende-Verschlüsselung unabhängig von verschlüsselten OSCI-ContentContainern (Der Autor nutzt Aufgabe A3). Des Weiteren wird DVDV zur Ermittlung des Empfängers und des zu verwendenden Schlüsselmaterials genutzt.
Auch bei der synchronen OSCI-Übermittlung kann zwischen Autor-Sender und Empfänger-Leser synchrones XTA verwendet werden, um die eine bessere Trennung der Aufgaben herbei zu führen. Konkret kann bspw. im Fachverfahren auf Seiten des Autors dann auf die Einbindung der OSCI-Bibliothek verzichtet werden.

[2] Siehe https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03123/TR-03123_node.html und https://www.xrepository.de/details/urn:xoev-de:bsi:standard:xhd , zuletzt aufgerufen am 16.12.2021

4 Erläuterung zum StoredMessage-Objekt

Die von der Governikus KG im Rahmen des IT-PLR Produkts Anwendung Governikus heraus gegebenen OSCI-Bibliothek ermöglicht die Serialisierung einer OSCI-Nachricht mittels StoredMessage-Objekten. In diesem Abschnitt wird die StoredMessage anhand einer Grafik erläutert.