Ministerium für Heimat, Kommunales,
Bau und Digitalisierung
des Landes Nordrhein-Westfalen

Whitepaper Ende-zu-Ende-Verschlüsselung im Zusammenspiel OSCI - XTA

Version 1.00 (Stand: 08.08.2022)

Autoren: Dr. Klaus Lüttich (Governikus); Marius Meierhöfer (Deloitte); Lars Santesson (Capgemini)
Review: Tim Bahnes (d-NRW); Stefan Rauner (Governikus)

Änderungshistorie

Nr.	Datum	Version	Änderungsgrund	durchgeführt von
1	10.02.2022	0.1	Initiale Erstellung	Lars Santesson (Capgemini, i. A. d-NRW)
2	11.02.2022	0.2	Feedback von Herrn Meierhöfer (Deloitte, i. A. IT.NRW) eingearbeitet	Lars Santesson (Capgemini, i. A. d-NRW)
3	17.02.2022	0.3	Feedback von Herrn Bahnes (d-NRW) eingearbeitet	Lars Santesson (Capgemini, i. A. d-NRW)
4	18.02.2022	0.4	Ergänzung der Abbildungen 3 und 4 mit einer Legende	Lars Santesson (Capgemini, i. A. d-NRW)
5	02.03.2022	0.5	Überarbeitung nach Termin am 01.03.2022	Marius Meierhöfer (Deloitte, i. A. d-NRW)
6	10.03.2022	0.6	Qualitätssicherung	Lars Santesson (Capgemini, i. A. d-NRW)
7	16.03.2022	0.7	Überarbeitung nach Termin am 15.03.2022	Marius Meierhöfer (Deloitte, i. A. d-NRW)
8	06.05.2022	0.8	Überarbeitung nach Termin am 21.04.2022	Dr. Klaus Lüttich (Governikus KG)
9	11.07.2022	0.85	Überarbeitung bzgl. Lösungsskizzen und anzupassenden Governikus-Produkten	Dr. Klaus Lüttich (Governikus KG)
10	27.07.2022	0.9	Abarbeitung der Änderungsvorschläge und Formatierung	Marius Meierhöfer (Deloitte, i. A. d-NRW)
11	28.07.2022	0.95	Anpassungen vor Übergabe an Review	Marius Meierhöfer (Deloitte, i. A. d-NRW)
12	08.08.2022	1.00	Einarbeitung Feedback vor Übergabe an d-NRW	Marius Meierhöfer (Deloitte, i. A. d-NRW)

INHALTSVERZEICHNIS

Abbildungsverzeichnis

Tabellenverzeichnis

I. Ausgangslage und Zielsetzung

Im Rahmen der Umsetzung von Einer-für-Alle (EfA)-Online-Diensten im OZG-Kontext müssen Antragsdaten über OSCI-Intermediäre und ggf. XTA-Server vom Online-Dienst bis hin zur empfangenden Fachbehörde versandt werden. Durch eine Ende-zu-Ende-Verschlüsselung soll sichergestellt werden, dass Betreiber von OSCI-Intermediären und zentralen XTA-Servern die Antragsdaten nicht mitlesen können. Mit der heute gelebten Praxis ist eine Ende-zu-Ende-Verschlüsselung nur zwischen XTA-Servern bzw. OSCI-Clients, die direkt OSCI verwenden möglich. Das vorliegende Dokument beschreibt sowohl die Ausgangslage als auch Ansätze, um die Ende-zu-Ende Verschlüsselung auf weitere Systeme auszudehnen. Zudem beschreibt es Zwischenlösungen auf dem Weg hin zu einer Ziellösung.

II. Grundlagen

Grundlagen zum Thema Antragsrouting beinhaltet das Dokument „Anleitung Antragsrouting NRW“[1]. Weitere Grundlagen im Kontext der Ende-zu-Ende-Verschlüsselung werden in diesem Kapitel festgehalten.

II.1. Überblick der Transportwege

Im Kontext des Antragsroutings bei EfA-Online-Diensten in NRW gibt es die in Abbildung 1 dargestellten Transportwege.

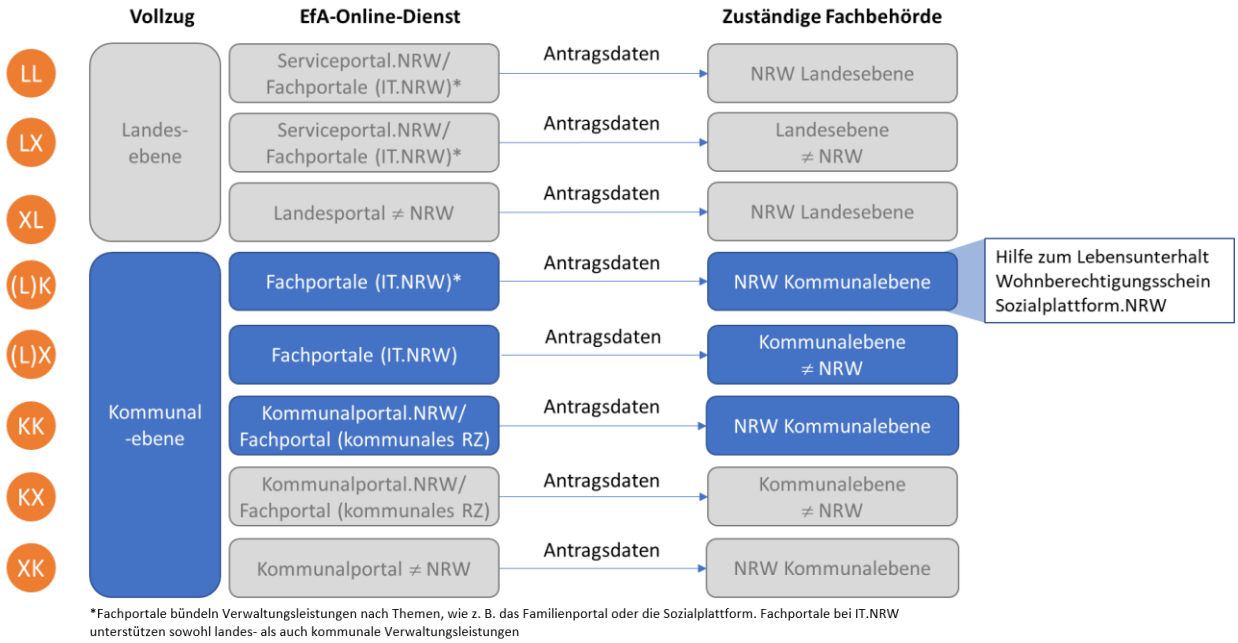
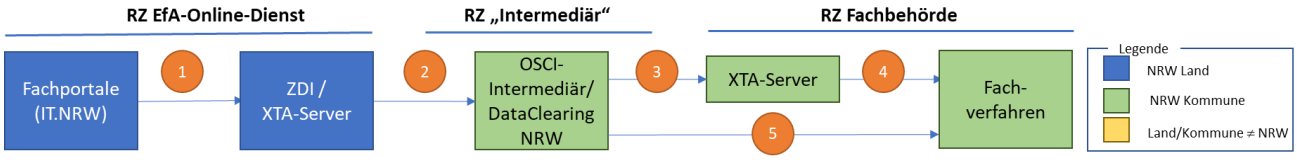


Abbildung 1: Transportwege Antragsrouting in NRW. Im Fokus sind die blau markierten Transportwege.

[1] https://ozg.nrw/service/dokumente

Die in Abbildung 1 dargestellten Kürzel bestehen aus zwei Großbuchstaben (L = Land NRW, K = Kommunalebene NRW, X = außerhalb NRW) , von denen der erste den Standort (Rechenzentrum) des EfA-Online-Dienstes und der zweite den Standort (Rechenzentrum) der zuständigen Fachbehörde darstellt. Bei den Transportwegen (L)K und (L)X steht das L im Klammern, da der Vollzug auf Kommunalebene ist, das Fachportal jedoch vom einem Landes-IT-Dienstleister betrieben wird. Durch die Klammer kann dieser Transportweg von LX mit Vollzug auf Landesebene unterschieden werden.

Betrachtet werden in diesem Dokument die blau markierten Transportwege. Insbesondere nimmt das Dokument Bezug auf dem Transportweg (L)K. Es handelt sich in diesem Fall um eine kommunale Leistung in Verbindung mit einem Online-Dienst, der auf einem Fachportal bei IT.NRW (Land) betrieben wird (bspw. die Sozialplattform). Der Antrag wird an Fachbehörden (bei Kommunen) in NRW transportiert, siehe Abbildung 2.



Hinweis: Bei der ZDI handelt es sich um die Zentrale Datenaustausch Infrastruktur bei IT.NRW, welche als XTA2-Server und OSCI- Sender fungiert.

Abbildung 2: Transportweg (L)K, Beispiel Sozialplattform (IT.NRW)

Das vorliegende Dokument nimmt Bezug auf die einzelnen Teilstrecken entsprechend dieser Abbildung.

II.2. Zu transportierende Daten

Es wird zwischen den folgenden zu transportierenden Daten unterschieden:

- Inhaltsdaten sind fachlich relevante Daten, wie z. B. XML-Daten und Anhänge, die ein Benutzer an einen anderen Benutzer senden möchte.
- Nutzungsdaten sind Daten, die zusätzlich zu den Inhaltsdaten ausgetauscht werden und dazu dienen, den Datenfluss zu kontrollieren sowie zu steuern.

II.3. Verschlüsselungszertifikate

Folgende Verschlüsselungszertifikate werden im Kontext des Antragsroutings eingesetzt:

1. Inhaltszertifikat des Lesers: Der Autor nutzt das Inhaltszertifikat, um Inhaltsdaten zu verschlüsseln. Der Leser, d. h. das empfangende Fachverfahren oder der OSCI-Client (bspw. COM Vibilia), hat den privaten Schlüssel, um die Inhaltsdaten zu entschlüsseln.
2. Transportzertifikat des OSCI-Intermediärs: Der Sender nutzt das Transportzertifikat des OSCI-Intermediärs, um den OSCI-Auftrag zu verschlüsseln. Ein OSCI-Auftrag enthält die Nutzungsdaten und für den Leser verschlüsselte Inhaltsdaten. Der OSCI-Intermediär hat den entsprechenden privaten Schlüssel.

3. Transportzertifikat des Empfängers: Der OSCI-Intermediär nutzt das Transportzertifikat des Empfängers, um die Antwort auf einen OSCI-Auftrag zu verschlüsseln. Der Empfänger, d. h. der XTA-Server auf Empfängerseite, das empfangende Fachverfahren oder der OSCI-Client (bspw. COM Vibilia), hat den entsprechenden privaten Schlüssel.

Das Verschlüsselungszertifikat des Senders wird hingegen nicht betrachtet, da es lediglich für Strecke 2 relevant ist.

II.4. Ver- und Entschlüsselung

Verschlüsselt werden:

- Inhaltsdaten (synonymer Begriff: „innerer Umschlag")
- Inhaltsdaten (verschlüsselt oder unverschlüsselt) ergänzt mit Nutzungsdaten („äußerer Umschlag"). Im Folgenden wird für diesen Fall vereinfacht der Begriff der Verschlüsselung von Nutzungsdaten verwendet, da dieser Begriff auch bei der Beschreibung der Transportprofile der XÖV-Standards verwendet wird.

Sowohl OSCI als auch XTA 2 enthalten Spezifikationen zur Verschlüsselung der Daten. Beide basieren auf dem XML-Encryption[2] Standard. Allerdings gibt es Abweichungen. Die Elemente ContentContainer und EncryptedData sind in OSCI und XTA 2 unterschiedlich ausgeprägt und entsprechend nur im Kontext der jeweiligen Spezifikation nutzbar. So ist z. B. ein auf der OSCI Spezifikation basierendes System nicht dazu in der Lage einen XTA 2 ContentContainer bzw. EncryptedData zu verarbeiten.

II.4.1 Spezifikation XML-Encryption OSCI V1.2

Die XML-Encryption basiert auf der World Wide Web Consortium (W3C)-Spezifikation http://www.w3.org/TR/xmlenc-core/xenc-schema.xsd (XML-Encryption).

Die OSCI Spezifikation enthält in Kapitel 11.3.3 eine Liste von nutzbaren Algorithmen.[3]

Innerhalb von OSCI kann es mehrere Inhaltsdatencontainer geben, welche unabhängig voneinander verschlüsselt und signiert werden können.[4] Zudem werden OSCI-Attachments einzeln verschlüsselt und per Referenz in eigenen MIME-Parts übermittelt.

[2] https://de.wikipedia.org/wiki/XML-Encryption
[3] OSCI 1.2 mit eingearbeiteten Korrigenda 1-7 und "Effiziente Übertragung großer Datenmengen S.231 ff.
[4] OSCI-Transport 1.2 - Entwurfsprinzipien, Sicherheitsziele und -mechanismen S.12

II.4.2 Spezifikation XML-Encryption XTA 2 Version 3

Die Spezifikation der XML-Encryption bei XTA 2 Version 3 (http://xoev.de/transport/xta/211/) basiert ebenfalls auf der W3C-Definition (https://www.w3.org/TR/xmlenc-core/xenc-schema.xsd)[6].

Die XTA 2 Spezifikation enthält weniger Vorgaben mit Hinblick auf erlaubte Verschlüsselungsalgorithmen. In Kapitel 2.4.5 des XTA2-Standards (Version 3) wird lediglich auf das Schema von XEnc verwiesen.[7]

XTA2 bietet im Gegensatz zu OSCI lediglich die Nutzung eines einzelnen ContentContainers an.[8]

II.5. DVDV

DVDV enthält für einen bestimmten Dienst, z. B. den Antrag auf Hilfe zum Lebensunterhalt, Informationen, die für den Versand einer verschlüsselten Nachricht notwendig sind. Pro Dienst wird ein DVDV-Eintragungskonzept erstellt, das beschreibt, wie Eintragungen in das DVDV erfolgen sollen. Alle in Kapitel II.2 aufgeführten Zertifikate werden im DVDV hinterlegt. Ziel ist es, dass die Kommune individuell bestimmen kann, welcher OSCI-Intermediär eingesetzt werden soll und welche Zertifikate für Empfänger sowie Leser vorgesehen sind.

II.6. Vorgehen Datentransport bei etablierten Transportverfahren

Um Herausforderungen im Kontext der Ende-zu-Ende-Verschlüsselung genauer zu erfassen, ist es notwendig, bisherige bereits etablierte Transportverfahren zu verstehen, da diese einen Einfluss auf den Funktionsumfang bereits produktiver Transportlösungen haben. Daher werden in diesem Kapitel bisher etablierte Transportverfahren im Kontext OSCI/XTA beschrieben.

II.6.1 XInneres

Das XInneres-Basismodul ist eine gemeinsame Grundlage für den Datenaustausch, die im Meldewesen (XMeld), zwischen den Staatsämtern (XPersonenstand) und in der Ausländerverwaltung (XAusländer) verwendet wird. XInneres enthält ein Transportprofil, das die Vorgaben für den Datenaustausch beschreibt. Der folgende Ablauf beschreibt die praktische Umsetzung und nimmt Bezug auf die Teilstrecken in Abbildung 2.

- Teilstrecke 1: Autor – Sender: Es erfolgt neben TLS keine weitere Verschlüsselung der Inhaltsdaten.
- Teilstrecke 2: Sender (XTA-Server) – OSCI-Intermediär: Der XTA-Server verschlüsselt die Inhaltsdaten und Nutzungsdaten (XML-Encryption) entsprechend der OSCI-Spezifikation, siehe Kapitel II.4.1. Die Verschlüsselung der Inhaltsdaten erfolgt mit dem Transportzertifikat des Empfängers und die Verschlüsselung der Nutzungsdaten mit Hilfe des Transportzertifikats des empfangenden OSCI-Intermediärs.

[5] Siehe hier: Beim xenc-schema.xd Element „Reference List" steht in der W3G Standard: „<choice minOccurs="1" maxOccurs="unbounded">" und in der XTA 2 Spezifikation „<choice maxOccurs="unbounded>"
[6] Siehe hier: Beim xenc-schema.xd Element „Reference List" steht in der W3G Standard: „<choice minOccurs="1" maxOccurs="unbounded">" und in der XTA 2 Spezifikation „<choice maxOccurs="unbounded>"
[7] Spezifikation XTA2 (Version 3.1) S.24 f.
[8] Spezifikation XTA2 (Version 3.1) S.154

- Vorbereitung Teilstrecke 3-5: OSCI-Intermediär: Der OSCI-Intermediär entschlüsselt die Nutzungsdaten mit dem eigenen privaten Schlüssel. Er bereitet den Transport vor, indem er die Nutzungsdaten (XML-Encryption) entsprechend der OSCI-Spezifikation verschlüsselt. Die Verschlüsselung erfolgt mit Hilfe des Transportzertifikats des Empfängers.
- Teilstrecke 3: OSCI-Intermediär – XTA-Server: Der XTA-Server holt die Antragsdaten vom OSCI-Intermediär ab. Der XTA-Server führt eine Entschlüsselung der Nutzungsdaten und der Inhaltdaten durch. Die Entschlüsselung (XML-Encryption) wird auf Grundlage der OSCI-Spezifikation vorgenommen, siehe Kapitel. II.4.1. Für die Entschlüsselung wird der private Schlüssel des Empfängers genutzt, d. h. es wird ein privater Schlüssel für beide Entschlüsselungen (Inhalts- und Nutzungsdaten) eingesetzt.
- Teilstrecke 4: XTA-Server – Fachverfahren: Das Fachverfahren holt die unverschlüsselte Antragsdaten über eine TLS-gesicherte Verbindung vom XTA-Server ab. Eine zusätzliche Verschlüsselung der Inhaltsdaten erfolgt in der Regel nicht. Es besteht somit kein Bedarf, die Inhaltsdaten auf Grundlage der XML-Encryption in der XTA 2 Spezifikation zu entschlüsseln, siehe Kapitel II.4.2.
- Teilstrecke 5: OSCI-Intermediär – Fachverfahren: Das Fachverfahren holt die Antragsdaten direkt vom OSCI-Intermediär ab. Es führt eine Entschlüsselung der Nutzungsdaten und der Inhaltdaten durch. Die Entschlüsselung (XML-Encryption) wird auf Grundlage der OSCI-Spezifikation vorgenommen, siehe Kapitel. II.4.1. Für die Entschlüsselung wird der private Schlüssel des Empfängers genutzt, d. h. ein privater Schlüssel für beide Entschlüsselungen (Inhalts- und Nutzungsdaten). Auch der OSCI-Client (COM Vibilia) holt die Antragsdaten vom OSCI-Intermediär über diesen Weg ab.

Zusammengefasst gilt:

- Beim Datentransport haben die XTA-Server (Sender und Empfänger) Zugriff auf unverschlüsselte Inhaltsdaten, d.h. die XTA-Server übernehmen jeweils Aufgaben der Rollen Autor bzw. Leser im Auftrag von Autor bzw. Leser. Dies ist explizit von einigen Bedarfsträgern, die den XTA-Server COM Despina einsetzen so gefordert und muss eine valide Implementierungsoption bleiben.
- Das Transportzertifikat des Empfängers wird genutzt, um sowohl Inhaltsdaten als auch Nutzungsdaten zu verschlüsseln, d. h. es wird ein Zertifikat für beide Verschlüsselungen eingesetzt. Es wird kein separates Zertifikat für die Verschlüsselung der Inhaltsdaten verwendet.
- Verschlüsselungen (XML-Encryption) erfolgen ausschließlich auf Grundlage der OSCI-Spezifikation und nicht auf Grundlage der XTA-Spezifikation, siehe Kapitel II.4.

II.7. Eingesetzte Technologien für den Transport von Antragsdaten

Folgende Technologien werden für den Transport von Antragsdaten eingesetzt:

II.7.1 OSCI 1.2-Bibliothek

Die Governikus GmbH & Co. KG stellt eine OSCI Bibliothek[9] im Rahmen des IT-PLR Produkts „Anwendung Governikus" zum Download zur Verfügung. Die Bibliothek implementiert OSCI in der Version 1.2. Sie soll in

[9] https://www.governikus.de/osci-bibliothek/

Clientsystemen wie z. B. Online-Diensten und in Fachverfahren auf Verwaltungsseite implementiert werden. Die OSCI 1.2-Bibliothek wird in Java und .NET herausgegeben.

II.7.2 Governikus COM Tauri (OSCI-Intermediär)

Governikus COM Tauri realisiert einen OSCI-Intermediär entsprechend der OSCI V1.2 Spezifikation. Die Ent- und Verschlüsselung wird auf Grundlage der XML-Encryption-Spezifikation von OSCI V1.2 vorgenommen, siehe Kapitel II.4.1.

II.7.3 Governikus COM Despina (XTA-Server) und weitere XTA-Server im Einsatz bei XInneres

Governikus COM Despina realisiert einen XTA Server entsprechend der XTA 2 Version 3 Spezifikation. Governikus COM Despina ist auf den Datentransport entsprechend dem Vorgehen von XInneres ausgerichtet. Dies hat folgende Konsequenzen:

- COM-Despina ist nicht in der Lage, verschlüsselte Antragsdaten zu erhalten (Teilstrecke 1 in Abbildung 2).
- COM-Despina ist nicht in der Lage, verschlüsselte Antragsdaten an das Fachverfahren zu geben (Teilstrecke 4 in Abbildung 2)
- COM-Despina nutzt den privaten Schlüssel des Empfängers, um sowohl Inhaltsdaten als auch Nutzungsdaten zu entschlüsseln. Eine Entschlüsselung der Inhalts- und Nutzungsdaten mit jeweils getrennten Zertifikaten ist nicht möglich.
- COM-Despina führt keine Verschlüsselung und Entschlüsselung entsprechend der XTA-Spezifikation durch, siehe Kapitel II.4.2.

Es ist davon auszugehen, dass sonstige XTA-Server im Einsatz bei XInneres, z. B. von Dataport und ekom21, ebenfalls diese Einschränkungen haben.

II.7.4 OSCI-Client (Governikus COM Vibilia)

Ein OSCI-Client wird eingesetzt, wenn die empfangende Fachbehörde kein Fachverfahren hat oder wenn das Fachverfahren nicht in der Lage ist, maschinenlesbare Daten automatisch zu empfangen und zu verarbeiten. Governikus bietet für diesen Zweck Governikus COM Vibilia an. Es handelt sich um eine Client-Anwendung, die auf dem Arbeitsplatzrechner des Sachbearbeiters installiert wird.

Governikus COM Vibilia holt die Antragsdaten direkt beim OSCI-Intermediär ab und entschlüsselt diese entsprechend der OSCI 1.2 Spezifikation, siehe Kapitel II.4.1. COM Vibilia nutzt das Zertifikat des Empfängers, um sowohl Inhaltsdaten als auch Nutzungsdaten zu entschlüsseln. Eine Entschlüsselung der Inhalts- und Nutzungsdaten mit jeweils getrennten Zertifikaten ist nicht möglich.

Governikus COM Vibilia führt die Entschlüsselung (XML-Encryption) auf Grundlage der OSCI-Spezifikation durch. Sie ist nicht in der Lage Antragsdaten zu entschlüsseln, wenn diese entsprechend der XTA 2-Spezifikation verschlüsselt worden sind, siehe Kapitel II.4.

III. Ende-zu-Ende Verschlüsselung im OZG-Kontext

Im Folgenden wird auf die Ende-zu-Ende Verschlüsselung bei EfA-Online-Diensten im OZG-Kontext eingegangen. Zunächst werden die Anforderungen festgehalten. Anschließend werden Zwischenlösungen und die angestrebte Ziellösung beschrieben.

III.1. Varianten einer Verschlüsselung der Inhaltsdaten

Die OSCI und XTA Standards sowie die eingesetzten Produkte, müssen in der Lage sein, unterschiedliche Varianten der Übertragung von Daten mit Inhaltsverschlüsselung zu unterstützten. Diese sind in Tabelle 1 aufgeführt.

Tabelle 1: Mögliche Verschlüsselungsvarianten

#	Autor	Sender	Empfänger	Leser
1	XTA2 **ohne** verschlüsselte Inhaltsdaten	Inhaltsdatenverschlüsslung durch Sender im Auftrag des Autors	Inhaltsdatenentschlüsselung durch Empfänger im Auftrag des Lesers	XTA2 **ohne** verschlüsselte Inhaltsdaten
2	XTA2 **mit** verschlüsselten Inhaltsdaten	Übernahme der verschlüsselten Daten in die OSCI-Nachricht	Übergabe der verschlüsselten Inhaltsdaten per XTA2 an den Leser	XTA2 **mit** verschlüsselten Inhaltsdaten
3	XTA2 **mit** verschlüsselten Inhaltsdaten	Übernahme der verschlüsselten Daten in die OSCI-Nachricht	Entschlüsselung durch Empfänger im Auftrag des Lesers	XTA2 **ohne** verschlüsselte Inhaltsdaten
4	XTA2 **ohne** verschlüsselte Inhaltsdaten	Inhaltsdatenverschlüsslung durch Sender im Auftrag des Autors	Übergabe der verschlüsselten Inhaltsdaten per XTA2 an den Leser	XTA2 **mit** verschlüsselten Inhaltsdaten
5	Verwendung der OSCI-Bibliothek zur Verschlüsselung der Inhaltsdaten		Verwendung der OSCI-Bibliothek zur Entschlüsselung der Inhaltsdaten	
6	XTA2 **ohne** verschlüsselte Inhaltsdaten	Inhaltsdatenverschlüsslung durch Sender im Auftrag des Autors	Verwendung der OSCI-Bibliothek zur Entschlüsselung der Inhaltsdaten	
7	XTA2 **mit** verschlüsselten Inhaltsdaten	Übernahme der verschlüsselten Daten in die OSCI-Nachricht	Verwendung der OSCI-Bibliothek zur Entschlüsselung der Inhaltsdaten	
8	Verwendung der OSCI-Bibliothek zur Verschlüsselung der Inhaltsdaten		Entschlüsselung durch Empfänger im Auftrag des Lesers	XTA2 **ohne** verschlüsselte Inhaltsdaten
9	Verwendung der OSCI-Bibliothek zur Verschlüsselung der Inhaltsdaten		Übergabe der verschlüsselten Inhaltsdaten per XTA2 an den Leser	XTA2 **mit** verschlüsselten Inhaltsdaten

Die Lösungsansätze gliedern sich dabei anhand eines Stufenmodells, welches unterhalb in Tabelle 2 dargestellt wird.

Tabelle 2: Stufenmodell der Änderungsvorschläge

#	Zeitraum	Reichweite des Ansatzes	Erreichung E2E Verschlüsselung	Notwendigkeit von Absprachen zwischen den Teilnehmern
1	Kurzfristig	Pilotprojekt Sozialplattform	Anhand der Zwischenlösung in Kapitel IV.1.2	Viel Absprache notwendig
2	Mittelfristig	Interessierte Projekte	Anhand der Handreichung in Kapitel V	Absprache notwendig
3	Langfristig	Alle Nutzer der XTA2 & OSCI Infrastruktur	Anhand der Vorschläge zur Anpassung der Spezifikation in Kapitel VI	Keine Absprache notwendig

III.2. Anforderungen

Im OZG-Kontext beziehen sich die Anforderungen in erster Linie auf die Varianten, die:

- eine Ende-zu-Ende Verschlüsselung von Rechenzentrum des Fachportals bis hin zum Rechenzentrum der empfangenden Fachbehörde/Fachverfahren ermöglichen
- eine Kommunikation vom Fachportal bis hin zum OSCI-Intermediär über XTA-Server unterstützen und
- die Kommunen die vollständige Entscheidungsfreiheit gibt, wie Antragsdaten zu empfangen sind. Dies umfasst sowohl die Möglichkeit einer Ende-zu-Ende-Verschlüsselung bis hin zum Fachverfahren als auch eine Abholung von unverschlüsselten Inhaltsdaten aus einem XTA-Server.

Konkret handelt es sich um die Verschlüsselungsvarianten 2, 3, 7 und 9 siehe Tabelle 1. Für diese Varianten gelten folgende Anforderungen:

1. Der EfA-Online-Dienst sendet verschlüsselte Inhaltsdaten an den XTA-Server (Teilstrecke 1 entsprechend Abbildung 2). Die Verschlüsselung (XML-Encryption) erfolgt mit dem Zertifikat des Lesers.
2. Der XTA-Server kann die Inhaltsdaten nicht einsehen/entschlüsseln (nach Teilstrecke 1).
3. Der XTA-Server verschlüsselt die Nutzungsdaten mit dem Zertifikat des OSCI-Intermediärs (nach Teilstrecke 1).
4. Der XTA-Server sendet verschlüsselte Nutzungsdaten an den OSCI-Intermediär (Teilstrecke 2).
5. Der OSCI-Intermediär entschlüsselt die Nutzungsdaten (nach Teilstrecke 2).
6. Der OSCI-Intermediär kann die Inhaltsdaten nicht einsehen/entschlüsseln (nach Teilstrecke 2).
7. Der OSCI-Intermediär verschlüsselt die Nutzungsdaten mit dem Transportzertifikat des Empfängers (XTA-Server bzw. Fachverfahren auf Empfängerseite).
8. Die Fachbehörde kann die Antragsdaten wie folgt empfangen:
   8.1. Empfang über XTA-Server: Der XTA-Server entschlüsselt die Nutzungsdaten und in Absprache mit dem Zuständigen für den Datenschutz auch die Inhaltsdaten. Das Fachverfahren holt die unverschlüsselten Antragsdaten vom XTA-Server ab.

8.2. Empfang über XTA-Server: Der XTA-Server entschlüsselt die Nutzungsdaten. Das Fachverfahren holt die weiterhin verschlüsselten Antragsdaten vom XTA-Server ab und führt, eine Entschlüsselung der Inhaltsdaten durch. Der XTA-Server (Empfänger) kann die Inhaltsdaten (in Variante 2) nicht einsehen/entschlüsseln (nach Teilstrecke 3).
8.3. Das Fachverfahren holt die Antragsdaten direkt vom OSCI-Intermediär ab und führt eine Entschlüsselung der Nutzungsdaten sowie der Inhaltsdaten durch.
8.4. Empfang über COM-Vibilia: COM-Vibilia holt die Antragsdaten über den OSCI-Intermediär und führt eine Entschlüsselung der Inhaltsdaten und der Nutzungsdaten durch.

9. Es soll möglich sein, unterschiedliche Zertifikate für die Verschlüsselung der Inhaltsdaten und der Nutzungsdaten zu verwenden. Die Kommunen haben die Möglichkeit in das DVDV identische oder unterschiedliche Zertifikate für die Verschlüsselung der Inhaltsdaten und der Nutzungsdaten einzutragen.

Darüber hinaus müssen die Produkte und Standards die weiteren Varianten 1, 4, 5, 6, 8, 9 unterstützten, auch wenn sie im OZG-Kontext in NRW keine Rolle spielen.

III.3. Herausforderungen bei der Umsetzung der Anforderungen

Es gibt aktuell folgende Herausforderungen bei der Umsetzung der Anforderungen:

- Die Verschlüsselung und Entschlüsselung von Daten (XML-Encryption) ist bei OSCI und XTA 2 unterschiedlich ausgeprägt. Somit kann der Leser beim Transportweg 5 (siehe Abbildung 2) keine Entschlüsselung von Inhaltsdaten auf Grundlage der OSCI-Spezifikation vornehmen, wenn der Autor die Verschlüsselung entsprechend der XTA Spezifikation vorgenommen hat, siehe Kapitel.II.4.
- Ebenfalls ist zu beachten, dass auch in keiner der beiden Spezifikationen definiert ist, wie ein verschlüsselter XTA2-ContentContainer per OSCI 1.2 übertragen werden könnte.
- Eine funktionierende Entschlüsselung ist daher nur möglich, wenn genau definiert wird, wie der Empfänger die Antragsdaten abholt (XTA-Server, OSCI-Direkt, OSCI-Client).
- COM Vibilia und bereits etablierte XTA-Server (COM Despina, ekom21, Dataport etc.) sind nicht in der Lage eine Entschlüsselung (XTA-Encryption) auf Grundlage der XTA-Spezifikation vorzunehmen.
- COM Vibilia und bereits etablierte XTA-Server (COM Despina, ekom21, Dataport etc.) können aktuell nur Daten entschlüsseln, wenn Inhalts- und Nutzungsdaten mit demselben Zertifikat verschlüsselt werden.

IV. Zwischenlösungen

Die hier aufgeführten Zwischenlösungen können umgesetzt werden, ohne dass die OSCI- und XTA-Standards verändert werden und ohne dass bereits etablierte Transportlösungen (OSCI-Intermediäre, XTA-Server, OSCI-Clients) angepasst werden müssen.

IV.1.1 Zwischenlösung Stufe 1

Der Transportweg für Zwischenlösung Stufe 1 ist in Abbildung 3 dargestellt.

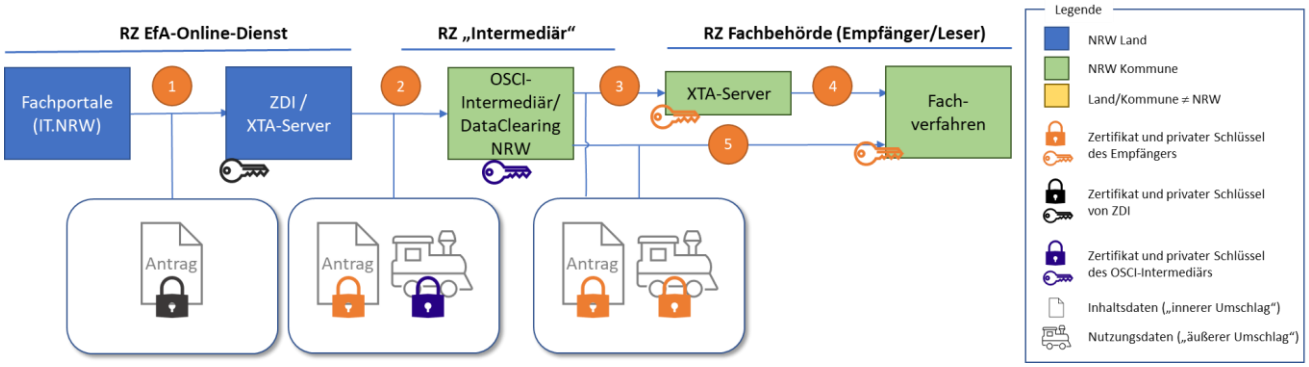


Abbildung 3: Transportweg Zwischenlösung Stufe 1

Der Ablauf ist wie folgt:

- Das Fachportal schickt verschlüsselte Inhaltsdaten an die ZDI (XML-Encryption entsprechend XTA 2 Spezifikation).
- Verschlüsselung mit einem Zertifikat der ZDI.
- Die ZDI entschlüsselt die Inhaltsdaten und verschlüsselt sie erneut (XML-Encryption entsprechend OSCI Spezifikation). Verschlüsselung mit dem Transportzertifikat des Empfängers.[10] ➔ Konsequenz: ZDI kann die Inhaltsdaten lesen
- Die ZDI verschlüsselt die Nutzungsdaten („äußerer Umschlag“). (XML-Encryption entsprechend OSCI-Spezifikation). Verschlüsselung mit dem Transportzertifikat des OSCI-Intermediärs.
- OSCI-Intermediär entschlüsselt den äußeren Umschlag und verschlüsselt diesen erneut, diesmal mit dem Transportzertifikat des Empfängers. Der Zustand der im OSCI-Intermediär abzuholenden Nachricht ist somit genau definiert (XML-Encryption entsprechend OSCI-Spezifikation).
- Der XTA-Server entschlüsselt die Nutzungsdaten und Inhaltsdaten mit dem privaten Schlüssel des Transportzertifikats.
- Das Fachverfahren holt die unverschlüsselten Inhaltsdaten.

[10] Falls das Fachverfahren die Daten direkt ohne XTA erhält, übernimmt das Fachverfahren die Rollen Empfänger und Leser

- Das Fachverfahren holt die Antragsdaten direkt beim OSCI-Intermediär ab und führt die Entschlüsselung der Nutzungs- und Inhaltsdaten durch (ein Zertifikat). Das gleiche Vorgehen gilt für OSCI-Clients (COM Vibilia).

Verbleibende nicht erfüllte Anforderungen sind, siehe Kapitel III.1:

- Der EfA-Online-Dienst verschlüsselt die Antragsdaten (XML-Encryption) mit dem Zertifikat der ZDI und nicht mit dem Zertifikat des Lesers (siehe Anforderung 1).
- Der XTA-Server (Sender) (hier ZDI) kann die Inhaltsdaten einsehen/entschlüsseln (nach Teilstrecke 1) (siehe Anforderung 2).
- Der XTA-Server (Empfänger) bietet für das Fachverfahren keine Möglichkeit an, verschlüsselte Inhaltsdaten abzuholen (siehe Anforderung 8.2). Die Wahlfreiheit auf Empfängerseite, ob entschlüsselte oder verschlüsselte Datenpakete abgeholt werden sollen, soll weiter bestehen bleiben.
- Der XTA-Server (Empfänger) kann die Inhaltsdaten einsehen, da diese unverschlüsselt sind (siehe Anforderung 8.1).
- Es ist nicht möglich, unterschiedliche Zertifikate für die Verschlüsselung der Inhaltsdaten und der Nutzungsdaten zu verwenden (siehe Anforderung 9).

Notwendige Anpassungen:

Die hier beschriebene Zwischenlösung ist bereits umgesetzt. Es sind keine weiteren Anpassungen notwendig.

IV.1.2 Zwischenlösung Stufe 2

Der Transportweg für Zwischenlösung Stufe 2 ist in Abbildung 4 dargestellt.

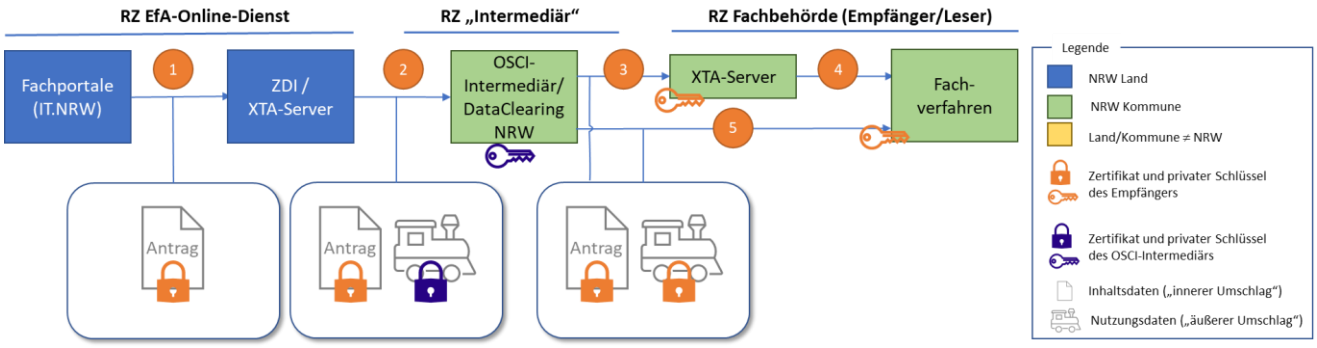


Abbildung 4: Transportweg Zwischenlösung Stufe 2

Diese Zwischenlösung entspricht Stufe 1, mit den folgenden Abweichungen:

- Das Fachportal verschlüsselt die Inhaltsdaten mit dem Transportzertifikat des Empfängers und nicht mit dem Zertifikat der ZDI. (Die Verschlüsselung erfolgt wie in Zwischenlösung Stufe 1 auch mit einer XML-Encryption entsprechend der OSCI-Spezifikation und nicht entsprechend der XTA-Spezifikation).

- Die ZDI muss somit die Inhaltsdaten nicht entschlüsseln und erneut verschlüsseln.

Auf diesem Weg werden im Gegensatz zur beschriebenen Zwischenlösung Stufe 1 folgende Anforderungen erfüllt:

- Der EfA-Online-Dienst verschlüsselt Antragsdaten (XML-Encryption) mit dem Zertifikat des Lesers (siehe Anforderung 1).
- Der XTA-Server (Sender) (hier ZDI) kann die Inhaltsdaten nicht einsehen/entschlüsseln (nach Teilstrecke 1) (siehe Anforderung 2).

Verbleibende nicht erfüllte Anforderungen, d. h. nicht erfüllte Anforderungen, sind, siehe Kapitel III.1:

- Der XTA-Server (Empfänger) bietet für das Fachverfahren keine Möglichkeit an, verschlüsselte Inhaltsdaten zu empfangen (siehe Anforderung 8.2).
- Der XTA-Server (Empfänger) kann die Inhaltsdaten (in Variante 3) einsehen, da diese unverschlüsselt sind (siehe Anforderung 8.1).
- Es ist nicht möglich, unterschiedliche Zertifikate für die Verschlüsselung der Inhaltsdaten und der Nutzungsdaten zu verwenden (siehe Anforderung 9).

Notwendige Anpassungen:

Die hier beschriebene Zwischenlösung erfordert eine Anpassung des Fachportals, damit das Fachportal eine Verschlüsselung der Antragsdaten entsprechend der OSCI-Spezifikation mit dem Transportzertifikat des Empfängers vornehmen kann. Zusätzlich ist eine Anpassung der ZDI notwendig, da diese nun OSCI Objekte anstelle der erwarteten XTA Objekte erhält. Diese müssen zur Funktion der Übergangslösung in die zu erstellende OSCI Nachricht eingebracht werden.

IV.1.3 Handreichung zu den Zwischenlösungen

In diesem Kapitel sollen im Sinne einer Handreichung die notwendigen Festlegungen zum Einsatz der Zwischenlösungen 2 dokumentiert werden, damit interessierte Projekte anhand dieser eine Ende-zu-Ende-Verschlüsselung im Sinne der Verschlüsselungsvarianten 2, 3 und 7 implementieren können. Zu diesen zählt u.a. auch eine allgemeingültige Dokumentation des Vorgehens der Zwischenlösung Stufe 2 aus Kapitel IV.1.2.

Ziel ist es die vorgeschlagenen Anpassungen und weiterführenden Vorschläge zunächst als Handreichung durch die KoSIT veröffentlichen zu lassen und nachfolgend (siehe Kapitel VI) eine Erweiterung der Spezifikationen zu erreichen.

IV.1.3.1. Festlegungen im Hinblick auf die XTA2 (v3) Spezifikation

In den folgenden Unterkapiteln werden die notwendigen Festlegungen im Rahmen der Handreichung im Hinblick auf die XTA2 Spezifikation beschrieben. Als Ausgangspunkt wird die Version 3 von XTA2 genutzt, da diese die aktuelle Version mit Relevanz für die Praxis darstellt.[11]

IV.1.3.2. Festlegung der zulässigen Verschlüsselungsalgorithmen

Damit die Daten in einem OSCI 1.2 konformen Verschlüsselungsformat übermittelt werden können, müssen einige Festlegungen hinsichtlich der zu verwendenden Algorithmen getroffen werden. Zusätzlich muss die von OSCI 1.2 vorgegebene Nutzung von XML-Encryption eingehalten werden, um eine Kompatibilität mit vorhandenen OSCI-Implementierungen sicherzustellen.

In der OSCI Spezifikation ist in Kapitel 11.3.3 eine Liste von nutzbaren Algorithmen festgelegt.[12] Aus dieser Liste wird für diese Handreichung `http://www.w3.org/2009/xmlenc11#aes256-gcm` und `http://www.w3.org/2009/xmlenc11#rsa-oaep` gewählt.

Die Verwendung des Algorithmus und die weiteren Besonderheiten bei der Verwendung von XML-Encryption können dem folgenden Beispiel entnommen werden.

Folgende Regeln sind zu beachten (Normative Definitionen sind der OSCI-1.2-Spezifikation und den Korrigenda-Dokumenten zu entnehmen):

- Es muss die Länge des verwendeten Initialisierungsvektors für AES-GCM explizit mit dem Element IvLength angegeben werden. Die Länge muss 96Bit bzw. 12 Byte groß sein.
- Für die Schlüsselverschlüsselung muss RSA-OAEP verwendet werden und es müssen die im Beispiel angegebene MaskGenerationFunction (MFG) und die angegebene DigestMethod verwendet werden.
- Der verwendete öffentliche Schlüssel für die asymmetrische Verschlüsselung muss mittels RetrievalMethod angegeben werden. Die URI muss der XML-ID eines CipherCertificates in NonIntermediaryCertificates entsprechen.

Dieses XML-Beispiel dient nur der Illustration:

```
<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="encryptedContents" MimeType="text/xml">
    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes256-gcm">
        <osci128:IvLength xmlns:osci128="http://xoev.de/transport/osci12/8" Value="12"/>
    </xenc:EncryptionMethod>
    <ds:KeyInfo>
        <xenc:EncryptedKey>
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#rsa-oaep">
                <xenc11:MGF xmlns:xenc11="http://www.w3.org/2009/xmlenc11#" Algo-
rithm="http://www.w3.org/2009/xmlenc11#mgf1sha256"/>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
```

[11] Spezifikation XTA2 (Version 3.1): https://www.xoev.de/sixcms/media.php/13/XTA2Version3.zip
[12] OSCI 1.2 mit eingearbeiteten Korrigenda 1-7 und "Effiziente Übertragung großer Datenmengen S.231 ff.

```
            </xenc:EncryptionMethod>
            <ds:KeyInfo>
                <ds:RetrievalMethod Type="http://www.w3.org/2000/09/xmldsig#X509Data"
URI="#reader0_cipher_d85a4ba5c417e1fc3a95f8680e9a365086817133eddce719e03b5a154e293692"/>
            </ds:KeyInfo>
            <xenc:CipherData>
                <xenc:CipherValue>[..]</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedKey>
    </ds:KeyInfo>
    <xenc:CipherData>
        <xenc:CipherValue>[..]</xenc:CipherValue>
    </xenc:CipherData>
</xenc:EncryptedData>
```

IV.1.3.3. Aufbau eines abgespeckten OSCI ContentContainer in XTA2

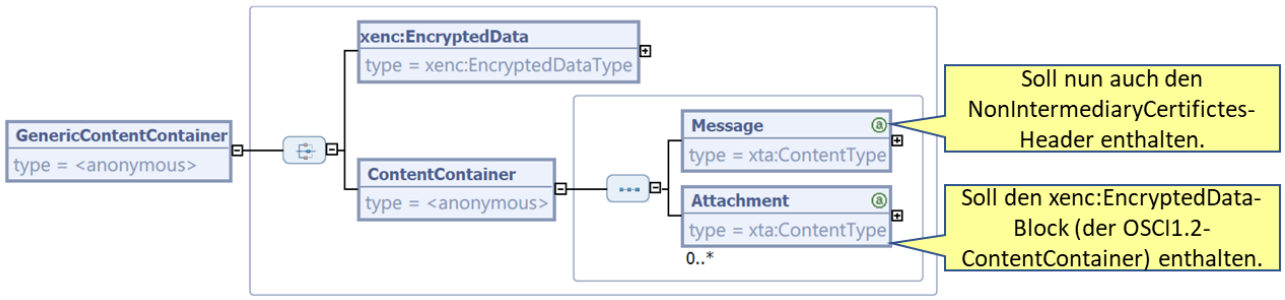


Abbildung 5: Position der OSCI-Elemente in XTA2 für Zwischenlösung

Bei der Verwendung von OSCI-ContentContainer werden folgende Einschränkungen genutzt:

- Alle Bestandteile (Dateien) der Fachnachricht werden als `<osci:Content> <osci:Base64Content>` codiert, so dass alle Daten im OSCI-ContentContainer eingebettet sind.
- Falls der OSCI-ContentContainer signiert wird, muss das Zertifikat mittels RetrievalMethod über die XML-ID referenziert werden. Das Zertifikat muss dann im XML-Block NonIntermediaryCertificates hinterlegt werden.

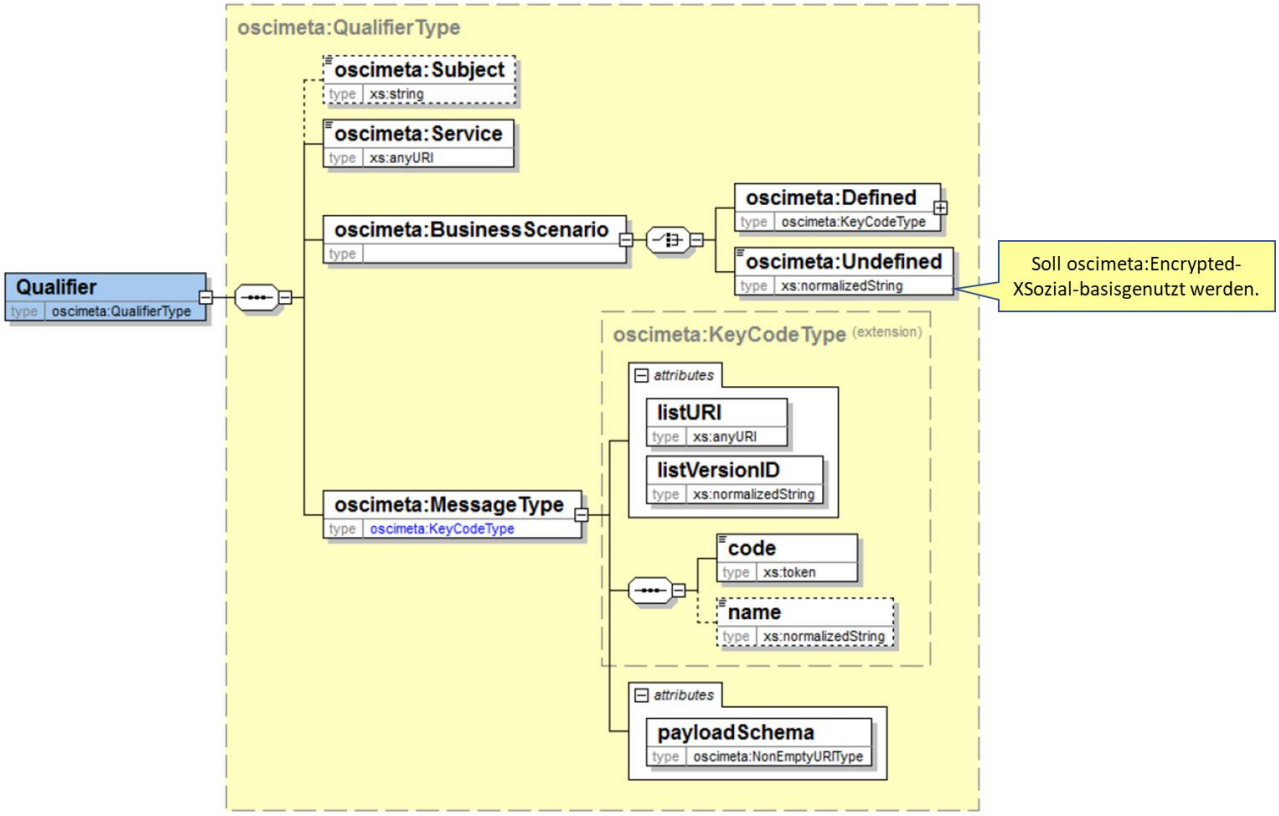
Beispiel für einen OSCI-ContentContainer vor der Verschlüsselung (gekürzt für Illustrationszwecke):

```
<osci:ContentContainer Id="contentcontainer0" xmlns:ds="http://www.w3.org/2000/09/xmld-
sig#" xmlns:osci="http://www.osci.de/2002/04/osci" >
      <ds:Signature>
            [..]
            <ds:KeyInfo>
                  <ds:RetrievalMethod URI="#author0_signa-
ture_2945f1001a2c674333cd55ae50bbd103452659cdbb3bbb9271a033311f2957f1"/>
            </ds:KeyInfo>
      </ds:Signature>
      <osci:Content>
            <osci:Base64Content Id="messageText">TmFjaHJpY2h0ZW50ZXh0</osci:Base64Con-
tent>
      </osci:Content>
      <osci:Content>
            <osci:Base64Content Id="form.xml">PGZvcm0+YmxhPC9mb3JtPg==</osci:Base64Con-
tent>
      </osci:Content>
```

```
      <osci:Content>
       <osci:Base64Content Id="xsozialxslt.xml">PHhzbHQ+Ymx1YjwveHNsdD4=</osci:Base64Con-
tent>
      </osci:Content>
</osci:ContentContainer>
```

IV.1.3.4. Erweiterung der MessageMetaData zur Steuerung der Übertragungsstrecke

Durch die Festlegung auf eine ID (bspw. „`Encrypted-XSozial-Basis`“) für das „`BusinessScenario/Undefined`“ wird dem XTA-Server mitgeteilt, dass die oben genannten Teile der XTA-Nachricht zu entnehmen sind.



V. Ziellösung

In diesem Kapitel sollen diejenigen Vorschläge und Erweiterungen dokumentiert werden, welche notwendig sind, um die Standards OSCI & XTA2 dazu zu befähigen, ohne das Heranziehen einer Handreichung, eine Ende-zu-Ende-Verschlüsselung für die Verschlüsselungsvarianten 2, 3, 7 und 9 zu ermöglichen (siehe Tabelle 1). Insofern diese Anpassungen im Rahmen einer XTA2-Extension Verwendung findet, kann eine native Verschlüsselung der Inhaltsdaten zwischen Autor und Leser inklusive verschiedenartiger Übergange zwischen OSCI und XTA2 sichergestellt werden. Dieses Dokument unterstützt somit die Spezifikationen bei der Erfüllung weitergehender Datenschutzanforderungen.

Um die Anforderungen in Kapitel III.1 zu erfüllen, muss die Ziellösung insbesondere die folgenden Änderungen umsetzen:

- Verwendung der OSCI 1.2 und XTA 2 Standards für einen definierten Übergang von verschlüsselten Inhaltsdaten, die ein Autor in einen XTA-Sendeauftrag einbettet bzw. die ein Leser einer XTA-Abholauftragsantwort entnimmt.
- Nutzung der um eine zusätzliche programmiertechnsiche API erweiterten OSCI 1.2 Bibliothek, die Autor und Sender sowie Empfänger und Leser bei ihren Aufgaben für die Ende-zu-Ende-Verschlüsselung unterstützt. Es wird die bei der Zwischenlösung definierte API-Erweiterung verwendet.
- Erweiterungen an bestehenden und bereits etablierten OSCI-Clients und XTA-Servern sind vorzunehmen, sofern die Ende-zu-Ende-Verschlüsselung auf der kompletten Strecke verwendet werden soll. Governikus COM Vibilia und COM Despina können auch so genutzt werden, dass der Leser die Entschlüsselung an die jeweilige Software delegiert, so dass dem Leser direkt die entschlüsselte Fachnachricht übergeben wird (siehe Strecke 5 in Abbildung 2). Für diese Variante muss die empfangende Software nicht angepasst werden. Für eine umfassende Nutzung der Ende-zu-Ende-Verschlüsselung müssen mindestens die Governikus-Lösungen (COM Despina) und auch weitere Lösungen wie OSCI-Implementierungen und XTA-Server bei z. B. Procilon, Dataport und ekom21 angepasst werden.

Es ist geplant diese Ziellösung im Dialog mit Herstellern von Transportlösungen und der KoSIT zu erarbeiten.

Die aktuell gängigen Implementierungen basieren darauf, dass Fachportale und Fachverfahren im Dialog mit einem XTA-Server Inhaltsdaten in Klartext senden und empfangen können (Verschlüsselungsvariante 1 in Tabelle 1). Darüber hinaus kann die Kommunikation direkt mit einem OSCI-Intermediär, d. h. ohne den Einsatz eines XTA-Servers auf Sender- oder Empfängerseite erfolgen (Verschlüsselungsvarianten 5, 6 und 8).

V.1.1 Vorgeschlagene Erweiterung der XTA2 (v5) Spezifikation

In den folgenden Unterkapiteln wird die vorgeschlagene Erweiterung der XTA2 Spezifikation in Form einer Extension beschrieben. Eine Extension beschreibt eine zusätzliche Parametrisierung der Kernmethoden von XTA2. Diese können definiert werden um spezifische Bedarfe (in diesem Fall das Übermitteln verschlüsselter Datenpakte von XTA2 zu OSCI), die von XTA2 in seiner ursprünglichen Form nicht vorgesehen sind, abzudecken.

Als Ausgangspunkt wird der Entwurf vom 05.05.2022 der Version 5 von XTA2 genutzt, da die Fertigstellung für Anfang 2023 geplant ist. Im Folgenden werden die Inhalte einer XTA2-Extension beschrieben, die Festlegungen für ein E2E-verschlüsselte Verwendung von XTA2 und OSCI 1.2 macht. Diese XTA2-Extension wird im Folgenden als „XTA2-E2E-Enc-Extension" bezeichnet.

V.1.1.1. Festlegung der zulässigen Verschlüsselungsalgorithmen

In Kapitel 2.4.5 des XTA2-Standards wird lediglich auf das Schema von XEnc verwiesen und es wird nur die Verschlüsselung des XTA-ContentContainers ermöglicht.[13] Innerhalb der OSCI Spezifikation wird hingegen in Kapitel 11.3.3 eine Liste von nutzbaren Algorithmen angegeben und es wird jeweils zur Strukturierung des Payloads ein OSCI-ContentContainer verwendet, der dann verschlüsselt wird.[14] Entsprechend können mit OSCI-Implementierungen nur Nachrichten verarbeitet werden, welche der OSCI 1.2 Spezifikation entsprechen, siehe auch Kapitel II.4.

Die Autoren dieses Dokuments schlagen daher vor in der XTA2-E2E-Enc-Extension eine Festlegung der zulässigen Verschlüsselungsalgorithmen vorzunehmen. Diese Algorithmen werden eine Teilmenge der zulässigen Algorithmen für OSCI sein, um eine Kompatibilität der Standards sicherzustellen. Es bietet sich an, diese Algorithmen in einem von der OSCI- und XTA-Spezifikation unabhängigen Dokument festzuhalten, siehe auch Kapitel **Error! Reference source not found.**.

V.1.1.2. Erweiterung der MessageMetaData zur Steuerung der Übertragungsstrecke

Um die Ende-zu-Ende-Verschlüsselung unabhängig von Absprachen zwischen den beteiligten Rollen zu gestalten, ist eine zusätzliche Steuerung notwendig. Aus der OZG-Anforderung zur Ende-zu-Ende-Verschlüsselung ergibt sich, dass der Autor bereits die Inhaltsdaten verschlüsselt. Beim XTA2-Sendeauftrag gibt der Autor an, dass die Daten in verschlüsselter Form gemäß der XTA2-E2E-Enc-Extension an den Sender übergeben werden.

Damit der Wunsch nach Ende-zu-Ende-Verschlüsselung eindeutig zugeordnet werden kann, schlagen die Autoren des Dokuments die Nutzung der MessageMetaData und des dort vorhandenen Elements Extensions vor. Hier soll die neu definierte Extension E2EEncryption genutzt werden, siehe **Error! Reference source not found.**. Diese soll nachfolgenden Elementen der Transportinfrastruktur anzeigen, dass das Element EncryptedData vom Sender unverändert in die OSCI-Nachricht übernommen werden sollen. Ansonsten erfolgt eine Verarbeitung gemäß den aktuellen Implementierungen.

[13] Spezifikation XTA2 (Version 3.1) S.24 f.
[14] OSCI 1.2 mit eingearbeiteten Korrigenda 1-7 und "Effiziente Übertragung großer Datenmengen S.231 ff.

Tabelle 3: Illustration der Ziellösung

Kindelemente von MessageMetaDataType				
Kindelement	Typ	Anz.	Ref.	Seite
wsa:MessageID (ref)		**1**	B.1	109
Der eindeutige Identifikator des Transportauftrags (siehe Abschnitt 2.3.1.1 auf Seite 53).				
Reader	*xta-core:PartyType*	**1**	2.3.2.2	56
Angaben zum Leser.				
Originators	*xta-core:OriginatorsType*	**1**	2.3.1.7	55
Angaben zum Autor und Sender.				
Qualifier	*xta-core:QualifierType*	**1**	2.3.1.8	55
Informationen zur Einordnung der Nutzlast auf Anwendungsebene.				
MessageSize	*xs:positiveInteger*	**1**		
Größe des Objekts GenericContentContainer (globales Element im Body) in Bytes.				
DeliveryAttributes	*xta-core:DeliveryAttributesType*	**1**	2.3.1.4	54
Zeitstempel der Transportetappen.				
Extensions	*xta-core:ExtensionsType*	**0..1**	2.3.10.1	68
Eine Liste von Erweiterungen (Extensions), welche die Funktion des XTA Kerns nach eigener Spezifikation ergänzen. Die Liste kann aus mehreren Erweiterungen bestehen.				
Extension	*xta-core:ExtensionType*	**0..n**	2.3.10.2	69
Eine Erweiterung der Kernparameterinhalte.				
Identifier	*xs:anyURI*	**1**		
Eindeutige Kennung der verwendeten Erweiterung als URI-Angabe: urn:xoev-de:kosit:standard:xta2:extension:e2e-osci-encryption-mmd				
Version	*xs:string*	**1**		
Verwendete Version der Erweiterung nach dem Semantic Versioning Prinzip: 1.0.0				
Data	*xs:anyType*	**1**		
Enthält Daten, die mit einem eigenen Schema definiert und nach einer dazugehörigen Spezifikation der Erweiterung verwendet werden müssen.				
osci:NonIntermediaryCertificates	*osci:NonIntermediaryCertificatesTemplate*	**1**		

Im Element NonIntermediaryCertificates sind nur die beiden folgenden Einträge relevant, die beliebig oft vorkommen dürfen.

- CipherCertificateOtherReader
- SignatureCertificateOtherAuthor

V.1.1.3. Umgang mit n OSCI ContentContainern

Eine Herausforderung im Übergang zwischen den Protokollen stellt die unterschiedliche Behandlung des Elements ContentContainer (Inhaltsdatencontainer) dar. Innerhalb von OSCI kann es mehrere Inhaltsdatencontainer geben, welche unabhängig voneinander verschlüsselt und signiert werden können.[15] XTA2 bietet hingegen lediglich die Nutzung eines einzelnen ContentContainers an.[16]

Eine problemlose Übernahme einer XTA2 Nachricht (ein ContentContainer) in eine OSCI Nachricht (bietet n ContentContainer) ist somit möglich, eine Übernahme einer OSCI Nachricht (ggf. mehrere ContentContainer) in eine XTA2 Nachricht hingegen nicht. Dies ist insbesondere für die Variante 9 in Tabelle 1 kritisch, da u. U. im Rahmen der Erzeugung einer OSCI-Nachricht ggf. mehrere ContentContainer definiert und verschlüsselt wurden, die nun beim Empfang in einen XTA-Container kombiniert werden müssten.

Entsprechend wird vorgeschlagen, dass aus Version 5 der XTA2 Spezifikation der Extensions-Mechanismus verwendet wird, um OSCI-EncryptedData-Elemente zu übertragen, die verschlüsselte OSCI-ContentContainer enthalten. Jeder dieser Container muss eine eindeutige ID erhalten, die auf OSCI-Ebene weiterverwendet wird.

Im beigefügte Code-Beispiel (siehe Kapitel IV 1.3.3) ist lediglich ein Anwendungsfall von 1 bis n ContentContainern abgebildet. Das Beispiel geht nicht auf die Möglichkeit ein, verschachtelte Content Container einzusetzen, da diese Möglichkeit in der Praxis nur selten Verwendung findet.[17]

Durch den gewählten Ansatz werden im Rahmen von XTA2 lediglich weitere Optionen zur Datenübermittlung geschaffen. Für bestehende Verfahren, welche auf XTA2-ContentContainer und XTA2-EncryptedData setzen, wie z.B. die Verfahren des Meldewesens, besteht aus technischer Sicht kein Handlungsbedarf, da die durch die Verfahren genutzten Funktionen nicht angepasst oder verändert werden. Perspektivisch vereinfacht sie das Zusammenspiel zwischen OSCI und XTA allerdings erheblich.

Ein alternatives, weniger invasives Vorgehen in Bezug auf die Handhabung von n OSCI ContentContainern würde die Behandlung von diesen als Attachements darstellen. Bei diesem Vorgehen würde allerdings wichtige Steuerungsinformationen (z.B. die Referenz ID) verloren gehen. Weiterhin würden ggf. zwischen den Teilnehmern vereinbarte Logiken basierend auf diesen Informationen nicht weiter unterstützt werden können. Daher wird diese Variante nicht empfohlen.

V.1.1.4. Zentrales Dokument zur Pflege der erlaubten Verschlüsselungsalgorithmen

Zur Vereinfachung der Pflege der erlaubten Verschlüsselungsalgorithmen in den Spezifikationen für XTA2 und OSCI wird vorgeschlagen eine entsprechende Liste in einem separaten Dokument zu erstellen und aus beiden Spezifikationen heraus auf dieses Dokument zu verweisen.

[15] OSCI-Transport 1.2 - Entwurfsprinzipien, Sicherheitsziele und -mechanismen S.12
[16] Spezifikation XTA2 (Version 3.1) S.154
[17] OSCI-Transport 1.2 - Entwurfsprinzipien, Sicherheitsziele und -mechanismen S.12

VI. Vorgeschlagene Anpassungen in der Referenzimplementierung Governikus

VI.1. Notwendige Anpassungen für die Zwischenlösungen

In den nachfolgenden Unterkapiteln werden die zur Umsetzung der Zwischenlösung notwendigen Anpassungen in der Referenzimplementierung von Governikus beschrieben. Betroffen im Sinne der Zwischenlösung sind dabei die Produkte in Tabelle 4.

Tabelle 4: Zusammenfassung der notwendigen Änderungen der Governikus Referenzimplementierung für Zwischenlösungen

Applikation	**Gewünschtes Verhalten**
OSCI Bibliothek	• Einlesen von NonIntermediaryCertificates-Header ermöglichen (notwendig beim Sender und ggf. beim Leser) • Schreiben (Serialisieren) des NonIntermediaryCertificates-Header (notwendig für Empfänger und Autor) • Direktes Einlesen von Xenc:EncryptedData-OSCI ermöglichen • MessageMetaData-Header mit übertragen (API vorhanden, Sample fehlt)

VI.2. Notwendige Anpassungen für die Ziellösung

In den nachfolgenden Unterkapiteln werden die zur Umsetzung der spezifikationsseitigen Änderungsvorschlägen notwendigen Anpassungen in der Referenzimplementierung von Governikus beschrieben. Betroffen im Sinne der Ziellösung sind dabei die Produkte in Tabelle 5.

Tabelle 5: Zusammenfassung der notwendigen Änderungen der Governikus Referenzimplementierung für Ziellösung

Applikation	**Gewünschtes Verhalten**
OSCI Bibliothek	• Siehe Zwischenlösung VI.1
COM Despina	• Konfiguration erweitern, dass verschlüsselte Datenpakete vorgehalten werden können (Entscheidung, ob Leser verschlüsselte oder entschlüsselte Daten erhalten möchte) • Nutzung der neues APIs zur Generierung von OSCI Nachrichten
COM Vibilia	• Umgang mit MessageMetaData implementieren