



Bericht Praxistest OSCI in NRW

Version: 6
Stand: 09.05.2022
Ansprechperson: Tim BAHNES (ozg@d-nrw.de)

Änderungshistorie			
Datum	Version	Änderung	Autor
11.03.2022	1	Initiale Version	Tim BAHNES
17.03.2022	2	Internes Review	Tim BAHNES
07.04.2022	3	Review MWIDE eingearbeitet	Tim BAHNES
21.04.2022	4	Version für Steuerungskreis Sicherer Transport	Tim BAHNES
09.05.2022	5, 6	Feedback Steuerungskreis Sicherer Transport eingearbeitet	Tim BAHNES

INHALT

1	Ausgangslage	4
2	Zielsetzung	5
2.1	Ziele mit Priorität 1	5
2.1.1	Informationen über OSCI-Intermediäre sammeln	5
2.1.2	Testverfahren für Prüfung eines OSCI-Intermediärs	5
2.1.3	Test der am Projekt beteiligten OSCI-Intermediäre	5
2.2	Ziele mit Priorität 2	5
2.2.1	Test Anbindung Empfänger ohne Fachverfahren	5
2.2.2	Test Anbindung Empfänger mit Fachverfahren	5
3	Testverfahren zur Prüfung der OSCI-Infrastruktur	6
3.2	Testscenario 1: Anbindung eines OSCI-Intermediärs	6
3.3	Testscenario 2: Kommune ohne Fachverfahren	7
3.4	Testscenario 3: Kommune mit Fachverfahren und OSCI-/XTA-Schnittstelle	8
4	Ergebnisse des Praxistests	9
4.1	Informationen über OSCI-Intermediäre sammeln	9
4.1.2	Ergebnisse	9
4.1.3	Erkenntnisse	11
4.1.4	Maßnahmen	12
4.2	Testscenario 1: Anbindung eines OSCI-Intermediärs	12
4.2.1	Ergebnisse	12
4.2.2	Erkenntnisse	14
4.2.3	Maßnahmen	14
4.3	Testscenario 2: Kommune ohne Fachverfahren	14

4.3.1	Ergebnisse	14
4.3.2	Erkenntnisse	14
4.3.3	Maßnahmen	15
4.4	TestszENARIO 3: Kommune mit Fachverfahren und OSCI-/XTA-Schnittstelle	15
4.4.1	Ergebnisse	15
4.4.2	Erkenntnisse	15
4.4.3	Maßnahmen	16
5	Maßnahmen	17

5.1	Aufbau Know-How Installation XTA-Server (Governikus COM Despina)	17
5.2	Optimierung Governikus COM Despina	18
5.3	Referenz-Implementierung der OSCI-/XTA-Anbindung für Fachverfahrens-Hersteller	18
5.4	Veröffentlichung der OSCI-Bibliothek unter neuem Label	20
5.5	Verstärkte Umsetzung von XTA-Schnittstellen und XÖV-Standards in Fachverfahren	20
5.6	Nutzung der Middleware-Komponenten als XTA-Server	21
5.7	Erstellung von OSCI-/XTA-Grundlagendokumentationen	21
5.8	Kommunale Support-Organisationseinheit für Datenaustausch OZG	22
5.9	Bundesweit verfügbare OSCI-Intermediäre erfassen	23
5.10	Verantwortliche Stelle für Anschluss an sichere Transportinfrastruktur	24
5.11	Kommunale Beauftragte für Transportinfrastruktur	24
5.12	Best-Practice-Vorgaben für E2E-Verschlüsselung mittels OSCI/XTA	25

1 Ausgangslage

In der AL Runde vom 08.06.2021 wurde von NRW eine Umfrage unter den Bundesländern initiiert, mit dem Ziel den Grad der Erfüllung der EfA-Mindestkriterien in Bezug auf die OSCI-/XTA-Infrastruktur auf der Empfängerseite zu ermitteln. Ergebnis: „Die OSCI Infrastruktur ist fast überall vorhanden, Lücken müssen geschlossen werden. Gleichwohl können die faktisch vorhandenen Infrastrukturkomponenten häufig in der Praxis noch nicht produktiv genutzt werden.“

Mit der Umsetzung der Sozialplattform im Themenfeld Arbeit und Ruhestand treibt NRW zurzeit die Entwicklung der auf einer Plattform gebündelten EfA-Leistungen des Themenfeldes voran. Dabei wird parallel auch der XÖV Standard XSozial fortentwickelt und gem. der EfA-Vorgaben mit den wesentlichen Fachverfahrensherstellern abgestimmt.

Um die EfA-konforme Nachnutzung einzelner oder aller Dienste der Plattform durch alle Länder und Kommunen grundsätzlich zu ermöglichen, ist ein funktionsfähiger verschlüsselter OSCI-konformer Datenversand der XSozial-Dateien an die Länder sowie eine Bereitstellung der Dateien mittels XTA bis zu den Fachverfahren in den Kommunen unerlässlich.

Dieser, theoretisch weitgehend existierenden Datentransfer, soll nun mit jedem Land praktisch in Form eines Ende-zu-Ende Tests praktisch verprobt werden.

Da wir uns hier an vereinbarten Standard bewegen, wäre dieser Praxistest als Beleg für die Funktionsfähigkeit des länderübergreifenden Datenaustausches dann auch auf andere fachliche Szenarien übertragbar und stellt damit aus Sicht von NRW eine wichtige qualitätssichernde Maßnahme für die erfolgreiche EfA Umsetzung des OZG dar.

2 Zielsetzung

Für die Durchführung des Praxistests wurden im Vorfeld die folgenden Ziele definiert und priorisiert. Dabei wurden alle Ziele mit Priorität 1 versehen, die die grundsätzliche Erreichbarkeit der OSCI-Intermediäre zum Ziel haben. Die Verantwortung für die Anbindung der Fachverfahren liegt innerhalb des jeweiligen Landes, ist aber ein, im Sinne aller Beteiligten, sinnvoller Prüfpunkt. Ziele zur Prüfung der angebotenen Fachverfahren wurden daher mit Priorität 2 versehen.

2.1 Ziele mit Priorität 1

2.1.1 Informationen über OSCI-Intermediäre sammeln

Erstellen einer Liste der zu testenden OSCI-Intermediäre. Dabei werden sowohl grundlegende Informationen wie URL und Zertifikate gesammelt, aber auch mögliche Voraussetzungen für einen erfolgreichen Test (bspw. Registrierung des Originator Zertifikats).

2.1.2 Testverfahren für Prüfung eines OSCI-Intermediärs

Als Basis für alle im Rahmen dieses Projekts durchzuführenden Tests soll ein einheitliches Testverfahren entwickelt werden, das dann genutzt wird, um zu prüfen, ob ein OSCI-Intermediär von einem Sender erreichbar ist und Nachrichten empfangen kann.

Der Test soll möglichst einfach und mit geringem Aufwand, insbesondere auf Seiten des zu testenden OSCI-Intermediärs, durchführbar sein.

Das Testverfahren soll nach Abschluss des Projekts weiterhin anwendbar sein, um neue oder nicht am Projekt beteiligte Intermediäre zu testen.

2.1.3 Test der am Projekt beteiligten OSCI-Intermediäre

Das Testverfahren wird auf alle am Praxistest beteiligten OSCI-Intermediäre angewendet und das Ergebnis dokumentiert.

2.2 Ziele mit Priorität 2

2.2.1 Test Anbindung Empfänger ohne Fachverfahren

Test der Anbindung eines Empfängers ohne Fachverfahren.

2.2.2 Test Anbindung Empfänger mit Fachverfahren

Test der Anbindung eines Fachverfahrens über einen der zu testenden OSCI-Intermediäre.

3 Testverfahren zur Prüfung der OSCI-Infrastruktur

Für den Test der Antragstrecke ausgehend von der Sozialplattform wird zwischen den folgenden drei Szenarien unterschieden. Eine detaillierte Dokumentation¹ der Testverfahren wurde an die teilnehmenden Bundesländer übermittelt.

3.2 Testscenario 1: Anbindung eines OSCI-Intermediärs

Ziel: Übermittlung einer Nachricht an ein Test-Postfach des zu testenden OSCI-Intermediärs.

Dieses Testscenario deckt die manuelle Übertragung einer beliebigen OSCI-Nachricht von einem OSCI-Sender (hier: ZDI²) zum OSCI-Intermediär ab. Nicht im Fokus sind: Sozialplattform, DVDV, XSozial, Empfänger in den Kommunen, Fachverfahren.

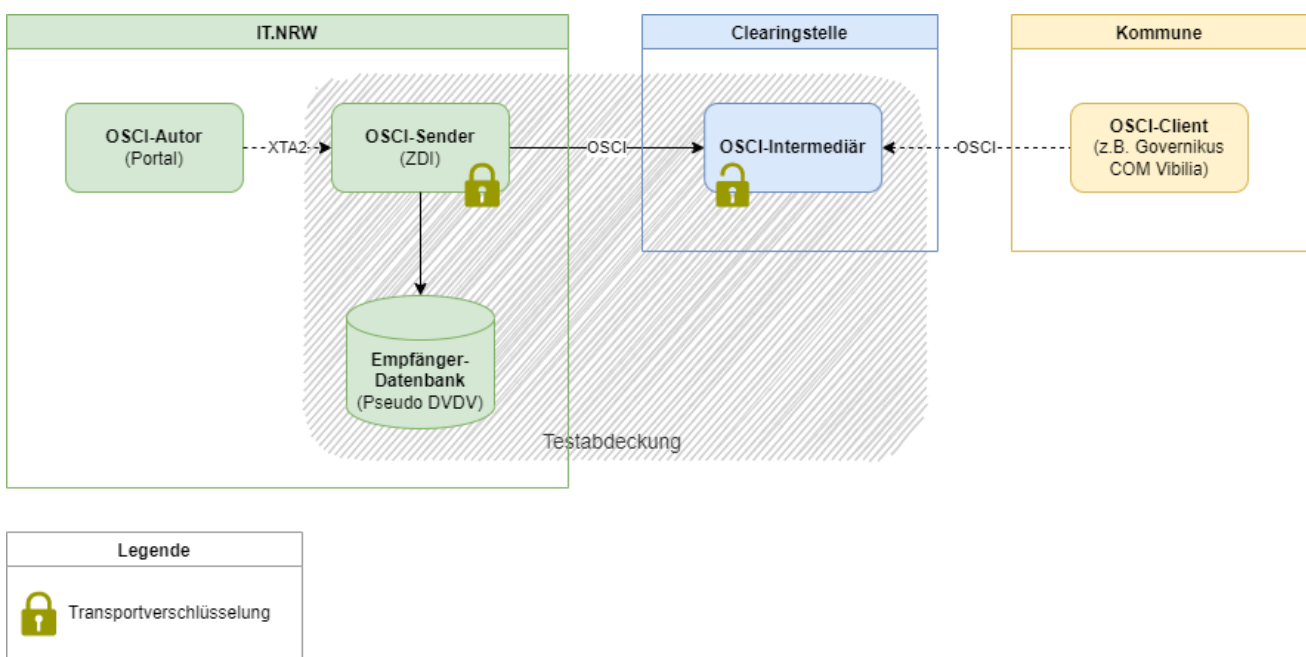


Abbildung 1: Testscenario 1 "Anbindung eines OSCI-Intermediärs"

- Vom OSCI-Sender wird eine OSCI-Nachricht in Richtung OSCI-Intermediär abgesendet.
- Die Nachricht ist nicht inhaltsverschlüsselt, wird aber transportverschlüsselt übertragen.

¹ 20210924_TestkonzeptOSCIIntermediäre.pptx

² Zentrale Dateninfrastruktur: von mehreren Portalen genutzte OSCI-Sendekomponente bei IT.NRW

- Auf dem empfangenden OSCI-Intermediär wird geprüft, ob die Nachricht mit der angegebenen ID fehlerfrei übermittelt wurde. In diesem Fall ist der Test erfolgreich abgeschlossen.

3.3 Testscenario 2: Kommune ohne Fachverfahren

Ziel: Ausgehend von der Sozialplattform kann eine Fachnachricht über die ZDI und Clearingstelle hinweg an einen OSCI Client in einer Kommune übertragen werden.

Dieses Testscenario deckt den Weg vom Portal bis zum OSCI-Client in der Kommune ab.

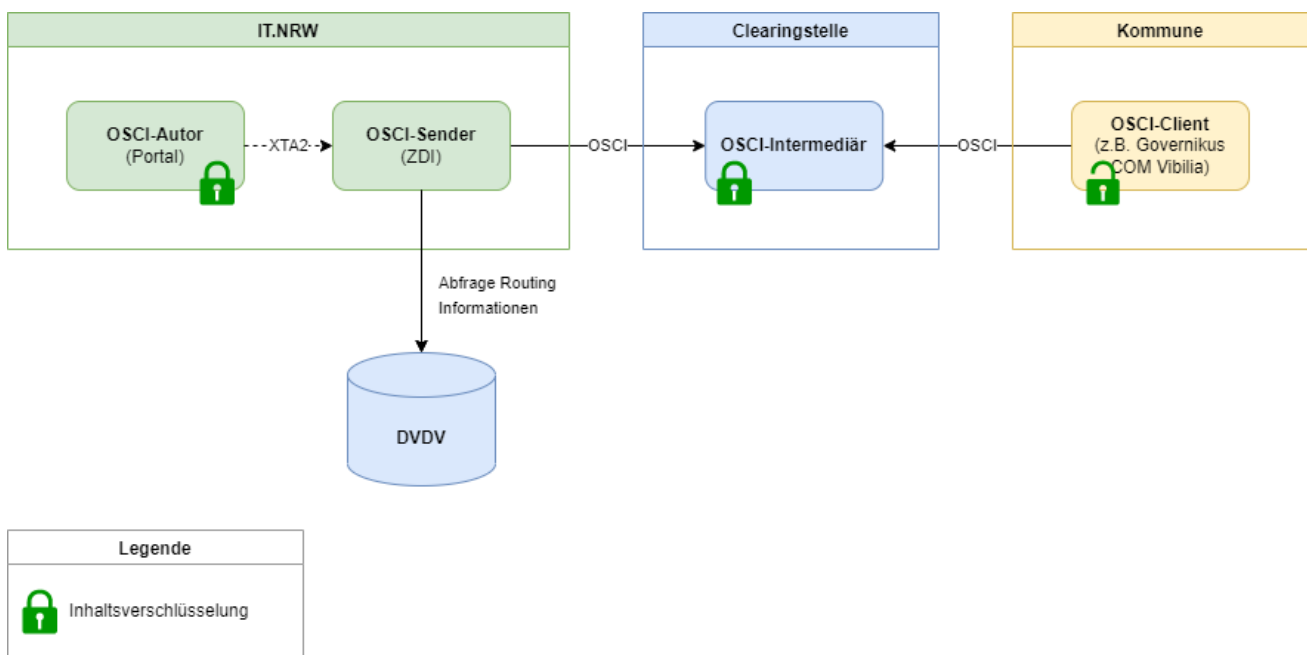


Abbildung 2: Testscenario 2 "Kommune ohne Fachverfahren"

- Aus dem Portal wird über ein Antragsformular eine Fachnachricht an die ZDI übermittelt.
- Die ZDI ermittelt aus dem DVDV den OSCI-Intermediär.
- Die Nachricht wird gemäß des OSCI-Standards sowohl transport- als auch inhaltsverschlüsselt übertragen.
- Die Fachnachricht wird mittels OSCI an den OSCI-Intermediär übertragen.
- In der Kommune kann die Fachnachricht über einen OSCI-Client abgerufen werden. In NRW erfolgt dies im Rahmen der Sozialplattform für die Pilotkommunen mit Hilfe von Governikus COM Vibilia.

3.4 TestszENARIO 3: Kommune mit Fachverfahren und OSCI-/XTA-Schnittstelle

Ziel: Test deckt den kompletten Weg von Portal zum Fachverfahren ab.

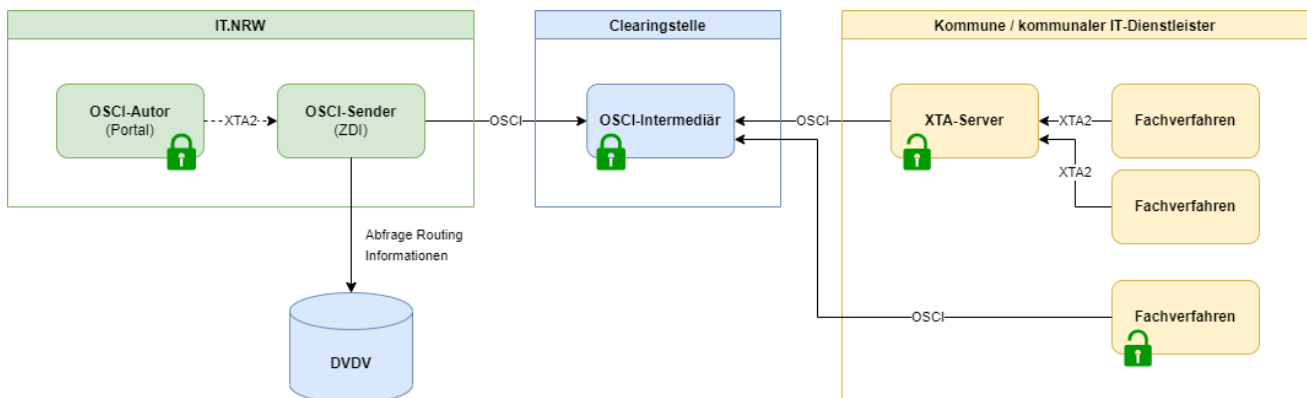


Abbildung 3: TestszENARIO 3 "Kommune mit Fachverfahren und OSCI-/XTA-Schnittstelle"

- Aus dem Portal wird über ein Antragsformular eine Fachnachricht an die ZDI übermittelt.
- Die ZDI ermittelt aus dem DVDV den OSCI-Intermediär.
- Die Nachricht wird gemäß des OSCI-Standards sowohl transport- als auch inhaltsverschlüsselt übertragen.
- Die Fachnachricht wird über OSCI an den OSCI-Intermediär übertragen.
- In der Kommune (bzw. beim betreibenden IT-Dienstleister) holt das Fachverfahren die Nachricht entweder über einen XTA-Server oder direkt mittels OSCI vom Intermediär ab.

4 Ergebnisse des Praxistests

4.1 Informationen über OSCI-Intermediäre sammeln

4.1.2 Ergebnisse

Es erfolgte eine Kontaktaufnahme mit allen von den Bundesländern benannten Ansprechpersonen. Die durchgeführten Abstimmungsgespräche behandelten folgende Themen:

- Erläuterung des Vorhabens.
- Vorstellung der Sozialplattform und der zugrundeliegenden Antragsrouting-Architektur.
- Vorstellung der geplanten Testszenarios.
- Klärung erster Vorgaben und technischer Parameter.

Im Nachgang wurden von den Ansprechpersonen die benötigten Informationen vervollständigt. Die folgende Tabelle fasst den aktuellen Stand zusammen:

Bundesland	Status ³	Hersteller Intermediär	Intermediär Land	Intermediär Kommunen
Baden-Württemberg	⌚	Governikus Esslingen	nein für DVDV, ja für EGVP	ja
Bayern	✓	Governikus	ja	ja
Berlin	⌚	Governikus	ja	ja
Brandenburg	✗	Governikus	ja	ja
Bremen Hamburg Sachsen-Anhalt Schleswig-Holstein	✓	Governikus	ja	ja
Hessen	✓	Governikus	nein, in Planung	ja
Niedersachsen	⌚	abhängig vom Fachverfahren	ja	ja
Nordrhein-Westfalen	✓	Governikus Esslingen	ja	ja
Mecklenburg- Vorpommern	⌚	Governikus	ja	ja
Rheinland-Pfalz	⌚	Governikus	ja	ja
Saarland	✗	Governikus	ja	ja
Sachsen	✓	Governikus	ja	ja
Thüringen	⌚	Governikus	ja	ja

Tabelle 1: Ergebnisse der Informationssammlung

- ³ ✓ = Informationssammlung abgeschlossen
 ⌚ = Informationssammlung noch unvollständig
 ✗ = keine Ansprechperson benannt

4.1.3 Erkenntnisse

Ansprechpersonen schwierig zu ermitteln

- Einige Bundesländer haben keine initialen Ansprechpersonen benannt. In einigen Fällen gestaltete es sich schwierig, die Personen zu finden, die über die entsprechenden technischen Informationen verfügten, da fachliche und technische Ansprechpersonen unterschiedlich waren.

Fehlendes Wissen über OSCI-Infrastruktur

- Bei den direkten Ansprechpartnern ist Wissen sowohl über OSCI im Allgemeinen, aber auch die eingesetzte Infrastruktur vorhanden. Im Umfeld (Projektleitungen, Kommunen usw.) gibt es aber viele Wissenslücken und daraus resultierende Missverständnisse.

Fehlender Wissenstransfer

- Die technische Betreuung der OSCI-Infrastruktur ist in einigen Fällen fast vollständig an externe Berater:innen ausgelagert. Hier kann es dann zu Know How Verlusten kommen, wenn Berater:innen wechseln und der notwendige Wissenstransfer nicht stattgefunden hat.
- Weitere Probleme waren Wechsel in der Verantwortlichkeit oder sogar die vollständige Auflösung der zuständigen Teams, immer verbunden mit entsprechendem Wissensverlust.

Fehlendes Wissen über die OSCI-Infrastruktur des Meldewesens

- Im Meldewesen sind seit vielen Jahren Infrastrukturen auf Basis von OSCI im Betrieb.
- Es wurde festgestellt, dass dieses Wissen in den meisten Fällen in den Ressorts des Meldewesens verblieben ist und somit die Nutzung für andere Verfahren, wie bspw. das Sozialwesen, zunächst nicht in Betracht gezogen wurde.

Unterschiedliche IT-Landschaften und Strategien

- Einige Bundesländer haben sich zusammengeschlossen und nutzen denselben IT-Dienstleister für ihre OSCI-Infrastruktur.
- Bei der Bereitstellung der Infrastruktur für die Kommunen erfolgt dies in einigen Fällen zentral durch das Bundesland, in anderen liegt die Anbindungsverantwortung vollständig bei den Kommunen bzw. deren lokalen IT-Dienstleistern.
- In wenigen Fällen gibt es noch keine Strategie oder Planung für eine OSCI-Infrastruktur im EfA-Kontext.

Bereitschaft für weitere Zusammenarbeit und Informationsaustausch

- Bei allen Bundesländern, mit denen Kontakt aufgenommen wurde, bestand durchgehend eine hohe Bereitschaft und Engagement für die Zusammenarbeit im Rahmen des Praxistests und einen darüberhinausgehenden Informationsaustausch.

Erreichbarkeit mittels OSCI gegeben

- Bei allen kontaktierten Bundesländern ist die Erreichbarkeit über OSCI gegeben, konnte aber noch nicht in allen Fällen durch den Praxistest bestätigt werden.

4.1.4 Maßnahmen

- Erstellung von OSCI-/XTA-Grundlagendokumentationen (siehe 5.7)
- Kommunale Support-Organisationseinheit für Datenaustausch OZG (siehe 5.8)
- Bundesweit verfügbare OSCI-Intermediäre erfassen (siehe 5.9)

4.2 Testscenario 1: Anbindung eines OSCI-Intermediärs

4.2.1 Ergebnisse

Auf Basis des in Abschnitt 3.2 beschriebenen Testscenarios 1 wurde zunächst mit Dataport ein Testpilot durchgeführt und die Erreichbarkeit des OSCI-Intermediärs überprüft. Ziel war, das Testverfahren zu validieren und ggf. zu optimieren. Im weiteren Verlauf werden nun die Tests mit weiteren Bundesländern geplant und durchgeführt.

Die folgende Tabelle dokumentiert den aktuellen Stand der Ergebnisse:

Bundesland	Status Testszenario 1	Bemerkung
Baden-Württemberg	⌚ Test ausstehend	Intermediär noch nicht freigeben.
Bayern	✓ Test erfolgreich	
Berlin	⌚ Test ausstehend	Technische Informationen noch unvollständig.
Brandenburg	✗ -	Keine Ansprechperson benannt.
Bremen Hamburg Sachsen-Anhalt Schleswig-Holstein	✓ Test erfolgreich	Testpilot erfolgreich in 02/2022.
Hessen	⌚ Test ausstehend	Wurde bereits im Rahmen des HzL Vorprojekts an die ZDI angebunden. Test wird aber wiederholt, da u.a. das Zertifikat abgelaufen ist.
Niedersachsen	⌚ Test ausstehend	Technische Informationen noch unvollständig.
Nordrhein-Westfalen	✓ Test erfolgreich	Anbindung von drei OSCI-Intermediären innerhalb NRW im Rahmen der SozPI erfolgreich.
Mecklenburg-Vorpommern	⌚ Test ausstehend	Technische Informationen noch unvollständig.
Rheinland-Pfalz	⌚ Test ausstehend	Technische Informationen noch unvollständig.
Saarland	✗ -	Keine Ansprechperson benannt.
Sachsen	✓ Test erfolgreich	
Thüringen	⌚ Test ausstehend	Technische Informationen noch unvollständig.

Tabelle 2: Ergebnisse Testszenario 1 "Anbindung eines OSCI-Intermediärs"

4.2.2 Erkenntnisse

Zeitaufwändige Ermittlung technischer Informationen

- Die Ermittlung der technischen Informationen nimmt viel Zeit in Anspruch. Häufig waren diese unvollständig oder fehlerhaft.

Freischaltung aller OSCI-Intermediäre in hochsicheren Umgebungen

- In hochsicheren Netzumgebungen dürfen nur bekannte IP-Adressen aus dem Netzbereich adressiert werden. Dies führt dazu, dass bei zentralen Dateninfrastrukturen wie bspw. der ZDI in NRW alle OSCI-Intermediäre separat freigeschaltet werden müssen.
- Zwar ist die Zahl der OSCI-Intermediäre begrenzt, kommen jedoch neue hinzu oder werden die URLs bestehender Intermediäre geändert, reicht es nicht aus, diese im DVDV zu aktualisieren, sondern es müssen auch bspw. Firewall-Freischaltungen erfolgen. D.h. in den Rechenzentren müssen derartige Änderungen bekannt gemacht werden.

4.2.3 Maßnahmen

- Bundesweit verfügbare OSCI-Intermediäre erfassen (siehe 5.9)
- Verantwortliche Stelle für Anschluss an sichere Transportinfrastruktur (siehe 5.10)
- Kommunale Beauftragte für Transportinfrastruktur (siehe 5.11)

4.3 TestszENARIO 2: Kommune ohne Fachverfahren

4.3.1 Ergebnisse

Die folgenden Erfahrungen stammen aus den Tests der Anbindung der ersten Pilotkommunen in NRW im Rahmen der EfA-Leistung HzL auf der Sozialplattform. Diese bilden im Weiteren die Grundlage für Tests mit anderen Bundesländern.

Zum Start der Sozialplattform wurden vier Pilotkommunen an die Sozialplattform angebunden. Dabei wurde als OSCI-Client die Governikus Software COM Vibilia eingesetzt. Hierbei handelt es sich um eine temporäre Lösung, da die Kommunen grundsätzlich über eine Fachanwendung verfügen, diese aber noch nicht über die notwendige XTA-Schnittstelle sowie einen Import der Fachnachrichten im XSozial-Standard verfügt. Sobald diese Funktionen umgesetzt sind, erfolgt eine direkte Anbindung an die Transportstrecke.

4.3.2 Erkenntnisse

Kommunen noch nicht ausreichend vorbereitet

- Insbesondere Kommunen ohne Fachverfahren sind noch unvorbereitet auf den Empfang von Nachrichten aus EfA-Online-Diensten, da hierfür bisher noch keine Notwendigkeit bestand.
-

Fehlende OSCI-Clients

- Bisher gibt es in vielen Kommunen noch keine Möglichkeit, OSCI-Nachrichten aus EfA-Online-Diensten zu empfangen.
- In wenigen Fällen sind Lösungen wie Governikus COM Vibilia im Einsatz. Hierbei handelt es sich aber um reine Arbeitsplatzlösungen, was häufig organisatorische Probleme wie bspw. Vertretungsregelungen mit sich bringt.
- Die für das Meldewesen vorhandenen OSCI-Clients sind spezialisiert auf diesen Anwendungsbereich. Ob diese auch für den Empfang anderer Nachrichten aus EfA-Online-Diensten geeignet ist, muss noch geprüft werden.

4.3.3 Maßnahmen

- Kommunale Support-Organisationseinheit für Datenaustausch OZG (siehe 5.8)
- Nutzung der Middleware-Komponenten als XTA-Server (siehe 5.6)

4.4 TestszENARIO 3: Kommune mit Fachverfahren und OSCI-/XTA-Schnittstelle

4.4.1 Ergebnisse

Bisher wurden noch keine Fachverfahren direkt über die OSCI-Transportstrecke an die Sozialplattform angebunden. In Vorbereitung auf diese Anbindung findet aber bereits ein intensiver Austausch mit mehreren Fachverfahrens-Herstellern statt, die auf Basis des XSozial-Standards eine Anbindung planen. Die daraus resultierenden Erkenntnisse werden hier geteilt.

4.4.2 Erkenntnisse

Umsetzung von XÖV-Standards in den Fachverfahren

- EfA-Online-Dienste müssen gemäß EfA-Mindestanforderung DS₃ eine strukturierte Ausgabe des Antrags im XFall-Format oder nach einem XÖV-Standard erzeugen. Diese Anträge müssen von den Fachverfahren eingelesen werden können, die Umsetzung erfolgt in vielen Fällen aber nur zögerlich.

Fachverfahren unterstützen weder OSCI noch XTA

- Viele Fachverfahren im Sozialwesen verfügen weder über eine OSCI- noch über eine XTA-Schnittstelle. Ähnliche Erfahrungen liegen auch aus dem Bereich Wohnungswesen vor. Es wäre zu prüfen, ob diese Aussage auch auf weitere Bereiche übertragbar ist.
 - Eine OSCI-Anbindung ist mit Hilfe der Governikus OSCI-Bibliothek zwar mit überschaubarem Aufwand möglich, allerdings wird die Integration dieser Bibliothek oft abgelehnt (Gründe dafür wurden leider nur sehr unspezifisch genannt).
-

- Für eine Anbindung über eine XTA-Schnittstelle fehlen den Herstellern gut zugängliche Dokumentationen. Es existieren zwar umfangreiche Spezifikationen, aber nur rudimentäre Beispiele. Insbesondere das Testen der Schnittstelle gestaltet sich aufgrund fehlender Testumgebungen schwierig. Zum Zeitpunkt des Praxistests befand sich eine XTA-Testumgebung der KoSIT in der Entwicklung. Diese ist aktuell aber nur umständlich über einen Dienstleister erhältlich.

Fehlende XTA-Anbindung in den Kommunen

- Viele Kommunen bzw. deren IT-Dienstleister haben bisher noch keine Erfahrung bei der Anbindung von Fachverfahren mittels XTA-Schnittstellen.
- Produkte wie bspw. der Governikus COM Despina sind anspruchsvoll bei der Installation und im Betrieb.

Diskrepanzen zwischen OSCI und XTA2 Spezifikation

- Von den Herstellern wurden Abweichungen zwischen den Spezifikationen von OSCI und XTA berichtet. Die Hersteller wurden gebeten, diese der KoSIT mitzuteilen.

Entschlüsselung im Fachverfahren noch nicht möglich

- Aus datenschutzrechtlicher Betrachtung besteht der Wunsch, die Fachnachrichten erst im Fachverfahren zu entschlüsseln.
- Nach aktuellem Stand ist eine Übergabe von inhaltsverschlüsselten Nachrichten zwischen XTA und OSCI aber nicht vorgesehen. Bisherige Verfahren verschlüsseln entweder eigenständig außerhalb der Standards oder die Inhaltsverschlüsselung erfolgt nur auf der OSCI-Transportstrecke.
- Die fehlende Möglichkeit einer E2E-Verschlüsselung wurde bereits von der KoSIT erkannt und Lösungsalternativen im Dokument „Ende-zu-Ende-Verschlüsselung in einer XTA-OSCI-Infrastruktur (Version 0.8, Entwurf)“⁴ beschrieben. Diese Lösungen müssen aber noch weiter ausgearbeitet und ggf. in den entsprechenden Software-Produkten umgesetzt werden.

4.4.3 Maßnahmen

- Verstärkte Umsetzung von XTA-Schnittstellen und XÖV-Standards in Fachverfahren (siehe 5.5)
- Referenz-Implementierung der OSCI-/XTA-Anbindung für Fachverfahrens-Hersteller (siehe 5.3)
- Aufbau Know-How Installation XTA-Server (Governikus COM Despina) (siehe 5.1)
- Optimierung Governikus COM Despina (siehe 5.2)
- Best-Practice-Vorgaben für E2E-Verschlüsselung mittels OSCI/XTA (siehe 5.12)

⁴ https://www.xoev.de/sixcms/media.php/13/OSCI_E2E_Verschlueselung.pdf

5 Maßnahmen

Die folgenden Maßnahmen leiten sich aus den in Abschnitt 4 dargestellten Erkenntnissen ab. Die Maßnahmen werden in NRW zum Teil schon umgesetzt bzw. werden aktuell geprüft, ob sie umsetzbar sind.

Im Weiteren sollte durch den Steuerungskreis Sicherer Transport geprüft werden, welche der Maßnahmen ggf. in anderen Bundesländern ebenfalls hilfreich sein könnten.

5.1 Aufbau Know-How Installation XTA-Server (Governikus COM Despina)

Hintergrund

- Governikus COM Despina wird als XTA-Server eine wichtige Rolle in der Antragsstrecke spielen.
- Die Installation von COM Despina ist anspruchsvoll und erfordert umfangreiche Kenntnisse des Produkts.
- Wenig Know How in den Kommunen bzw. bei den beauftragten IT-Dienstleistern.
- Der Rollout von COM Despina für viele Kommunen erfordert Ressourcen bei den Kommunen bzw. deren IT-Dienstleistern.

Ziele

- Aufbau von Know How für Installation und Betrieb von Governikus COM Despina.
- Bereitstellung einer schnell betriebsfähigen Installation, die einfach an die produktiven Bedingungen in einer Kommune angepasst werden kann.
- Effizienter und schneller Rollout einer Anbindungsmöglichkeit für die Kommunen.

Details

Beispiel-Installation:

- Die Beispiel-Installation soll vor allem den Know How Aufbau bei den zukünftigen Betreibern ermöglichen.
 - Bereitstellen einer (spezifischen) Anleitung zur Installation.
 - Beispiel-Installation kann direkt getestet werden. Sende- und Empfangs-Client sowie Test-Zertifikate werden bereitgestellt.
 - Optional OSCI-Testintermediär zentral bereitstellen (ggf. kann der OSCI-Testintermediär von Governikus genutzt werden).
-

Unterstützung Rollout:

- Bereitstellen eines vorbereiteten Installations-Pakets für die Kommunen, das bereits an die grundlegenden Anforderungen von Kommunen im Bundesland (hier NRW) angepasst ist und nur minimal konfiguriert werden muss.
- Basiert idealerweise auf der oben angesprochenen Beispiel-Installation.
- Möglich wäre eine Installation in einer virtuellen Umgebung (bspw. Docker).
- Die Möglichkeiten eines solchen Installations-Pakets werden aktuell beim KDN evaluiert und im Anschluss soll eine Verteilung an die Kommunen geplant werden.

5.2 Optimierung Governikus COM Despina

Hintergrund

- Die Installation von COM Despina erfordert insbesondere bei Betreibern mit wenig Erfahrung intensiven Support durch Governikus. Dies verzögert die Installation und bindet Support-Ressourcen bei Governikus.

Ziele

- Vereinfachung von Installation und Betrieb von COM Despina.
- Support durch Governikus nur in Ausnahmefällen notwendig.

Details

- Verbesserung der Dokumentation für Administration und Installation.
- Konfigurationen müssen nachvollziehbar und durch IT-Dienstleister der Kommunen ohne Support von Governikus durchführbar sein.
- Verbesserte Admin-Oberfläche, so dass der Administrator COM Despina vollständig über die Oberfläche einrichten kann, also bspw. ohne Datenbankimport.

5.3 Referenz-Implementierung der OSCI-/XTA-Anbindung für Fachverfahrens-Hersteller

Hintergrund

- Bei Fachverfahrens-Herstellern ohne Erfahrung bei der Anbindung über eine OSCI-/XTA-Schnittstelle ist Wissensaufbau aufwändig.
-

Ziele

- OSCI-/XTA-Anbindung im Rahmen einer einfach nachvollziehbaren Referenz-Implementierung dokumentieren und leicht zugänglich verfügbar machen.

Details

Referenz-Implementierung:

- Quellcode einer Referenz-Implementierung für die OSCI-/XTA-Anbindung als Open Source bereitstellen. Code muss durch FV-Hersteller anpassbar sein. Die Referenz-Implementierung soll sowohl OSCI als auch XTA berücksichtigen.
- Bisher werden Beispiele und Bibliotheken nur für Java und .NET angeboten. Es gibt aber immer mehr Implementierungen, die auf Node.js (Javascript/Typescript) basieren und entsprechend berücksichtigt werden sollten.
- Die korrekte Anwendung einer E2E-Verschlüsselung muss durch die Referenz-Implementierung abgedeckt werden.
- Die bereits existierenden Quellcode-Beispiele der KoSIT und von Governikus können hierfür die Basis bilden.
- Es sollten Referenz-Systeme zur Verfügung stehen, gegen die die Implementierungen der FV-Hersteller entwickelt und getestet werden können.
- Für OSCI steht hier aktuell ein Test-Intermediär von Governikus zur Verfügung. Hier könnte der Zugang durch ein Tutorial erleichtert werden, das alle Schritte beschreibt, wie mit diesem Intermediär entwickelt und getestet werden kann.
- Eine XTA-Testumgebung wird aktuell von der KoSIT entwickelt. In dieser Umgebung kann u.a. die Konformität zu bestehenden Standards getestet werden. Einzelne FV-Hersteller testen bereits mit dieser Testumgebung, weitere Hersteller für den Test der Testumgebung werden gesucht.
- Bei der KoSIT wird aktuell ein öffentliches Portal für die XTA-Testumgebung vorbereitet.

Know How Transfer:

- Workshops mit FV-Herstellern durchführen in der eine Anbindung direkt im Workshop realisiert wird und Fragen geklärt werden können. Als Basis können die bereits existierenden Code-Beispiele dienen.
- In den Workshops könnten auch Grundlagen für Referenzimplementierungen für bisher nicht berücksichtigte Programmierumgebungen geschaffen werden.
- Zentrale Anlaufstelle bei Fragen zur Referenz-Implementierung (OSCI und XTA) einrichten.

5.4 Veröffentlichung der OSCI-Bibliothek unter neuem Label

Hintergrund

- Die von Governikus bereitgestellte OSCI-Bibliothek wird von vielen Fachverfahrensherstellern nicht eingesetzt. Als Argument wird häufig vorgebracht, keine Bibliotheken von anderen Firmen einbinden zu wollen.

Ziele

- Akzeptanz der OSCI-Bibliothek erhöhen, damit mehr Fachverfahrenshersteller diese für die Umsetzung von OSCI-Anbindungen nutzen.

Details

- Es sollte deutlich werden, dass es sich um die OSCI-Bibliothek der deutschen Verwaltung handelt, die von Governikus bereitgestellt wird.
- Die Bibliothek und die dazugehörigen Informationen sollten an einer zentralen Stelle bereitgestellt werden, so dass deutlich wird, dass diese Teil der OSCI-Infrastruktur des IT-PLR ist.

5.5 Verstärkte Umsetzung von XTA-Schnittstellen und XÖV-Standards in Fachverfahren

Hintergrund

- Viele Hersteller von Fachverfahren bieten noch keine XTA2-Schnittstellen für ihre Fachanwendungen an.
- XÖV-Standards werden nur zögerlich umgesetzt.

Ziele

- Alle FV-Hersteller sollten für Produkte, die im EfA-Kontext eingesetzt werden, XTA2-Schnittstellen anbieten und die in den Diensten verwendeten XÖV-Standards umsetzen.

Details

- Bei aktuellen Anbindungen von Fachverfahren gibt es Medienbrüche, da die Fachverfahren nicht direkt per OSCI oder XTA an die Transportstrecke angebunden sind. Teilweise müssen die Nachrichten über COM Vibilia abgerufen und dann manuell ins Fachverfahren eingegeben oder importiert werden.
 - Die Fachverfahrens-Hersteller sollten angehalten werden, XTA-Schnittstellen in ihre Produkte zu integrieren und die XÖV-Standards umzusetzen. Bei den Herstellern fehlt das wirtschaftliche Interesse, dies umzusetzen, da bisher noch wenig Forderung von Seiten der Kommunen hierzu existiert. In vielen Fällen stellt sich auch die Frage der Finanzierung, wenn Hersteller diese Anforderungen zwar umsetzen
-

würden, dies aber als Change Request finanziert haben wollen. In diesem Fall würde dann bspw. eine Kommune eine Schnittstelle für alle anderen Kommunen mitfinanzieren, was in der Regel abgelehnt wird.

5.6 Nutzung der Middleware-Komponenten als XTA-Server

Hintergrund

- In allen Kommunen stehen grundsätzlich OSCI-Empfänger bspw. im Rahmen der EGVP- oder Meldewesen-Infrastruktur zur Verfügung. Häufig werden hierfür Middleware-Komponenten genutzt, die aber nur für spezifische Fachlichkeit eingesetzt werden.
- Diese Infrastruktur wird aktuell noch nicht im Rahmen von OZG-Diensten genutzt, da entweder das Wissen fehlt, ob und wie diese genutzt werden kann oder die eingesetzte Middleware verfügt nicht über geeignete Schnittstellen zu den eingesetzten Fachverfahren.
- Eine Anbindung von Fachverfahren muss entweder direkt über OSCI erfolgen oder über eine XTA-Schnittstelle, die dann aber über ein sicheres Netz kommunizieren muss.

Ziele

- Aufbau einer XTA-Infrastruktur, über die in den Kommunen Fachverfahren angebinden werden können.

Details

- Im Rahmen von Verfahren wie XMeld, Xausländer oder Xpersonenstand sind Kommunen grundsätzlich bereits in der Lage, Nachrichten über einen OSCI-Transportweg zu empfangen.
- Dazu werden u.a. Middleware-Komponenten wie IRIS, proGOV oder OK.KOMM eingesetzt.
- Die Middleware-Komponenten bieten häufig schon Schnittstellen zu Fachverfahren oder Postkorbfunktionalitäten für den Abruf von Nachrichten ohne angeschlossenes Fachverfahren.
- Der IT-PLR sollte beschließen, dass diese Middleware-Komponenten mit XTA₂-Schnittstellen ausgestattet werden, so dass über diese Komponenten der Anschluss weiterer Fachverfahren mittels XTA ermöglicht wird und eine fachunabhängige Transportinfrastruktur entsteht.

5.7 Erstellung von OSCI-/XTA-Grundlegendokumentationen

Hintergrund

- Dokumentationen bestehen in der Regel nur aus Spezifikationen, die aber Grundlagenwissen nur eingeschränkt vermitteln können.
-

Ziele

- Auch Personen aus fachlichen oder nicht-technischen Bereichen sollen in die Lage versetzt werden, sich grundlegende Zusammenhänge und Funktionsweise der OSCI-Infrastruktur anzueignen.

Details

- Es sollten Grundlagendokumentationen erstellt werden, die das notwendige Wissen auf einer Überblicksebene vermitteln, so dass Funktionsweise und Zusammenhänge klar werden. Auf weitergehende vertiefende Information sollte hingewiesen und die entsprechenden Quellen referenziert werden.

5.8 Kommunale Support-Organisationseinheit für Datenaustausch OZG

Hintergrund

- Häufig ist das Wissen über Transportwege und Anbindungsmöglichkeiten stark verteilt, was die Anbindung einzelner Kommunen deutlich erschwert.
- Die einzusetzenden Software-Komponenten für den OZG Datenaustausch sind noch nicht in allen Kommunen flächendeckend im Betrieb und daher nicht immer das notwendige Know How vorhanden.

Ziele

- Aufbau des für den OZG Datenaustausch notwendigen Wissens an zentraler Stelle.
- Länderspezifische Anbindungsmöglichkeiten und das Wissen sollten zentral bekannt sein und bei Bedarf an die Kommunen oder externe Kommunikationspartner vermittelt werden können.
- Zentrale Stelle soll Kommunen und IT-Dienstleister beim Einsatz der Software-Komponenten für den OZG Datenaustausch unterstützen können.

Details

- Anbindungsoptionen mit Best-Practices festlegen.
- Aufbau von Know How für die benötigten Software-Komponenten (bspw. XTA-Server).
- Durchführung von Schulungen/Workshops zu
 - Standards wie OSCI/XTA
 - Anbindungsoptionen
 - notwendigen Technologien
 - Software-Produkten (insb. Installation und Konfiguration sowie Bedienung)
- Unterstützung bei der Software-Beschaffung.
- Wissenstransfer in die Kommunen bzw. zu deren IT-Dienstleistern.

Maßnahme in NRW und bundesweit:

- In NRW wird für diesen Zweck aktuell durch den KDN eine kommunalen Support-Organisationseinheit aufgebaut.
- Bundesweit könnte hier ein Verbund von Support-Dienstleistern geschaffen werden, die gemeinsames Know How teilen und den Support der Kommunen in den jeweils zugehörigen Bundesländern übernehmen.

5.9 Bundesweit verfügbare OSCI-Intermediäre erfassen

Hintergrund

- Bei der Einführung neuer Online-Dienste müssen häufig die anzubindenden OSCI-Intermediäre bekannt sein.
- Informationen zu OSCI-Intermediären der Bundesländer müssen aufwändig abgefragt werden.
- Daten sind zwar grundsätzlich auch im DVDV, können von dort aber nicht einfach abgerufen werden.
- IP-Adressen von OSCI-Intermediären müssen in Firewalls von hochsichereren Netzumgebungen freigeschaltet werden.

Ziele

- Informationsmöglichkeit über die verfügbaren OSCI-Intermediäre schaffen.

Details

- Liste aller OSCI-Intermediäre und bei welchen Einsatzszenarien diese zu nutzen sind (bspw. bei Unterscheidung zwischen Landesdiensten und kommunalen Diensten).
- Infos: URL, Zertifikate, Voraussetzungen für eine Anbindung usw.
- Von der AG Clearingstellenbetreiber wird eine Übersicht über die Betreiber von Clearingstellen und deren Intermediäre gepflegt, aus der einige der oben beschriebenen Informationen hervorgehen. Diese Liste wurde inzwischen auch auf der Seite der KoSIT veröffentlicht und damit leichter zugänglich gemacht⁵.
- Im DVDV wird außerdem aktuell die Möglichkeit geschaffen, über den Auskunftsklient eine Liste der Intermediäre ausgeben zu lassen. Diese Liste wird für Fachverfahrenshersteller auch über eine REST-Schnittstelle abrufbar sein. Der entsprechende Change Request wird voraussichtlich im Oktober 2022 umgesetzt sein.
Zugang zum Auskunftsklient können interessierte Nutzer dann über die Pflegenden Stelle des jeweiligen Bundeslandes erhalten. Weitere Informationen werden nach Umsetzung auf den DVDV-Seiten des ITZBund bereitgestellt⁶.

⁵ <https://www.xoev.de/downloads-2316#Standards>

⁶ <https://www.itzbund.de/DE/itloesungen/standardloesungen/dvdv/dvdv.html>

5.10 Verantwortliche Stelle für Anschluss an sichere Transportinfrastruktur

Hintergrund

- Es gibt noch kein ausreichendes Bewusstsein, dass es für den Anschluss an eine sicherere Transportinfrastruktur eine geregelte Verantwortlichkeit geben muss.

Ziele

- Schaffung einer zentralen verantwortlichen Stelle in jedem Bundesland für den Anschluss an die sichere Transportinfrastruktur.

Details

- Der IT-PLR sollte ein Verständnis dafür schaffen, dass auf Landesseite eine verantwortliche Stelle für den Anschluss geschaffen werden sollte.

5.11 Kommunale Beauftragte für Transportinfrastruktur

Hintergrund

- Bei der Planung eines Online-Dienstes ist Kenntnis über die technischen Möglichkeiten der anzuschließenden Kommunen erforderlich.

Ziele

- Für jede Kommune kann schnell ermittelt werden, welcher IT-Dienstleister für die Fachverfahren und IT-Dienste zuständig ist und welche technischen Möglichkeiten vorhanden sind.

Details

- Jede Kommune sollte über eine beauftragte Person verfügen, die Auskunft geben kann, wie die Kommune an die Transportinfrastruktur angeschlossen ist. Diese Ansprechperson kann auch durch einen von der Kommune beauftragten IT-Dienstleister gestellt werden und mehrere Kommunen verantworten.
 - Der/die Beauftragte sollte insbesondere über folgende Punkte Auskunft geben können:
 - Welcher IT-Dienstleister ist für die Kommune zuständig?
 - Welche im Rahmen der OZG Transportinfrastruktur relevanten technologischen Möglichkeiten sind vorhanden?
 - Gibt es Best Practices für Anbindungsszenarien, die unterstützt werden?
-

5.12 Best-Practice-Vorgaben für E2E-Verschlüsselung mittels OSCI/XTA

Hintergrund

- Die EFA-Mindestanforderung RT5 fordert eine E2E-Verschlüsselung bis zum durch die Behörde definierten Endpunkt.
- Datenschutz- und IT-sicherheitstechnische Regelungen erfordern eine nachvollziehbare und nachweisbare Verschlüsselung vom Online-Dienst bis in die Kommune. Es muss erkennbar sein, wann eine Nachricht den Einflussbereich des Lesers erreicht hat.

Ziele

- Einheitliche und EFA-konforme E2E-Verschlüsselung mittels OSCI/XTA.
- Festlegung von Best-Practices, wie dies mit OSCI/XTA realisiert wird.

Details

- Aktuelle Praxis ist es, dass Autoren Inhalte durch Dienstleister verschlüsseln lassen, die auch die Transportverfahren für die Datenübermittlung anbieten. Diesen steht hierfür die OSCI-Bibliothek zur Verfügung.
 - Wird diese aktuelle Praxis angewendet, müssen die Software-Komponenten für Autor/Sender (XTA-Server) bzw. Empfänger (XTA-Server)/Leser daher über gesicherte Netze miteinander kommunizieren.
 - Die Inhaltsverschlüsselung reicht in diesem Fall nicht von Autor zu Leser, sondern von Sender zu Empfänger.
 - Ziel wäre eine Verschlüsselung des Inhalts im Bereich des Autors vor Übergabe an den Sender (XTA-Server) und eine Entschlüsselung nach Übergabe durch den Empfänger (XTA-Server) in den Bereich des Lesers mittels XML-Encryption und somit vom Online-Dienst bis ins Fachverfahren.
 - Bisher muss der Autor für eine verschlüsselte Übergabe von Nachrichten zwischen XTA und OSCI das Vorgehen und die Umsetzung selbst festlegen und die Inhalte selbst verschlüsseln. Die OSCI-/XTA-Spezifikationen sollten Best-Practice-Vorgaben geben, wie eine Inhaltsverschlüsselung mittels XTA und OSCI zu realisieren ist.
 - Die Umsetzung der Best-Practice-Vorgaben müsste darüber hinaus in den entsprechenden Software-Produkten durchgeführt werden. Dies wären bspw. folgende Governikus Produkte: COM Despina, Governikus Suite (OSCI-Intermediär), SDK Bibliothek, evtl. COM Vibilia.
-