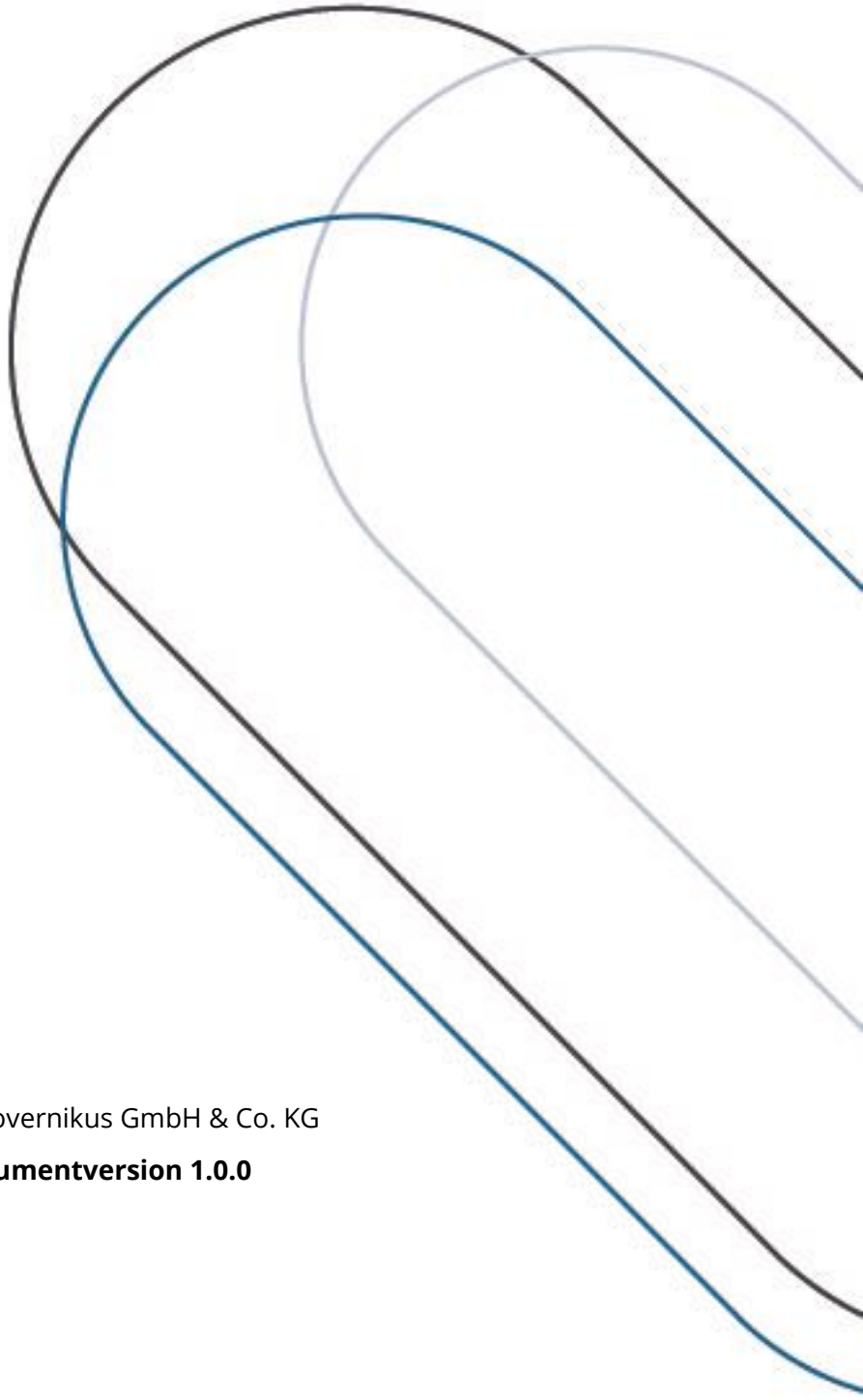
GOVERNIKUS

Leitfaden zum Einsatz von Governikus-Bausteinen in OSCI- und XTA-Infrastrukturen



Dokumentversion 1.0.0

Inhaltsverzeichnis

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

1 Vorwort

Der vorliegende Leitfaden zum Einsatz von Governikus Produkten und Komponenten ergänzt die vorhandenen Materialien zu OSCI und XTA und adressiert die Zielgruppe „Berater:innen/Projektleiter:innen“, die in vielen Digitalisierungsprojekten eine wichtige Rolle spielen.

Es sind die Berater:innen in den Projekten, die eine Lösungsarchitektur entwickeln. Wenn dieser Gruppe die Möglichkeiten der einzelnen Module und deren Kombinationsmöglichkeiten nicht bekannt ist, können Lösungen entstehen, die nicht das volle Potential von OSCI, XTA und der bestehenden organisatorischen und technischen Infrastruktur ausnutzen.

Dieser Leitfaden soll Berater:innen den Zugang zu den notwendigen Fakten und Zusammenhängen erleichtern, die für eine angemessene Definition und Umsetzung von Einsatzszenarien mit OSCI 1.2, XTA und Governikus Produkten und Komponenten notwendig sind.

Ziel dieses Leitfadens ist es, Basiswissen zu den einzelnen Aspekten der elektronischen Kommunikation in der Verwaltung leicht greifbar zu machen und Zusammenhänge darzustellen. Dabei wird keine Vollständigkeit in den Beschreibungen angestrebt, sondern es werden Verweise auf weitere Quellmaterialien zu dem jeweiligen Thema aufgeführt. Damit erhalten Interessierte die Möglichkeit, sich selbstständig detailliert in das jeweilige Thema mittels der Primärquellen einzuarbeiten.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

2 Fakten

2.1 Sichere Kommunikation, VIVA und TOM

Als eine Anforderung für die Umsetzung elektronischer Kommunikationsszenarien taucht meistens auf, dass die Kommunikation sicher sein soll. Woher kommt die Anforderung an eine sichere Kommunikation, wann kann eine Kommunikation als sicher betrachtet werden und was muss dazu unternommen werden?

Die Notwendigkeit für sichere Kommunikation ergibt sich unmittelbar aus dem für Transport relevanten Schutzbedarf der in dem Kommunikationsszenario zu transportierenden Daten und ist somit vom konkreten umzusetzenden Projekt abhängig. Eine generelle und immer passende Antwort bzw. Lösung gibt es nicht, es sei denn, Sie wollen immer die Anforderungen für den höchstmöglichen Schutzbedarf umsetzen. Das würde die Kostenstruktur für die Umsetzung und den Betrieb der Lösung maßgeblich beeinflussen und die Umsetzung in vielen Fällen teurer als notwendig werden lassen.

Daher ist zu Beginn und vor der Skizzierung einer möglichen Lösungsarchitektur festzustellen, welcher Schutzbedarf vorliegt, um zu identifizieren, welche Maßnahmen zum Schutz der Daten umzusetzen sind und welche Schutzziele umzusetzen sind.

2.1.1 Schutz-/Gewährleistungsziele

Neben dem wahrscheinlich bekanntesten Schutzziel „Verfügbarkeit“ sind beim Entwurf der Lösungsarchitektur auf jeden Fall die weiteren VIVA Schutzziele[1] zu betrachten:

- Integrität
- Vertraulichkeit und
- Authentizität

Das reicht noch nicht, um Kommunikationsszenarien in und mit der öffentlichen Verwaltung zu betrachten. Hier fehlt noch der Aspekt der Nachweisbarkeit, also die Möglichkeit, beweisen zu können, ob eine bestimmte Kommunikation zu einem Zeitpunkt stattgefunden hat oder nicht. Und das am besten rechtssicher.

Was genau steht hinter diesen Begriffen?

Vertraulichkeit

Vertraulichkeit bedeutet, dass die Daten nicht für jeden sichtbar sind. Sie dürfen nur von bestimmten Menschen, Systemen oder auch Rolleninhaber:innen gesehen und verwendet werden. Zur Modellierung eines Kommunikationsszenarios sollten Sie als Basis das 4-Corner Modell verwenden. Dort erstellt der Autor die Daten für den Leser. Die wesentlichen Aspekte des

[1] VIVA Schutzziele: Das sogenannte VIVA-Prinzip umfasst genau die vier grundlegenden Schutzziele, d. h., es geht um die Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

4-C-Modells finden Sie an anderer Stelle in diesem Leitfaden. Werfen Sie am besten jetzt einen kurzen Blick auf unsere Zusammenfassung des 4-C Modells (siehe Kap. 2.2).

Integrität

Unter Integrität der Daten ist zu verstehen, dass die Daten nicht nachträglich verändert werden bzw. wurden. Dass also der Leser (Rolle aus dem 4C-Modell) die Daten genau so bekommt wie der Autor (Rolle aus dem 4C-Modell) sie erstellt hat. Tatsächlich lässt sich das nicht sicherstellen. Aber wir können Mechanismen verwenden, die es ermöglichen zu erkennen, ob die Daten nachträglich verfälscht wurden.

Authentizität

Sind die Daten von der Person, die behauptet, der:die Autor:in zu sein? Oft ist die Feststellung der Authentizität der erste Schritt bei der Prüfung, ob eine Autorisierung für eine Abfrage, Änderungsmeldung oder eine andere Funktionalität überhaupt vorliegt.

Nachweisbarkeit

Hat die Kommunikation wirklich stattgefunden? Ist der Antrag (rechtzeitig) versendet worden? Wurde die Entscheidung oder das Ergebnis den Anfragenden übermittelt? Fragen wie diese möchte man im Nachhinein sicher beantworten können.

Verfügbarkeit, **I**ntegrität, **V**ertraulichkeit und **A**uthentizität sind wohl die vier bekanntesten Schutzziele der DSGVO (Datenschutzgrundverordnung). In diesem Abschnitt wurde der Fokus auf die im Kommunikationsszenario auszutauschenden Daten beschränkt. Bei der Umsetzung eines Kommunikationsszenarios ist die Umsetzung der Schutzziele gleichermaßen für die IT-Systeme und Prozesse sicherzustellen.

Weitere Informationen:

Rost, Martin, 2022: Das Standard-Datenschutzmodell (SDM) - Einführung, Hintergründe und Kontexte zum Erreichen der Gewährleistungsziele, Wiesbaden, Springer-Vieweg; ISBN 978-3-658-38879

2.1.2 Maßnahmen, TOM

TOM steht in diesem Leitfaden für **T**echnisch **O**rganisatorische **M**aßnahmen. Das sind Maßnahmen, die durchgeführt werden, um ein Ziel zu erreichen. An dieser Stelle fokussieren wir uns auf Maßnahmen zur Umsetzung der oben benannten Schutzziele.

Verschlüsselung zur Sicherstellung der Vertraulichkeit

Statt der Original-Daten werden die Daten so verändert, dass sie nicht ohne weiteres lesbar bzw. verstehbar sind. Wirft jemand einen Blick auf die verschlüsselten Daten, sieht die Person nichts Sinnvolles. Keine Namen, Daten und Fakten, sondern eine chaotisch erscheinende Abfolge von Zeichen.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Denn die Daten wurden vom Autor für den Leser verschlüsselt. Wenn alles richtiggemacht wurde, kann nur der vom Autor intendierte Leser die Daten mittels Entschlüsselung wieder in die Form bringen, die der Autor ursprünglich angelegt hat. Mit der Maßnahme Verschlüsselung kann die Vertraulichkeit der Daten für den Leser sichergestellt werden.

Ein Einstieg, wie Verschlüsselung/Entschlüsselung funktioniert, was für Arten von Verschlüsselung es gibt und was zu beachten ist, findet sich ebenfalls in diesem Leitfaden (siehe Kap. 0).

Hashwerte zum Nachweis der Integrität

Neben dem Dokument selbst wird zusätzlich eine Art Fingerabdruck erstellt, der ebenfalls mit an den Leser übermittelt wird. Autor und Leser verwenden den gleichen Mechanismus, um den Fingerabdruck zu ermitteln. Wenn der vom Leser erzeugte Fingerabdruck (Hashwert) mit dem vom Autor mitgesendeten übereinstimmt, ist das Dokument sehr wahrscheinlich nicht verändert worden.

Zur Ermittlung des Hashwertes wird eine mathematische Funktion verwendet, die für eine beliebig lange eingegebene Zeichenfolge eine Zahl ermittelt.

Der Fingerabdruck/Hashwert sollte vom Autor signiert werden, um nicht unbemerkt geändert werden zu können. Sonst würden wir nicht merken, dass die Nachricht zusammen mit dem Hashwert verändert wurde.

Wie eine Integritätsprüfung durch Hashes und Signaturen erfolgen kann, findet sich weiter unten in diesem Leitfaden (siehe Kap. 2.3.2).

Signaturen zum Nachweis der Authentizität

Eine Signatur kann man sich stark vereinfacht als eine Art Stempel vorstellen, der zusätzlich an den Daten angebracht wird. Wie bei den früheren Siegel-Stempeln[2] wird bei der Anbringung der Signatur etwas verwendet, auf das nur der Ersteller des Dokuments Zugriff hat. Quasi eine Art moderner Siegel-Stempel. Das heutige Äquivalent ist der private Signaturschlüssel. Dieser darf unter keinen Umständen weitergegeben werden.

Bei Erhalt der Nachricht kann geprüft werden, ob das Siegel gebrochen wurde. Dazu wird beim Empfang der Nachricht mit dem öffentlichen Teil des Signaturschlüssels geprüft, ob die Nachricht mit dem Siegel desjenigen signiert wurde, von dem wir es annehmen.

Protokollieren, um Nachweisbarkeit zur ermöglichen

Um nachweisen zu können, dass eine Nachricht gesendet oder empfangen wurde, werden die einzelnen Bearbeitungsschritte von den beteiligten IT-Komponenten protokolliert. Das Protokoll kann zusammen mit der Nachricht versendet werden oder es kann auch von einem Server abgerufen werden.

Die Integrität und Authentizität des Protokolls sind durch Signaturen sicherzustellen. Sonst ließen sich die Protokolle sehr einfach fälschen.

[2] Achtung: Entspricht nicht dem in der eIDAS-Verordnung verwendeten Siegel-Begriff.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Im Falle der OSCI Kommunikation protokolliert der OSCI-Manager (COM Tauri) die einzelnen Bearbeitungsschritte in der Kommunikation, sendet das Protokoll – auch Laufzettel genannt – mit der Nachricht mit und erlaubt zusätzlich, gezielt den Laufzettel einer Nachricht abzurufen.

2.2 Autor, Sender, Empfänger und Leser: Das 4-Corner-Modell

Zusammenfassung und Einordnung

In der Registermodernisierung und auf EU-Ebene wird das 4-Corner-Modell genutzt, um eine Kommunikation zu beschreiben, in der zwei Kommunikationspartner (Autor, Leser) Nachrichten nicht direkt austauschen, sondern über jeweils einen anderen Partner (Sender bzw. Empfänger).

Die Rollen tragen mit ihren Aufgaben gemeinsam dazu bei, einen fachlichen Prozess umzusetzen:

- Diese Rollen tragen die gemeinsame Verantwortung für den Gesamtprozess.
- Die Rollen können einen Teil ihrer Aufgaben an Dritte delegieren.
- Die Verantwortung ist nicht delegierbar.

Das 4-Corner-Modell hilft, Anforderungen an die sichere Datenübermittlung zu identifizieren und abzubilden.

Es ermöglicht, systematisch zu erkennen:

- aus welchen Aufgaben ein Prozess besteht,
- wie sich die Aufgaben auf unterschiedliche Rollen verteilen und wie die Rollen zusammenwirken,
- welche Anforderungen sich für die verschiedenen Rollen ergeben,
- wo Einflussbereiche enden und entsprechend Übergänge stattfinden.

Das 4-Corner-Modell

- ist technikunabhängig.
- beschreibt anhand der Rollen Einflussbereiche, ohne die Umsetzung einzuschränken.
- Die Aufgaben einer Rolle können durch mehrere Organisationen erbracht werden.
- Die Gesamtverantwortung und damit Steuerung müssen klar zugeordnet sein (i. d. R. bei einer Organisation liegen).
- Eine Organisation kann in mehreren Rollen Aufgaben übernehmen oder die Verantwortung innehaben.
- Hierbei ist auf Einflussgrenzen zu achten, z. B. welche Rollen eine Fachnachricht im Klartext sehen dürfen.
- Hierbei ist auf Konflikte zu achten, z. B. kann eine beauftragte Stelle nicht die Auftraggebende Stelle kontrollieren.

Die Rollen im 4-Corner-Modell

Der folgende Abschnitt gibt nur eine sehr kurze Zusammenfassung der Rollen, so dass ein genereller Eindruck entsteht. Eine umfangreichere Beschreibung findet sich in den angegebenen Quellen.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Autor

Der Autor ist für den Inhalt der Nachricht und deren Gestaltung verantwortlich. Es ist seine Aufgabe, Authentizität und Integrität der Nachricht und deren Vertraulichkeit sicherzustellen. Wenn notwendig, signiert und verschlüsselt er den Inhalt.

Sender

Der Sender ist für den Transport der Nachricht zum Empfänger verantwortlich. Es ist seine Aufgabe, den vereinbarten Transportkanal zu verwenden und die für den Transport notwendige Infrastruktur zu betreiben.

Empfänger

Der Empfänger nimmt die Nachrichten für den Leser entgegen und stellt sicher, dass sie nur dem adressierten Leser zur Verfügung gestellt werden. Dabei überprüft er die Nutzung der Methoden des Transportkanals.

Leser

Der Leser ist für den Erhalt der Nachricht und deren Verarbeitung verantwortlich. Er muss sicherstellen, dass der Eingang der Nachricht nachvollziehbar ist und die vereinbarten Schutzziele eingehalten werden.

Weitere Informationen: XTA Rahmenbedingungen:

https://www.xoev.de/xta/rahmenbedingungen

Technische Perspektiven der Registermodernisierung; Peter Parycek, Simon Sebastian Hunt & Basanta E.P. Thapa
https://www.oeffentliche-it.de/documents/10181/188095/Technische+Perspektiven+der+Registermodernisierung.pdf

2.3 Ein bisschen angewandte Kryptografie

„Was ist Kryptografie und warum ist sie so wichtig?“ fragt Klaus Schmeh in seinem Buch „Kryptografie, Verfahren – Protokolle – Infrastruktur“ und gibt in dem Kapitel eine kurze und eine lange Antwort. Die kurze Antwort in Kapitel 2.1.1 auf Seite 9 lautet:

> *Kryptografie ist die Lehre von der Verschlüsselung von Daten.*

Die längere Antwort in Kapitel 2.1.2 ist deutlich umfangreicher und enthält Aussagen wie:

- Kryptografie ist eine Wissenschaft.
- Ein wichtiges Hilfsmittel der Kryptografie ist die Mathematik.
- Ein anderes wichtiges Hilfsmittel ist der Computer.

Wer an weitergehenden Informationen zur Kryptografie und ihren Anwendungsbereichen interessiert ist, findet diese in dem oben benannten Buch von Klaus Schmeh.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Weitere Informationen:

Schmeh, Klaus, 2013: Kryptografie, Verfahren – Protokolle – Infrastrukturen; dpunkt.verlag; 5. aktualisierte Auflage; ISBN 978-3-86490.015-0

Algorithmen und Schlüssellängen

Kryptografische Algorithmen sind mathematische Verfahren, die zur Verschlüsselung und Entschlüsselung von Daten verwendet werden. Die Verwendung eines geeigneten Algorithmus ist von entscheidender Bedeutung, da nicht alle Algorithmen gleich sicher sind.

Die Länge der kryptografischen Schlüssel ist ebenfalls ein Faktor für die Sicherheit. Die Schlüssellänge bestimmt die Berechnungsdauer des kryptografischen Verfahrens und somit die Zeit, die benötigt wird, mittels Brute-Force-Angriffen die Verschlüsselung zu brechen. Mit zunehmender Rechenleistung ist es notwendig, längere Schlüssel zu verwenden.

Anwendungen, die veraltete Algorithmen und zu kurze Schlüssellängen verwenden, sind anfällig für Angriffe und es besteht die Gefahr, dass die Umsetzung der Maßnahmen zur Umsetzung der VIVA-Schutzziele versagen. Dies liegt daran, dass Angreifende mit ausreichender Rechenleistung und Zeit veraltete Verschlüsselungsalgorithmen und kurze Schlüssel brechen können. Darüber hinaus können Fortschritte in der Kryptoanalyse und Quanten-Computing die Sicherheit von Algorithmen und Schlüssellängen, die heute als sicher gelten, in Zukunft gefährden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht mit der BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ eine Bewertung und Einschätzung zur Sicherheit bestimmter kryptographischer Methoden und Schlüssellängen. Diese sind bei der Umsetzung kryptografischer Verfahren zu beachten.

Die Technische Richtlinie wird regelmäßig überprüft und bei Bedarf aktualisiert.

Weitere Informationen:

BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html

2.3.1 Vertrauliche Kommunikation durch Verschlüsselung

Bei der Verschlüsselung (engl. encryption) wird der Klartext der zu schützenden Information in einen Geheimtext übersetzt.

Die Übersetzung erfolgt anhand eines Verschlüsselungs-Algorithmus, der eine festgelegte Folge von Operationen auf den Klartext und einen Schlüssel anwendet.

Die Wiedergewinnung des Klartextes aus dem Geheimtext wird als Entschlüsselung (engl. decryption) bezeichnet.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Wird für Ver- und Entschlüsselung jeweils der gleiche Schlüssel verwendet, spricht man von einem symmetrischen Verschlüsselungsverfahren.

Werden unterschiedliche Schlüssel eingesetzt, spricht man von einem asymmetrischen Verfahren.

Während der private Schlüssel geschützt und geheim gehalten werden muss, soll der öffentliche Schlüssel anderen möglichst einfach zur Verfügung gestellt werden. Zum Beispiel durch Verzeichnisdienste.

Symmetrische Verschlüsselung

- Die Sicherheit des Verfahrens beruht auf einem gemeinsamen Geheimnis von Sender und Empfänger.
- Sender und Empfänger haben sich bereits vor der Kommunikation auf ein Verschlüsselungsverfahren und einen geheimen Schlüssel geeinigt.
- Der Austausch des geheimen Schlüssels muss auf einem sicheren Weg erfolgen.
- Solche Verschlüsselungsverfahren werden auch als Secret-Key-Verfahren bezeichnet.
- Im symmetrischen Fall müssen die Kommunikationspartner vor dem Austausch verschlüsselter Nachrichten Kontakt aufnehmen und auf sicherem Weg einen gemeinsamen geheimen Schlüssel austauschen.

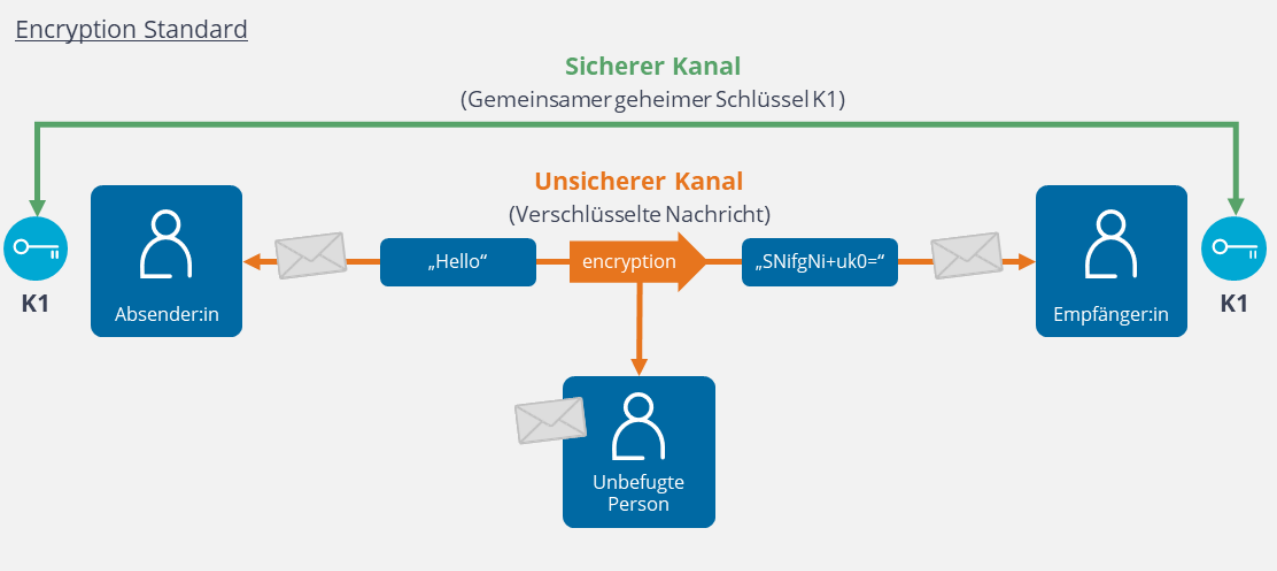


Abbildung 1: Symmetrische Verschlüsselung, schematischer Ablauf

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Asymmetrische Verschlüsselung (Public-Key-Verfahren)

- Jeder Kommunikationspartner besitzt ein Schlüsselpaar, bestehend aus einem öffentlichen Schlüssel (engl. public key) und einem privaten Schlüssel (engl. private key).
- Der öffentliche Schlüssel wird für alle Kommunikationspartner öffentlich und jederzeit zugänglich gespeichert. Er kann in Verzeichnisdiensten abgelegt werden.
- Der private Schlüssel muss geheim gehalten werden.

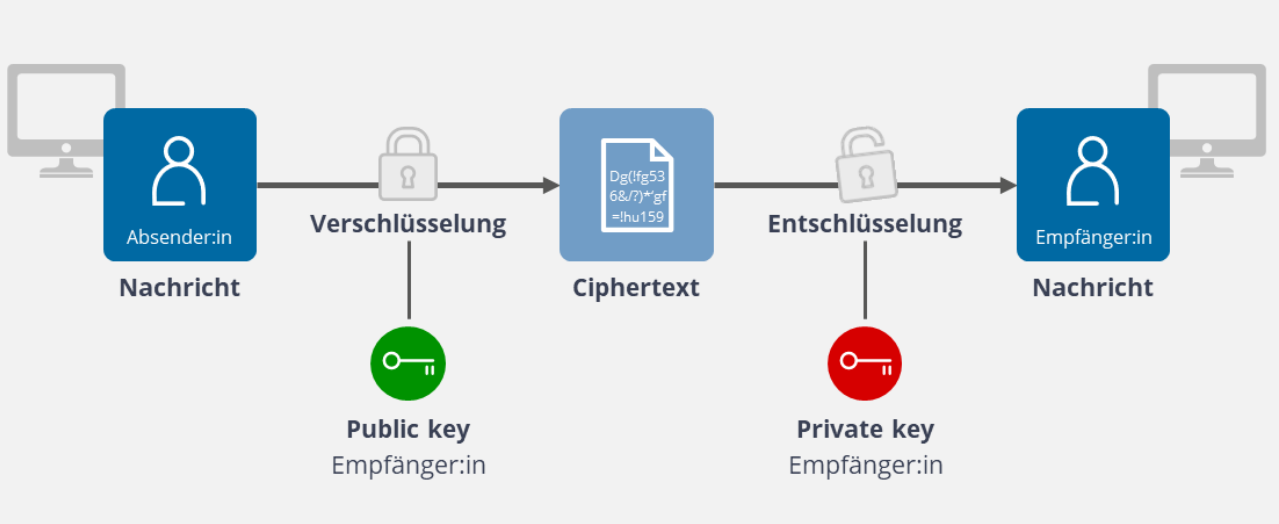


Abbildung 2: Asymmetrische Verschlüsselung (Public-Key-Verfahren), schematischer Ablauf

Hybrid-Verfahren

Da die asymmetrische Verschlüsselung viel Rechenleistung benötigt und das Hauptproblem der symmetrischen Verschlüsselung die Schlüsselübergabe ist, gibt es als dritte Möglichkeit die hybride Verschlüsselung. Dabei wird über die asymmetrische Verschlüsselung ein symmetrischer Schlüssel ausgetauscht, um die Herausforderung der Schlüsselübergabe von der symmetrischen Verschlüsselung zu lösen. Die eigentlichen Daten sind dann symmetrisch verschlüsselt.

- Als erstes wird zufällig ein symmetrischer Sitzungsschlüssel erzeugt.
- Daraufhin wird die Nachricht mit dem Sitzungsschlüssel verschlüsselt und
- der Sitzungsschlüssel mit dem öffentlichen Schlüssel des Empfängers oder Lesers verschlüsselt.
- Neben der verschlüsselten Nachricht wird auch der verschlüsselte Sitzungsschlüssel übertragen.
- Nach dem Empfang wird der verschlüsselte Sitzungsschlüssel entschlüsselt und
- die verschlüsselte Nachricht damit entschlüsselt.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

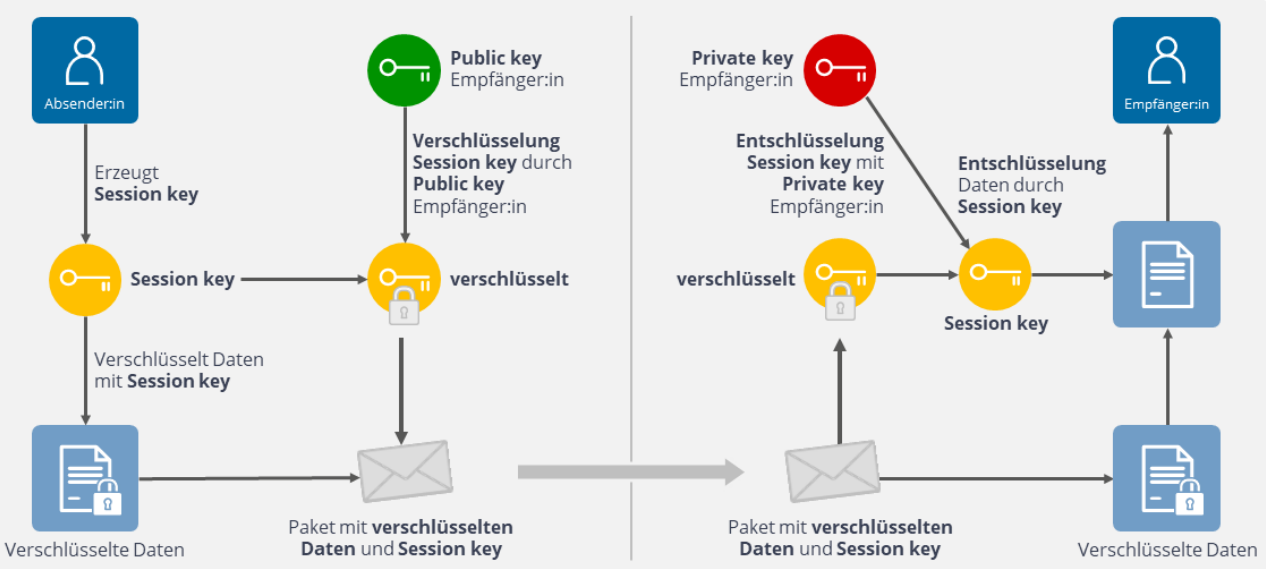


Abbildung 3: Hybrid-Verfahren, schematischer Ablauf

2.3.2 Integritätsprüfung durch Hashes und Signaturen

Signaturen und Hashes sind wesentliche Instrumente zur Prüfung von Integrität und Authentizität von Dokumenten. Der Einsatz dieser Maßnahmen kann zwar das nachträgliche Verändern eines Textes nicht verhindern, sondern ermöglicht es festzustellen, ob die Integrität oder auch Authentizität durch Manipulationen verloren gegangen ist.

Hashbildung durch Hashfunktionen

Hashfunktionen sind mathematische Funktionen, die mittels eines Algorithmus für eine beliebig lange Zeichenfolge (z. B. ein Vertragsdokument als PDF-Dokument) eine Prüfsumme fester Länge (einen Hashwert) erstellen.

Dabei generiert die Hashfunktion für verschiedene Dokumente unterschiedliche Prüfsummen. Von einem Hashwert kann kein Rückschluss auf das Dokument gezogen werden.

Abbildung 4: Konvertierung eines Dateiinhalts in einen Hashwert

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Und wie funktioniert das Übertragen?

- Berechnung: Der Autor/Sender erstellt den Hash-Wert der zu übermittelnden Nachricht und sendet ihn gemeinsam mit der Nachricht.
- Prüfung: Der Empfänger berechnet den Hash-Wert der empfangenen Nachricht und vergleicht ihn mit dem erhaltenen Hash-Wert. Wenn die Hash-Werte übereinstimmen, kann der Empfänger davon ausgehen, dass die Nachricht intakt ist.

Einen ausreichenden Schutz haben wir noch nicht, da sowohl die Originalnachricht als auch der Hashwert in der Nachricht verändert werden können. Verwendet der Angreifer hier denselben Algorithmus zur Berechnung der Prüfsumme, merkt der Empfänger/Leser nicht, dass die Daten verändert wurden. Um dies bemerken zu können, muss der Hashwert vom Autor/Sender signiert werden.

Hash-Funktionen werden auch bei der Speicherung und Prüfung von Passwörtern verwendet. Weder wird das Password eines Benutzers auf dem System gespeichert, noch wird das Kennwort bei einem Login mit Benutzername und Kennwort an den Server übermittelt. Gespeichert, übertragen und verglichen werden die Hashwerte des Kennworts.

Signatur

Bei signierten Dokumenten können die Authentizität und Integrität geprüft werden. Ob also das Dokument nach der Erstellung nachträglich verändert wurde (Integrität) und ob es von demjenigen stammt, der sich als Autor ausgibt (Authentizität).

Wie funktioniert das? Stark vereinfacht so:

- Signieren: Der Autor verwendet seinen privaten Schlüssel, um ein Dokument zu verschlüsseln.
- Verifizieren: Der Leser verwendet den öffentlichen Schlüssel des Autors/Senders, um das Dokument zu entschlüsseln. Wenn er einen sinnvollen lesbaren Text bekommt, ist das Dokument vom Autor.

Für die Verifikation gehen wir davon aus, dass der private Schlüssel des Autors nicht kompromittiert ist, dass also nur der Autor Zugriff auf den Schlüssel hat.

Tatsächlich wird nicht das ganze Dokument verschlüsselt, sondern der Hashwert des Dokuments, der zusammen mit dem Dokument zur Verfügung gestellt wird.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

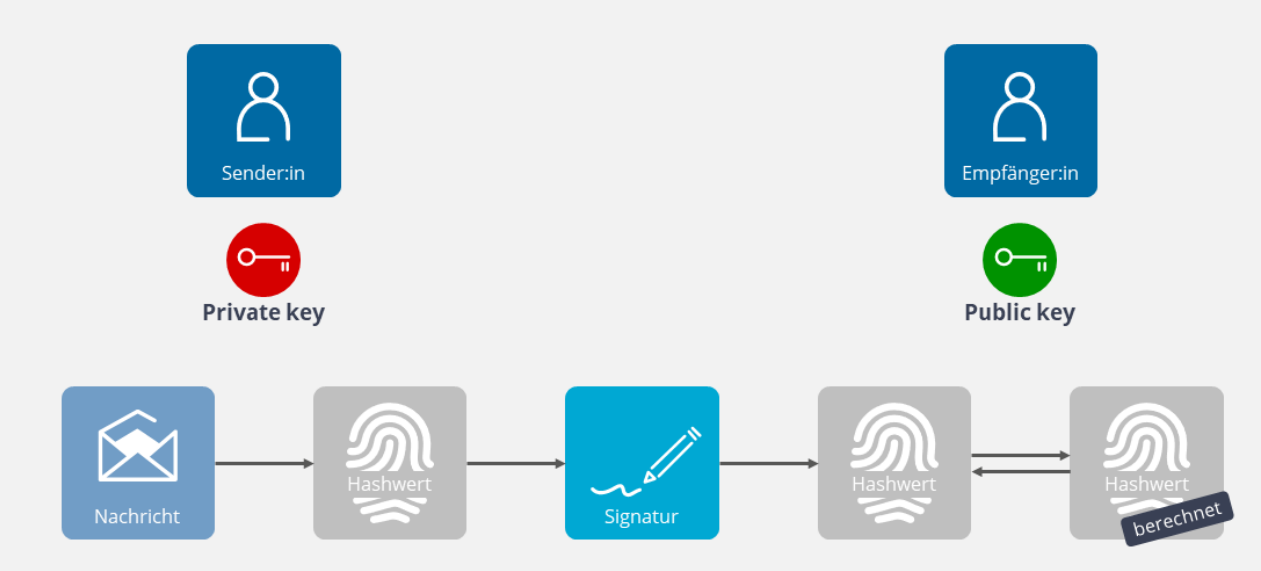


Abbildung 5: Hashwerterstellung und -Prüfung einer Signatur

2.3.3 Zertifikate als Container für öffentliche Schlüssel

Wie kann ein öffentlicher Schlüssel einer Person zugeordnet und aufbewahrt werden? Mittels eines Zertifikats.

Zertifikate verbinden die Identität (von Personen oder Organisationen oder Maschinen) und den öffentlichen Schlüssel miteinander. Die Informationen zur Identität werden zusammen mit dem öffentlichen Schlüssel in einer standardisierten Struktur zusammengefasst. Das Zertifikat selbst ist signiert, so dass eine Manipulation des Zertifikats – zum Beispiel der Austausch des öffentlichen Schlüssels – erkannt werden kann.

X509 oder auch ISO/IEC 9594-8 ist ein Standard, der den Aufbau bzw. die Struktur der in Public Key Verfahren verwendeten Zertifikate beschreibt.

Wahrscheinlich ist Ihnen schon ein OpenPGP-Zertifikat begegnet. PGP-Zertifikate werden für das von Phil Zimmermann entwickelte „Pretty Good Privacy“ (PGP)-Verfahren zum Verschlüsseln und Signieren von Daten verwendet.

Weitere Informationen:
Schmeh, Klaus, 2013: Kryptografie, Verfahren – Protokolle – Infrastrukturen; dpunkt.verlag; Kapitel 27 Digitale Zertifikate; 5. aktualisierte Auflage;
ISBN 978-3-86490.015-0
Rost, Martin, 2022: Das Standard-Datenschutzmodell (SDM) - Einführung, Hintergründe und Kontexte zum Erreichen der Gewährleistungsziele, Wiesbaden, Springer-Vieweg; ISBN 978-3-658-38879

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

2.4 Datenschutz und die Datenschutzgrundverordnung (DSGVO)

„Aufgabe des Datenschutzes ist es, Personen davor zu schützen, dass sie durch die Nutzung ihrer personenbezogenen Daten durch Dritte in der Ausübung von Grundrechten beeinträchtigt werden“. (BSI, IT Grundschutz Baustein CON 2 „Datenschutz“). In Artikel 5 DSGVO sind die Grundsätze für die Verarbeitung personenbezogener Daten aufgeführt.

Die Einhaltung von Datenschutzgesetzen und -vorschriften ist beim Design, der Implementierung und dem Betrieb von Anwendungen unerlässlich. Daher ist im Projektvorhaben von Anfang an sicherzustellen, dass die Anforderungen des Datenschutzes umgesetzt werden.

Einige ausgewählte Aspekte des Datenschutzes sind:

- Datensparsamkeit: Es sind nur die Daten zu verwenden, die für den beabsichtigten Zweck erforderlich sind. Nachrichten sollen nur die erforderlichen Informationen enthalten, um das Kommunikationsziel zu erreichen.
- Vertraulichkeit: Sicherstellung, dass Daten nicht unbefugt offengelegt werden. Verschlüsselung ist eine Maßnahme zur Umsetzung des Gewährleistungsziels Vertraulichkeit.
- Verschlüsselung soll gewährleisten, dass Daten während der Übertragung vertraulich bleiben. Idealerweise kann nur der adressierte Leser (4-Corner-Modell) selbst Zugriff auf den entschlüsselten Inhalt der Nachricht bekommen. Für die bei der Kommunikation beteiligten Systeme ist technisch kein Zugriff auf den Inhalt möglich (Ende-zu-Ende-Verschlüsselung zwischen Autor und Leser).
- Sicherheitsmaßnahmen wie Firewalls und regelmäßige Sicherheitsüberprüfungen sind entscheidend, um Datenschutz in der Kommunikation zu gewährleisten. Die Speicherung und Verarbeitung von Daten müssen in einer sicheren Umgebung erfolgen, um vor Datendiebstahl und unbefugtem Zugriff geschützt zu sein.

Weitere Informationen:

BSI, IT Grundschutz Baustein CON 2 „Datenschutz“:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/03_CON_Konzepte_und_Vorgehensweisen/CON_2_Datenschutz_Edition_2023.html

Rost, Martin, 2022: Das Standard-Datenschutzmodell (SDM) - Einführung, Hintergründe und Kontexte zum Erreichen der Gewährleistungsziele, Wiesbaden, Springer-Vieweg; ISBN 978-3-658-38879

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

2.5 Ablauf sicherer Kommunikation, Beispielszenario

Unter der Annahme, dass Bob sicher eine Nachricht an Alice übermitteln möchte.[3] Sicher bedeutet in diesem Fall, dass:

- der Inhalt der Nachricht nur von Alice gelesen werden können soll (Schutzziel Vertraulichkeit),
- es wichtig ist zu erkennen, ob die Nachricht nachträglich verändert wurde (Integrität),
- Alice prüfen kann, ob die Nachricht wirklich von Bob stammt (Authentizität).

In diesem Szenario agiert Bob als Verfasser des Nachrichteninhalts in der Rolle Autor. Er erstellt den Inhalt und muss sicherstellen, dass die Schutzziele für dieses Kommunikationsszenario erreicht werden.

1. Um die Integrität der Nachricht prüfen zu können, erstellt Bob den Hashwert für den Nachrichteninhalt.
2. Aufgrund des Schutzziels „Authentizität“ signiert er den Hashwert des Inhalts, indem er ihn mit seinem privaten Signaturschlüssel verschlüsselt. Das ist die Signatur.
3. Um den Inhalt der Nachricht inkl. Signatur nur für Alice lesbar zu machen, benötigt er den öffentlichen Schlüssel von Alice. Den kann er beispielsweise in einem Verzeichnisdienst finden.
4. Mit dem öffentlichen Schlüssel verschlüsselt Bob den Nachrichteninhalt für Alice.
5. Bob sorgt dafür, dass Alice die Nachricht bekommt.
6. Wenn Alice die Nachricht bekommt, wird sie als erstes den Nachrichteninhalt mit ihrem passenden privaten Schlüssel entschlüsseln. Vielleicht hat Bob der Nachricht das Zertifikat mit dem verwendeten öffentlichen Schlüssel der Nachricht angefügt, so dass Alice weiß, welchen privaten Schlüssel sie verwenden muss, wenn sie mehrere Schlüssel verwendet.
7. Nun berechnet Alice den Hashwert des Nachrichteninhalts, entschlüsselt den von Bob verschlüsselten Hashwert mit dem öffentlichen Signatur-Schlüssel von Bob und prüft beide Werte.
8. Sind die Werte gleich, ist die Nachricht nicht verändert worden und stammt von Bob.

2.6 OSCI 1.2

OSCI und die OSCI-Intermediärs-Implementierung Governikus COM Tauri (Produkt des IT-Planungsrates) werden u. a. im Elektronischen Rechtsverkehr (ERV), dem elektronischen Abfallnachweisverfahren und im Bereich der Innenverwaltung für bspw. Meldewesen und Beantragung hoheitlicher Dokumente flächendeckend eingesetzt.

[3] Zur Geschichte von Alice und Bob: https://cryptocouple.com/

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Das OSCI-Protokoll ist auf hohe Flexibilität bzgl. Kommunikationsart, Nachrichtenformat und Anwendung kryptografischer Maßnahmen zur Umsetzung von Schutzzielen gemäß identifizierten Schutzbedarf ausgerichtet.

Bei Verwendung des OSCI-Protokolls können sicher und nachweisbar Daten über potentiell unsichere TCP/IP basierte Netze wie zum Beispiel das Internet übermittelt werden. OSCI Transport ist aus Sicht der Applikationsebene (OSI Layer 7) ein „eigenes" Netz, so dass von den darunterliegenden OSI Layern abstrahiert werden kann. Somit ist ein sicherer Datenaustausch ohne Verwendung von VPN Technologien oder SSL/TLS möglich.

Zur Umsetzung von Kommunikationsszenarien stehen unterschiedliche Produkte und Produkt-Komponenten der Governikus GmbH & Co KG. zur Verfügung. Zur Umsetzung können die in Kapitel 3 Lösungsbausteine beschriebenen Komponenten, die allesamt On Premise installiert und betrieben werden, und die in Kapitel 4 Services aufgeführten Dienste verwendet und kombiniert werden.

Nachrichtenaufbau/-format

Vereinfacht kann man sich eine OSCI-Nachricht wie einen Brief mit zwei Umschlägen vorstellen. Der äußere Umschlag enthält

- alle für den Transport notwendigen Daten,
- den aktuellen Laufzettel (Quittung) zum bisherigen Kommunikationsverlauf und
- einen weiteren Umschlag mit den Inhaltsdaten.

Der innere Umschlag enthält die fachlichen Daten der Nachricht und besteht aus mindestens einem Container mit einem Content. Während viele Nachrichten im XÖV-Umfeld dieses einfache Format haben, haben EGVP Nachrichten zwei Container.

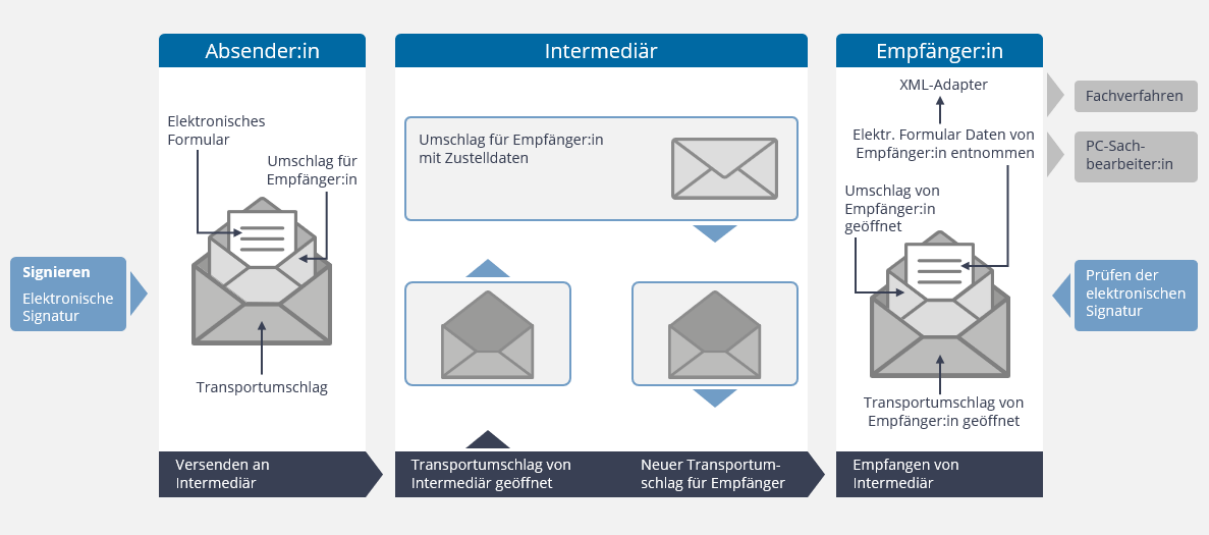


Abbildung 6: OSCI-Verfahrensablauf

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Etwas technischer formuliert klingt das so:

> In einer OSCI-Nachricht sind die zu übertragenden Daten in dem Element „ContentPackage“ abgelegt. Das Element „ContentPackage“ kann beliebig viele Inhaltsdaten-Container (Content Container) enthalten, in denen wiederum mehrere Inhalte (Elemente vom Typ „Content“) enthalten sind. Das Element „Content“ nimmt die eigentlichen Inhaltsdaten auf.

Wer es ganz genau wissen möchte oder muss, findet die ausführliche Beschreibung in der OSCI-Transport 1.2 Spezifikation in Kapitel 6.2 Bedeutung der Elemente mit Namespace http://www.osci.de/2002/04/osci, S. 32.

Die Definition der Fachdaten und deren Struktur erfolgt in unterschiedlichen Gremien, die regelmäßig neue Versionen der im XRepository veröffentlichten XÖV-Standards veröffentlichen.

Damit sich die Kommunikationspartner verstehen können, muss neben der Struktur des Nachrichteninhalts – in der XÖV meistens eine XML-Struktur – zusätzlich definiert werden, wo in der Nachricht welche Inhalte zu finden sind. Daher ist zu dokumentieren, in welchen Containern und Contents welche Inhaltsdaten abgelegt werden und welche Anforderungen es bzgl. Verschlüsselung, Signaturen, Algorithmen, Schlüssellängen und zu verwendenden Zertifikaten zu erfüllen sind. Diese Anforderungen bilden das Transportprofil. Diese Informationen werden für die Erstellung eines Eintragungskonzeptes für das DVDV benötigt.

Der Transport selbst wird dann mittels des OSCI Transport-Protokolls durchgeführt. Dabei sind alle für den Transport notwendigen Daten, wie zum Beispiel die verwendeten Zertifikate mit den öffentlichen Schlüsseln im äußeren Umschlag enthalten. Der jeweils aktuelle Laufzettel der Nachricht ist auch immer dabei. Auf dem Laufzettel ist quasi der Lebenslauf der Nachricht dokumentiert. Mit ihm wird nachgewiesen, ob und wann eine Kommunikation stattgefunden hat. Dazu gehört, wann die Nachricht von wem an wen versendet und ob und wann sie empfangen wurde.

Die in den Rollen Sender und Empfänger agierenden technischen Komponenten haben Zugriff auf den Inhalt des äußeren Umschlags. Wenn die Inhaltsdaten verschlüsselt sind, bleiben die übermittelten Informationen den Sender-/Empfänger-Komponenten verborgen bzw. sie „sehen“ nur eine chaotisch erscheinende Abfolge von Zeichen.

Weitere Informationen:

OSCI-Transport 1.2 Spezifikation:
https://www.xoev.de/osci-xta/standard-osci-transport-1-2/spezifikation-1-2-2472

XRepository: https://www.xrepository.de/

Synchron oder asynchron?

Mit OSCI 1.2 können sowohl synchrone als auch asynchrone Kommunikationsszenarien umgesetzt werden. Unter synchron verstehen wir an dieser Stelle, dass die Nachricht sofort und direkt vom Autor über den Sender und Empfänger zum Leser durchgestellt wird.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Damit das möglich ist, muss die Infrastruktur bei Leser und Empfänger online und empfangsbereit sein. Wählt ein Autor die synchrone Zustellung einer Nachricht, wird die IT-Infrastruktur des Empfängers die Nachricht unmittelbar an die in der Rolle Leser agierende technische Komponente weitergeben. Die Auslieferung der Nachricht an den Leser inklusive des Zeitpunktes wird auf dem Laufzettel vermerkt und der Autor bekommt die Rückmeldung über die erfolgreiche Zustellung. Die ausführliche Beschreibung dieser Kommunikationsart ist in der OSCI-Transport 1.2 Spezifikation in Kapitel 3.5.2 One-Way-Message, passiver Empfänger, Protokollierung beschrieben.

Soll der Leser direkt und unmittelbar mit einer Antwortnachricht reagieren, handelt es sich um das in Kapitel 3.5.3 beschriebene Request-Response Kommunikationsszenario.

Umfangreiche Informationen zur Umsetzung und zum Betrieb synchroner Kommunikationsszenarien finden sich in dem von der KoSIT bereit gestellten „Informationsblatt Synchrone Kommunikation mit OSCI-Transport 1.2“.

Bei der asynchronen Kommunikation ist es nicht notwendig, dass der adressierte Empfänger/Leser einer Nachricht immer online verfügbar ist. Versendet der Autor eine asynchrone Nachricht, wird diese nicht an den Empfänger durchgestellt, sondern auf einem sogenannten Intermediär abgelegt. Die Server-Software COM Tauri implementiert diese Rolle.

Die Nachricht bleibt auf COM Tauri so lange gespeichert, bis der Leser/Empfänger die Nachricht abholt. Dann wird die Nachricht als zugestellt markiert. Zugestellte Nachrichten werden je nach konfigurierter Aufbewahrungsfrist auf dem Intermediär gelöscht. Die Laufzettel zum Nachweis der Kommunikation werden nicht mit der Nachricht zusammen gelöscht.

Weitere Informationen:

OSCI Hilfsmittel:
https://www.xoev.de/osci-xta/standard-osci-transport-1-2/osci-hilfsmittel-23208

Informationsblatt Synchrone Kommunikation mit OSCI-Transport 1.2:
https://www.xoev.de/sixcms/media.php/13/Ko-SIT%20OSCI%20Synchr%20Komm_V3.9135.pdf

Was müssen meine Entwickler:innen wissen?

Tatsächlich funktioniert OSCI 1.2 ähnlich wie TLS: Es stellt einen sicheren Kanal zwischen zwei Kommunikationspunkten zur Verfügung. Ein Endpunkt ist die Fachanwendung, die über das OSCI 1.2 Protokoll Nachrichten/Daten austauschen möchte. Der andere Endpunkt ist eine COM Tauri-Instanz, die als Intermediär agiert.

Anders als bei SSL steuert die Anwendungsschicht dabei die anzuwendenden kryptografischen Operationen und verwendet dabei die für jeden frei zu verwendende OSCI 1.2 Bibliothek (Java oder .NET).

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Die Kommunikation zwischen Anwendung und COM Tauri findet innerhalb eines Dialogs statt, der von der Anwendung initiiert wird. Wie genau das funktioniert, ist in Kapitel 3.3 Dialoge der OSCI-Transport 1.2 Spezifikation beschrieben.

Die aktuelle Version der OSCI Bibliothek implementiert Funktionen für die Rollen Autor, Leser, Sender und Empfänger, mit denen OSCI 1.2 Kommunikationsszenarien umgesetzt werden können.

Zum Auslieferungsumfang der OSCI Bibliothek gehören Code-Beispiele zum Aufbau, Versand und Empfang von OSCI Nachrichten. So befinden sich die Programmbeispiele im Verzeichnis „/beispielanwendung/de/osci/osci12/samples“ der ZIP-Datei der Java Variante der OSCI 1.2 Bibliothek. Die Namen der Java-Quellcodedateien korrespondieren zu den Unterkapitelnamen von Kapitel 3.5 Szenarien der OSCI-Transport 1.2 Spezifikation.

Weitere Informationen:

Download der OSCI 1.2 Bibliothek und weitere hilfreiche Informationen:
https://www.governikus.de/service/osci-bibliothek/

OSCI-Transport 1.2 Spezifikation:
https://www.xoev.de/osci
https://www.xoev.de/osci/versionen

2.7 XTA als Zugang zu einer Transportinfrastruktur

Im Unterschied zu OSCI 1.2 definiert XTA kein Transportprotokoll und XTA-Server realisieren kein Transportverfahren. Vielmehr beschreibt und definiert XTA eine Schnittstelle für den Zugang zu anderen Transportverfahren und eine XTA-Umsetzung ermöglicht den Zugang zu Transportverfahren über eine standardisierte Schnittstelle.

XTA ist ein fachübergreifender und fachunabhängiger Standard, der die Anbindung zwischen Fachverfahren und Transportverfahren standardisiert. Die Fachverfahren beauftragen, steuern und überprüfen den Nachrichtentransport mittels der XTA Schnittstelle. Eine XTA-Instanz selbst steuert die Durchführung des Transports mittels des ausgewählten Transportprotokolls (aktuell meist OSCI 1.2).

In einem XTA-Kommunikationsszenario agieren

- das oder die beteiligte(n) Fachverfahren in den Rollen Autor und Leser und
- der oder die XTA-Server in den Rollen Sender und Empfänger.

Mit XTA können alle von OSCI 1.2 bekannten Kommunikation Szenarien:

- synchron,
- synchron mit Rückantwort und
- asynchron

angesprochen werden.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Bei Nutzung der XTA-Anbindung:

- werden die Fachanwendungen von der Ansteuerung notwendiger kryptografischer Funktionen entlastet,
- kann die Adressierung der Kommunikationspartner (Empfänger und Leser) direkt mittels DVDV Mechanismen erfolgen,
- können Anforderungen an den Transport (Servicequalitäten) definiert werden und bestimmt werden, wie mit Nichteinhaltungen der Qualitätsanforderungen umzugehen ist,
- kann nachgewiesen werden, ob und welche Servicequalitäten beim Transport eingehalten wurden.

Die Fachverfahren greifen auf die Funktionen einer XTA-Server-Instanz über Webservices (SOAP) zu.

Die Beschreibung der Funktionalitäten und der konkreten Webservice Schnittstellen sind in den XTA-Spezifikationen dokumentiert, die auf den Webseiten der KoSIT veröffentlicht sind. Die KoSIT koordinierte den Aufbau des Standards und ist für die Weiterentwicklung des Standards verantwortlich. Die Weiterentwicklung des Standards erfolgt mittels eines Expertengremiums, das von der KoSIT koordiniert wird.

Am meisten verbreitet und verfügbar sind Implementierungen der Version 3. Ab Version 4. ist definiert, welcher Umfang der Spezifikation mindestens zu implementieren ist, um eine zur Spezifikation konforme Implementierung zu haben. Mit den Konformitätsvorgaben sollen interoperable Implementierungen eines XTA-Transportadapters gefördert werden.

Mit Version 5 ist die Unterscheidung zwischen Kernfunktionalitäten und optionalen Erweiterungen eingeführt worden. Die Beschreibungen der Kernfunktionaltäten und Erweiterungen sind über die Einstiegsseite zur XTA Version 5. zu erreichen.

Weitere Informationen:

Einstiegseite zu den XTA Dokumenten der KoSIT:
https://www.xoev.de/xta

XTA Versionsübersicht:
https://www.xoev.de/xta/versionen

Einstiegseite zur aktuellen XTA Version 5:
https://www.xoev.de/xta/v5

2.8 Warum reicht nicht einfach TLS?

TLS steht für Transport Layer Security und ist ein Protokoll, welches die Schicht 4 des OSI Modells (verbindungsorientiertes TCP) um kryptografische Verschlüsselung erweitert. TLS ist der Name, unter dem das SSL (Secure Sockets Layer) Protokoll 1997 von der Internet Engineering Task Force (IETF) standardisiert wurde. Obwohl mittlerweile TLS 1.3 (RFC 8446) verfügbar ist, wird die Bezeichnung SSL häufig synonym verwendet.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

TLS realisiert einen sicheren Kanal für die Kommunikation über TCP durch Hinzufügen einer zusätzlichen Schicht zwischen TCP und der darüber liegenden Anwendung, in der alle kryptografischen Operationen stattfinden. Die Anwendung bekommt (weitestgehend) nichts von der Absicherung der Kommunikation durch Kryptografie mit.

Bezogen auf das 4-Corner-Modell findet eine Absicherung der Sender-Empfänger-Kommunikation statt, ohne dass Sender und Empfänger darauf Einfluss nehmen oder Kenntnis davon bekommen. Eine zielgerichtete Absicherung der Kommunikation zwischen Autor und Leser ist nicht möglich. Ohne weitere kryptografische Absicherung der zu übermittelnden Daten liegen diese bei Sender und Empfänger im Klartext vor. Der von OSCI 1.2 bekannte innere Umschlag fehlt hier und muss „nachgebaut“ werden.

Vor allem bietet TLS keine Quittungen oder Laufzettel für einzelne Nachrichten, um nachweisen zu können, ob und wann zwischen welchen Parteien eine Kommunikation stattgefunden hat. Und erst recht nicht, ob eine bestimmte Nachricht/Information gesendet oder empfangen wurde. Es wird auch nicht dokumentiert, welche kryptographische Absicherung zwischen Sender und Empfänger während der Nachrichtenübermittlung verwendet wurde.

Während für eine OSCI Nachricht auch nach dem Empfang geprüft werden kann, wer mit wem unter welcher kryptografischen Absicherung etwas versendet/empfangen hat, ist dies bei TLS nicht möglich.

Eine zusätzliche kryptographische Absicherung der Nachrichtenübermittlung basierend auf XML-DSig und XML-enc und der Quittierung wird bspw. auch bei eDelivery AS4 angewendet und ist keine Spezialität von OSCI. TLS wird bei AS4 zusätzlich verwendet um nicht durch SOAP/XML-Security-Mechanismen gesicherte Metadaten zu schützen.

2.9 DVDV

Was ist das und wozu dient es?

Das Deutsche Verwaltungsdiensteverzeichnis (DVDV) ist eine wichtige Infrastrukturkomponente für die Umsetzung der OSCI 1.2 basierten Kommunikation des eGovernments in Deutschland.

Analog zu einem Telefonbuch liefert das DVDV auf Anfrage die technischen Verbindungsparameter, um elektronische Dienste der öffentlichen Verwaltung über OSCI 1.2 ansprechen zu können. Zu einer Antwort gehören z. B. URLs, zuständige Intermediäre, Dienstbeschreibungen, Dienstbezeichner sowie für die sichere Kommunikation benötigtes Schlüsselmaterial (öffentliche Verschlüsselungsschlüssel).

Als weitere Funktion bietet das DVDV die Überprüfung an, ob eine Organisation im DVDV eingetragen ist und ob sie einen bestimmten Dienst aufrufen darf. Diese Überprüfung ist möglich, da angebotene elektronische Dienste einer Dienst-Kategorie zugeordnet werden und abgebildet wird, welche Organisationen welche Dienste bei einer anderen Organisation/Behörde aufrufen dürfen.

Die Anfragen an das DVDV stammen primär von automatischen elektronischen Fachverfahren und Online-Diensten der öffentlichen Verwaltung, die mit Hilfe der vom DVDV zurückgelieferten Daten eine rechtsverbindliche und sichere elektronische Kommunikation zu anderen Behörden und den von ihnen angebotenen Diensten aufbauen können.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Beim ITZBund wurde eine Koordinierende Stelle DVDV eingerichtet, die erste Ansprechpartnerin für sämtliche Anliegen von Beteiligten oder Interessierten am DVDV ist. Diese Koordinierende Stelle betreut und genehmigt auch die neuen oder geänderten Eintragungskonzepte.

Wer kann es benutzen und wen finde ich dort?

Verzeichnet werden und Daten abrufen können im DVDV sämtliche Behörden der deutschen öffentlichen Verwaltung auf Bundes-, Länder- und Kommunalebene. Außerdem gilt dies auch für Unternehmen, die mit der Erfüllung hoheitlicher Aufgaben betraut sind und zu mindestens 50% aus Mitteln der öffentlichen Hand finanziert werden.

Was wird benötigt, um einen Dienst eintragen zu lassen?

Die für Fachlichkeit eines Dienstes verantwortliche Stelle übernimmt die Rolle des „Daten-Providers“ und ist für die Erstellung des Eintragungskonzepts zuständig. Das zu erstellende Eintragungskonzept hat einen festgelegten Aufbau und einen starken Bezug zu dem zugrundeliegenden XÖV-Fachstandard (wie z. B. XMeld, XSozial, XInneres usw.).

Die folgende Liste zeigt einen Ausschnitt der im Eintragungskonzept zu beantwortenden Fragestellungen:

- Fachliche Beschreibung des Dienstes: Wer kommuniziert mit wem zu welchem Zweck?
- Ausgangslage: Fachliche Beschreibung des Vorhabens. Wie erfolgte die Kommunikation bisher? Gibt es gesetzliche Grundlagen / Fristen?
- Standard: Beruht das Vorhaben auf einem XÖV-Standard? Wenn ja: Benennen und kurz ausführen, wenn nicht: Vorhaben näher beschreiben.
- Dienste: Beschreibung der Dienste inkl. der Dienstnamen sowie Nennung der zulässigen Dienstnutzer und -anbieter.
- Zertifikate: Angaben zu den Zertifikaten, die zum Einsatz kommen dürfen bzw. müssen.
- Technische Aspekte: Handelt es sich um synchrone oder asynchrone Nachrichtenübertragungen? Erfolgt die Datenübermittlung per OSCI?
- Organisatorische Aspekte: Der Dienst-Provider (fachlich zuständige Stelle) ist mit Behörde, Ansprechpartner, E-Mail (Postfach) und Telefonnummer benennen.
- Pflegende Stellen: Übernehmen alle im DVDV-Kontext benannten Pflegenden Stellen oder einzelne, konkret zu benennende Pflegende Stellen die Pflege der Daten im DVDV?
- Intermediäre: Sollen nur bestimmte Intermediäre verwendet werden oder sind diese frei wählbar?

Für jeden einzelnen Dienst wird eine formale, rein technische Beschreibung im WSDL-Format benötigt. Diese ist ebenfalls vom zuständigen Daten-Provider zu liefern.

Neue bzw. aktualisierte Eintragungskonzepte müssen vor ihrer Verwendung freigegeben werden. In der Regel kontaktiert dazu der jeweilige Dienstprovider bereits in der Erstellungsphase die Koordinierende Stelle DVDV und klärt in einem iterativen Prozess die offenen Fragen. Anschließend wird das fertige Eintragungskonzept der Expertengruppe DVDV zur Genehmigung vorgelegt.

Für eine Vorlage zur Erstellung eines neuen Eintragungskonzepts bzw. den Zugriff auf bereits vorhandene Eintragungskonzepte ist die Koordinierenden Stelle DVDV zu kontaktieren.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

An wen wende ich mich um mich eintragen zu lassen?

Wenn sich eine Organisation im DVDV eintragen lassen möchte, muss sie sich an die für ihr Bundesland zuständige Pflegende Stelle wenden. Nur die jeweils zuständigen Pflegenden Stellen haben Schreibrechte auf dem DVDV (notwendig für Einträge und Änderungen), alle anderen Pflegenden Stellen können nur lesend zugreifen.

Falls nicht bekannt sein sollte, wer die für Sie zuständige Pflegende Stelle ist, kann man sich an die Koordinierende Stelle DVDV (dvdv@itzbund.de) wenden.

Wie kann ich DVDV Einträge abfragen?

Fachverfahrenshersteller, die den Zugriff auf das DVDV in ihre Produkte integrieren möchten, können auf frei verfügbare Ressourcen zurückgreifen. Das DVDV-Produktmanagement der FITKO bietet speziell für diese Zwecke entwickelte Bibliotheken für .Net und Java an. Interessenten registrieren sich bitte über die Seite https://docs.fitko.de/dvdv/register/ bei der Koordinierenden Stelle DVDV und erhalten dann Informationen zum Download von Bibliotheken, Dokumentation und Implementierungsbeispiele.

Bei Governikus wird im Auftrag des DVDV-Produktmanagements ein Testsystem betrieben, mit dem Fachverfahrenshersteller den Zugriff ihrer DVDV-Clients auf einen DVDV-Server erproben können, ohne dabei den Produktivbetrieb zu stören oder unabsichtlich echte Nachrichten an die verknüpften Fachverfahren zu senden.

Wo finde ich weitere Informationen?

Zentraler Anlaufpunkt für alle Fragen rund um das Deutsche Verwaltungsdiensteverzeichnis (DVDV) ist die im Auftrag der FITKO beim ITZBund eingerichtete Koordinierende Stelle DVDV. Ihre Mailadresse lautet: dvdv@itzbund.de Auf ihrer Website finden sich viele weitere Informationen rund um das DVDV, empfohlen sei auch die Lektüre der aktuellen DVDV-Verfahrensbeschreibung.

Downloads zu DVDV:

https://www.itz-bund.de/DE/itloesungen/standardloesungen/dvdv/downloads/downloads.html

2.10 SAFE

Wozu dient es?

SAFE (**S**ecure **A**ccess to **F**ederated **E**-Justice/E-Government) ist ein übergreifender Dienst für das Identitätsmanagement für E-Justice/E-Government.

SAFE ist als universelles, föderiertes Identitätsmanagementsystem konzipiert, das von sämtlichen Anwendungen der Justiz und der öffentlichen Verwaltungen als (Basis-)Dienst für die Authentisierung von Nutzenden verwendet werden kann.

SAFE ist eine Anwendung des IT-Planungsrats und wird als Konzept und auch als Produkt auf der Grundlage der Beschlüsse der Bund-Länderkommission für Informationstechnik in der Justiz (BLK) weiterentwickelt.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Als Adressbuch für den elektronischen Rechtsverkehr (ERV) erlaubt SAFE die Suche nach Teilnehmenden z. B. anhand von Namen oder Adresse und liefert zu jedem Teilnehmenden die für die gesicherte Kommunikation notwendigen Meta-Daten. Dies sind z. B. die Adresse des jeweiligen Intermediärs und die Verschlüsselungszertifikate.

SAFE wurde als

- Adressbuch für die Teilnehmenden am elektronischen Rechtsverkehr (EGVP-Verbund) und
- Authentisierungsdienst, der auf der Basis von WS-Trust und SAML-Token die Anmeldung an beliebigen Anwendungen erlaubt

konzipiert.

Mit der Einführung der „besonderen Postfächer" im ERV (beBPo, beA, beN, eBO, beSt) werden nur noch geprüfte Identitäten im SAFE freigeschaltet. Die Prüfung erfolgt bei den unterschiedlichen besonderen Postfächern über verschiedene Wege.

Nicht jede:r Teilnehmende am elektronischen Rechtsverkehr (ERV) darf alle anderen Teilnehmenden in diesem Adressbuch sehen. Aus diesem Grund muss sich ein:e Teilnehmer:in vor der Suche gegenüber dem System authentisieren. Diese Authentisierung erfolgt ebenfalls mittels SAFE.

Um eine einfache Suche über unterschiedliche SAFE-Domains hinweg zu erlauben, wurde der Virtuelle Attribut-Service (VAS) eingeführt. Diese bei der BNotK betriebene Komponente nimmt Suchanfragen entgegen, leitet diese an die angeschlossenen SAFE-Domains weiter und aggregiert dann die Suchergebnisse für Anfragende. Änderungen am Datenbestand erfolgen über den optionalen Provisioning-Service.

Das Identitätsmanagement in SAFE basiert auf den Standards WS-Trust und SAML-Token. Die Komponente wird innerhalb des ERV z. B. für die Anmeldung der Nutzenden vor einer Suche im SAFE genutzt, aber auch z. B. um die eigenen Daten im SAFE über den Provisioning-Service zu bearbeiten.

Neben der SAFE-Spezifikation gibt es ein Fachkonzept, wie eine SAFE-Domain angelegt wird. Es gibt zahlreiche Installationen und unterschiedliche Implementierungen von SAFE, zum Beispiel bei der Justiz oder der Bundesnotarkammer. Die Domains sind dabei interoperabel.

Mittlerweile wird SAFE auch für die Anmeldung in anderen Bereichen genutzt. So erfolgt z. B. die Anmeldung am zentralen Akteneinsichtsportal der Justiz über SAFE. Es kommen kontinuierlich weitere Dienste hinzu.

Wie kann man sich anschließen?

Einen SAFE-Eintrag erhält eine Person oder Organisation mit der Eröffnung eines besonderen Postfaches.

Die Eröffnung ist für einige Organisationen (Behörden, AöR, ...) und Personengruppen (Anwält:innen, Gerichtsvollzieher:innen, Notar:innen, Steuerberater:innen, Wirtschaftsprüfer:innen, Patenanwält:innen, Berufsbetreuer:innen, ...) verpflichtend, andere können freiwillig ein elektronisches Bürger- und Organisationenpostfach (eBO) eröffnen.

Je nach Berufsgruppe findet eine automatische und zwangsweise Eintragung statt, oder eine Eintragung kann über das Formular in der Bezugsquelle beantragt werden. Als Beispiel für eine automatische Eintragung lassen sich Steuerberater:innen, Notar:innen und Anwält:innen aufführen. Hier erfolgt mit der Zulassung eine automatische Eintragung durch das zuständige Amt.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Wie kann ich auf SAFE zugreifen?

Es gibt als Fachverfahren eine Bibliothek (safe-sdk), die sich bei der Justiz anfordern lässt. Dieses JAVA-SDK erlaubt den einfachen Zugriff auf das EGVP-Adressbuch. Alle Dienste von SAFE können auch direkt über die entsprechenden Standards (WS-Trust, SAML-Protokoll, SOAP, WSDL, …) umgesetzt werden.

Wenn Fachverfahren die Authentisierung über SAFE nutzen wollen, müssen diese im Vorfeld Kontakt mit dem zuständigen Projektbüro (it-standards@justiz.de) aufnehmen.

Wie nutzt man es?

SAFE ermöglicht den sicheren und verschlüsselten Zugriff auf seine Dienste durch bekannte Nutzende, die entweder eine spezielle Client-Anwendung oder einen Webbrowser nutzen. Die Architektur von SAFE basiert auf Standards wie WS-Trust und SPML.

Die Justiz stellt ihre SAFE-Implementierung anderen Verwaltungen und Kammern unter gewissen Umständen zur Verfügung. So hat Governikus z. B. die SAFE-Domain für die Steuerberater:innen, betrieben bei der DATEV im Auftrag der Bundessteuerberaterkammer, mittels der SAFE-Implementierung der Justiz realisiert.

2.11 EGVP

EGVP steht für „Elektronisches Gerichts- und Verwaltungspostfach“. Es wird für die sichere elektronische Kommunikation zwischen Justizbehörden und Teilnehmenden des Elektronischen Rechtsverkehrs, wie Anwält:innen, Notar:innen, Steuerberater:innen, Bürger:innen und Organisationen sowie Behörden verwendet. Über den Austausch von Nachrichten können elektronische Akten und Dokumente übertragen werden.

EGVP realisiert die sichere Übermittlung von Nachrichten und Dokumenten mittels des Transports über OSCI 1.2. Mit dem EGVP werden Dokumente rechtssicher übermittelt. So gewährleistet die Verwendung elektronischer Signaturen die Authentizität und Integrität der übermittelten Inhalte.

Das EGVP ist ein wichtiges Element der Digitalisierung im deutschen Justizwesen und trägt zur Modernisierung und Effizienzsteigerung der rechtlichen Prozesse bei. Nutzende des EGVP benötigen eine Client-Software, um auf das System zuzugreifen und mit anderen Teilnehmenden zu kommunizieren. Diese Software ermöglicht das Verfassen, Signieren und Versenden von Dokumenten sowie den Empfang und die Verwaltung eingehender Nachrichten.

EGVP funktioniert auf einer zentralen Serverinfrastruktur, die für den Nachrichtenaustausch zwischen den Teilnehmenden zuständig ist.

EGVP ist darauf ausgelegt, mit anderen juristischen IT-Systemen kompatibel zu sein. Dies ermöglicht es Nutzenden, EGVP in bestehende Arbeitsabläufe zu integrieren und effizient mit anderen Systemen zu interagieren.

Für die Nutzung des EGVP ist eine Registrierung und Authentifizierung der Nutzenden am SAFE Verzeichnisdienst (siehe Kapitel 2.10) erforderlich. Dies stellt sicher, dass nur berechtigte Personen Zugriff auf das System haben und die Kommunikation den rechtlichen Anforderungen entspricht.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

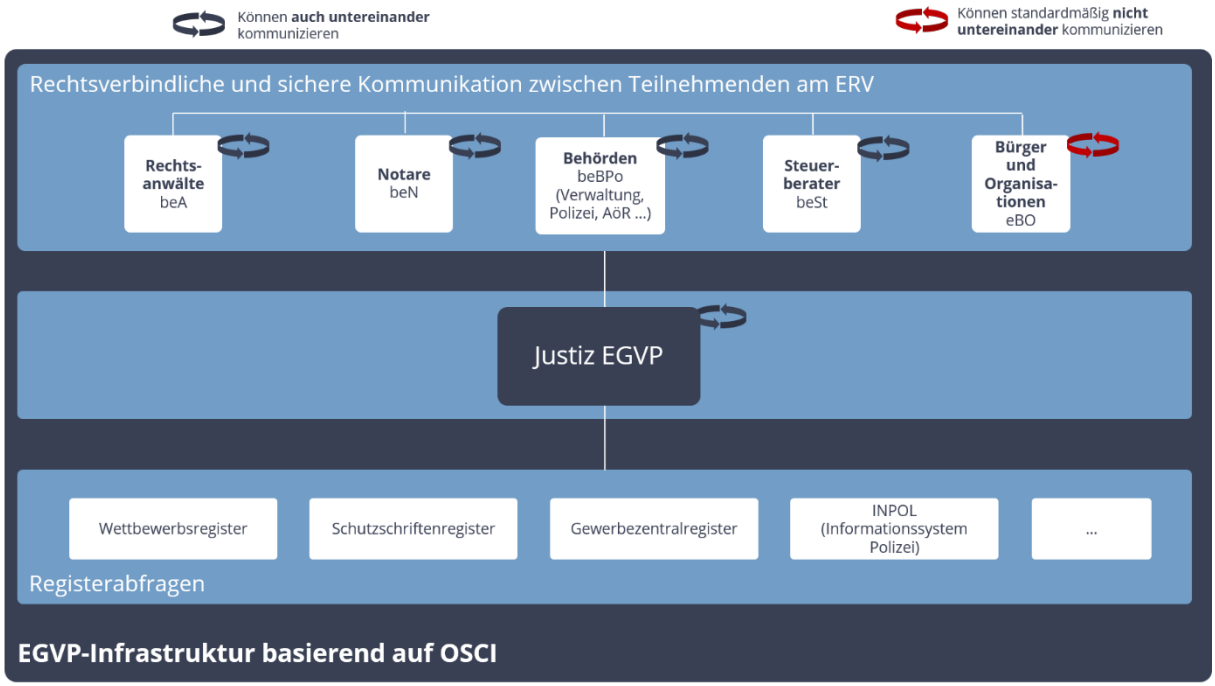


Abbildung 7: EGVP-Infrastruktur

Weitere Informationen:

https://egvp.justiz.de/

Anforderungen für die Teilnahme von Drittanwendungen am OSCI-gestützten elektronischen Rechtsverkehr“:
https://egvp.justiz.de/Drittprodukte/index.php

2.12 Peppol

Peppol bezeichnet eine in Europa und zunehmend auch international etablierte Infrastruktur. Sie dient der sicheren Übermittlung von strukturierten Daten im Kontext der elektronischen Beschaffung. Peppol ist entstanden aus dem europäischen Projekt PEPPOL "Pan-European Public Procurement OnLine". Die Governance der Peppol Infrastruktur und der zugehörigen Spezifikationen wird von OpenPeppol übernommen, einer Non-Profit Organisation nach belgischem Recht, die einem internationalen Verein mit demokratischen Strukturen vergleichbar ist.

Ein Ziel ist, dass Organisationen (öffentliche Stellen und wirtschaftliche Unternehmen), die unterschiedliche Systeme nutzen, miteinander elektronische Dokumente im Rahmen von Beschaffungsprozessen austauschen können, ohne spezielle Anpassungen vornehmen zu müssen. Peppol erleichtert dabei die öffentliche Beschaffung in der EU und darüber hinaus, indem es eine gemeinsame Plattform und Standards für die elektronische Kommunikation bietet.

Peppol BIS (Business Interoperability Specifications) definieren Geschäftsprozesse und zugehörige standardisierte Formate für Geschäftsdokumente für bspw. Rechnungsstellung oder Bestellungen.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Sie stellen sicher, dass Dokumente, die über das Peppol-Netzwerk gesendet werden, von allen Teilnehmenden gelesen und verarbeitet werden können.

Das Peppol-eDelivery-Netzwerk besteht aus Zugangspunkten (Access Points), über die die Teilnehmer:innen miteinander kommunizieren. Unternehmen und Behörden beauftragen einen Peppol Service Provider, der einen zugelassenen Peppol Access Point betreibt, um Dokumente zu senden und zu empfangen. Es verwendet ein 4-Corner-Modell, wobei die Sender und Empfänger (Corner 1 und 4) jeweils einen Access Point (Corner 2 und 3) nutzen. Die Peppol eDelivery Specifications definieren auf der Basis von ebms 3.0/AS4, wie der Transport zwischen den Access Points (Corner 2 und 3) abzusichern ist. Die Übergabe der Dokumente von C1 an C2 und C3 an C4 ist bewusst technisch nicht von Peppol geregelt worden, um den Service Providern ein möglichst flexibles Geschäftsmodell zu ermöglichen.

Der SML (Service Metadata Locator) ist ein zentraler Dienst, der die Identifizierung der Teilnehmenden im Netzwerk und die Ermittlung des zuständigen SMP (Service Metadata Publisher) mittels DNS ermöglicht. Der SMP ist ein Register, das von Peppol Service Providern betrieben wird und zu jedem zugeordneten Teilnehmer Informationen (Service Metadata) darüber enthält, wie mit ihm kommuniziert werden kann (z. B. welche Arten von Dokumenten er akzeptiert und welche technischen Spezifikationen verwendet werden sowie welcher Access Point mit welchem Schlüsselmaterial genutzt wird).

Das Vertrauensmodell von Peppol basiert auf einer gemeinsamen PKI, aus der für die Service Provider kryptographische Zertifikate für den Betrieb von Access Points und SMPs ausgestellt werden. Über die PKI-Struktur wird eindeutig festgelegt, ob im Test- oder Produktivsystem kommuniziert wird.

Weitere Informationen:

https://www.peppol.org

https://www.xeinkauf.de/peppol

https://www.oeffentliche-it.de/documents/10181/188095/Technische+Perspektiven+der+Registermodernisierung.pdf

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

3 Lösungsbausteine

3.1 Governikus MultiMessenger (GMM)

Produktbeschreibung (Welche Funktionen hat das Produkt?)

Der Governikus MultiMessenger (GMM) ist eine mandantenfähige, intelligente Kommunikationsplattform zur Umsetzung von Multikanalstrategien. Die Anbindung an verschiedene Nachrichtenkanäle für In- und Outbound-Nachrichten ermöglicht die Implementierung einer Virtuellen Poststelle, die Nachrichten in unterschiedlichsten Formaten empfängt, technisch-juristisch prüft und in ein gewünschtes Zielsystem zustellt. Dabei unterstützt der GMM im Kontext von Zugangseröffnungen und verwaltet zentral elektronische Identitäten sowie Zertifikate.

Ergänzt wird der GMM durch folgende weitere Anwendungen:

- **GMM ERV-Xtension** zur Erstellung des elektronischen Empfangsbekenntnis im Elektronischen Rechtsverkehr (ERV).
- **GMM Verzeichnisdienst-Connector (VDC)** zur Anbindung an den Verzeichnisdienst der Justiz (SAFE) sowie den DE-Mail-Verzeichnisdienst.
- **GMM SAFE-ID Manager** zum Anlegen und Verwalten von SAFE-Identitäten und -Zertifikaten.
- **GMM Content-Routing** zur automatisierten, regel- und inhaltsbasierten Weiterleitung von Nachrichten aus einem GMM-Postfach (VPF) über verschiedene Weiterleitungskanäle an andere Postfächer.

Einsatzzweck (Welche Umsetzungsziele werden mit dem Produkt adressiert?)

Der GMM kann alle in der öffentlichen Verwaltung und Justiz relevanten Nachrichten-Transportkanäle technisch-juristisch verarbeiten. Alle Nachrichten werden hinsichtlich der Authentizität, Integrität und Rechtsverbindlichkeit korrekt empfangen und geprüft. So können die Nachrichten auch an eAkte-Systeme oder beweiswerterhaltende Langzeitspeicherung (zum Beispiel Governikus DATA Aeonia) übergeben werden.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

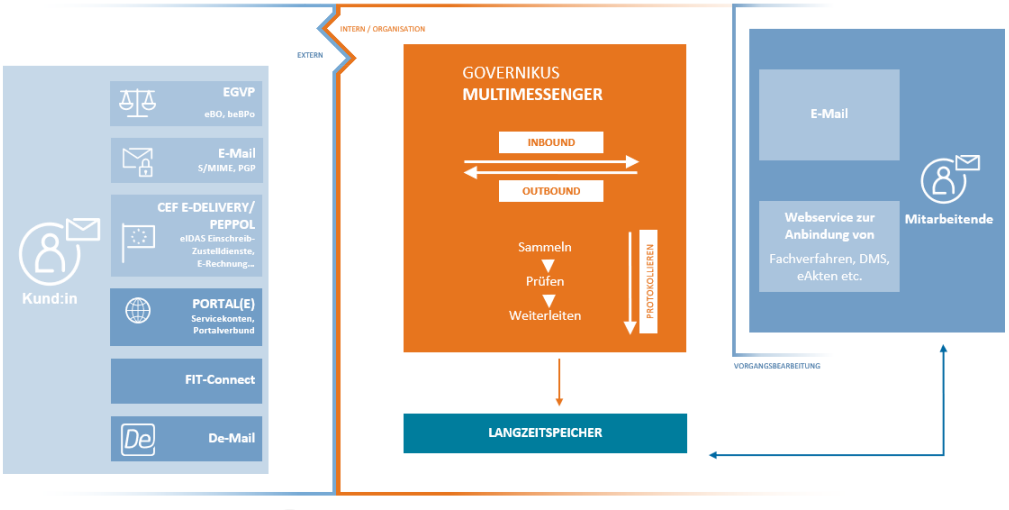


Abbildung 8:Governikus MultiMessenger als Multikanal-Plattform

In unterschiedlichen Einsatzszenarien kann GMM mit weiteren Governikus-Produkten kombiniert werden – zum Beispiel im Kontext des Elektronischen Rechtsverkehrs mit Governikus COM Tauri und Governikus COM Vibilia:

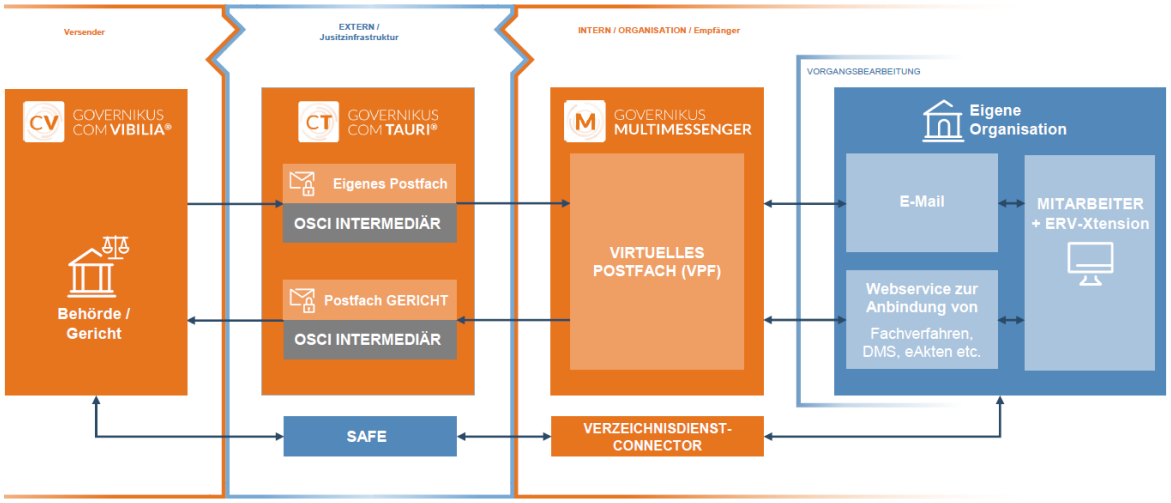


Abbildung 9: GMM im Zusammenspiel mit Governikus COM Vibilia als Desktop-Client und Governikus COM Tauri als OSCI-Intermediär im Elektronischen Rechtsverkehr.

Technologie (Kurzbeschreibung und Voraussetzungen)

GMM basiert auf Microsoft .NET und Java-Technologie und erfordert den Einsatz von Microsoft Windows Server 2016 oder 2019. Geplant ist, GMM künftig auch plattformunabhängig betreiben zu können. Für die Datenspeicherung wird ein Microsoft SQL-Server 2016, 2017 oder 2019 benötigt. Für das verwendete und auf JAVA basierende Adapter-Framework, das beispielsweise auch den Zugriff auf die Governikus Signatur-Prüfkomponenten ermöglicht, wird JBoss Enterprise Application Platform (EAP) benötigt.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

GMM wird kontinuierlich an neue Technologien angepasst und mit Fokus auf den Bedarf der Öffentlichen Verwaltung und der Justiz gepflegt.

Distribution (Wie und wo kann das Produkt bezogen werden?)

Seit 2017 ist Governikus MultiMessenger eine Anwendung des IT-Planungsrates. Stand Januar 2024 sind der Bund sowie elf Bundesländer der Anwendung Governikus MultiMessenger beigetreten, die damit auch deren Kommunen zur Nutzung zur Verfügung steht.

Die kontinuierliche und nachhaltige Pflege und Weiterentwicklung erfolgen in Abstimmung mit dem Bund und den Ländern, die dem Vertrag beigetreten sind. Der Abruf sowie Support der Anwendung erfolgen direkt über Governikus.

https://www.governikus.de/loesungen/it-planungsrat/anwendung-governikus-multimessenger/

3.2 COM Vibilia

Produktbeschreibung (Welche Funktionen hat das Produkt?)

Governikus COM Vibilia ist die Client-Anwendung zum Versand, Empfang, Bearbeiten und Verwalten von OSCI-Nachrichten. Durch die Verwendung des im eGovernment und eJustice im Einsatz befindlichen und bewährten OSCI-Transportprotokolls werden Nachrichten stark Ende-zu-Ende verschlüsselt, das Handling elektronischer Signaturen wird ermöglicht und somit Authentizität, Integrität und Vertraulichkeit gewährleistet.

Durch den Einsatz von elektronischen Signaturen sowie dem OSCI-Laufzettel als Protokollierungsquelle/für die Protokollierung können gesetzlich vorgeschriebene Schriftformerfordernisse eingehalten oder der rechtzeitige Versand bzw. Eingang von Fristsetzungen nachgewiesen werden.

Einsatzzweck (Welche Umsetzungsziele werden mit dem Produkt adressiert?)

COM Vibilia bietet ein Nachrichtenfenster für die Erstellung von OSCI-Nachrichten. Daneben kann über Export- und Importschnittstellen der Austausch von Daten mit Fachverfahren ermöglicht werden.

COM Vibilia ist so konzipiert, dass verschiedenste Einsatzszenarien – von Justiz über Behörde-zu-Behörde Kommunikation bis hin zu weiteren Einsatzszenarien in geschlossenen Nutzer:innenkreisen – bedient werden können.

Die Client-Anwendung COM Vibilia benötigt für den Einsatz folgende Serverprodukte:

- Governikus COM Tauri für das Handling von OSCI-Nachrichten
- Governikus DATA Varuna für die Validierung von Signaturen
- Verzeichnisdienst (SAFE, DVDV oder ein Registrierungsserver) für die Adressierung der Teilnehmenden

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

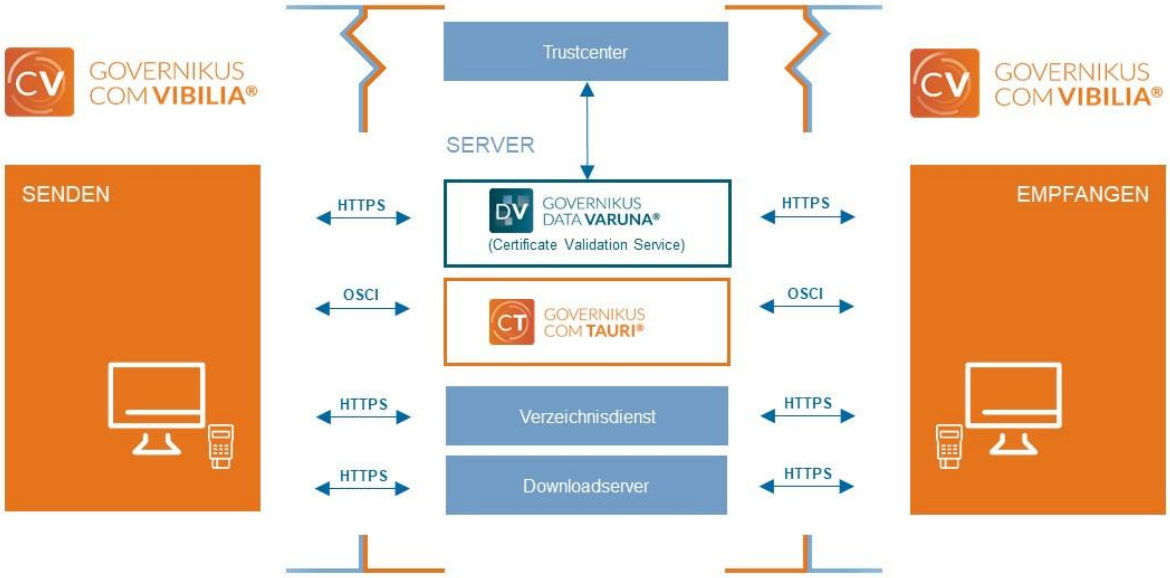


Abbildung 10: Protokolle und Dienste von COM Vibilia

Technologie (Kurzbeschreibung und Voraussetzungen)

COM Vibilia unterstützt als Betriebssysteme Windows und Ubuntu. COM Vibilia benötigt für die Ausführung eine Java-Laufzeitumgebung. Eine aktuelle Java-Version (OpenJDK) wird im Installer-Paket (.MSI) mitgeliefert und installiert und ausschließlich durch Governikus COM Vibilia verwendet. Der Download aktueller Versionen erfolgt dabei automatisch über ein integriertes Update-Modul. Alternativ ist die Bereitstellung der Anwendungsressourcen als ZIP-Archiv möglich – ohne Java und ohne automatisierte Aktualisierungsfunktion. Weitere Informationen finden sich in den Hard- und Softwarevoraussetzungen beschrieben im Anwenderhandbuch.

COM Vibilia wird kontinuierlich an neue Technologien angepasst und mit Fokus auf den Bedarf der Öffentlichen Verwaltung, der Justiz und weiterer Kunden gepflegt. Wo nötig, werden szenarienspezifische Funktionen umgesetzt (bspw. für die Zulassung als Drittprodukt im Elektronischen Rechtsverkehr).

Distribution (Wie und wo kann das Produkt bezogen werden?)

Governikus stellt im Rahmen des Produktes des IT-Planungsrates „Anwendung Governikus“ seit vielen Jahren Bund, Ländern und Kommunen rund um die Erzeugung und Validierung von Signaturen und Siegeln sowie Dokumenten alle notwendigen IT-Komponenten zur Verfügung, die für die sichere, rechtsverbindliche und durchgängig digitale Verwaltungsarbeit benötigt werden. Alle 16 Bundesländer sind dem Vertrag zur „Anwendung Governikus“ beigetreten und in enger Kooperation mit Vertreter:innen aus diesen Ländern und deren Kommunen werden diese Komponenten kontinuierlich angepasst, erweitert und gepflegt. Der Abruf sowie Support der Anwendung erfolgen über die sogenannten „Benannten Stellen“.

www.governikus.de/loesungen/it-planungsrat/anwendung-governikus

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

3.3 COM Tauri

Produktbeschreibung (Welche Funktionen hat das Produkt?)

Governikus COM Tauri ermöglicht den gesetzlich vorgeschriebenen sicheren Datenaustausch via OSCI 1.2. OSCI wird als Transportstandard flächendeckend eingesetzt, z. B. im Meldewesen, dem elektronischen Rechtsverkehr u.v.m. Aktuell werden bundesweit jährlich nahezu 2 Milliarden OSCI-Nachrichten über dezentral in Bundes-, Landes- und Kommunal-Rechenzentren betriebene COM Tauri Installationen ausgetauscht.

OSCI unterstützt den Schutz personenbezogener Daten sowie die Integrität der Daten durch eine starke Ende-zu-Ende-Verschlüsselung sowie durch den Einsatz elektronischer Signaturen. Die notwendigen Datenstrukturen für Quittungsmechanismen mit Zeitstempeln werden ebenfalls durch OSCI definiert. Ähnlich dem „Einschreiben mit Rückschein" kann somit lückenlos der Empfang und Abruf von Nachrichten nachgewiesen werden.

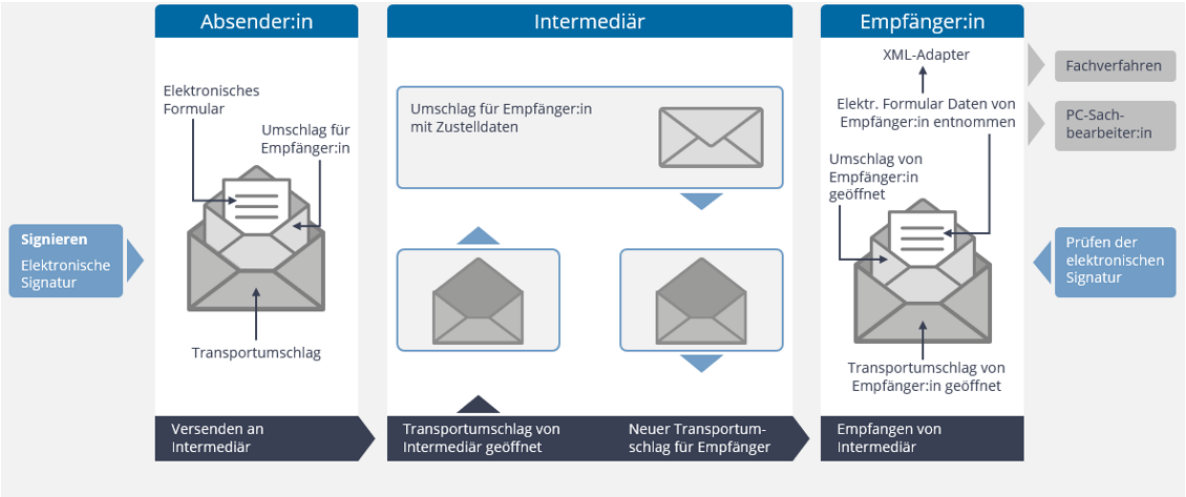


Abbildung 11: Das Prinzip des „Doppelten Umschlags" in der OSCI-Kommunikation

Einsatzzweck (Welche Umsetzungsziele werden mit dem Produkt adressiert?)

COM Tauri gewährleistet den sicheren und rechtsverbindlichen Datenaustausch via OSCI 1.2. Der Einsatz von OSCI 1.2. ist für eine Vielzahl von Anwendungsfällen gesetzlich vorgeschrieben.

COM Tauri implementiert dabei die Rolle des OSCI-Intermediärs und kann in Kombination mit weiteren Governikus-Produkten eingesetzt werden:

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

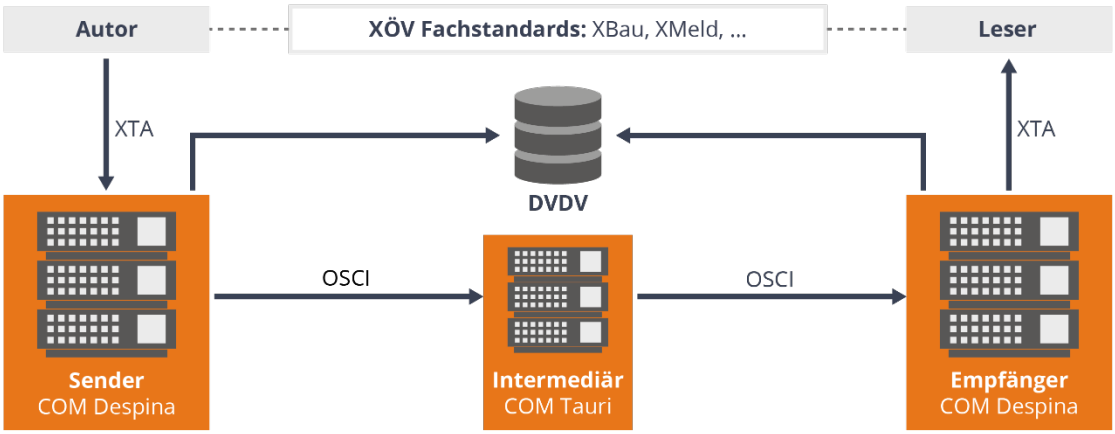


Abbildung 12: COM Tauri als Intermediär im Zusammenspiel mit COM Despina für XTA-Kommunikation

Auch die Verbindung mit COM Vibilia als Client ist möglich:

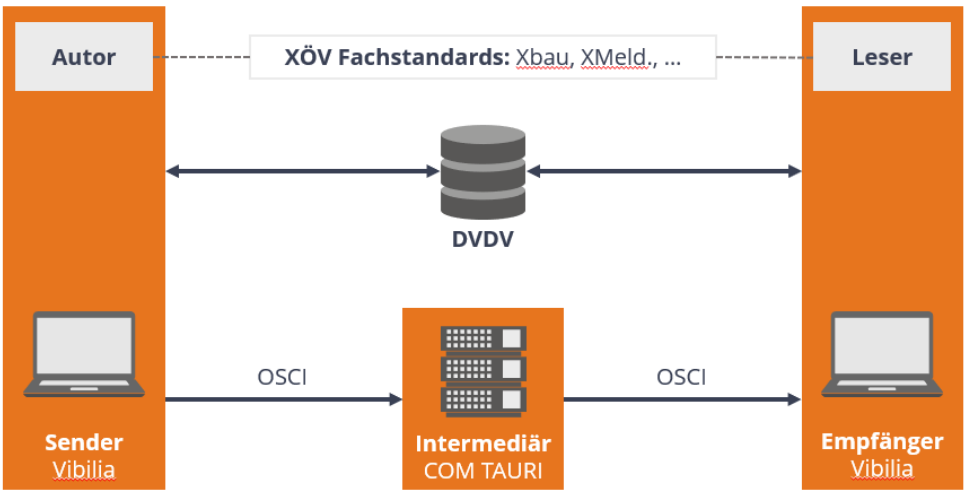


Abbildung 13: COM Tauri als Intermediär im Zusammenspiel mit COM Vibilia als Desktop-Client

Technologie (Kurzbeschreibung und Voraussetzungen)

COM Tauri nutzt JBoss als Application-Server. Als Betriebssysteme werden Windows Server, Linux und Ubuntu unterstützt. Weitere Informationen finden sich in den Hard- und Softwarevoraussetzungen für die Governikus Suite.

Zukünftig wird COM Tauri containerisiert in Kubernetes betrieben werden können.

COM Tauri wird kontinuierlich an neue Technologien angepasst und mit Fokus auf den Bedarf der Öffentlichen Verwaltung gepflegt.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Distribution (Wie und wo kann das Produkt bezogen werden?)

Governikus stellt im Rahmen des Produktes des IT-Planungsrates „Anwendung Governikus“ seit vielen Jahren Bund, Ländern und Kommunen rund um die Erzeugung und Validierung von Signaturen und Siegeln sowie Dokumenten alle notwendigen IT-Komponenten zur Verfügung, die für die sichere, rechtsverbindliche und durchgängig digitale Verwaltungsarbeit benötigt werden. Alle 16 Bundesländer sind dem Vertrag zur „Anwendung Governikus“ beigetreten und in enger Kooperation mit Vertreter:innen aus diesen Ländern und deren Kommunen werden diese Komponenten kontinuierlich angepasst, erweitert und gepflegt. Der Abruf sowie Support der Anwendung erfolgen über die sogenannten „Benannten Stellen“.

www.governikus.de/loesungen/it-planungsrat/anwendung-governikus

3.4 OSCI Bibliothek

Wozu dient sie?

Um die Hersteller von Software bei der Implementierung eines OSCI-Transportszenarios zu unterstützen, bietet der Lenkungsausschuss der IT-Planungsratsanwendung Governikus eine OSCI-Bibliothek und einen Testintermediär an, an den OSCI-Nachrichten geschickt werden können.

Die OSCI-Bibliothek ist eine Softwarebibliothek in Java und .NET die das OSCI-Protokoll gemäß der OSCI 1.2 Spezifikation implementiert. Die OSCI-Bibliothek bietet Entwickler:innen Werkzeuge und Funktionen, um ihre Anwendungen um OSCI-Kommunikation zu erweitern.

Die Bibliothek stellt die notwendigen Funktionen zur Verfügung, um Verschlüsselung, digitale Signaturen und sichere Kommunikation über das OSCI 1.2 Protokoll umzusetzen.

Wo finde ich weitergehende Informationen?

https://www.osci.de/bibliothek/index.htm

https://www.xoev.de/osci-1-2-bibliothek-funktionale-beschreibung-2626

https://www.governikus.de/service/osci-bibliothek/

Wer kann es verwenden?

Für jeden abrufbar unter: https://www.governikus.de/service/osci-bibliothek/ .

3.5 COM Despina DVDV/OSCI Edition

Produktbeschreibung (Welche Funktionen hat das Produkt?)

Governikus COM Despina DVDV/OSCI Edition bietet für Fachverfahren von Behörden einen Zugang zur auf XÖV-Standards basierender Datenübertragung, die mittels OSCI und DVDV durchgeführt wird. Dank XTA-Webservice-Schnittstelle realisiert COM Despina DVDV/OSCI Edition den Datenaustausch zwischen Fach- und Transportverfahren, unabhängig von den beim Transport verwendeten Kommunikationsprotokollen.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

XTA standardisiert den Austausch von Nachrichten zwischen Fach- und Transportverfahren und unterstützt zudem die automatisierte, fachunabhängige Weiterverarbeitung von Nachrichten. Die Datenübertragung des XTA-Protokolls wird mittels mutual Transport Layer Security (mTLS) abgesichert. XTA verwendet ein 4-Corner-Modells basierend auf den Rollen Autor und Leser der Anwendungsebene sowie Sender und Empfänger auf der Transportebene.

Einsatzzweck (Welche Umsetzungsziele werden mit dem Produkt adressiert?)

COM Despina DVDV/OSCI Edition kann in mehreren Szenarien eingesetzt werden. Über XTA werden die Anwendungsebene der Fachverfahren und der OSCI-Transportebene entkoppelt. Die DVDV/OSCI Edition ermöglicht sowohl die Behörde-zu-Behörde-Kommunikation als auch die Behörde-zu-Postfach/Servicekonto-Kommunikation. Dabei greift COM Despina DVDV/OSCI Edition auf Governikus COM Tauri (OSCI-Intermediär) zu. Bei der Behörde-zu-Behörde-Kommunikation werden in einem automatisierten Prozess die OSCI-Adressdaten über das Deutsche Verwaltungsdienstleverzeichnis (DVDV) ermittelt. Mit den vom DVDV übergebenen Daten wird eine OSCI-Nachricht aufgebaut und versendet.

In der nachfolgenden Abbildung ist das Zusammenspiel von COM Despina DVDV/OSCI mit COM Tauri zu sehen. COM Despina wird hierbei sowohl auf Seiten des Senders, als auch des Empfängers eingesetzt.

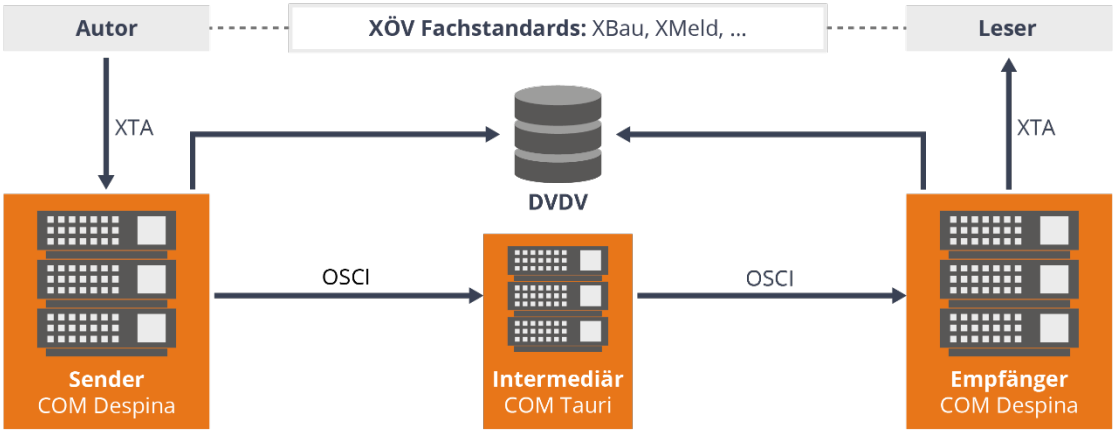


Abbildung 14: 4-Corner-Modell – COM Despina DVDV/OSCI Edition für XTA-Kommunikation im Zusammenspiel mit COM Tauri als Intermediär.

Technologie (Kurzbeschreibung und Voraussetzungen)

COM Despina DVDV/OSCI Edition nutzt JBoss als Application-Server. Als Betriebssysteme werden Windows Server, Linux und Ubuntu unterstützt. Weitere Informationen finden sich in den Hard- und Softwarevoraussetzungen für die Governikus Suite.

Zukünftig wird COM Despina DVDV/OSCI Edition in Kubernetes-Umgebungen betrieben werden können.

COM Despina DVDV wird kontinuierlich an neue Technologien angepasst und mit Fokus auf den Bedarf der Öffentlichen Verwaltung gepflegt.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Distribution (Wie und wo kann das Produkt bezogen werden?)

Governikus stellt im Rahmen des Produktes des IT-Planungsrates „Anwendung Governikus“ seit vielen Jahren Bund, Ländern und Kommunen rund um die Erzeugung und Validierung von Signaturen und Siegeln sowie Dokumenten alle notwendigen IT-Komponenten zur Verfügung, die für die sichere, rechtsverbindliche und durchgängig digitale Verwaltungsarbeit benötigt werden. Alle 16 Bundesländer sind dem Vertrag zur „Anwendung Governikus“ beigetreten und in enger Kooperation mit Vertreter:innen aus diesen Ländern und deren Kommunen werden diese Komponenten kontinuierlich angepasst, erweitert und gepflegt. Der Abruf sowie Support der Anwendung erfolgen über die sogenannten „Benannten Stellen“.

www.governikus.de/loesungen/it-planungsrat/anwendung-governikus

Wo finde ich weitergehende Informationen?

www.governikus.de/loesungen/it-planungsrat/anwendung-governikus

3.6 COM Despina Peppol/AS4 Edition

Produktbeschreibung (Welche Funktionen hat das Produkt?)

COM Despina Peppol/AS4 Edition ermöglicht den elektronischen Datenaustausch im Standard XRechnung gemäß der Europäischen Richtlinie sowie der darauf basierenden E-Rechnungs-gesetzgebung. Zusätzlich werden auch die weiteren Peppol Business Interoperability Specifications (BIS) im Post-Award-Bereich unterstützt. COM Despina Peppol/AS4 Edition bietet mittels XTA einen Zugang zu Peppol-AS4-Kommunikationsszenarien.

Peppol ist ein offenes Netzwerk, das allen registrierten Partnern erlaubt, über eine einzige Verbindung elektronische Dokumente im Zusammenhang mit elektronischen Beschaffungsprozessen (E-Procurement) auszutauschen. Die weltweite Governance des Peppol-Netzwerks erfolgt über die Non-Profit Organisation OpenPeppol (AISBL nach belgischem Recht). OpenPeppol ist eine demokratische, von Mitgliedern geführte Organisation, die sich aus Mitgliedern des öffentlichen und des privaten Sektors zusammensetzt. Sie standardisiert digitale Geschäftsprozesse, indem sie vereinheitlicht, wie Informationen strukturiert ausgetauscht werden.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

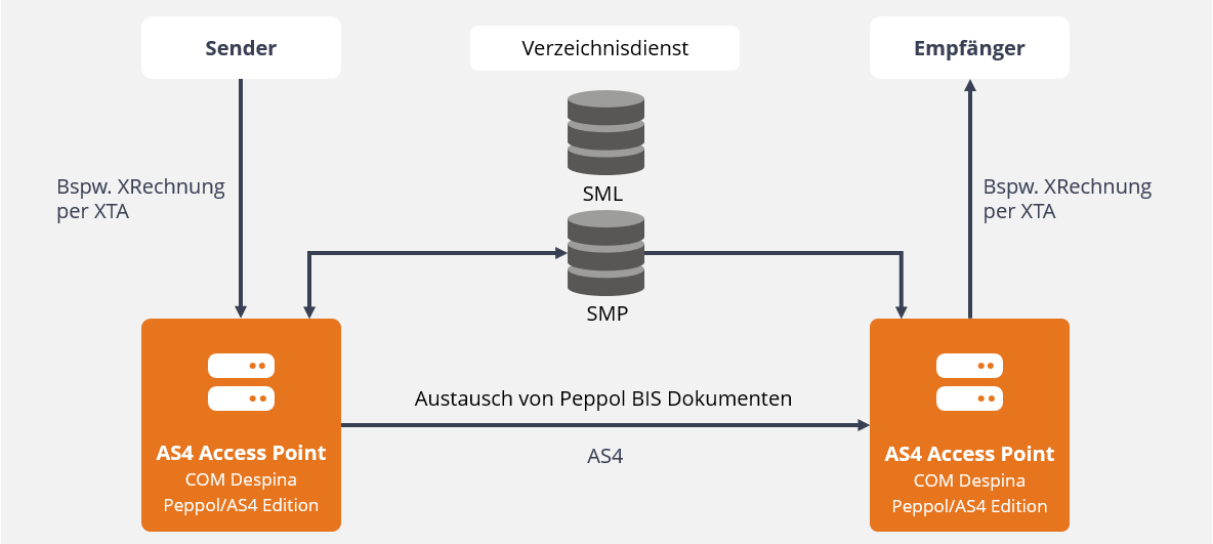


Abbildung 15: COM Despina Peppol/AS4 Edition im Peppol 4-Corner-Model

Einsatzzweck (Welche Umsetzungsziele werden mit dem Produkt adressiert?)

COM Despina Peppol/AS4 Edition gewährleistet den sicheren und rechtsverbindlichen Datenaustausch via auf OpenPeppol basierenden AS4-Kommunikationsszenarien.

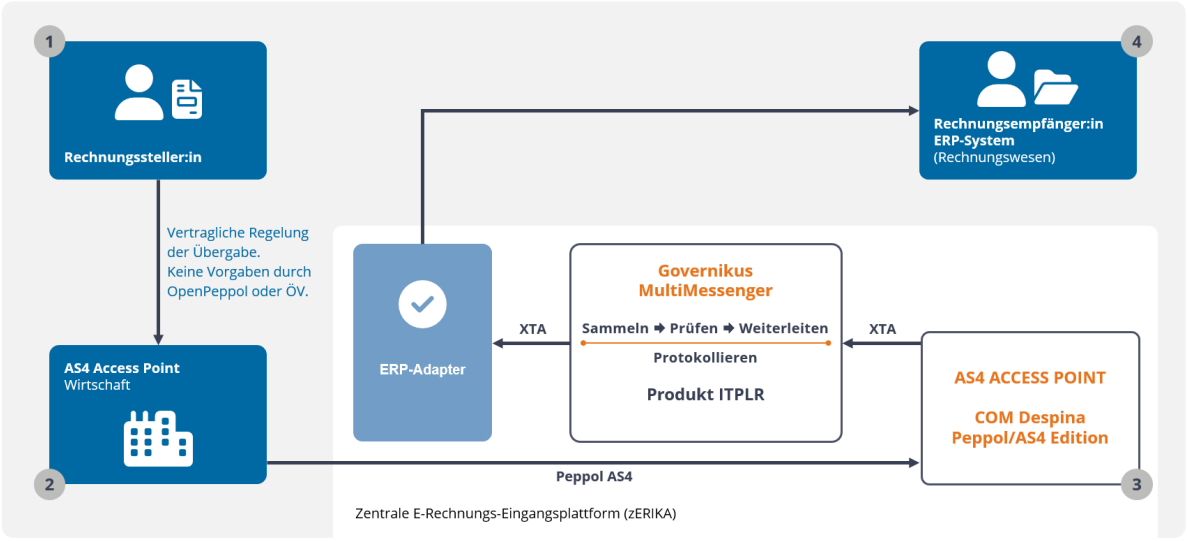


Abbildung 16: COM Despina Peppol/AS4 Edition im Einsatzszenario E-Rechnung im Zusammenspiel mit Governikus MultiMessenger

Technologie (Kurzbeschreibung und Voraussetzungen)

COM Despina Peppol/AS4 Edition nutzt JBoss als Application Server. Als Betriebssysteme werden Windows Server, Linux und Ubuntu unterstützt. Weitere Informationen finden sich in den Hard- und Softwarevoraussetzungen für die Governikus Suite.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Zukünftig wird COM Despina Peppol/AS4 Edition containerisiert in Kubernetes betrieben werden können.

COM Despina Peppol/AS4 Edition wird kontinuierlich an neue Technologien angepasst und mit Fokus auf den Bedarf der Öffentlichen Verwaltung gepflegt.

Distribution (Wie und wo kann das Produkt bezogen werden?)

Governikus stellt im Rahmen des Produktes des IT-Planungsrates „Anwendung Governikus" seit vielen Jahren Bund, Ländern und Kommunen rund um die Erzeugung und Validierung von Signaturen und Siegeln sowie Dokumenten alle notwendigen IT-Komponenten zur Verfügung, die für die sichere, rechtsverbindliche und durchgängig digitale Verwaltungsarbeit benötigt werden. Alle 16 Bundesländer sind dem Vertrag zur „Anwendung Governikus" beigetreten und in enger Kooperation mit Vertreter:innen aus diesen Ländern und deren Kommunen werden diese Komponenten kontinuierlich angepasst, erweitert und gepflegt. Der Abruf sowie Support der Anwendung erfolgen über die sogenannten „Benannten Stellen".

www.governikus.de/loesungen/it-planungsrat/anwendung-governikus

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

4 Services

4.1 COM Despina Referenzumgebung / XTA-Server

Wozu dient es?

Der COM Despina Testservice ist ein integraler Bestandteil der Referenzumgebung und ermöglicht eine Erprobung verschiedener Funktionen. Ein wesentliches Element hierbei ist der XTA-Server (COM Despina), der nicht nur für das Senden und Empfangen von XTA-Nachrichten verantwortlich ist, sondern auch in der Lage ist, OSCI-Nachrichten zu erstellen und an einen Intermediär zu übermitteln. Der Governikus Test-Intermediär kann dabei zusätzlich für das Testen dieser Funktionalitäten eingesetzt werden. Der COM Despina XTA-Server ist zudem darauf ausgelegt, Testantworten abzurufen, die anschließend über das XTA-Protokoll bereitgestellt werden.

Wer kann es benutzen?

Der Zugang zum COM Despina Testservice sowie zum Governikus Test-Intermediär steht allen offen, die sich für die Nutzung der Referenzumgebung registriert haben. Die Anbindung an die XTA2-Schnittstelle ist für Hersteller von Fachverfahrensclients gedacht, die den Versand und Empfang von XTA2-Nachrichten über OSCI testen möchten.

Wie nutzt man es?

Um den COM Despina Testservice und den Governikus Test-Intermediär nutzen zu können, ist eine Anmeldung über das auf der verlinkten Webseite bereitgestellte Anmeldeformular nötig. Im Rahmen der Referenzumgebung wird auch ein Soap-UI-Projekt bereitgestellt, welches schon so eingerichtet ist, dass direkt Nachrichten verschickt und empfangen werden können.

Für jeden Testuser werden zwei XTA-Benutzer mit jeweils eigenem Schlüssel für die SSL-Client-Authentisierung am XTA-Webservice bereitgestellt. Zusätzlich werden für die OSCI-Kommunikation zwei passende DVDV-Einträge mit entsprechendem Schlüsselmaterial für die OSCI-Kommunikation erstellt.

Weitere Informationen:

https://www.governikus.de/service/osci-xta-referenzumgebung/

4.2 XTA Testbed

Wozu dient es?

Ab Version 4 des XTA-Standards ist definiert, welcher Umfang der Spezifikation mindestens zu implementieren ist, um eine zur Spezifikation konforme Implementation zu haben. Mit den Konformitätsvorgaben sollen interoperable Implementierungen eines XTA-Transportadapters gefördert werden.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Eine Implementierung ist zu der genannten Version der XTA-Spezifikation konform, wenn:

- alle allgemeinen Anforderungen an die Anwendungsebene und zusätzlich
- alle Anforderungen an die Rollen erfüllt werden, die durch die Implementierung abgebildet werden (nur Autor, nur Leser oder Autor und Leser).

Das Dokument mit den Konformitätsvorgaben für eine spezifische Version des XTA Standards ist über die Einstiegsseite der Version zu erreichen.

Wer kann es benutzen?

Jeder kann sich registrieren und das XTA Testbed benutzen. Es gibt aktuell keine Einschränkungen oder Limits. Das XTA Testbed wird in der Praxis vor allem von Entwickler:innen, Organisationen und Herstellern von Fachverfahrensclients genutzt, die Transportadapter nach dem XTA-Standard implementieren möchten.

Wie nutzt man es?

Man meldet sich über das Anmeldeformular auf der verlinkten Webseite an. Im Rahmen der Referenzumgebung wird auch ein Soap-UI-Projekt bereitgestellt, welches schon so eingerichtet ist, dass direkt Nachrichten verschickt werden können. Alle Informationen werden nach der Anmeldung über ein Ticketsystem übergeben. Es werden 2 XTA-Benutzer mit einem jeweils eigenen Schlüssel für die SSL-Client-Authentisierung am XTA-WS bereitgestellt. Zusätzlich werden für die OSCI-Kommunikation 2 passende DVDV-Einträge mit entsprechendem Schlüsselmaterial für die OSCI-Kommunikation erstellt.

Weitere Informationen:

Registrierung unter:
https://www.governikus.de/service/osci-xta-referenzumgebung/

Einstiegseite für XTA 2 Version 3:
https://www.xoev.de/xta/v3

XTA-Konformitätsvorgaben zur Umsetzung von XTA 2 Version 3.x:
https://www.xoev.de/sixcms/media.php/13/XTA_Konformitaetsvorgaben_Produkt_XTA2V3.pdf

4.3 OSCI / Intermediär Testserver

Wozu dient es?

Um Fachverfahrensherstellern bei der Implementierung eines OSCI-Transportszenarios zu unterstützen, bietet der Lenkungsausschuss der IT-Planungsratsanwendung Governikus eine OSCI-Bibliothek und einen Testintermediär an, an den OSCI-Nachrichten geschickt werden können.

Zum Testen der Implementierung stellt die Governikus einen Testintermediär zur Verfügung, an den OSCI-Nachrichten gesendet werden können.

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

Wer kann es benutzen?

Interessierte Softwarehersteller.

Wie nutzt man es?

Informationen zum Leistungsumfang des Testintermediärs sind auf der Informationsseite zur OSCI 1.2 Bibliothek zu finden.

Informationsseite zur OSCI 1.2 Bibliothek: https://www.governikus.de/service/osci-bibliothek/

4.4 DVDV-Testsystem

Wozu dient es?

Das DVDV-Testsystem soll ermöglichen, dass Fachverfahrensherstellern die Anbindung an DVDV testen können.

Das DVDV-Testsystem liefert auf Anfragen nur solche Daten zurück, die dort zuvor durch die für das Testsystem zuständigen Pflegenden Stellen für die Testteilnehmer eingepflegt wurden.

Damit können die *technischen* Aspekte des Zugriffs auf das operative DVDV simuliert werden. Es handelt sich jedoch nicht um ein *fachliches* Testsystem, welches z. B. semantisch korrekte Antworten eines Fachverfahrens in einem XÖV-Standard liefert.

Wer kann es benutzen?

Das DVDV-Testsystem können alle Unternehmen und Organisationen, die bereits auf das operative DVDV zugreifen oder künftig zugreifen wollen, verwenden. Dies sind insbesondere Hersteller von Fachverfahren.

Voraussetzung für die Nutzung des DVDV-Testsystems sind die Anerkennung und Einhaltung der Nutzungsbedingungen.

Wie nutzt man es?

Die Teilnahme am DVDV-Testsystem ist kostenfrei möglich. Interessenten wenden sich bitte an die Koordinierende Stelle DVDV unter der Mailadresse dvdv@itzbund.de.

Auf dem DVDV-Testsystem sind ausschließlich Testzertifikate zu verwenden. Diese dürfen keinesfalls auch auf dem DVDV-Produktivsystem verzeichnet sein.

Governikus stellt im Rahmen des DVDV-Testsystems keinen OSCI-Intermediär bereit, der für fachliche Tests zur Nachrichtenübertragung im OSCI-Transport-Format genutzt werden könnte.

Downloads zu DVDV: https://www.itz-bund.de/DE/itloesungen/standardloesungen/dvdv/downloads/downloads.html

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

4.5 beBPo as a Service

Wozu dient es?

beBPo aaS bietet Bezugsberechtigten bzw. Verpflichteten die Möglichkeit, mit dem gewohnten E-Mail-Client (z. B. Outlook, Thunderbird) am Elektronischen Rechtsverkehr (ERV) teilzunehmen. Eine Installation von Governikus COM Vibilia auf dem Arbeitsplatzrechner ist nicht notwendig.

beBPo aaS ist insbesondere für Anwender:innen interessant, die

- ein mittleres bis hohes Nachrichtenaufkommen haben und/oder
- einen gleichzeitigen Zugriff von mehreren Personen auf ihr Postfach benötigen und/oder
- mit ihrem gewohnten E-Mail-Client (z. B. Outlook) weiterarbeiten möchten und/oder
- sich eine zeitliche Ersparnis wünschen, da keine Zertifikatserneuerung durch Kund:innen nötig ist und
- kein zusätzliches Virenprogramm benötigt wird und auch
- die Pflege und Wartung durch Governikus erfolgt.

Wer kann es benutzen?

Nutzen können es Behörden sowie Körperschaften und Anstalten des öffentlichen Rechts, zu nennen sind hier beispielsweise Sparkassen, kassenärztliche Vereinigungen, Berufsgenossenschaften etc.

Für Kund:innen, die kein beBPo erhalten, gibt es als Alternative eBO aaS. Dieses ist dem beBPo aaS sehr ähnlich, hat jedoch die Einschränkung, dass eBOs untereinander nicht mit anderen eBOs kommunizieren können.

Wie nutzt man es?

Die Anbindung eines beBPos erfolgt unter Nutzung des bestehenden E-Mail-Servers, sodass der gewohnte E-Mail-Client (z. B. Outlook) genutzt werden kann. Die gesetzlich geforderten elektronischen Empfangsbekenntnisse und Strukturdatensätze können mit der ERV-Xtension, einem nutzerfreundlichen Client, angezeigt, bestätigt und per Drag&Drop via E-Mail an die Justiz zurückgesandt werden.

Weitere Informationen:

Beschreibung des beBPo:
https://egvp.justiz.de/behoerdenpostfach/

Informationsbroschüre zu beBPo aaS:
https://www.governikus.de/wp-content/uploads/2024/05/beBPo-aaS_Produktbroschuere.pdf

Beschreibung der ERV-Xtension:
https://www.governikus.de/wp-content/uploads/2022/06/Infoblatt_GMM_ERV-Xtension.pdf

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de

4.6 eBO aaS

Wozu dient es?

eBO as a Service (eBO aaS) dient als digitale Brücke für Bürger:innen und privatrechtliche Organisationen zur sicheren und rechtskonformen Kommunikation mit Justizbehörden, Rechtsanwält:innen, Notar:innen und Steuerberater:innen. Es ermöglicht die Teilnahme am Elektronischen Rechtsverkehr (ERV), indem es den Austausch von Dokumenten und Nachrichten in einem gesetzlich festgelegten Rahmen vereinfacht. eBO aaS bietet eine effiziente Lösung, um mit der Justiz und anderen relevanten Parteien digital zu kommunizieren, ohne die Notwendigkeit, physische Dokumente zu versenden oder spezielle Software zu installieren.

Wer kann es benutzen?

Das eBO kann verwendet werden von:

- Banken und Versicherungen, die nicht als öffentlich-rechtliche Körperschaften gelten, inklusive ihrer nicht-öffentlichen Partner.
- Rechtschutzversicherungen.
- Unternehmen aus Industrie und Mittelstand.
- Einzelpersonen, Berufsgruppen und Organisationen, bei denen von einer erhöhten Zuverlässigkeit ausgegangen werden kann.

Wie nutzt man es?

Zur Nutzung von eBO aaS ist ein herkömmlicher E-Mail-Client wie Outlook in Verbindung mit einer ERV-Xtension notwendig. Diese Kombination ermöglicht es den Nutzenden, E-Mails und Anhänge im XML-Format der XJustiz-Strukturdatensätze zu erstellen und zu versenden, was dem normalen E-Mail-Versand sehr ähnlich ist. Durch diese Integration können Nutzende ohne umfangreiche Einarbeitung oder spezielle Softwareinstallationen am elektronischen Rechtsverkehr teilnehmen

Weitere Informationen:

Beschreibung des eBO:
https://egvp.justiz.de/buerger_organisationen/index.php

Informationsbroschüre zu eBO aaS:
https://www.governikus.de/wp-content/uploads/2024/05/eBO-aaS_Produktbroschuere.pdf

Beschreibung der ERV-Xtension:
https://www.governikus.de/wp-content/uploads/2022/06/Infoblatt_GMM_ERV-Xtension.pdf

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: 0421 204 95-0
securecommunication@governikus.de
governikus.de