

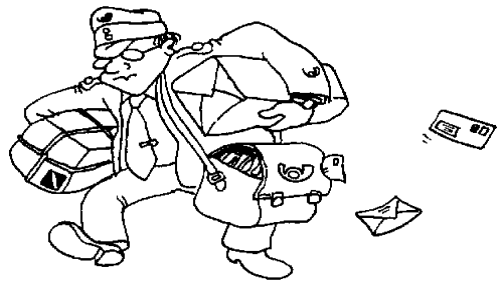


Inhalt

- Bekannte Transportmechanismen
- OSCI – Warum?
- Überblick und Sicherheitsziele
- OSCI-Nachricht
- Challenge / Response
- Rollenmodelle
- OSCI-Transport / Laufzettel
- Verschiedene Ebenen der Kommunikation
- OSCI-Auftragstypen

Ziele

- Zweck von OSCI-A und OSCI-B erkennen
- Rollenmodell verstehen
- Verschiedene Ebenen einer Nachricht identifizieren
- Die wichtigsten Auftragstypen von OSCI-Transport kennen



	<ol style="list-style-type: none">1. osci_spezifikation_1_2_deutsch.pdf2. osci_entwurfsprinzipien_1_2.2110.pdf
--	---

Bekannte Transportmechanismen

Bekannte Transportmechanismen, bei denen die Vertraulichkeit der Daten gewährleistet sein soll:


- SSL – Klassischer Transportmechanismus für das Web um Daten verschlüsselt zu übertragen (HTTPS).
- PGP – Clientseitiges Programm, welches direkt für verschiedene Bereiche Daten nach dem Hybridverfahren verschlüsseln kann.
- IPSEC – Sichert z.B. für VPN (Virtual Private Network) eine feste sichere Verbindung über das Internet.


OSCI- Warum?

OSCI ist ein **Datenaustauschformat und Protokoll** für die sichere Übertragung von Nachrichten auf Basis der digitalen Signatur über das Internet oder andere vergleichbare Kommunikationsmedien.

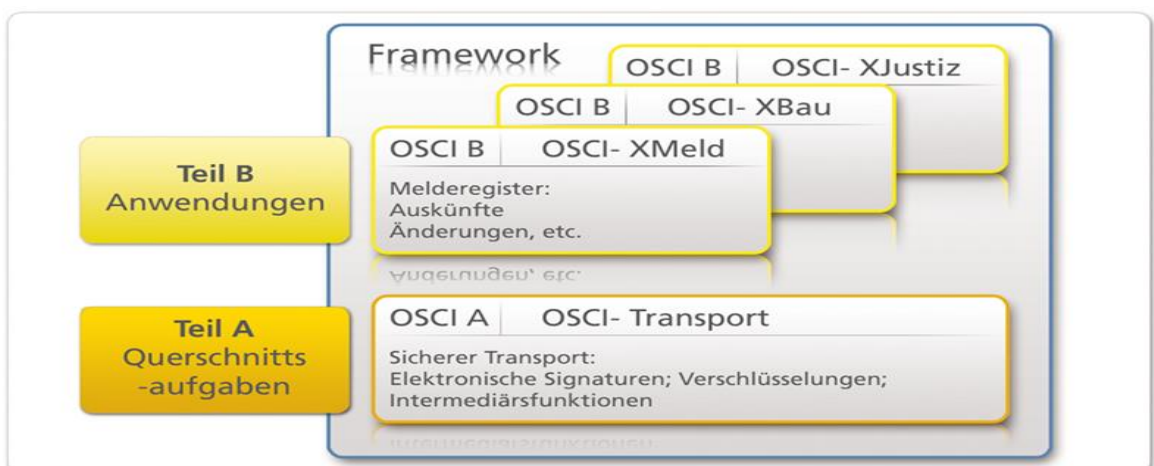
OSCI ermöglicht...

- die Erstellung eines „**OSCI-Laufzettels**“, welcher die gesamte Transaktion einer Nachricht von der Erstellung bis zum Ziel protokolliert.
- die Nachvollziehbarkeit einer Kommunikation/Transaktion durch den „OSCI-Laufzettel“.
- die Protokollierung der Gültigkeit der beteiligten Zertifikate einer Nachricht.
- die Protokollierung diverser Zeitpunkte innerhalb der Transaktion.
- die Trennung von Transport/Nutzungsdaten und Inhaltsdaten.
- die Erfüllung der Anforderungen des Signaturgesetzes.

	Die Virtuelle Poststelle (VPS) des Bundes für die Initiative Bund-Online 2005 basiert auf dem OSCI Protokoll.
---	---

 **Governikus KG** OSCI 1.2 5

OSCI: Überblick und Sicherheitsziele



Sicherheitsziele von OSCI

Inhalt:

- Authentizität / Integrität der Inhaltsdaten
 - *Signatur durch Ersteller (Autor), alle Signatur-Niveaus*
- Vertraulichkeit der Inhaltsdaten
 - *Verschlüsselung für den Empfänger mit öffentlichem Schlüssel*

Transport:

- Nachvollziehbarkeit und Zurechenbarkeit
 - *Signaturen, Quittungsmechanismen, Zeitstempel, Protokollierung*
- Sicherstellung der Authentizität von Sender / Empfänger in einer Kommunikation
 - *Challenge / Response*
- Authentizität / Integrität der Nutzungsdaten
 - *Signatur des Senders*

OSCI-Nachricht (1/2)

```
<?xml version="1.0" encoding="UTF-8" ?>

<soap:Envelope xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:osci="http://www.osci.de/2002/04/osci"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/ soapGetMessageId.xsd
http://www.w3.org/2000/09/xmldsig# oscisig.xsd http://www.w3.org/2001/04/xmlenc# oscienc.xsd">
+ <soap:Header>
+ <soap:Body xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:osci="http://www.osci.de/2002/04/osci"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" Id="body">
</soap:Envelope>
```

OSCI-Nachricht (2/2)

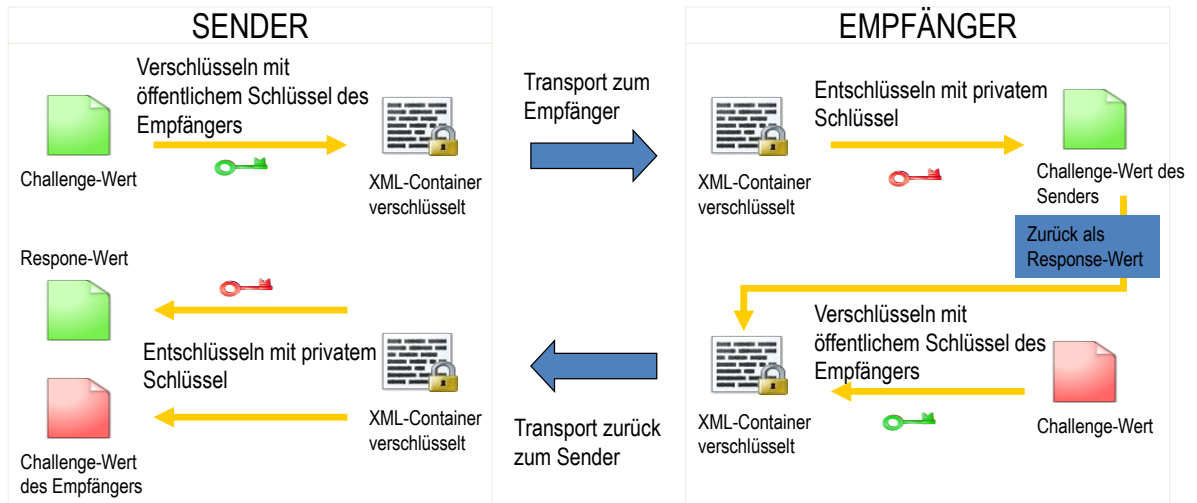
OSCI-Nachricht zusammengefasst

- Gesamte Nachricht im Tag **<soap:Envelope>**
- Transportdaten im Tag **<soap:Header>**
- Inhaltsdaten im Tag **<soap:Body>**

Challenge/Response

- In jeder OSCI-Kommunikation wird über einen Challenge-Wert sichergestellt, dass der Sender und auch der Empfänger über den privaten Schlüssel verfügen.
- Dieser Challenge-Wert wird vor jedem Senden erzeugt und neben weiteren Kommunikationsparametern als Inhalt eines Tags innerhalb einer XML-Struktur (OSCI) übermittelt.
- Dieses XML-Dokument wird in seiner Gesamtheit mit dem öffentlichen Zertifikat des Kommunikationspartners verschlüsselt.
- Grundsätzlich werden immer zwei Challenge-Werte übermittelt: Der vom jeweiligen Sender erzeugte Challenge-Wert und der vom Kommunikationspartner zuvor übermittelte Challenge-Wert, welcher als Response-Wert zurückgegeben wird.
- Auf diesem Wege ist sichergestellt, dass beide Kommunikationspartner in der Lage sind, den XML-Container mit ihrem privaten Schlüssel zu entschlüsseln und somit die Kommunikation nicht durch einen Dritten kompromittiert werden kann.

Challenge/Response Übersicht



OSCI-Nachricht (Challenge/Response)

```
<?xml version="1.0" encoding="UTF-8" ?>
<soap:Header>
  <osci:ControlBlock xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:osci="http://www.osci.de/2002/04/osci"
    xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ConversationId="11308546058280" Id="controlblock" SequenceNumber="0"
    soap:actor="http://schemas.xmlsoap.org/soap/actor/next" soap:mustUnderstand="1">
    <osci:Response>l6/FiCLiJBcdSg==</osci:Response>
    <osci:Challenge>kQ51JQnN7zsq2A==</osci:Challenge>
  </osci:ControlBlock> <Weitere Transportdaten und Tags>
</soap:Header>
<soap:Body xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:osci="http://www.osci.de/2002/04/osci"
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Id="body">
  <osci:ContentPackage>
    <osci:ContentContainer xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:osci="http://www.osci.de/2002/04/osci"
      xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Id="contentcontainer0">
    <osci:Content>
      <osci:Base64Content Id="content0">QW55IGNvbnRlbnQgZGF0YS4=</osci:Base64Content>
    </osci:Content>
    </osci:ContentContainer>
  </osci:ContentPackage>
</soap:Body>
```

Rollenmodell OSCI Übersicht

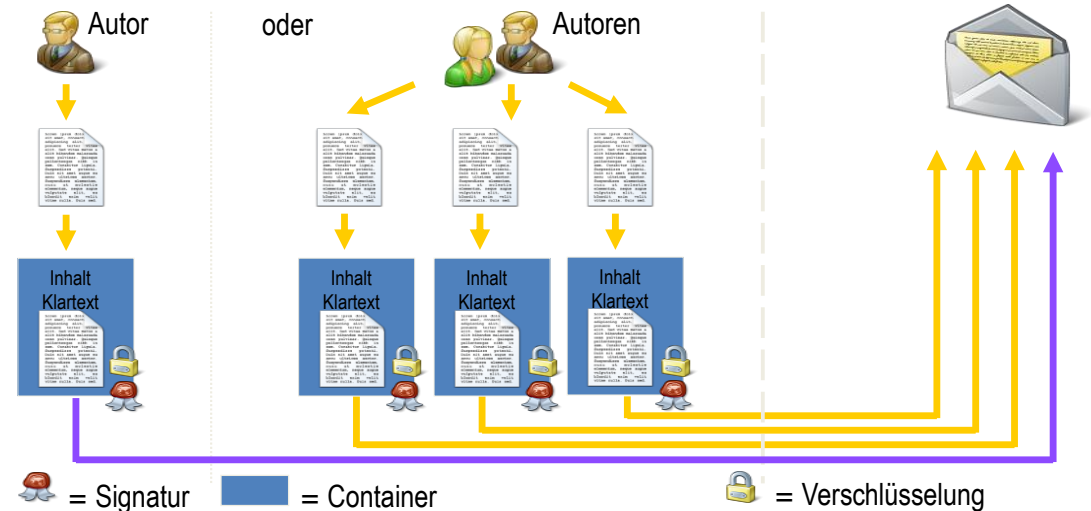
Folgende Rollen werden in OSCI unterschieden

- | | |
|--|--------------|
| • Autor einer Nachricht (Inhalt) : | Author |
| • Sender einer Nachricht (Transport): | Originator |
| • Vermittler (Transport): | Intermediary |
| • Empfänger einer Nachricht (Transport): | Addressee |
| • Leser einer Nachricht (Inhalt): | Reader |

Rollenmodell Autor

- Grundsätzlich gilt: Autor im Sinne des Rollenmodells ist die Einheit, die Inhaltsdaten erstellt und signiert. Es kann sich auch um mehrere Autoren mit unterschiedlichen Inhaltsdaten handeln.
- Ebenfalls können mehrere Autoren den gleichen Inhalt signieren (Mehrfachsignatur).
- Die Inhaltsdaten werden in einem oder mehreren Content-Tags eines XML-Containers zusammengefasst. Dieser wird signiert und stellt die eigentliche Signatur des Autoren dar.
In OSCI werden Binär- und ASCII-Dateien niemals direkt signiert!
- Die Inhaltsdaten können ebenfalls auf Containerebene durch den Autor mit dem öffentlichen Schlüssel des Lesers verschlüsselt werden.
- Bei dem Autor handelt es sich im Regelfall um eine natürliche Person. Autor kann aber auch eine technische Funktion sein.
Ebenso gilt dies im Zusammenhang mit mehreren Autoren.

Rollenmodell Übersicht Autor/en



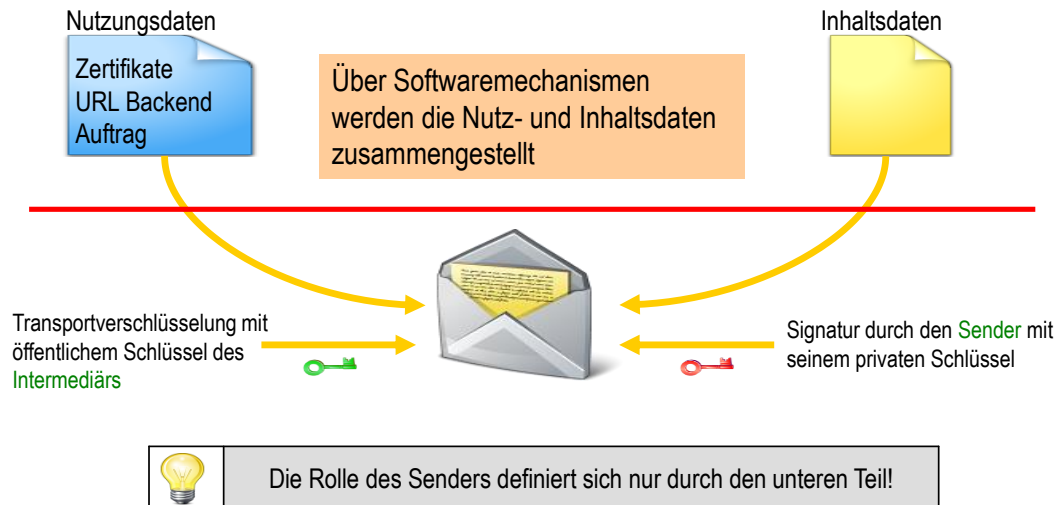
Rollenmodell Sender

- Sender im Sinne des Rollenmodells ist die Einheit, die auf Transportebene signiert und verschlüsselt.
- Die Nutzungs- und die Inhaltsdaten werden in einem Umschlag für den Sender durch Softwarefunktionalitäten bereitgestellt.

Die Nutzungsdaten umfassen folgende Informationen bzw. Inhalte für den Intermediär und auch für den Empfänger:

- das Signier- und Chiffrier-Zertifikat der Autoren und des Senders
- das Chiffrier-Zertifikat der Leser und des Empfängers
- Betreff-Informationen
- Zeitstempel (Zu welchen Zeitpunkt lag die Nachricht vor?)
- Auftragstyp (Was soll der Intermediär mit der Nachricht machen?)
- URL des Backends (Wohin soll die Nachricht geschickt werden?)
- Rückverschlüsselungszertifikat für den Client (Mit welchem Zertifikat soll die Antwort zum Client verschlüsselt werden?)

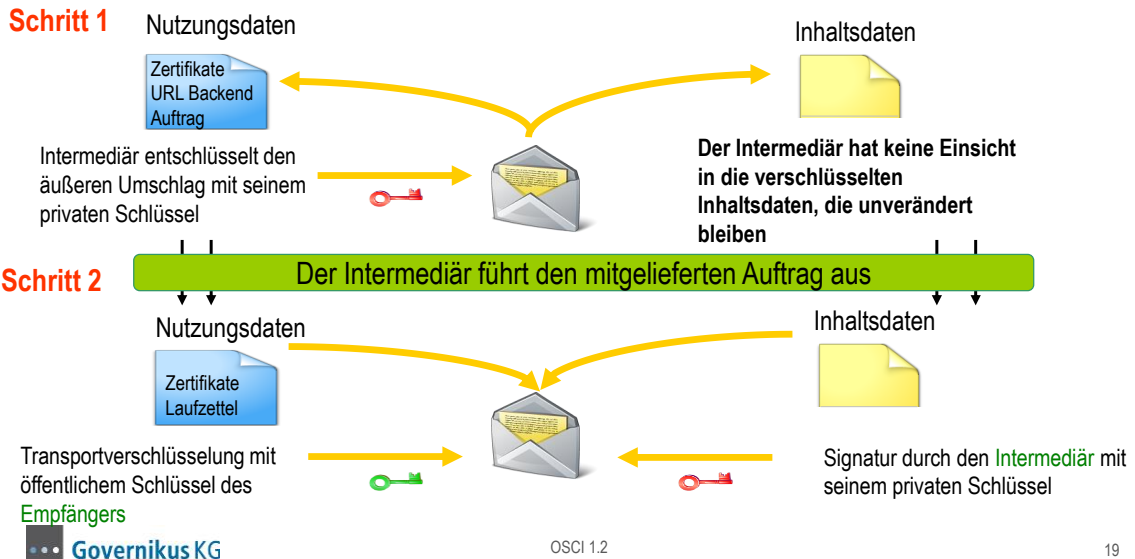
Rollenmodell Sender Übersicht



Rollenmodell Intermediär

- Der Intermediär hat nur Einsicht in die Transportdaten, nicht in die Inhaltsdaten.
- Er entschlüsselt den äußeren Umschlag mit seinem privaten Schlüssel.
- Der Intermediär interpretiert die Nutzungsdaten und führt den mitgelieferten „Auftrag“ aus.
- Bei asynchroner Kommunikation (z. B. Communicator) werden die Inhaltsdaten in der Datenbank des Intermediärs gespeichert. Auf Transportebene wird erst bei Abholung der Nachricht verschlüsselt und signiert.
- Bei synchroner Nachricht verschlüsselt der Intermediär erneut den Transportumschlag mit dem öffentlichen Schlüssel (im Zertifikat) des Empfängers und die Nachricht wird nicht gespeichert.
- In beiden Fällen kann der Intermediär den Transport signieren.
- Der Supplier ist dabei der Empfänger der OSCI-Nachricht.

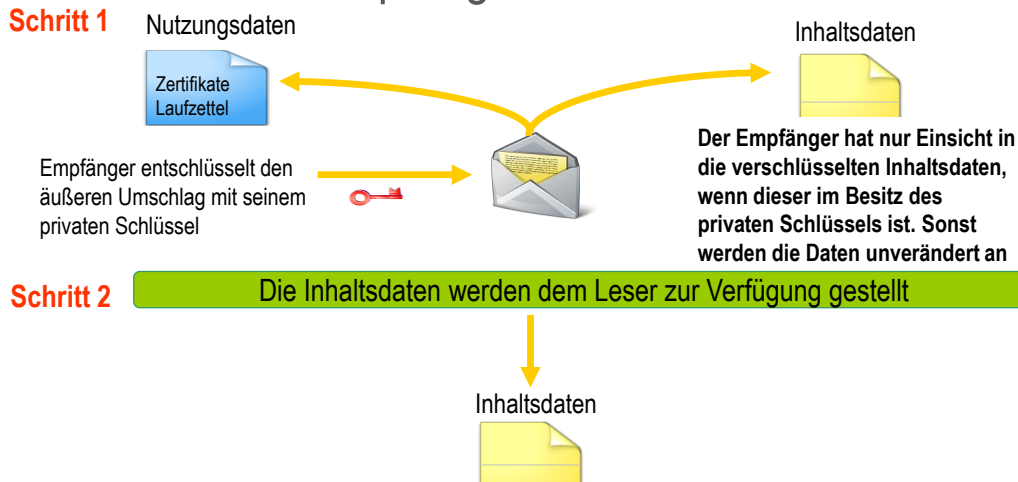
Rollenmodell Intermediär Übersicht



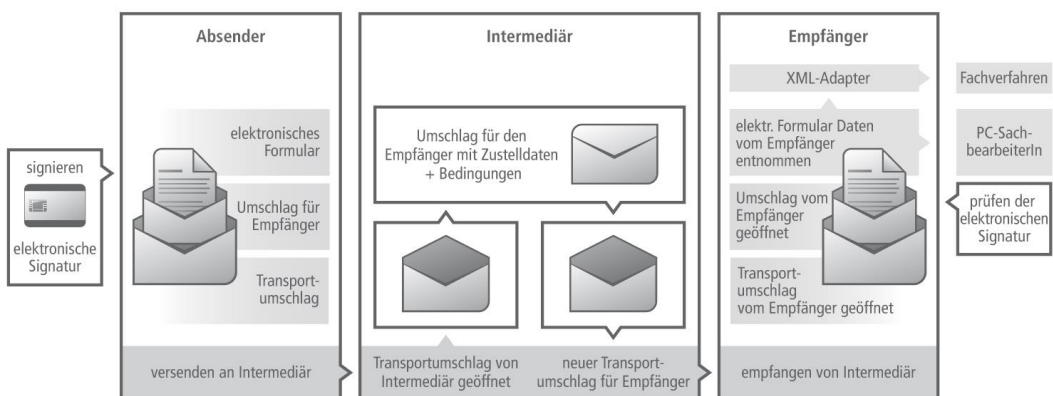
Rollenmodell Empfänger

- Der Empfänger ist in seiner Rolle auf gleicher Ebene wie der Sender.
- Er ist im Sinne des Rollenmodells die Instanz, die auf Transportebene entschlüsseln kann.
- Er stellt dem Leser die Inhaltsdaten (verschlüsselt oder unverschlüsselt) zur Verfügung.

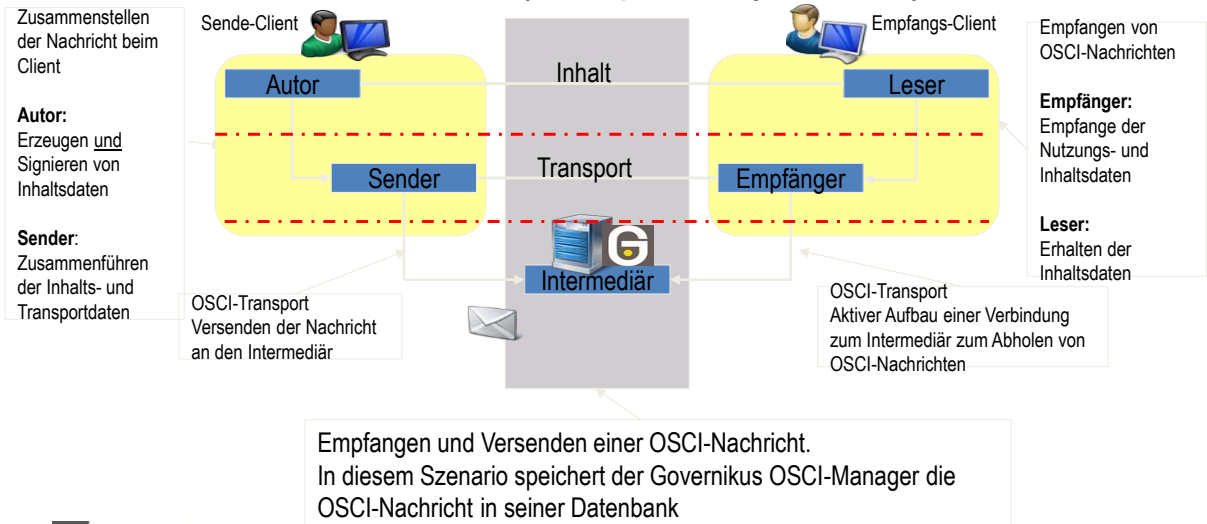
Rollenmodell Empfänger Übersicht



OSCI-Transport: „Doppelter Umschlag“



Rollenmodell: Ebenen (Beispiel Asynchron)



OSCI-Laufzettel

- Der OSCI-Laufzettel wird für jede Transaktion vom Intermediär angelegt.
- Er kann unabhängig von der eigentlichen Nachricht auch nachträglich abgeholt werden.
- Folgende Daten beinhaltet der Laufzettel (Processcard):
 - MessageID
 - Diverse Zeitpunkte (Eingang der Nachricht beim Intermediär, Änderung des Laufzettels, etc...)
 - OSCI-Subject
 - Issuer, Subject und Seriennummer der beteiligten Zertifikate
 - Prüfergebnisse der beteiligten Zertifikate

Verschiedene Ebenen der Kommunikation

Geschäftsvorfallebene:

- Ein oder mehrere Autoren stellen einem oder mehreren Lesern Informationen (Inhaltsdaten) zur Verfügung.

Nachrichtenebene:

- Ein Nachrichtensender schickt eine OSCI-Nachricht an einen Nachrichtenempfänger. Client und Intermediär können beide Rollen wahrnehmen.

Auftragsebene:

- Ein Client richtet einen Auftrag an einen Supplier. Der Auftrag enthält eine Arbeitsanweisung mitsamt allen zur Erledigung des Auftrages notwendigen Daten.

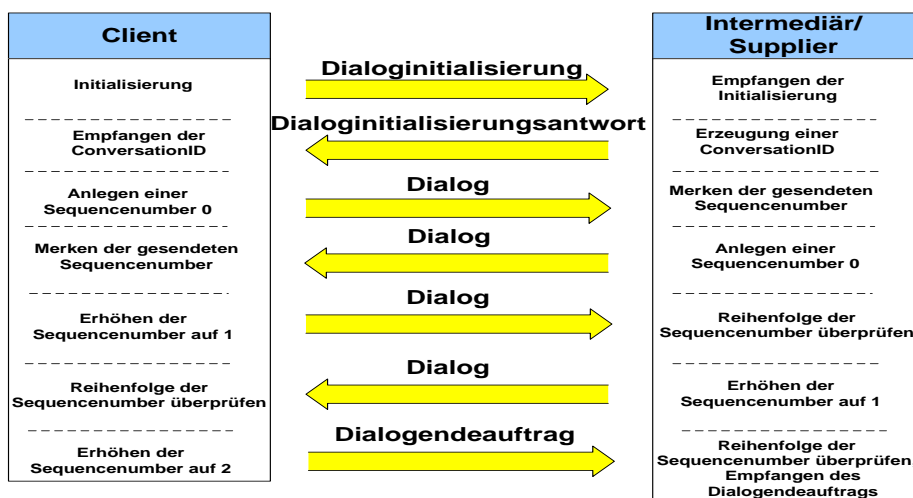
Dialoge

- Der Begriff des Dialogs betrifft die Auftragsebene von OSCI-Transport.
Auftrag-Antwort-Paare werden zu Dialogen zusammengefasst.
Jeder Dialog umfasst mindestens ein Auftrag-Antwort-Paar.
- Unterschieden wird zwischen einem expliziten und impliziten Dialog.
- Ein Dialog besteht zwischen genau einem Client und einem Supplier.

Expliziter Dialog

- Ein expliziter Dialog wird identifiziert durch die ihm zugeordnete **ConversationID**. Die ConversationID wird vom Supplier vergeben. Sie ist in dem Sinne eindeutig, da ein Supplier jede ConversationID nur ein einziges Mal vergibt.
- Innerhalb eines expliziten Dialogs nummerieren Client und Supplier ihre Nachrichten unabhängig voneinander bei 0 beginnend durch. Die Nummer des jeweiligen Auftrags / der jeweiligen Auftragsantwort wird als **SequenceNumber** bezeichnet.
- Durch Angabe des Suppliers, der ConversationID und der SequenceNumber lässt sich sowohl jeder Auftrag als auch jede Auftragsantwort eindeutig identifizieren.
- Bei einem expliziten Dialog wird die Kommunikation von der Initialisierung bis zur Beendigung des Dialogs überwacht.

Expliziter Dialog Übersicht



OSCI-Auftragstypen

Dialogspezifische Aufträge:

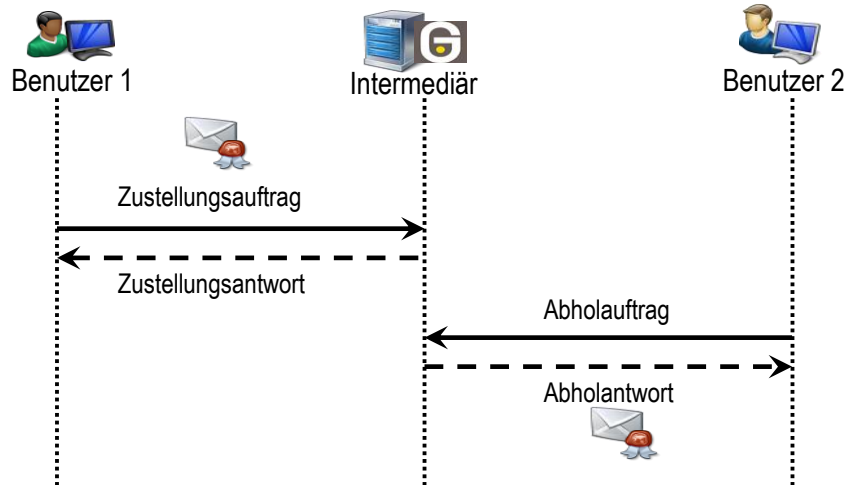
- Dialoginitialisierungsauftrag: Ein Client eröffnet einen expliziten Dialog.
- Dialogendeauftrag: Ein Client beendet einen expliziten Dialog.
- MessageID-Anforderungsauftrag: Ein Benutzer fordert eine MessageID bei einem Intermediär an (impliziter Dialog).

OSCI-Auftragstypen Asynchron

Aufträge bezüglich asynchroner Kommunikation:

- Zustellungsauftrag: Ein Benutzer sendet eine Zustellung an einen Intermediär, damit dieser sie zur Abholung durch einen anderen Benutzer bereit hält.
- Abholauftrag: Ein Benutzer holt bei einem Intermediär eine Zustellung ab, die ein anderer Benutzer zuvor mittels eines Zustellungsauftrags eingereicht hat.
- Laufzettelabholauftrag: Ein Benutzer holt einen oder mehrere Laufzettel bei einem Intermediär ab. In einem Laufzettel wird der Weg einer Zustellung von einem Sender zu einem Empfänger protokolliert.

Asynchrone Kommunikation Übersicht

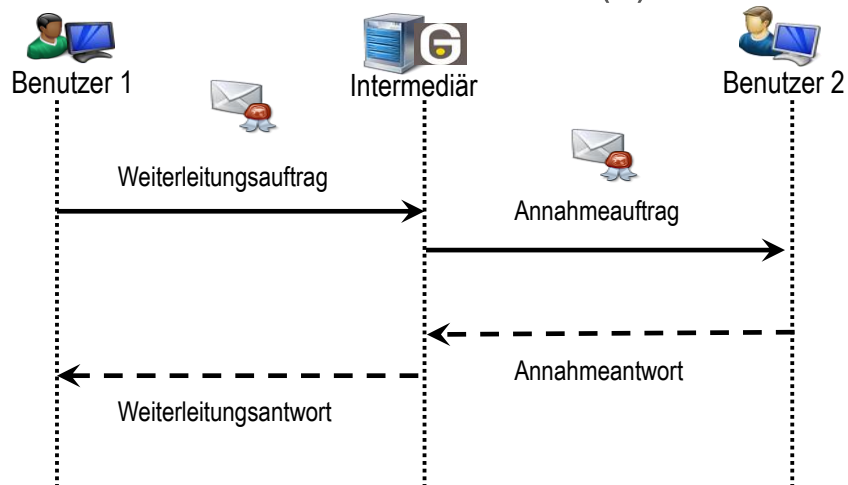


OSCI-Auftragstypen Synchron

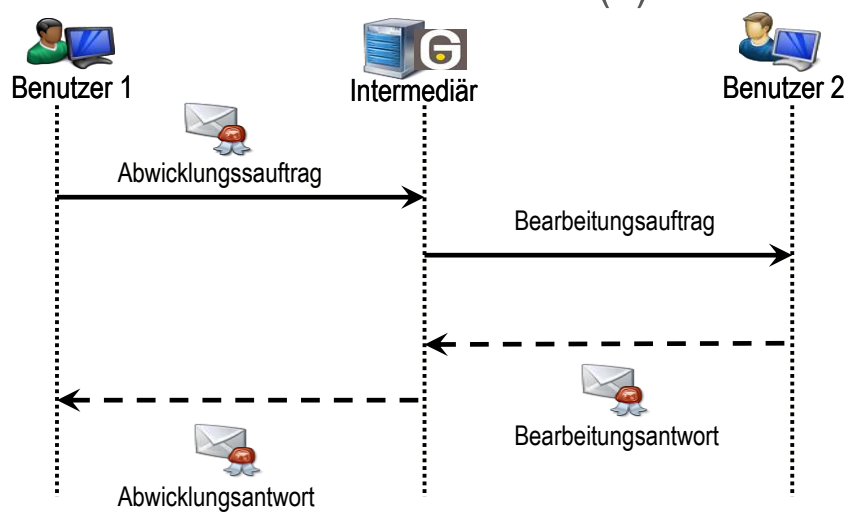
Aufträge bezüglich synchroner Kommunikation:

- Weiterleitungsauftrag: Ein Benutzer sendet eine Zustellung an einen Intermediär, damit dieser sie an einen Dienstanbieter weiterleitet.
- Annahmearauftrag: Der Intermediär sendet einen Annahmearauftrag an ein passives Backend.
- Abwicklungsauftrag: Ein Benutzer sendet eine Zustellung an einen Intermediär, damit dieser sie an einen Dienstanbieter weiterleitet. Der Benutzer fordert auftragsbezogene Daten als Rückantwort.
- Bearbeitungsauftrag: Der Intermediär initiiert einen expliziten Dialog mit dem Backend. Hierbei wird eine neue MessageID erzeugt. Der Dienstanbieter liefert eine Rückantwort, die dem Sender über dem Intermediär übermittelt wird.

Synchrone Kommunikation Übersicht (1)



Synchrone Kommunikation Übersicht (2)



Vielen Dank
für Ihre
Aufmerksamkeit!

