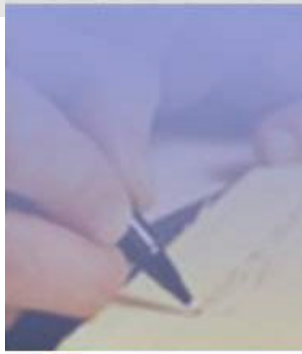
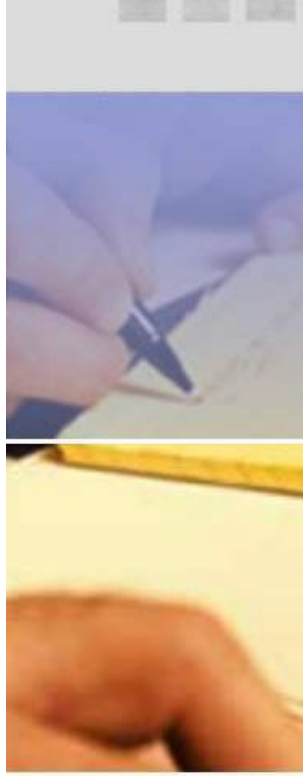


GovLink

**ein Framework für rechtsverbindlichen Austausch von strukturierten Dokumenten (Formularen)**

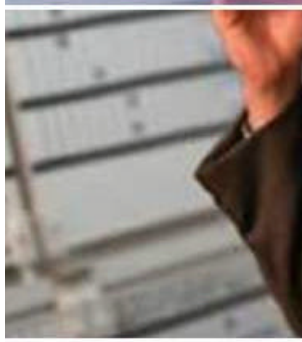
# genda



- Ausgangssituation im Projekt GovLink
- Anforderungen an den rechtsverbindlichen Austausch von strukturierten Dokumenten
- Lösungssuche
- OSCI (Online Services Computer Interface )
- OSCI-Implementierung (Governikus)
- Zusammenfassung / Ausblick

Kapitel

1



# Ausgangssituation im Projekt GovLink

## „Wie alles begann …“

# Gemeinsames Bedürfnis nach rechtsverbindlichem Transport

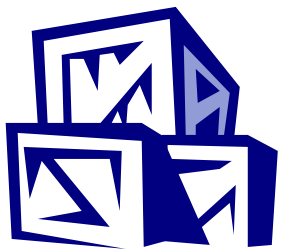


**Mehrere Anwendungen haben dieselbe Grundanforderung:**

**Sie benötigen einen rechtsverbindlichen Transport von strukturierten Dokumenten.**

Beispiele:

- Handelsregister (Anmeldung für Eintrag)
- Elektronischer Rechtsverkehr (JusLink)



# Gründe für die Entwicklung oder Evaluation eines Standards



- Verkürzung von Projektzeiten
- Interoperabilität
- Investitionsschutz
- Erreichbarkeit der „kritischen Masse“

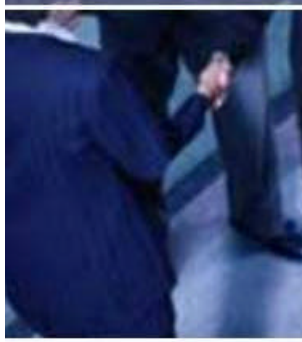
# Auftrag GovLink

Entwicklung und Evaluation eines Frameworks für den rechtsverbindlichen, elektronischen Austausch strukturierter Dokumente unter Berücksichtigung folgender Aspekte:

- Rechtsverbindlichkeit und Sicherheit
- Schliessen von Prozessketten
- Eliminierung von Medienbrüchen
- Verwendung von Industrie-Standards
- Flexibilität und Ausbaumöglichkeit

Kapitel

2



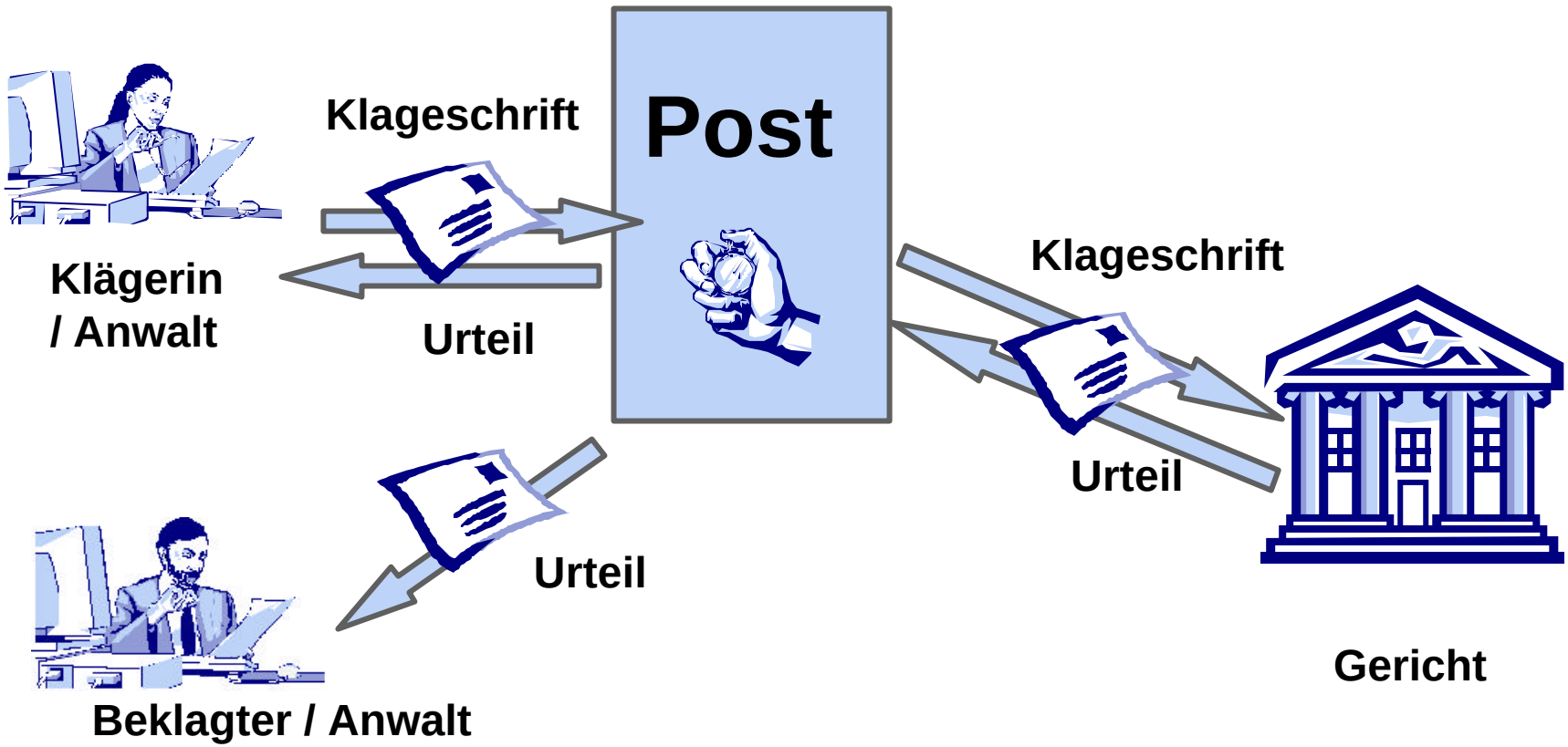
# Anforderungen an den rechtsverbindlichen Austausch von strukturierten Dokumenten

## „Sicher ist nicht genug!“

# Problemstellung anhand eines Beispiels

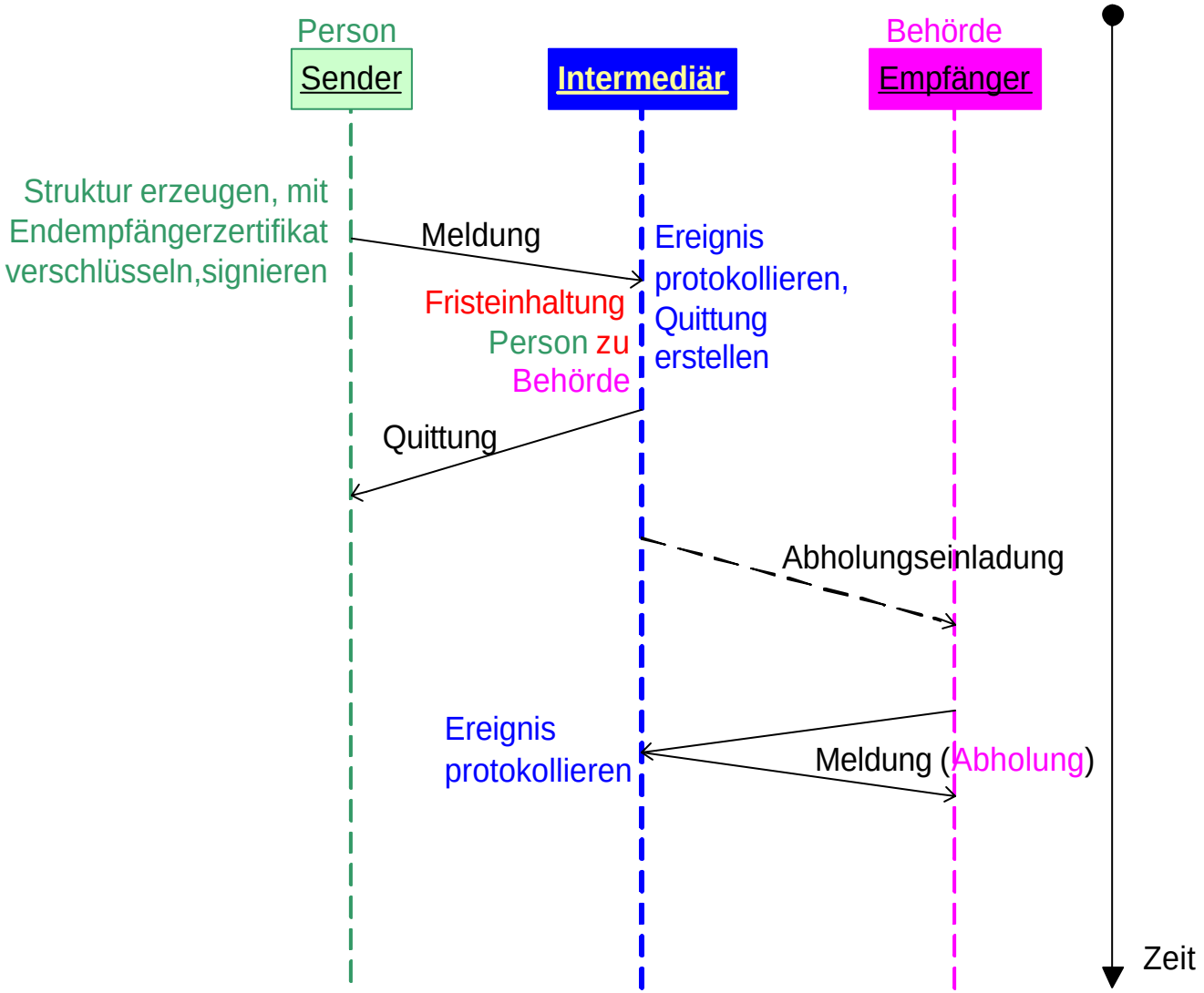


Einreichung einer Klageschrift bei Gericht
Zustellung eines Urteils durch das Gericht



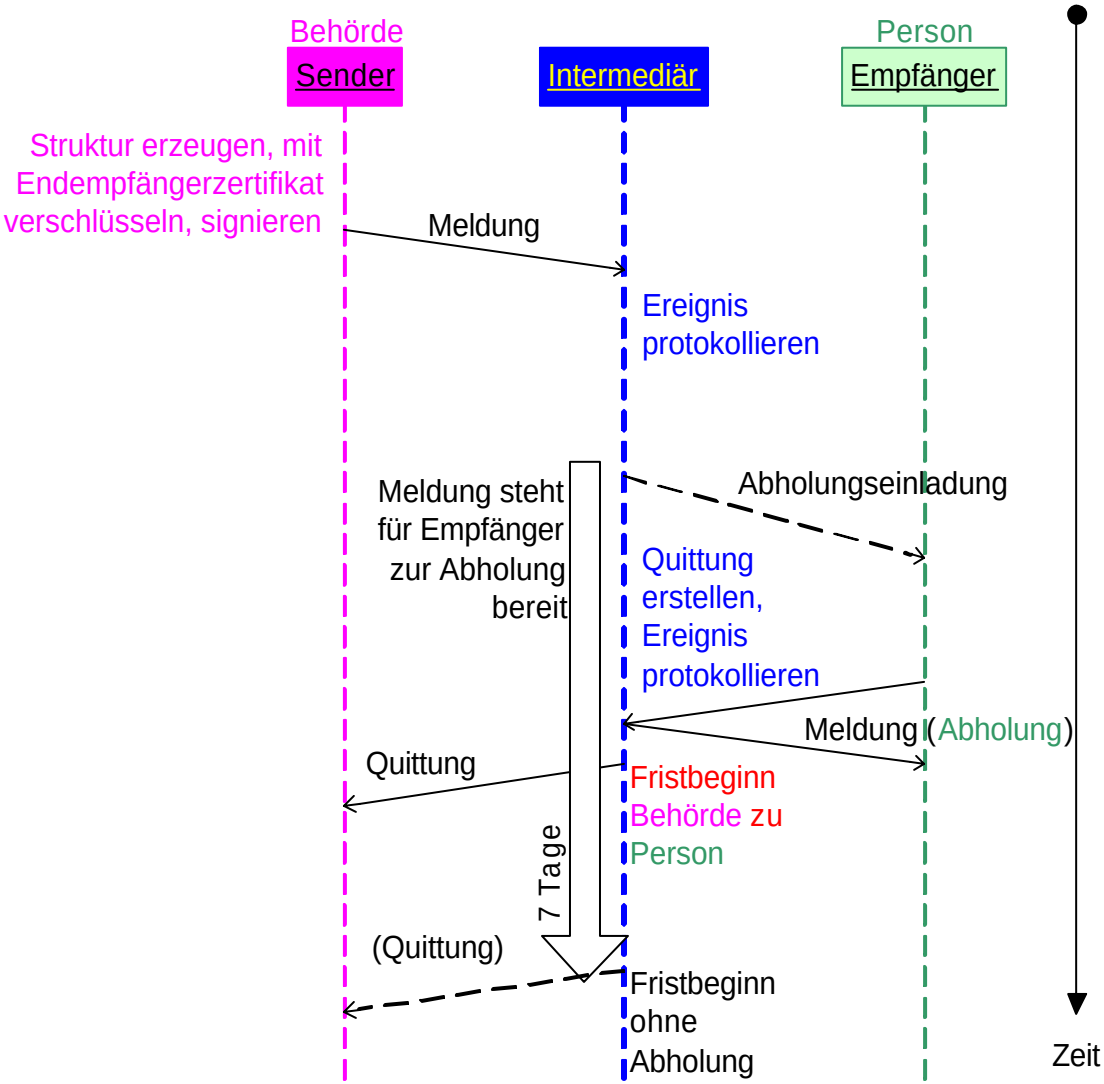
# Der eingeschriebene Brief von einer Person zur Behörde

## nforderungen



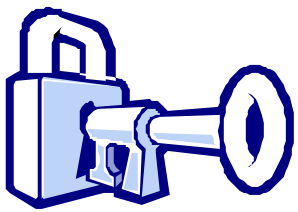
# Der eingeschriebene Brief von einer Behörde zu einer Person

nforderungen



# Die vier klassischen Elemente sicherer Kommunikation





**Nichtabstreitbarkeit**

Der Absender kann nachträglich nicht bestreiten, die Nachricht gesendet zu haben

**Authentizität**

Bei den Teilnehmern handelt es sich um die Personen / Organe, für die sie sich ausgeben

**Integrität**

Die Nachricht erreicht den Empfänger unverändert

**Vertraulichkeit**

Nur der Empfänger ist in der Lage, die Nachricht zu lesen

# Weitere Elemente

**Protokollierung**
(Nachvollziehbarkeit der Übermittlung)

**Absendezeitpunkt**

Es wird protokolliert, wann eine Nachricht abgesendet bzw. dem Transportmedium übergeben wurde

**Zustellungszeitpunkt**

Es wird protokolliert, wann eine Nachricht abgeholt bzw. zugänglich gemacht wurde

**Anforderungen an die Struktur von Meldungen**

**Integrierbarkeit**

Integration in die Arbeitsabläufe und die Systemumgebung der Anwender

**Automatisierbare Verarbeitung**

Automatisierbare Verarbeitung der Meldung und ihres Inhalts

Kapitel

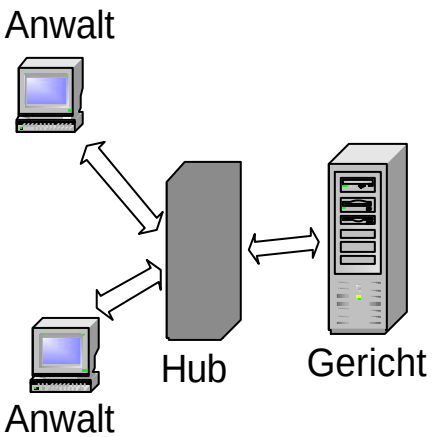
3

# Lösungsfindung

**3.1 Architektur**
**3.2 Beurteilung der klassischen Transport-Technologien**
**3.3 Analyse von Standardisierungs-Initiativen**
**3.4 Eigenentwicklung**
**3.5 OSCI 1.2**

**„Warum nicht einfach E-Mail?“**

**„Welche Technologien und Architekturen kommen für den Austausch strukturierter Dokumente im Justizbereich überhaupt in Frage?“**




- Ein unabhängiger Dritter muss den Sendezeitpunkt einer Meldung sicher protokollieren (Fristeinhaltung)
- Ein unabhängiger Dritter muss den Abholungszeitpunkt einer Meldung sicher protokollieren (Fristbeginn)
- Ein unabhängiger Dritter muss die Zustellungszeitpunkte dem Sender und Empfänger mit signierter Quittung bestätigen können
- Signaturprüfung und eventuell andere zusätzliche Services sollten zentral angeboten werden können

**Folglich ist eine Hub-Architektur (Intermediär) notwendig**

**Vorteile:**

- Große Verbreitung von Mail-Clients
- Infrastruktur bereits vorhanden
- Kostengünstiger Betrieb
- Einbettung von Zertifikaten möglich

**Nachteile:**

- Wenig strukturiert
- Keine verbindliche Zustellung
- Transaktionszeitpunkte nicht transparent
- Keine brauchbare Protokollierung

**Fazit:**

Ohne signierte Quittierung der Transportzeitpunkte für die rechtsverbindliche Kommunikation ungeeignet

# Web-Formularapplikation

**Vorteile:**

- Server- und Client-Authentifizierung möglich
- Strukturierung möglich
- Protokollierung möglich
- Installation beim Client entfällt (Web-Browser)

**Nachteile:**

- Clientseitige Signatur und Verschlüsselung der Daten nicht möglich
- Die Möglichkeiten von Browserformularen sind beschränkt

**Fazit:**

Ohne clientseitige Signatur und Verschlüsselung für die rechtsverbindliche Kommunikation ungeeignet

**Vorteile:**

- Übertragungsformat stark strukturiert
- Verschlüsselte Übertragung möglich
- Ausgereifte Protokollmechanismen vorhanden

**Nachteile:**

- Zugeschnitten auf Bedürfnisse von Handel, Banken, … Weniger geeignet für Mix strukturiert/unstrukturiert
- Aufwändiger Konverter erforderlich
- Hoher Aufwand bei Änderungen am Datenformat
- I.d.R. keine digitale Signatur vorgesehen

**Fazit:**

Für branchenübergreifende Kommunikation sowie B2C- und rechtsverbindliche G2C-Kommunikation eher ungeeignet

# Fazit

- Die klassischen Technologien erfüllen die Anforderungen an den rechtsverbindlichen Austausch von Dokumenten nur teilweise.

# .3 Analyse von Initiativen mit govlink-ähnlichem Anforderungsprofil

## tandardisierungs-Initiativen

Standardisierungsgremien

- W3C; BizTalk-Framework; ebXML

E-Government-Initiativen

- Grossbritannien; Deutschland; …

Initiativen der schweizerischen Post

- Tumbleweed; Mosaic

Initiativen im Rechtsumfeld

- Lexml; LegalXML

# Fazit

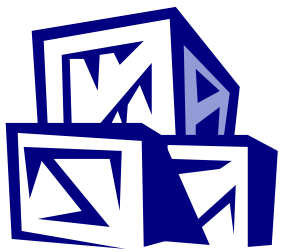
- Standardisierungs-Initiativen erfüllen die Anforderungen an den rechtsverbindlichen Austausch von struturierten Dokumenten nur teilweise.

- Insbesondere fehlen Funktionen / Konzepte für die Protokollierung von Zustellungen durch einen vertrauenswürdigen Dritten (virtuelle Poststelle, Intermediär).

# .4 Eigener Transport-Standard (GovLink-Standard)



- Spezifikation eines eigenen Transport-Standards
  - Intermediär-/Hub-Architektur
  - Teilnehmerverwaltung (Closed User Group)
  - Protokollierung von Zustellungen (Quittungen)
  - Signature
  - Encryption



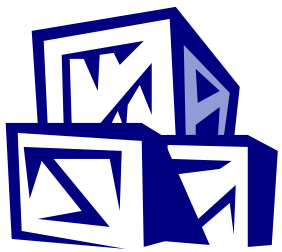
- „Proof Of Concept“ bestehend aus :
  Java APIs zum Transportstandard; Intermediär; Anwaltsclient

# OSCI-Standard V1.2 (Herbst 02)

- Veröffentlichung des deutschen OSCI-Standards V1.2
- Vergleich zwischen OSCI V1.2 und GovLink-Standard
- GovLink-Standard wird vorerst eingefroren

  Gründe zugunsten von OSCI:

  – Inhaltliche Äquivalenz
  – Grössere Chance einer europäischen Verbreitung
  – Ökonomische Überlegungen bezüglich der Pflege



Kapitel

4

# OSCI (Online Services Computer Interface)

## 4.1 Einführung OSCI
## 4.2 Eigenschaften von OSCI

**„Der europäische Standard, der die GovLink Anforderungen weitgehend abdeckt“**

# Entstehung von OSCI

## Bund Online 2005:

- Ziel der E-Government-Strategie der deutschen Bundesverwaltung:
  400 Dienstleistungen/Verfahren des Bundes online

## Städtewettbewerb Media@Komm:

- Wettbewerb im Rahmen von Bund Online 2005
  Sieger: OSCI-Standard der Stadt Bremen

## Zuständigkeit für Pflege und Weiterentwicklung:

- OSCI-Leitstelle Bremen

# Empfehlungen für OSCI Standard

**Europäische Kommission:**

- Würdigung von OSCI als vorbildliche e-Government-Initiative

**(Deutsches) Bundesamt für Sicherheit in der Informationstechnik:**

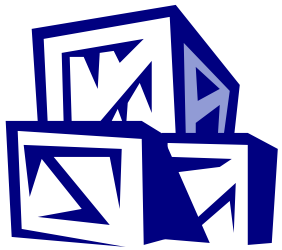
- Bescheinigung der Tauglichkeit des Standards für e-Government

**(Deutsches) Bundesministerium des Innern:**

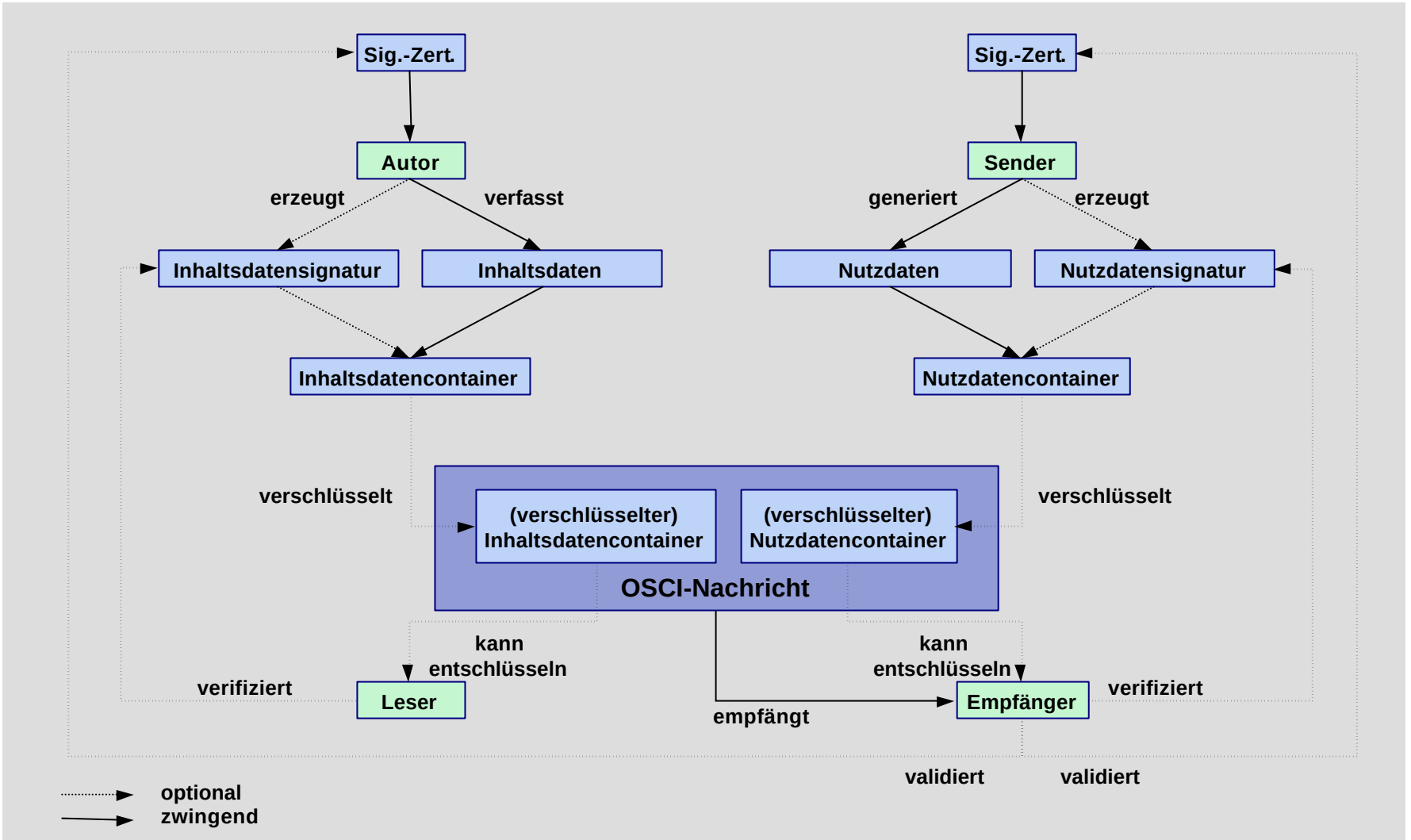
- OSCI als verbindlicher Standard für e-Government-Transaktionen

# Bestandteile von OSCI

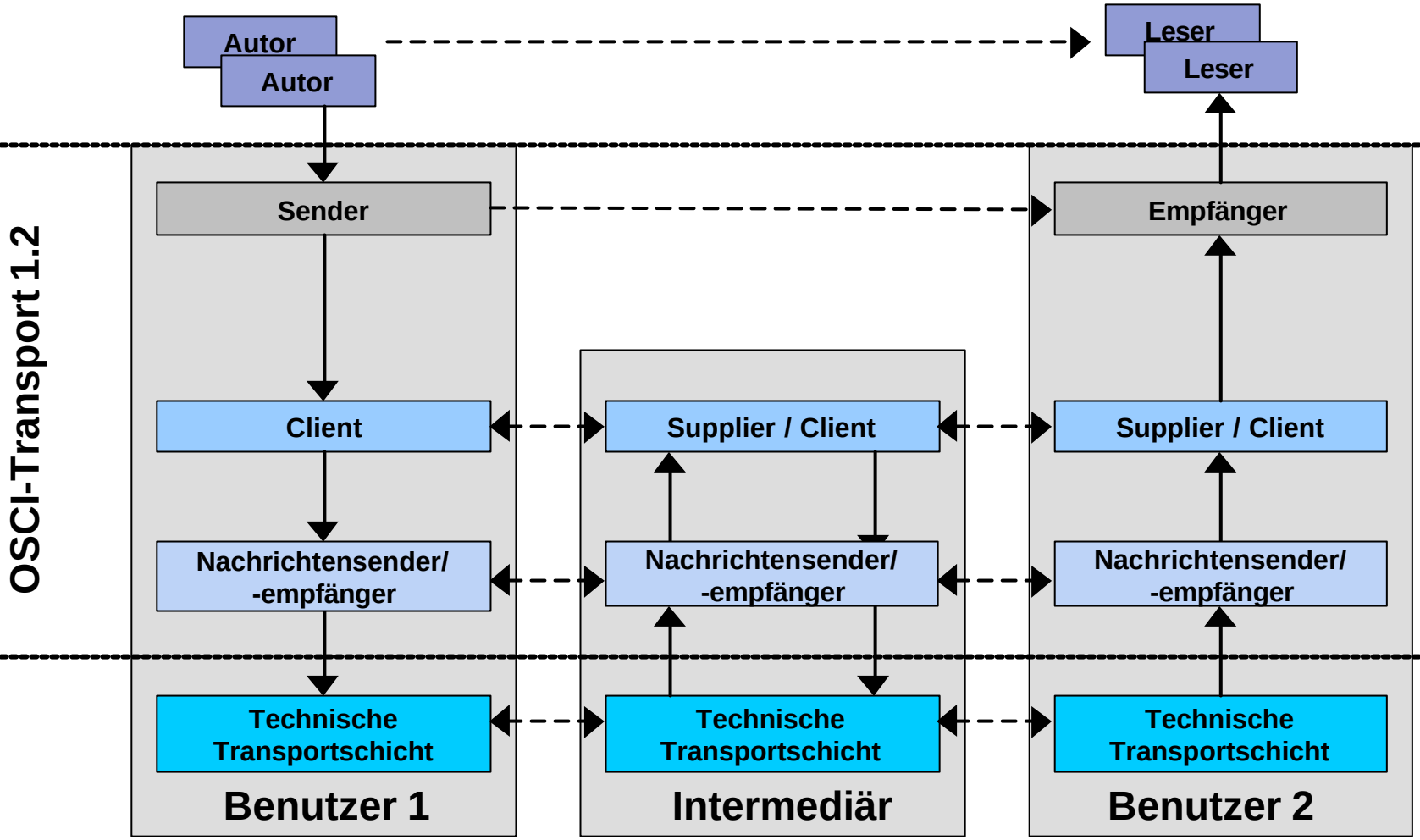
- Beschreibung des Nachrichtenaustauschs
  - Rollenmodell
  - Schichtenmodell
  - Authentifizierung der Kommunikationspartner
  - Intermediär
  - Kommunikationsszenarien
- Sicherheitskonzept
  - Digitale Signatur
  - Verschlüsselung
- Reaktionsvorschriften und Rückmeldungen
- Protokollierung / Quittungen
- Nachrichtenaufbau



# OSCI-Rollenmodell

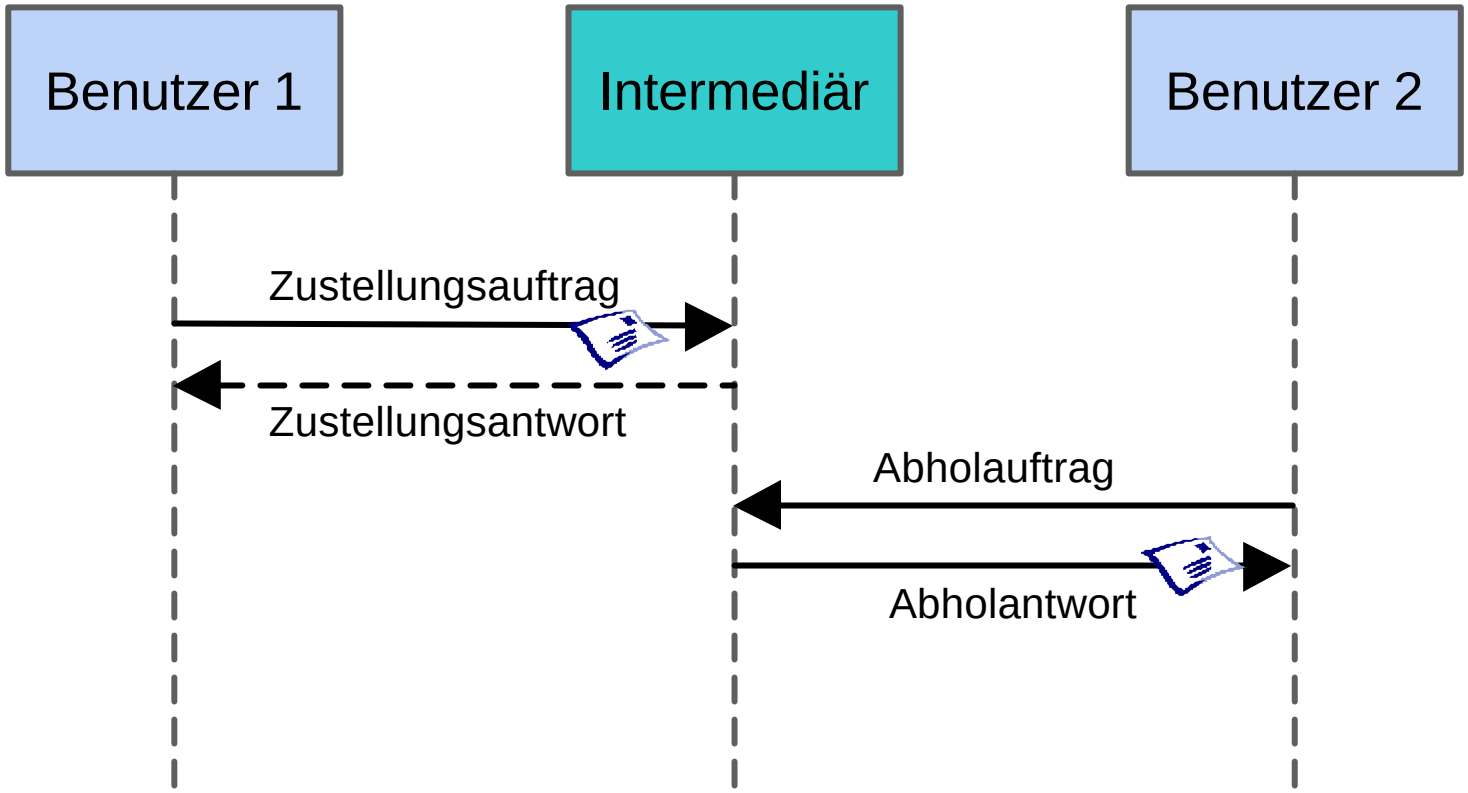


# OSCI-Schichtenmodell

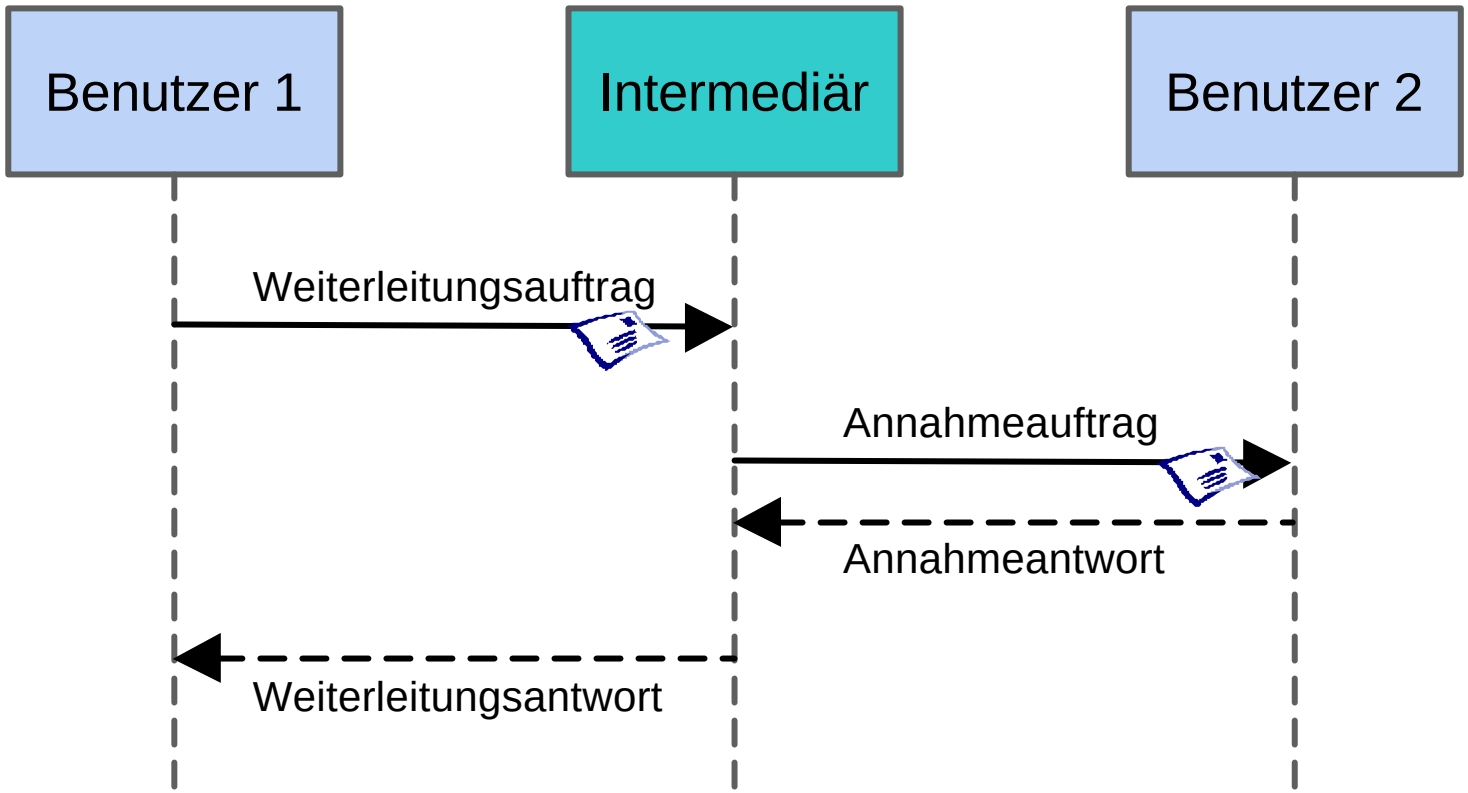


# OSCI-Intermediär - Aufgaben

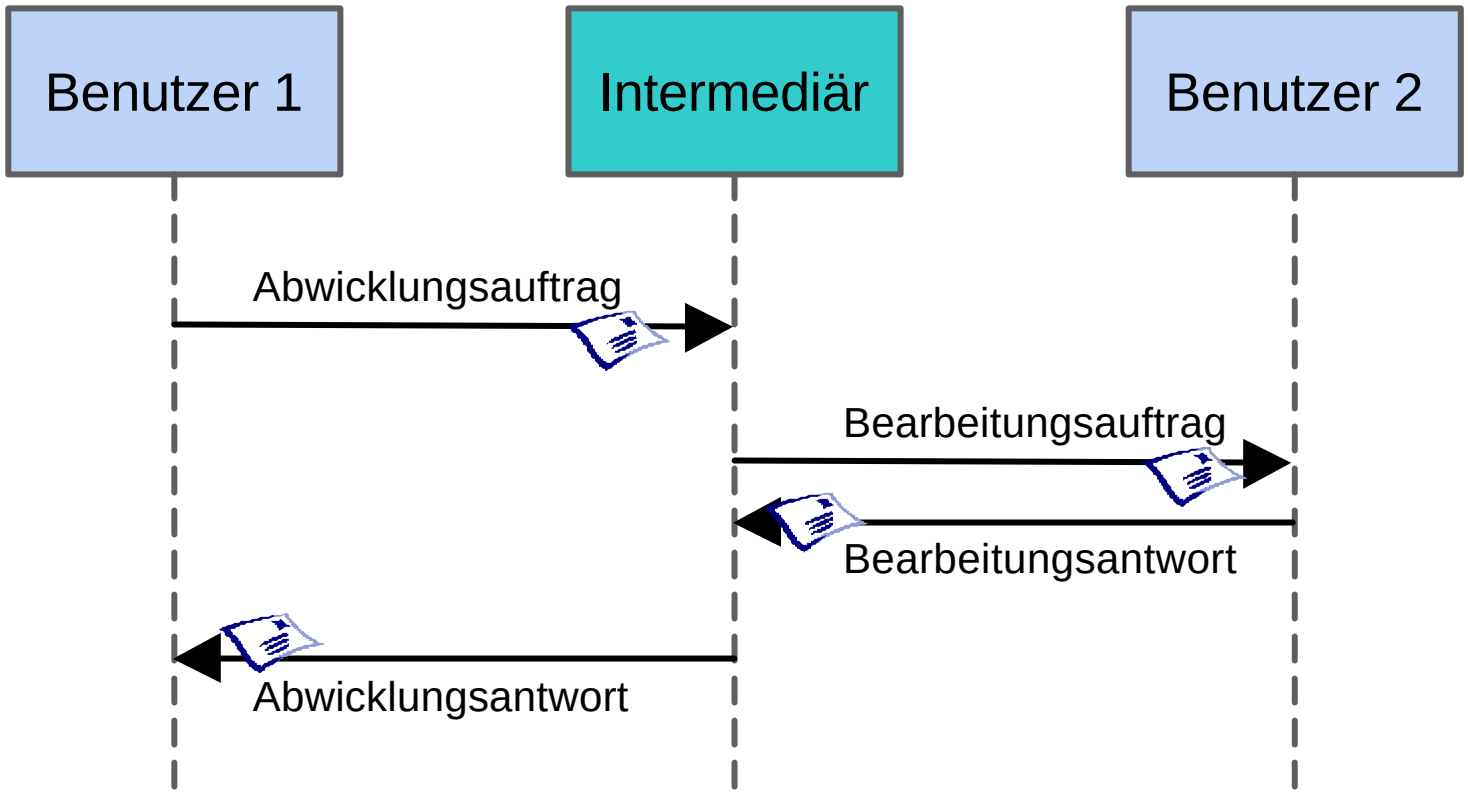
- Protokollierung des Meldungsverkehrs
- Auslieferung von Quittungen (Laufzettel) zum Meldungsverkehr
- Zertifikatsprüfung
- Verwaltung der „Postfächer“

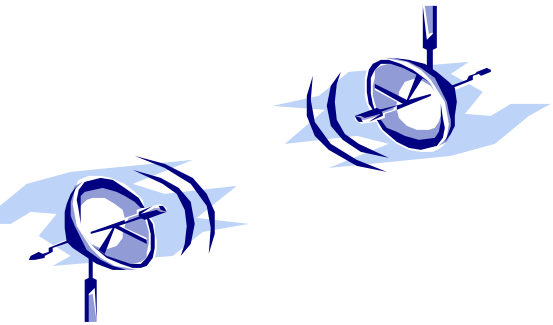



Zustellung der Meldung durch den Sender an den Intermediär.
Empfänger holt Meldung beim Intermediär ab.




Zustellung der Meldung durch den Sender an den Intermediär.
Intermediär leitet Meldung sofort an den Empfänger weiter.

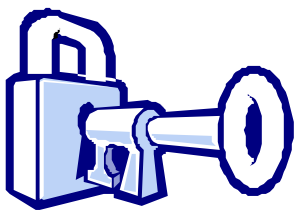

Benutzer 1
Intermediär
Benutzer 2
Abwicklungsauftrag
Bearbeitungsauftrag
Bearbeitungsantwort
Abwicklungsantwort



- Authentifizierung durch Zertifikat
- Bei jedem Schritt in einer OSCI-Session wird die Benutzerauthentizität und Meldungsreihenfolge sichergestellt
- OSCI benötigt keinen verschlüsselten Transportkanal (SSLT), weil die ganze Meldung ohnehin verschlüsselt wird (sog. doppelter Umschlag)

# Sicherheitskonzept (Zertifikatsniveau)

- Fortgeschrittene Signatur
  - Das Zertifikat ist auf einer Diskette oder dem PC gespeichert (Soft-Zertifikat)
- Qualifizierte Signatur (GovLink)
  - Das Zertifikat befindet sich auf einer Smartcard



- Akkreditierte Signatur
  - Qualifizierte Signatur mit Zertifikat eines akkreditierten Zertifikatsanbieters

- Fehlermeldungen auf Nachrichtenebene
- Rückmeldungen auf Auftragsebene

# Protokollierung / Quittungen

- **Der Intermediär führt zu jeder Zustellung einen Laufzettel.**

**Protokollierung:**

- Zeitpunkt der Einreichung beim Intermediär
- Zeitpunkt der Weiterleitung an den Empfänger beziehungsweise die Abholung durch den Empfänger
- Gültigkeit der verwendeten Zertifikate

- **Der (signierte) Laufzettel kann jederzeit vom Sender oder Empfänger beim Intermediär angefordert werden**

# In OSCI verwendete Standards

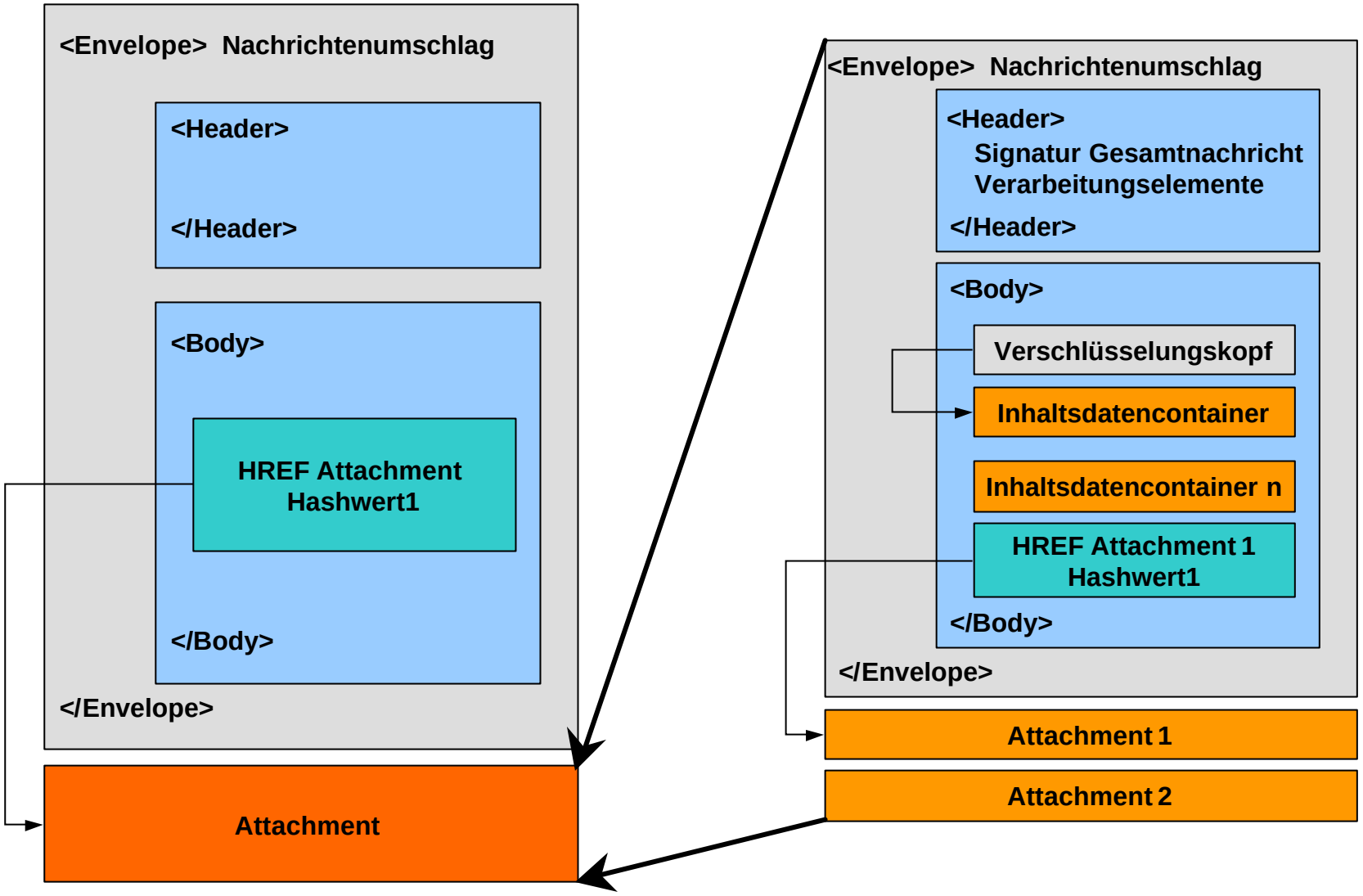
**W3C-Standards:**

- SOAP im Document-Style mit Attachments
- XML-Encryption zur Verschlüsselung von XML-Dokumenten
- XML-Signature zur Signatur von XML-Dokumenten

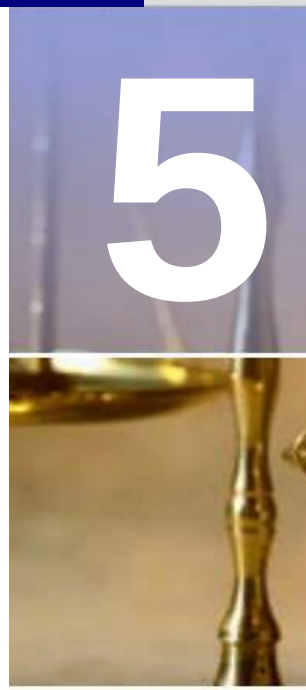
**Security:**

- RSA
- SHA-1
- Two-Key-Triple-DES / Aes-128 /192 /256
- X509v3 Zertifikate

# Nachrichtenaufbau (doppelter Umschlag)



Kapitel




# OSCI-Implementierung

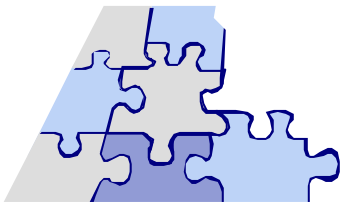
## 5.1 OSCI Produkte
## 5.2 OSCI im praktischen Einsatz

**„Ohne Implementierung läuft gar nichts!“**

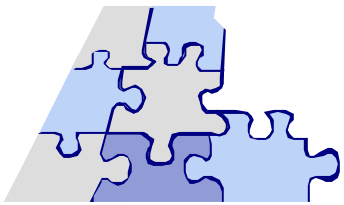
# Governikus von bremen-online-services

Bausteinlösung für kommunale Anwendungen

- Sehr enge Zusammenarbeit zwischen der OSCI-Leitstelle und bremen-online-services
- Der aktuelle Governikus Release 1.1 implementiert die inoffizielle OSCI-Version 1.1
- Ende 2003 wird Governikus 2.0 mit der Implementierung von OSCI 1.2 auf dem Markt erscheinen



Basismodule für die Abwicklung einer rechtsverbindlichen elektronischen Kommunikation mit OSCI 1.2 sind von der OSCI Leitstelle bei bremen-online-services in Auftrag gegeben worden
(Verfügbarkeit Ende 2003).



- Finanzämter
- Gerichte
- Hochschulen (Bremen; Bremerhaven)
- Deutsche Post AG
- Deutsche Telekom AG
- UNICEF
- Sparkasse Bremen
- Diverse Amtsstellen (Stadtplanung und Bauamt; Kfz-Zulassungsstelle; Standesamt; Stadtamt)
- Diverse Private (Zeitungsverlage; Fussballvereine)

## Meldewesen (Einwohnerkontrolle): OSCI-XMeld

- Elektronische Abwicklung von An- und Abmeldungen bei Gemeinden über das Internet:
  - Einfache Melderegister-Auskunft
  - Rückmeldung
  - Melderegister-Nachführung

- Standardisierung von Inhaltsdaten

Im Auftrag der deutschen Bundesregierung wird OSCI-XMeld, ein standardisierter Datenaustausch im Meldewesen, entwickelt (OSCI-Transport für die Übermittlung / OSCI-XMeld für strukturierte Inhaltsdaten).

- **Justizbereich: OSCI-XJustiz**
  Die deutsche Justizministerkonferenz plant eine Standardisierung der Inhaltsdaten im juristischen Bereich, als Voraussetzung eines bundesweit einheitlichen elektronischen Rechtsverkehrs.

- Analoges Projekt zu JusLink in der Schweiz

Kapitel

6

# Zusammenfassung / Ausblick

## 6.1 Zusammenfassung
## 6.2 Ausblick

**„Was nun?“**

- **Ausgangssituation im Projekt GovLink**
  - Mehrere Anwendungen benötigen rechtsverbindlichen Transport von Dokumenten
- **Anforderungen an den rechtsverbindlichen Dokumenten-Austausch**
  - „Eingeschriebener Brief“
  - Nichtabstreitbarkeit; Authentizität; Integrität; Vertraulichkeit
  - Protokollierung und Quittierung der Übermittlungszeitpunkte
- **Lösungssuche**
  - Klassische Technologien; Initiativen mit ähnlichem Anforderungsprofil; Eigenentwicklung; ökonomische Überlegungen führen zu OSCI
- **OSCI**
  - Der deutsche (europäische) Standard, der die GovLink Anforderungen weitgehend abdeckt
- **OSCI-Implementierung**
  - Implementierung des OSCI 1.2 Standards durch bremen-online-services bis Ende 2003

# Ausblick GovLink (OSCI)

- Präsentation und Vorstellung von OSCI bei ISB, Guichet virtuel, den Kantonen und interessierten Organisationen
- In welchen Bereichen soll OSCI zum verbindlichen Standard werden?
- Zusammenarbeit der Schweiz mit OSCI-Leitstelle etablieren (Vertretung der CH-Interessen bei der Weiterentwicklung)
- Technische Zusammenarbeit mit bremen-online-services (Einflussnahme auf Weiterentwicklung Governikus)
  - Spezifikation des Deltas von GovLink/JusLink Anforderungen (Gültigkeitsdauer der Meldungen; Teilnehmerverwaltung)
  - Realisierung PKI-Anbindung (PKI des BIT)

**Wir danken für Ihre Aufmerksamkeit.**