Koordinierungsstelle
für IT-Standards

Freie
Hansestadt
Bremen

XTA Serviceprofile

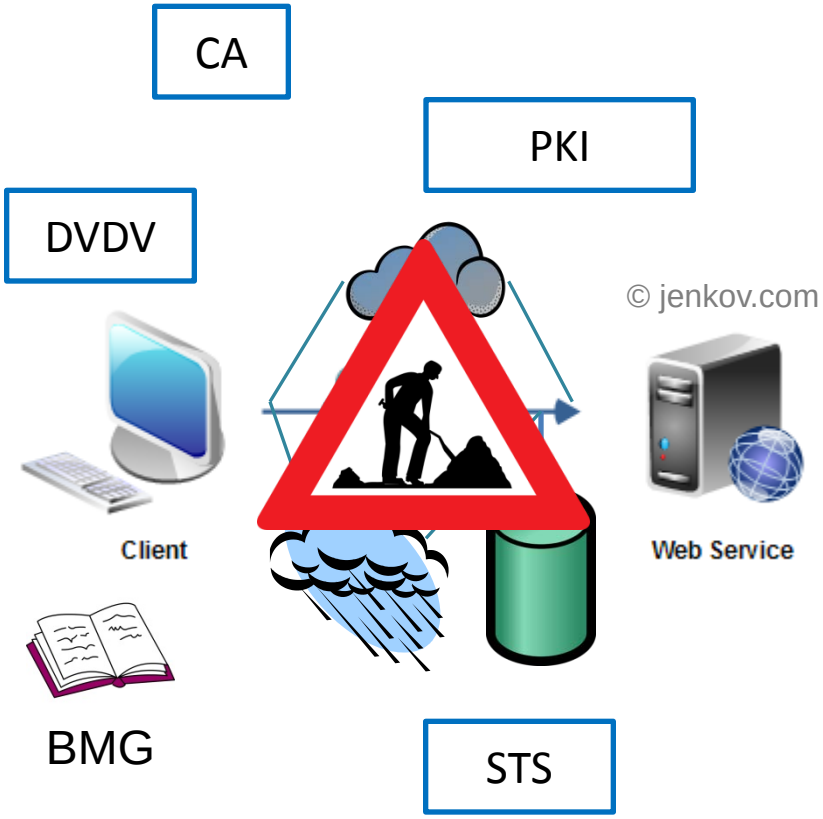
- Was ist das?
- Warum braucht man das?
- Wieso sind die so kompliziert ?

Frank Steimke| Koordinierungsstelle für IT-Standards (KoSIT)
13. 11. 2015| 8. XÖV Konferenz| Bremen

Sichere Webservices im E-Government

Koordinierungsstelle für IT-Standards

- Zertifikate
- Kryptografie
- Signaturen
- Verzeichnis-dienst
- Authentisierung
- Postfächer
- Landesnetz
- Verbindungs-netz
- Fristen
- Quittungen
- Fehler

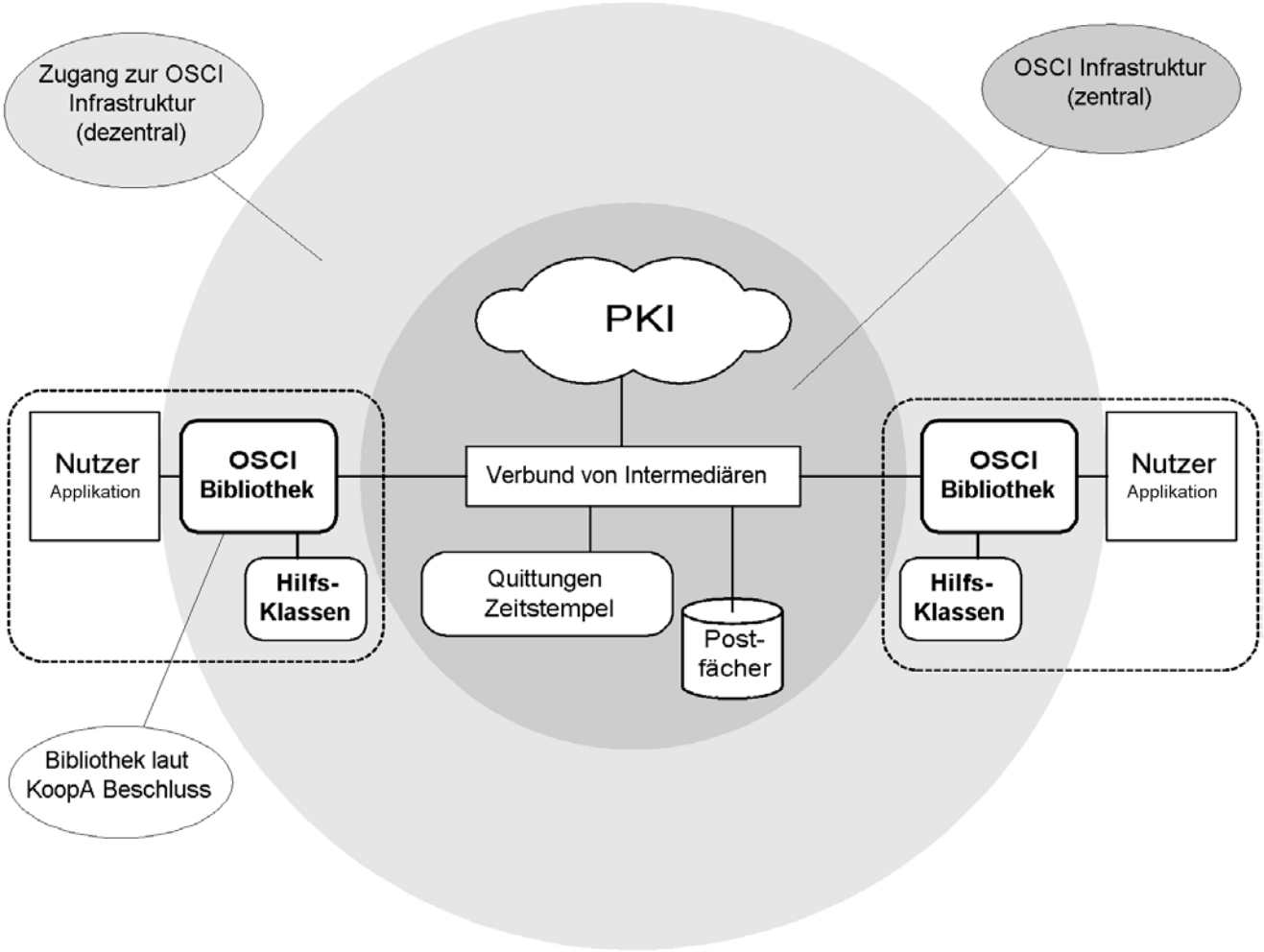


- Rechtliche Vorgabe (Land)
- Rechtliche Vorgabe (Bund)
- Fachstandard
- Transportprofil
- IT-NetzG
- BSI Grundschutz
- Sicherheits-leitlinie (IT-PLR)

- Dienststelle / Behörde
- Aufsichts-behörde
- Dienstleister (RZ)
- Kontrollbehörde (LfDI)

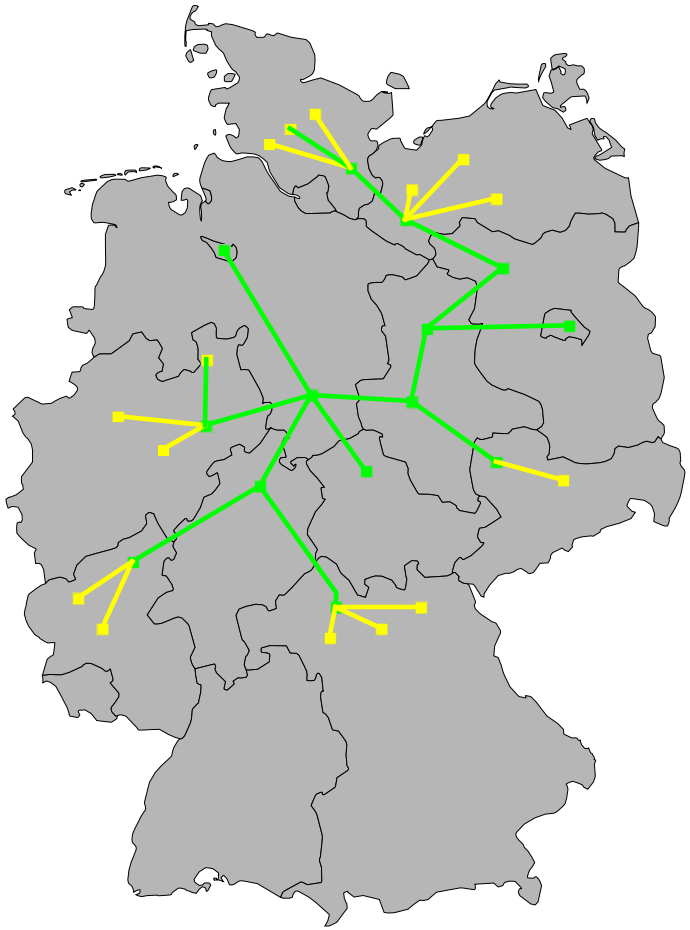
Diensteprovider	DVDV Koordination	Pflegende Stelle (Bund / Land)

Erster Lösungsversuch (3 / 2006)

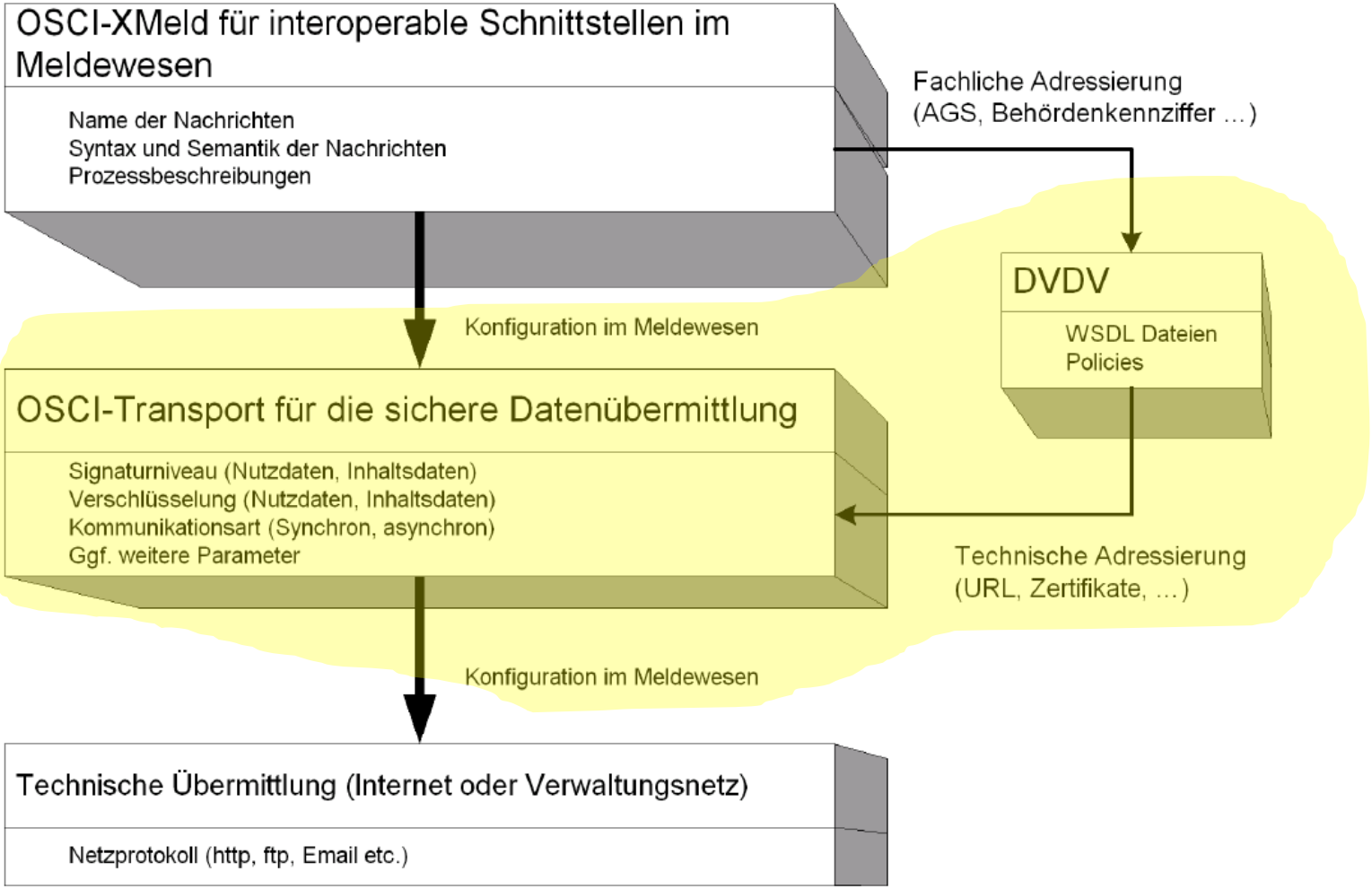


Verbund von Clearingstellen (Vision 3 / 2006)

Koordinierungsstelle für IT-Standards



OSCI Transport Profil (1)



OSCI Transport Profil (2)

Koordinierungsstelle für IT-Standards

Mit Hilfe der WSDL we präzise spezifiziert. Für deren Belangen des Pr tragen. Sämtliche in die sind in der WSDL-Besch

1. URL (Protokoll, IP-A
2. ggf. URL des Empfä
3. Verschlüsselungs- u
4. Erfordernis und Nive
5. Erfordernis der Vers
6. Angabe der OSCI-Tr
7. Schemata der Inhalt
8. Struktur der Inhaltsd
9. Erfordernis und Nive
10. Erfordernis von Vers
11. zur Verschlüsselung
12. zur Prüfung von Sigr

Tabelle V.C.2. Festlegungen für Datenübermittlungen gemäß § 33 BMG

Nr.	Mechanismus	Regelung
1	Signatur der Inhaltsdaten	Die Inhaltsdaten **müssen** signiert werden. Als Hash-Algorithmus ist ausschließlich **SHA-256** zu verwenden. Das Signaturzertifikat muss von der TESTA-CA ausgestellt und zum Zeitpunkt der Signaturerstellung gültig sein.
	Erläuterung: Die Signatur der Inhaltsdaten dient der Authentisierung des Autors (nur Meldebehörden bzw. Vermittlungsstellen sind berechtigt, Nachrichten gemäß § 33 BMG zu versenden). Gleichzeitig wird die Integrität der Nachrichten (Schutz vor unberechtigter Manipulation) sichergestellt. Es ist die Signatur der Organisationseinheit zu nutzen, welche die Inhaltsdaten erstellt (keine Signatur einer Person). Die ausschließliche Verwendung von SHA-256 als Hashalgorithmus dient einer einheitlichen Regelung aller auf OSCI–Transport basierenden Kommunikation.	
2	Verschlüsselung der Inhaltsdaten	Die Inhaltsdaten der Nachricht **müssen** verschlüsselt werden. Der hierzu zu verwendende öffentliche Schlüssel des Empfängers ist dem im DVDV hinterlegten Zertifikat der TESTA-CA zu entnehmen. Ist ein solches Zertifikat nicht vorhanden oder nicht gültig, dann darf keine Datenübermittlung stattfinden, da die geforderte Sicherheit der Datenübermittlung nicht gewährleistet werden kann.
	Erläuterung: Die *Vertraulichkeit* der Inhaltsdaten ist durch Ende-zu-Ende Verschlüsselung sicherzustellen. Die *Ende-zu-Ende Verschlüsselung* bezieht sich ggfs. nur auf die OSCI-Transport Verbindung von / zu Vermittlungsstellen. In diesen Fällen sind die geforderten Sicherheitsmechanismen zwischen Vermittlungsstelle und Meldebehörde durch andere Maßnahmen sicherzustellen.	
3	Signatur der Nutzungsdaten	Die Nutzungsdaten **können** signiert werden.
	Hinsichtlich des zu nutzenden Zertifikates und des zu nutzenden Hash-Algorithmus gelten die Regelungen der Nummer 1 entsprechend.	
4	Verschlüsselung der Nutzungsdaten	Die Nutzungsdaten **müssen** verschlüsselt werden.
	Hinsichtlich des zu nutzenden öffentlichen Schlüssels gelten die Regelungen der Nummer 2 entsprechend.	
5	Kommunikationsszenario	Jeder Diensteanbieter im Bereich des § 33 BMG (also jede Meldebehörde bzw. die von ihr beauftrage Vermittlungsstelle) **muss** alle hier relevanten Operationen eines Dienstes *Request-Response (ohne Protokollierung)* im Sinne von [OSCI–Transport 2002] anbieten.

otokollsyntax formal und
. definiert, die den beson-
tencontainern Rechnung
lle V.C.3 auf Seite 1199)
reibungslemente sind:

ediärs

uest/response etc.)

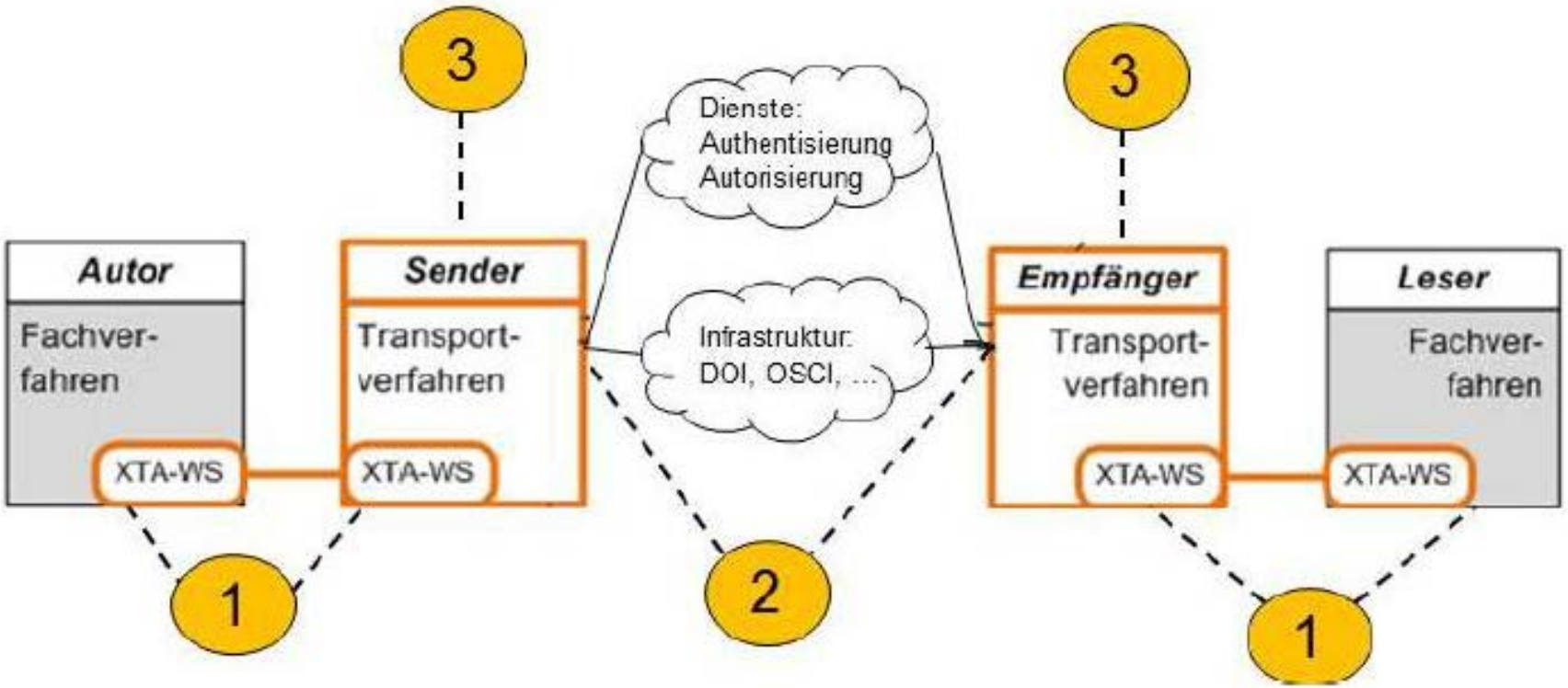
Zertifikate
te Zertifikate

Erkenntnis aus acht Jahren Betrieb

Koordinierungsstelle für IT-Standards

- Nachrichtentransport ist mehr als „Postfach & PKI“
  - Intermediäre sind nett … aber sie allein lösen das Problem nicht
- Konzeptionelle Unterscheidung Fachverfahren / Transport
  - Fachverfahren erteilt einen Transportauftrag
  - Entlastung von Logistik, Überwachung, Nachweispflichten
- **Die Nachrichtenübermittlung ist ein eigener Service**
  - Entsprechend vereinbarter Bedingungen und einschlägiger Vorgaben
- Die Vorgaben für den Transport sind vielfältig
  - Rechtlich, fachlich, technisch
  - Sie sollten präzise, nachvollziehbar und prüfbar beschrieben werden
- Es gibt wenige, immer wiederkehrende Konstellationen

Zweiter Lösungsversuch (2013)



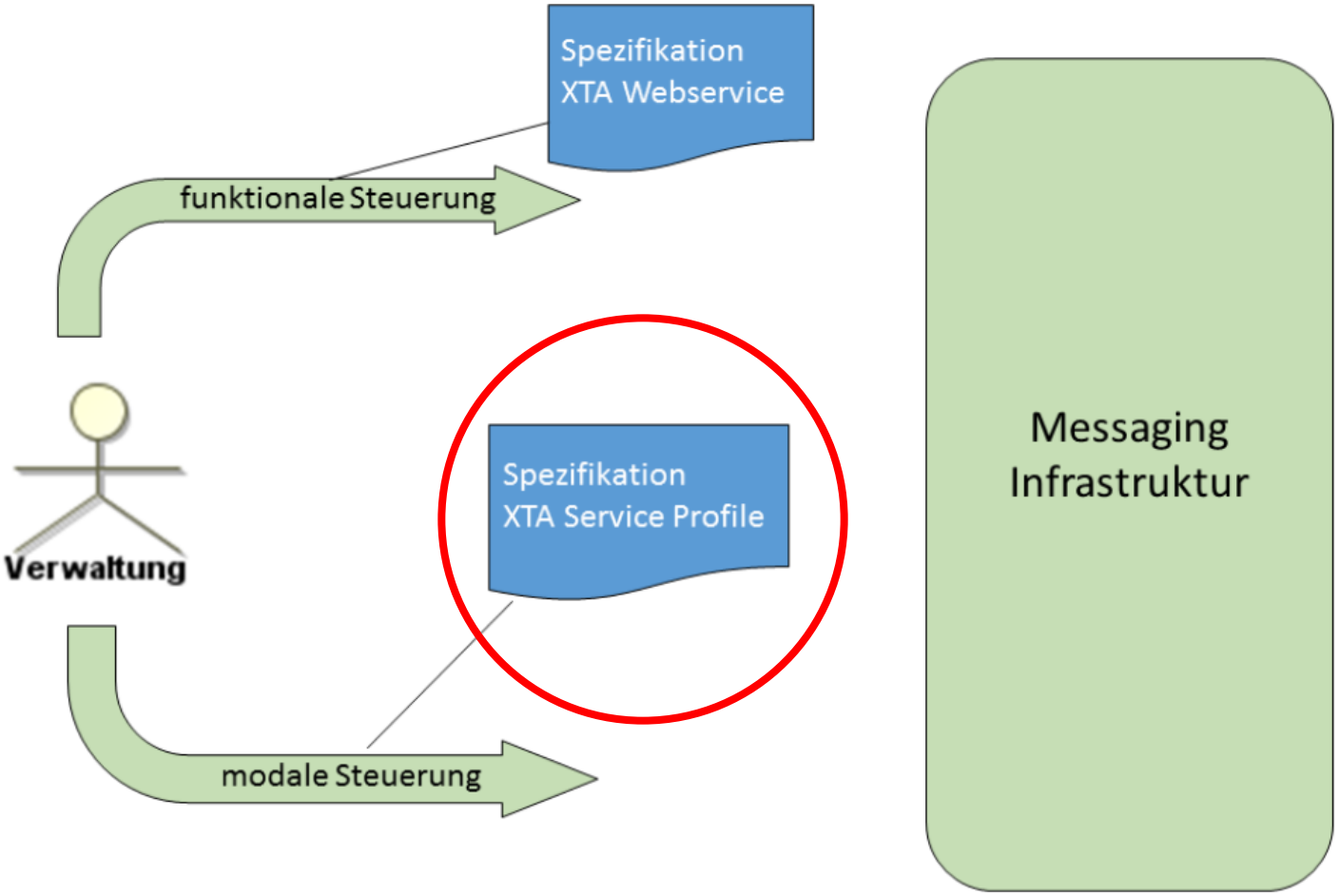
Was regelt ein SLA für den Nachrichtentransport

Koordinierungsstelle für IT-Standards

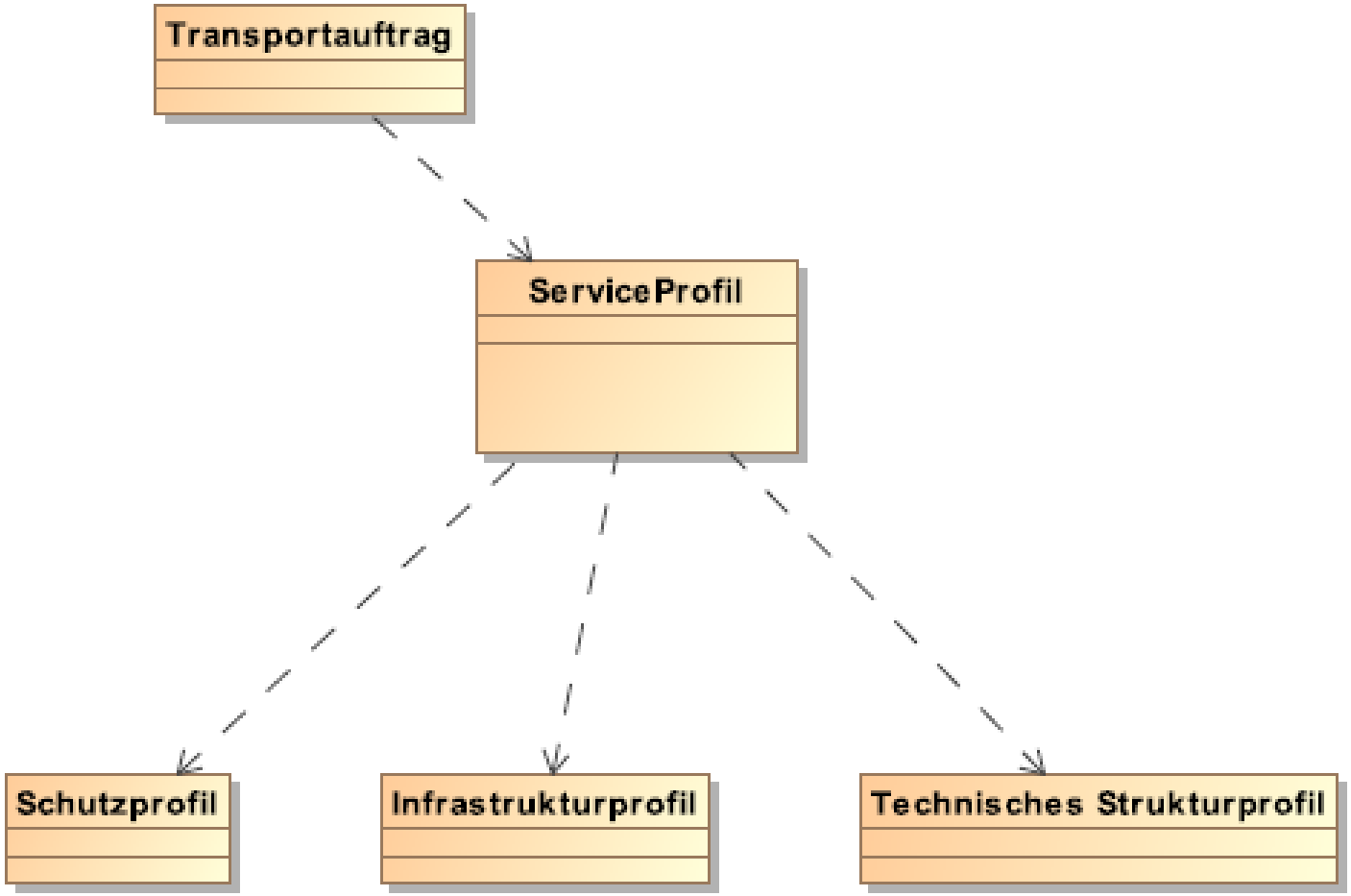
- Leistungsniveau (Verfügbarkeit, Fristen, …)
- Datenschutz und –sicherheit gemäß rechtlicher Vorgaben
- Kryptografische Mechanismen
- Infrastrukturnutzung (Netze, zentrale Komponenten, …)
- Szenario (synchron / asynchron ?)
- Technische Konfiguration (Interoperabilität)
- etc. pp.

Wie beschreibt man den Service „Nachrichtentransport“

Koordinierungsstelle für IT-Standards



Komponenten der qualitativen Beschreibung



Zwischenstand: XTA Service Profile …

Koordinierungsstelle für IT-Standards

- Was ist das?
  - Eine formale Beschreibung der Anforderungen an einen Service
  - Der Service heißt „Transportiere eine Nachricht von A nach B“
- Warum braucht man das?
  - Weil die Vielzahl von Rahmenbedingungen und Rechtsvorschriften und die heterogene IT-Infrastruktur der Verwaltungen zu einer Art *„Logistik – Branche des E-Government“* geführt hat.
- Warum sind die so kompliziert ?
  - Weil es (bei gewachsenen Strukturen) der erste Versuch ist, Rollen und Verantwortlichkeiten der Transporteure formal zu beschreiben.
  - Weil ein gemeinsames Verständnis mühsam hergestellt werden muss.
  - Weil Beschreibungsmittel fehlen (es gibt keine Vorbilder).

Koordinierungsstelle
für IT-Standards

Freie
Hansestadt
Bremen

Vielen Dank für Ihre Aufmerksamkeit!

Frank Steimke | frank.steimke@finanzen.bremen.de | KoSIT

Koordinierungsstelle
für IT-Standards

Freie
Hansestadt
Bremen

XTA Service Profile
→ worin besteht die Lösung?

Yorck Rabenstein,]init[AG
Bremen, 13.11.2015

Worum geht es?

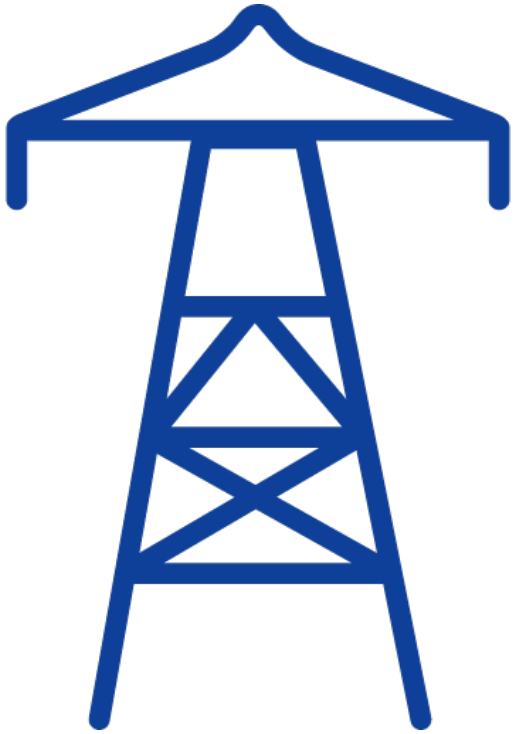
Datenschutz

Logo: http://www.freepik.com,
CC BY 3.0

Worum geht es? (2)

Datensicherheit

Worum geht es? (3)



Infrastruktur

Worum geht es? (4)

Art der Kommunikation

Worum geht es? (5)

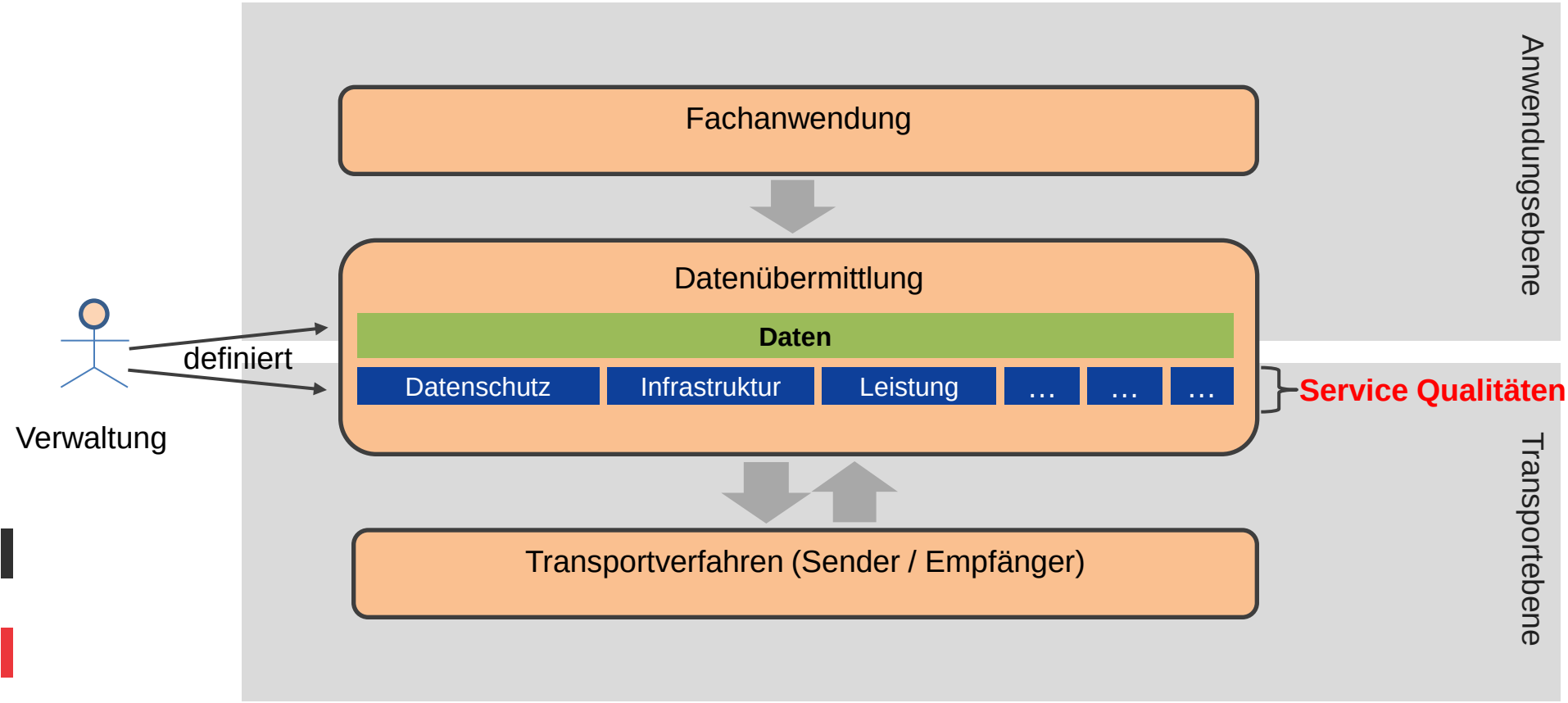
Erforderliches Leistungsniveau

Logo: http://www.simpleicon.com,
CC BY 3.0

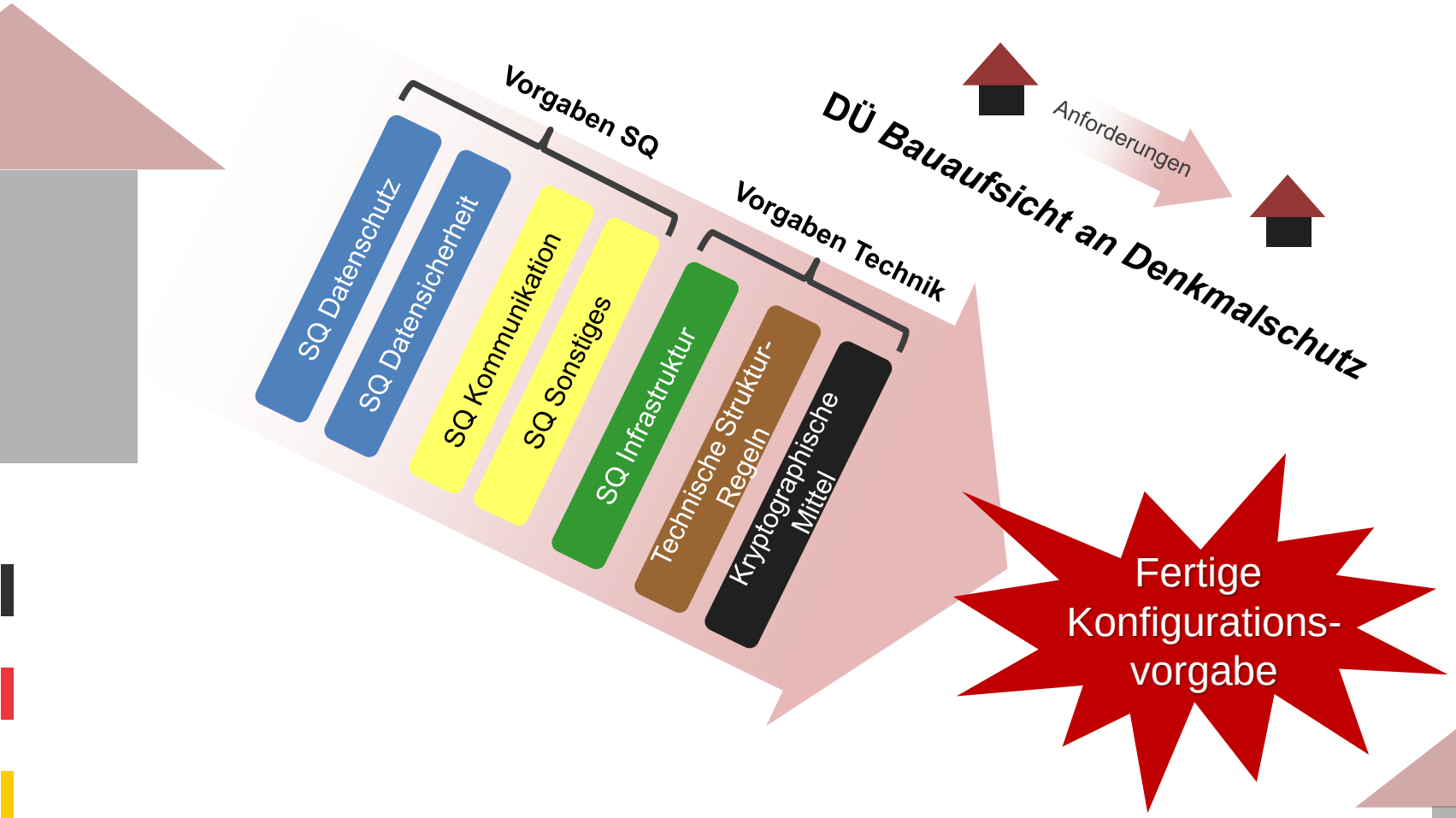
Worum geht es? (6)

Aufbau der Transportnachrichten

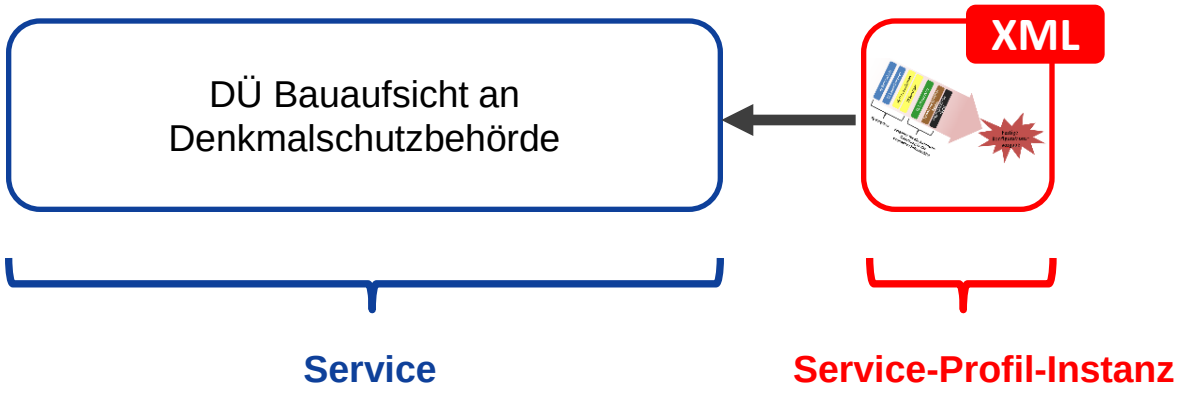
Service Qualitäten



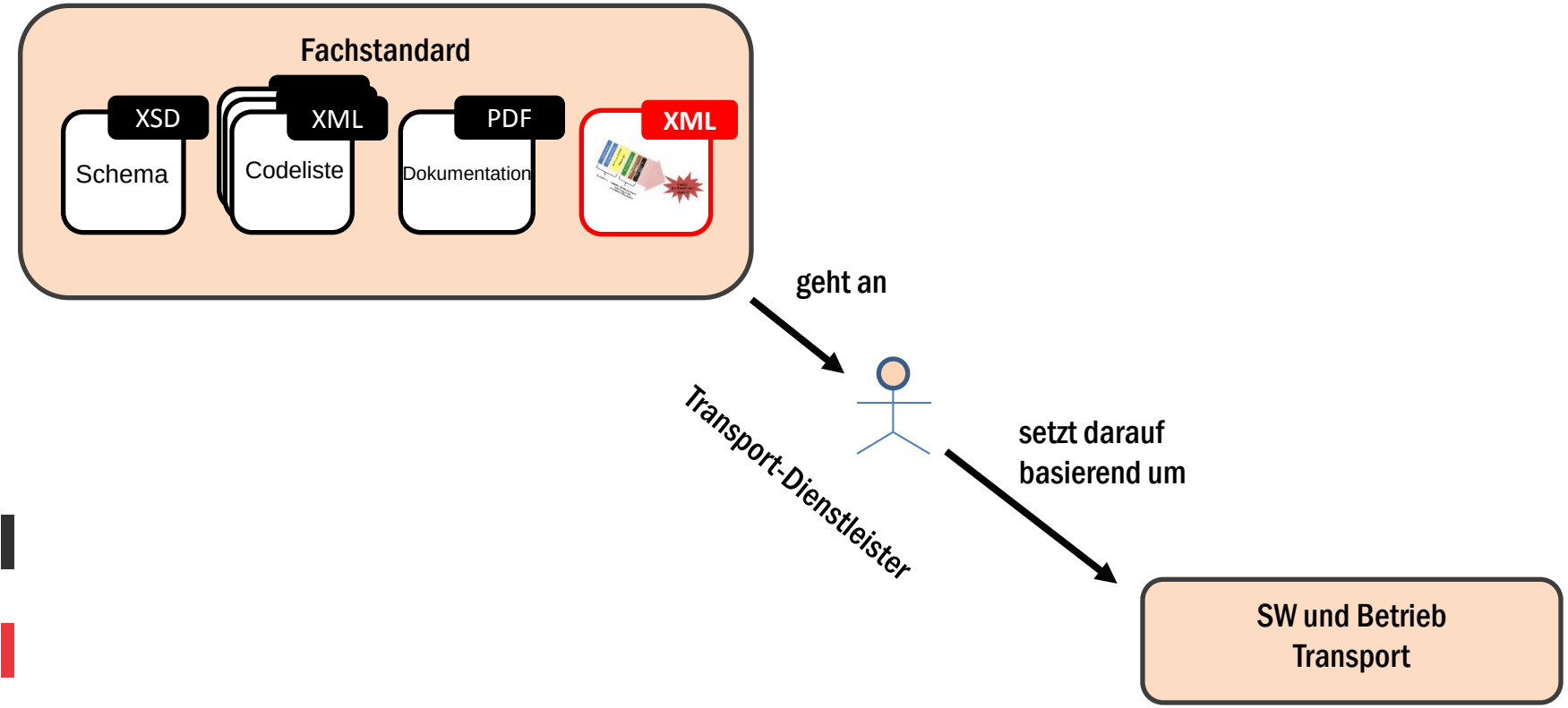
Der Weg zur Konfigurationsvorgabe



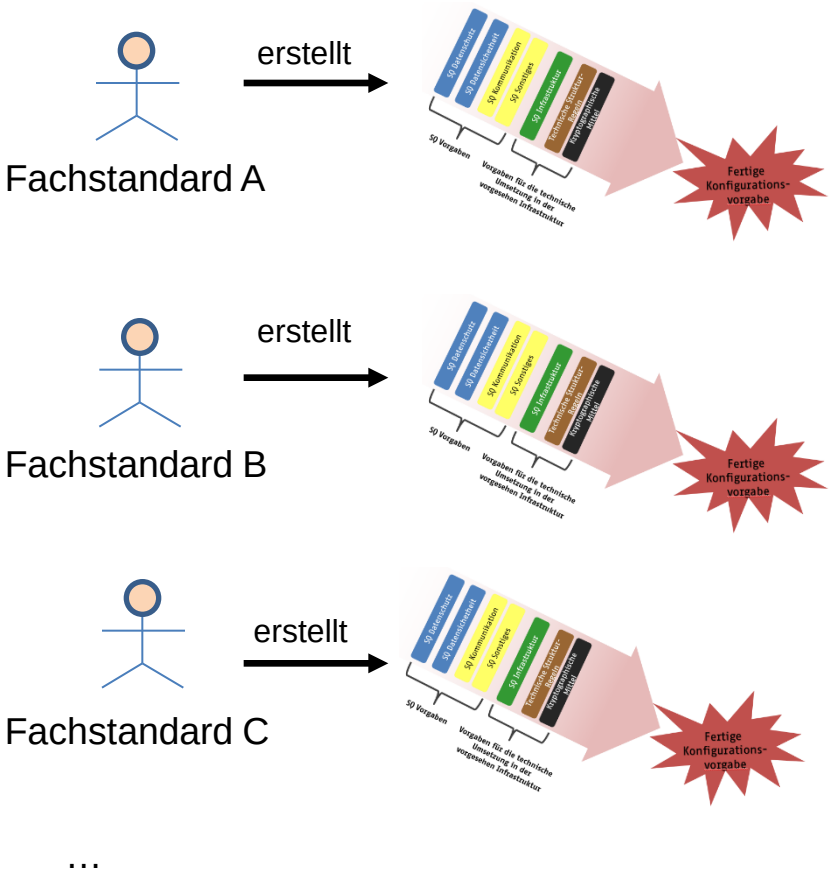
Service-Profil-Instanz



Anwendung der Konfigurationsvorgabe



Profilierung



Vielzahl an Konfigurationen unzweckmäßig!

daher…

Profilierung