der Kommunikationsstandard für digitale Prozessketten

Anwendungsleitfaden
mit Beispielen aus der Praxis

Version 1.0
Ausgabestand 1.0.1

Herausgeber:

AWV – Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V.
Düsseldorfer Str. 40
65760 Eschborn
Vereinsregister 73 VR 5158, Amtsgericht Frankfurt am Main
Telefon: 0 61 96/7 77 26-0
Fax: 0 61 96/7 77 26-51
Mail: info@awv-net.de
Web: www.extra-standard.de, www.awv-net.de.

Der vorliegende Anwendungsleitfaden zum eXTra Kommunikationsstandard wurde von Mitarbeiterinnen und Mitarbeitern des AWV-Arbeitskreises 2.1 „Vereinheitlichung von Datenübermittlungssystemen“ im Fachausschuss 2 „Verwaltungs-vereinfachung und Entbürokratisierung im personalwirtschaftlichen Umfeld“ entwickelt.

Änderungsprotokoll

Version 1.0.1

Autor[en]	Datum	Beschreibung
[gelöscht]	25.05.2018	Neue Bezeichnung als eXTra Kommunikations-standard. Bezugspunkt ist eXTra der Version V1.5, mit dem neuen PlugIn BusinessProcess und der neuen Standardnachricht RepeatResponseRequest, jedoch (noch) ohne Berücksichtigung von DocumentSets

Erstausgabe Version 1.0.0

Autor[en]	Datum	Beschreibung
[gelöscht]	02.02.2016	Erstausgabe Version 1.0.0

Inhaltsverzeichnis

1. Allgemeines

1.1. Notation

Verweise auf Stellen innerhalb dieses Dokumentes referenzieren die Absatznummer und schließen sie in runde Klammern ein (z.B. „(4)“); die Referenz selbst ist als Link ausgestaltet. Verweise auf externe Dokumente haben die Form eines Kurznamens aus Großbuchstaben und stehen in eckigen Klammern, z.B. [XSD]. Wird innerhalb des externen Dokumentes auf ein bestimmtes Kapitel verwiesen, so wird das Kapitel nach dem Trennzeichen # aufgeführt, z.B. [KOMP#5.11] bzw. der Name des Kapitels [DSIG#Transport-Ebene]. Der Kurzname selbst ist wiederum als Textmarke definiert, so dass der Link damit zu den Referenzen im Anhang (4.1) führt.

Ist ein Begriff im Glossar (4.2) erläutert, so wird er bei der ersten Verwendung im Dokument mit einem Link zum Glossar versehen und vorangestellten „ⓘ“ versehen, z.B. „ⓘ PlugIns“.

Hervorhebungen sind *kursiv* gesetzt.

1.2. Zielgruppen

Das vorliegende Dokument richtet sich an Projektleiter, technisch orientierte Gremien und Arbeitsgruppen eines ⓘ Datenübermittlungsverbundes bzw. an Verantwortliche eines ⓘ Fachverfahrens, die einen elektronischen Nachrichtenaustausch für Fachnachrichten definieren wollen.
Besonders hilfreich für das Verständnis dieses Dokumentes ist die Kenntnis des Dokumentes Einführung in den eXTra-Standard [EINF], sowie des Ebenen- und Rollenmodells des eXTra-Standards, wie sie ausführlich im Kompendium [KOMP] dargelegt sind.

1.3. Zielsetzung des Anwendungsleitfadens

Dieses Dokument hat zwei Schwerpunkte, einen theoretischen (2) und einen praktisch-anschaulichen (3). Zum einen will es Hilfestellung geben bei der theoretischen Frage welche Aspekte beim Entwurf und der Gestaltung eines Datenübermittlungsverbundes ganz allgemein und speziell bei einem eXTra-spezifischen Datenübermittlungsverbund auftreten und in welcher Reihenfolge sie behandelt werden können. Die Aspekte und die damit zusammenhängenden Fragestellungen werden hier aufgeführt, aber nicht inhaltlich diskutiert. Vielmehr wird jeweils auf das oder die Dokumente verwiesen, in denen diese Fragestellungen aus

Sicht von eXTra näher behandelt werden, z.B. auf die Design Guidelines [DSIG], die Best Practices [BEST], den Überblick über die Standardnachrichten [UMSG], die ⓘ Profilierung [PROF] und die Versionierung [VERS], um die wichtigsten zu nennen.
Angrenzende Gebiete, die im eXTra-Standard nicht explizit behandelt werden, wie das zum Einsatz kommende DFÜ-System oder das Themengebiet der Sicherheit, werden hier – weil sie wesentlicher Bestandteil bei der Gestaltung eines Datenübermittlungsverbundes sind – etwas ausführlicher behandelt. Dabei wird Bezug genommen auf die internationale Standardisierung und die Dokumente „eXTra und Webservices“ [EXWS] bzw. „Sicherheit und Verfügbarkeit in eXTra“ [EXSEC].

Diese Dokumente und sämtliche öffentlichen Informationen über eXTra sind im Internet unter der Adresse http://www.extra-standard.de abrufbar.

Für den eiligen Leser, der sich nur für die Themen interessiert, die für sein spezifisches ⓘ Betriebsmodell relevant sind, liegt ein Fahrplan pro Betriebsmodell vor, der ihn entsprechend leitet (2.2.1.4).

Den zweiten Schwerpunkt bilden als praktisches Anschauungsmaterial Beispiele existierender eXTra-spezifischer Datenübermittlungsverbünde: der gesetzlichen Krankenversicherungen GKV, der Deutschen Rentenversicherung DRV (einerseits mit Arbeitgebern, andererseits mit dem Deutschen Post Rentenservice DPRS) und dem XUV-Datenübermittlungsverbund der Unfallversicherung. Diese Beispiele zeigen exemplarisch einerseits die Vielfalt unterschiedlicher eXTra-spezifischer Datenübermittlungssysteme und andererseits das sehr weite Spektrum möglicher Lösungen auf der Basis von eXTra.
Pro Beispiel werden in kompakter Darstellung neben den wichtigsten Gründen, die für die Entscheidung pro eXTra und der konkreten Ausgestaltung maßgeblich waren, sowie dem Steckbrief und der gegebenen ⓘ Topologie des Datenübermittlungsverbundes auch die angewendeten eXTra-Strukturen des Sende- und Holprozesses (die Gestaltung der eXTra-Ebenen und der Header) aufgezeigt.
Die aktuelle Basis von eXTra bildet bei der Unfallversicherung (3.3) und der Rentenversicherung mit ihrem Fachverfahren „elektronisch unterstützte Betriebsprüfung euBP“ (3.2.1) eXTra der Version V1.3, während die gesetzliche Krankenversicherung GKV (3.1) und die Rentenversicherung mit dem Fachverfahren „Sofortmeldungen“ (3.2.1) eXTra V1.4, sowie beim „System Single Point of Contact SPoC“ (3.2.2) eXTra V1.3.1 (inhaltlich gleichbedeutend mit eXTra V1.4) verwendet.

1.4. Überblick über eXTra

Da dieses Dokument Datenübermittlungsverbünde im Allgemeinen unter Berücksichtigung des eXTra Kommunikationsstandards betrachtet, ist es sinnvoll sich zunächst einen Überblick zu eXTra und dessen charakteristischen Eigenschaften zu verschaffen.

Der eXTra Kommunikationsstandard mit integrierter Logistik und Datenübermittlung, ist ein gemeinschaftlich von Unternehmen und Behörden entwickelter, offener, frei verfügbarer, generischer Standard.
eXTra ist ein leichtgewichtiges und flexibles ⓘ XML-Protokoll für die Gestaltung einfacher wie komplexer, dialog- wie massendatenfähiger Datenaustauschsysteme mit Unterstützung typischer ⓘ Prozessketten, das eine einheitliche Abwicklung logistischer Funktionen bei völliger Transparenz gegenüber Daten, Infrastrukturen, Diensten und Protokollen ermöglicht.

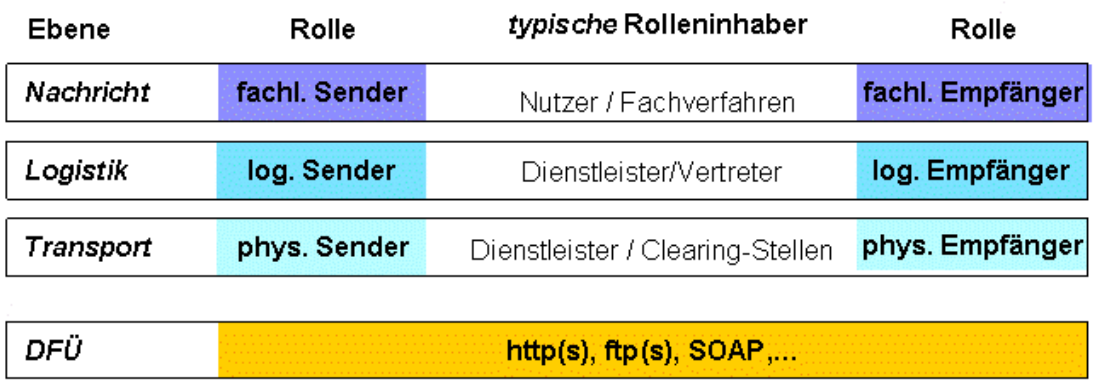

Bild 1: Das abstrakte Architekturmodell des eXTra Kommunikationsstandards mit seinem Ebenen- und Rollenmodell.

Weitere Informationen, wie die Entstehungsgeschichte, die eXTra-Philosophie und das eXTra-Modell (siehe Bild 1), den eXTra-Basis-Standard, die ⓘ Profilierung und den daraus erzeugten verbundspezifischen eXTra-Standard, den Nutzen von eXTra, aber auch eine Abgrenzung was eXTra nicht beinhaltet, findet man in den beiden Dokumenten zum Einstieg in eXTra, der Einführung in den eXTra-Standard [EINF] und dem Kompendium [KOMP].

2. Relevante Aspekte beim Entwurf und der Ausgestaltung eines Datenübermittlungsverbundes

2.1. Klärung grundsätzlicher Aspekte

Bevor mit den Überlegungen zur Konzeption und Ausgestaltung begonnen werden kann, sollten zuerst grundsätzliche Aspekte geklärt werden.

Dazu zählen folgende Fragen:

1) Wer legt die Charakteristik des verbundspezifischen eXTra Standards und dessen Anwendung im spezifischen Datenübermittlungsverbund, die Teilnahmebedingungen (Sender/Empfänger), die Regeln des laufenden Betriebs sowie das Verhalten der anzubindenden Fachverfahren fest?
   a) Ist es ein Gremium (in der Verwaltung oder der Wirtschaft)?
   b) Ist es eine einzelne Partei, eine autonome Behörde oder ein autonomes Unternehmen?
   ⇨ Gibt es noch kein Gremium oder keine diesbezügliche kompetente Stelle, sollte sie ins Leben gerufen werden, um einen ordnungsgemäßen Betrieb und eine Weiterentwicklung gewährleisten zu können.
2) Welche Rahmenbedingungen gelten für Fachverfahren, Kommunikation, Logistik und Datenübermittlung?
   a) Gibt es gesetzliche Grundlagen bzw. Verordnungen einer Behörde, die einzuhalten sind?
   b) Fußt das Datenübermittlungsverfahren bzw. die angebundenen Fachverfahren auf Festlegungen einer autonomen Unternehmung?
   c) Existiert eine Meldepflicht/Bringschuld oder eine Holpflicht/Holschuld, der ereignisorientiert oder periodisch zu definierten Zeitpunkten nachzukommen ist?
3) Existiert bereits ein Datenübermittlungsverbund oder soll dieser neu geschaffen werden?
   a) Welche funktionalen, nichtfunktionalen (z.B. Performance) und Sicherheitsanforderungen sind bekannt?
   b) Wenn der Datenübermittlungsverbund bereits existiert, soll dieser um weitere Fachverfahren und/oder die zu bedienende Topologie ausgeweitet oder modernisiert bzw. standardisiert oder neu strukturiert werden?

c) Soll im Zuge einer Neu- bzw. Restrukturierung eines existierenden Datenübermittlungsverbundes die Aufgabenzuordnung zu den einzelnen Teilnehmern auf Empfängerseite neu geordnet werden, weil es zu Rollenverschiebungen bei den Teilnehmern kommt?

Damit wird z.B. folgendes Szenario adressiert: Wenn auf Empfängerseite statt einer Vielzahl von Instanzen in der Doppelrolle als ⓘ physikalischer Empfänger und verwertendem Fachverfahren künftig ein zentraler Zugang zur Empfängerseite etabliert werden soll – eine ⓘ Clearingstelle, technisch ein eXTra-ⓘServer in der Rolle als einzigem physikalischen Empfänger. Wobei damit möglicherweise eine zusätzliche Zielsetzung verfolgt wird, nämlich eine Zentralisierung der Aufgabenstellungen eines Identity-Managements, sowie der Sicherheit und Verfügbarkeit des gesamten Datenübermittlungsverbundes weg von den einzelnen Instanzen hin zum zentralen Zugangssystem.

4) Welche Teilnehmer fungieren als Sender?

a) Wie viele Teilnehmer mit ihren erzeugenden Fachverfahren werden am Datenübermittlungsverbund auf Senderseite kurzfristig und wie viele mittel- bis langfristig teilnehmen?

⇨ Dies dient der Einschätzung, welche Kapazität für das Empfangssystem vorgesehen werden muss

b) Wie homogen oder heterogen sind die Teilnehmer mit ihren charakteristischen Eigenschaften auf der Senderseite?

⇨ Auch dies dient der Einschätzung, welche Kapazität für das Empfangssystem vorgesehen werden muss, bzw. von welcher Transaktionslast und Datenvolumina man ausgehen muss. Wenn es nur Teilnehmer gibt, die jeweils eine Anwendung einsetzen, in die die Rolle eines physikalischen Senders integriert ist, kann man von einem Einzelbetrieb und der Übermittlung einzelner fachlicher Nachrichten ausgehen. Wenn es jedoch auf Senderseite auch Dienstleister/Service-RZs gibt, die im Auftrag vieler Teilnehmer agieren, ist von einem Massenbetrieb mit entsprechend hohem Datenvolumen auszugehen. Dies gilt insbesondere dann, wenn das angebundene Fachverfahren an definierten Stichtagen beliefert werden muss und damit am Stichtag mit einer Spitzenlast zu rechnen ist.

c) Über welches Mindestniveau – Knowhow, technische, organisatorisch-personelle und finanziellen Mittel – muss ein Teilnehmer verfügen? Wie hoch ist die Einstiegshürde in den Datenübermittlungsverbund?

5) Wie viele Fachverfahren mit welchen Betriebsmodellen sollen angebunden werden?
   a) Gibt es im Datenübermittlungsverbund z.B. sowohl Dialogverfahren als auch asynchron arbeitende batchorientierte Verfahren?
   b) Gibt es Fachverfahren mit evtl. unterschiedlichen Prozessketten?

6) Welche Topologie muss das Datenübermittlungsverfahren bedienen?
   a) Gibt es genau einen oder mehrere Annahmestellen als physikalische Empfänger?
   b) Gehören der physikalische, ⓘ logische und fachliche Empfänger der gleichen Partei an, oder sind es jeweils eigenständige Parteien?
   c) Wenn der (möglicherweise einzige) physikalische Empfänger eine eigenständige Partei ist, z.B. ein Service-RZ, bietet dann dieses Service-RZ seine Dienste nur einem einzigen oder sogar mehreren Datenübermittlungsverbünden an? Oder anders ausgedrückt, stellt der physikalische Empfänger eine eigenständige Partei dar und ist deren Dienst multimandantenfähig?

7) Welches Schutzniveau muss der physikalische Empfänger, das eXTra-Empfangssystem bieten, z.B. gegenüber Angriffsszenarien aus dem Internet?

8) Welches Sicherheitsniveau (in Bezug auf den Datenschutz, Vertraulichkeit und Integrität der Daten) fordern die logischen Empfänger und Fachverfahren?

9) Welches Risiko liegt beim Dateneigentümer, wenn Angreifer die Schutzmaßnahmen außer Kraft gesetzt haben und die Daten in falsche Hände geraten oder verfälscht wurden, d.h. welches Risikoprofil haben die Dateneigentümer?

2.2. Die zu behandelnden Teilaspekte

Eine strenge Abgrenzung einzelner im Folgenden zu behandelnder Teilaspekte ist schwierig. Vielmehr beeinflussen sie sich zumeist gegenseitig. Z. B. Ist der geforderte Schutzbedarf nicht allein dadurch geklärt, dass die fachlichen Daten personenspezifische Daten enthalten. Hier gehen u.a. genauso die Topologie des Datenübermittlungsverbundes, der Schutzbedarf des Empfangsservers, das DFÜ-Protokoll, die Datenübermittlung über Unternehmensgrenzen oder innerhalb eines Unternehmens sowie das Betriebsmodell des Fachverfahrens mit in die Schutzbedarfsfeststellung ein. Ein ähnliches Zusammenspiel ganz unterschiedlicher Aspekte gibt es auch bei den Fragen welche DFÜ-Protokolle eingesetzt werden können oder wie viele eXTra-Ebenen notwendig und sinnvoll sind, etc.

2.2.1. Charakteristik des Fachverfahrens, Klärung des Betriebsmodells

Zentraler Punkt bei der Gestaltung eines verbundspezifischen eXTra Standards und dessen Verwendung in einem Datenübermittlungsverfahren ist die Ermittlung der Charakteristik der anzubindenden Fachverfahren und der damit induzierten Betriebsmodelle.
Ein ganz wichtiges Kriterium, das den Typus eines Fachverfahrens festlegt, ist dessen Arbeitsweise. Arbeitet das Fachverfahren auf Empfängerseite synchron – ist es z.B. ein Dialogverfahren, das auf die Aktivitäten der Senderseite sofort reagiert – oder arbeitet es asynchron? Asynchron heißt, dass das Fachverfahren auf Empfängerseite nach seinem eigenen Rhythmus arbeitet, also unabhängig von den Aktivitäten der Senderseite, sei es die Übermittlung fachlicher Daten in einem Sendeprozess oder das Anfordern fachlicher Nachrichten in einem Holprozess.

2.2.1.1. Das synchron arbeitende Fachverfahren, das Dialogverfahren

Das Fachverfahren auf Senderseite sendet mit einem Vorgang fachliche Daten an das zugeordnete Fachverfahren auf Empfängerseite. Dieses kann immer sofort (synchron in dieser Anschaltung) eine Antwort/ Rückmeldung bzw. ein Ergebnis liefern. D.h. im Falle einer Anfrage, Anforderung einer Auskunft/Berechnung oder einer Anforderung fachlicher Daten durch den Sender enthält die Rückmeldung des Empfängers die entsprechenden fachlichen Daten. Für den Fall, dass der Sender fachliche Daten zur Verarbeitung durch das Fachverfahren auf Empfängerseite übermittelt, enthält die Rückmeldung bereits das Ergebnis der Verarbeitung.
Welche logische Bedeutung die gesendeten fachlichen Daten, bzw. die fachlichen Daten einer Rückmeldung haben, ist für eXTra ohne Bedeutung.
Für eXTra gibt es nur einen Prozess, den Dialogprozess.

2.2.1.2. Das asynchron arbeitende Fachverfahren

Das asynchron arbeitende Fachverfahren kennt möglicherweise mehrere Prozesse, bzw. eine entsprechende Prozesskette, d.h. eine Folge logisch zusammen gehöriger Prozesse. Die Frage ist nun, mit welchem Prozess eine Prozesskette für ein asynchron arbeitendes Fachverfahren auf Empfängerseite beginnt: ist es ein Sendeprozess der Senderseite, nämlich die Belieferung mit fachlichen Daten oder ist es auf Empfängerseite ein Bereitstellungsprozess, der fachliche Daten für die Senderseite zum Abholen mittels Holprozess bereitstellt?

Der Sendeprozess

Der Sendeprozess mit fachlichen Daten ist entweder der einzige oder der erste Prozess einer Prozesskette, den die Senderseite an die Empfängerseite übermittelt. Das Fachverfahren auf Empfängerseite kann nicht sofort, sondern erst später – asynchron – die übermittelten fachlichen Daten verarbeiten und eine Antwort/Rückmeldung bzw. ein Ergebnis liefern. D.h. das Fachverfahren auf Empfängerseite ist in den Sendevorgang prinzipiell nicht involviert.

Die Senderseite hat die Möglichkeit den Sendevorgang so zu parametrieren, dass sie an einer oder an keiner Antwort/Rückmeldung des eXTra-Empfangssystems im Sinne einer Empfangsbestätigung interessiert ist.

Zusatzfragen:

Liegt eine Bringschuld des Senders vor, z.B. auf Grund gesetzlicher Vorgaben, womöglich gekoppelt an vorgegebene Abgabezeitpunkte?

Hat der Sender die Möglichkeit beim Sendeprozess eine Empfangsbestätigung des eXTra-Empfangssystems zu verlangen, um den rechtzeitigen Sendeprozess nachweisen zu können?

Der Holprozess

Welches Szenario liegt für den Holprozess vor?

Szenario 1:

Ist der Holprozess der zweite Prozess in einer Prozesskette, in der die Senderseite das Verarbeitungsergebnis eines vorangegangenen Sendeprozesses abholen will?

Zusatzfrage: Gibt es für das Fachverfahren auf Senderseite die Verpflichtung fachliche Nachrichten abzuholen (Holschuld)?

Szenario 2:

Ist der Holprozess der erste (oder einzige) Prozess einer Prozesskette, in dem die Senderseite die von der Empfängerseite bereitgestellten fachlichen Daten abholen will – ohne einen vorangegangenen Sendeprozess. Das ist klassisch das Szenario, dass ein Server Daten bereitstellt, die von Clients angefordert werden.

Für den Holprozess bietet der eXTra-Standard Unterstützung durch spezifische fachliche Nachrichten an, den sog. eXTra-Standardnachrichten [UMSG].

Der Bestätigungsprozess

Der Bestätigungsprozess ist ohne vorhergehenden Holprozess nicht sinnvoll. Will die Empfängerseite explizit die Bestätigung eines erfolgreichen, vorhergehenden Holprozesses?

Gibt es für das Fachverfahren auf Senderseite die Verpflichtung das Verarbeitungsergebnis seiner gesendeten Nachrichten als fachliche Nachricht abzuholen (Holschuld)?

Im Falle einer Holschuld verlangt dann das Fachverfahren auf Empfängerseite eine Bestätigung über den Erhalt der abgeholten fachlichen Nachrichten von der Senderseite?

Gibt es für das Fachverfahren auf Empfängerseite die Verpflichtung der Senderseite das Verarbeitungsergebnis als fachliche Nachricht zur Verfügung zu stellen (Bringschuld)?

Im Falle einer Bringschuld verlangt dann das Fachverfahren auf Empfängerseite eine Bestätigung über den Erhalt der abgeholten fachlichen Nachrichten von der Senderseite, um damit nachweisen zu können, dass die Empfängerseite ihrer Bringschuld nachgekommen ist?

Für den Bestätigungsprozess bietet der eXTra-Standard Unterstützung durch spezifische fachliche Nachrichten an, den sog. eXTra-Standardnachrichten [UMSG].

2.2.1.3. Festlegung des Betriebsmodells

1. Ist zwischen dem Fachverfahren auf Senderseite und demjenigen auf Empfängerseite nur genau ein einziger Prozess definiert?
   1.1. Ist dieser eine Prozess ein Dialogprozess?
   →Betriebsmodell ***Dialogbetrieb***
   1.2. Ist dieser eine Prozess ein Sendeprozess
   →Betriebsmodell ***einfacher Sendebetrieb***
   1.3. Ist dieser eine Prozess ein Holprozess?
   →Betriebsmodell ***einfacher Holbetrieb***

2. Zwischen dem Fachverfahren auf Senderseite und demjenigen auf Empfängerseite sind mehrere Prozesse definiert.
   Es werden drei Prozesse betrachtet, die in einer Prozesskette zusammenwirken können: der Sende-, Hol- und Bestätigungsprozess.
   2.1. Hat die Senderseite immer die Initiative, d.h. baut sie DFÜ-technisch immer die Verbindung auf, egal ob der Prozess ein Sende-, Hol- oder Bestätigungsprozess ist?
   2.1.1. Besteht die Prozesskette aus zwei Prozessen, dem Sende- und Holprozess?
   → Betriebsmodell ***Sende- Holbetrieb***

2.1.2. Oder besteht sie aus dem Hol- und Bestätigungsprozess?

→ Betriebsmodell ***Hol- Bestätigungsbetrieb***

2.1.3. Besteht die Prozesskette aus den drei Prozessen, dem Sende-, Hol- und Bestätigungsprozess?

→ Betriebsmodell ***Sende- Hol- Bestätigungsbetrieb***

2.2. Haben beide Seiten – die Senderseite wie auch die Empfängerseite – die Möglichkeit jeweils einen Sendeprozess zu initiieren, unabhängig davon, welche logische Bedeutung der jeweilige Sendeprozess hat? Die Antwort der Empfängerseite, also die eXTra-Response – in der Bedeutung z.B. einer Empfangsbestätigung oder einer fachlichen Nachricht – wird hier gegebenenfalls als Sendeprozess dargestellt, den die Empfängerseite initiiert.

→ Betriebsmodell ***beiderseitiger einfacher Sendebetrieb***

Weitere Einzelheiten zu diesen Fragestellungen sind bei den Design Guidelines [DSIG#3] und bei den Best Practices [BEST#2.2] sowie dem Überblick über die eXTra-Standardnachrichten [UMSG] zu finden.

2.2.1.4. Fahrplan für die Betriebsmodelle

Im Folgenden – nach der Klärung, welches Betriebsmodell vorliegt – wird für die eiligen Leser pro Betriebsmodell ein sog. Fahrplan zusammengestellt, der mittels Links auf die Kapitel dieses Dokuments verweist, die für dieses Betriebsmodell von besonderem Interesse sind.

Der zu einem spezifischen Betriebsmodell gehörende Fahrplan ist in der folgenden Tabelle in der Spalte zu finden, die dem Betriebsmodell zugeordnet ist.

	Dialogbetrieb	Einfacher Sendebetrieb	Beiderseitiger einfacher Sendebetrieb	Einfacher Holbetrieb	Sende- Holbetrieb	Hol- Bestätigungs-betrieb	Sende- Hol-Bestätigungsbetrieb
Schutz, Sicherheit und Verfügbarkeit	2.2.2	2.2.2	2.2.2	2.2.2	2.2.2	2.2.2	2.2.2
DFÜ-Ebene und DFÜ-Protokolle für das entsprechende Betriebsmodell	2.2.3	2.2.3	2.2.3	2.2.3	2.2.3	2.2.3	2.2.3
Das Ebenenkonzept und die Anzahl erforderlicher Ebenen	2.2.4	2.2.4	2.2.4	2.2.4	2.2.4	2.2.4	2.2.4
Identifikation und Identifikatoren	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5
Handhabung von Fehlern und Störungen					2.2.6	2.2.6	2.2.6
Testunterstützung	2.2.7		2.2.7		2.2.7	2.2.7	2.2.7
Nachvollzug und Auskunftsfunktionen					2.2.8	2.2.8	2.2.8
Profilierung	2.2.9	2.2.9	2.2.9	2.2.9	2.2.9	2.2.9	2.2.9
Dynamische Aspekte im laufenden Betrieb Zeitstempel		2.2.10.1	2.2.10.1	2.2.10.1	2.2.10.1	2.2.10.1	2.2.10.1
Dynamische Aspekte im laufenden Betrieb Sendeprozess		2.2.10.2	2.2.10.2		2.2.10.2		2.2.10.2
Dynamische Aspekte im laufenden Betrieb Holprozess			2.2.10.3	2.2.10.3	2.2.10.3	2.2.10.3	2.2.10.3
Dynamische Aspekte im laufenden Betrieb Bestätigungsprozess						2.2.10.4	2.2.10.4
Dynamische Aspekte im laufenden Betrieb Zusammenspiel der beiden Fachverfahren auf Sender- und Empfängerseite					2.2.10.5	2.2.10.5	2.2.10.5

2.2.2. Schutz, Sicherheit und Verfügbarkeit

Richtschnur für das Vorgehen zur Erfüllung von Schutzzielen wie Verfügbarkeit, Integrität, Vertraulichkeit und Zurechenbarkeit sollte die Maßgabe „security by design“ sein. Sicherheit kann erfahrungsgemäß nur unzulänglich im Nachhinein in ein Verfahren, System oder eine Installation gebracht werden, wenn dieses bereits besteht. Dies gilt insbesondere dann, wenn die Kommunikation mit mannigfachen Bedrohungen über öffentliche Netze, z.B. dem Internet stattfindet.

2.2.2.1. Allgemeines zu Sicherheitsniveau und Sicherheitsmittel

Im Folgenden wird davon ausgegangen, dass sich ein Teilnehmer eines Datenübermittlungsverbundes zuerst registrieren muss, bevor er dessen Dienste in Anspruch nehmen kann.

Betrachtungsgegenstand ist neben der Ebene des Registrierungs- und Prüfprozesses der Identität eines neuen Teilnehmers und der Ausgabe eines geeigneten Sicherungsmittels auch der laufende Betrieb der miteinander kommunizierenden DFÜ-Systeme – Sicherheit auf DFÜ- bzw. Transportebene – und der miteinander kooperierenden Fachverfahren – Sicherheit auf Anwendungsebene (der eXTra-Standard ist auf der Anwendungsebene angesiedelt).

Für jede dieser drei Ebenen stellt sich die Frage, welches Sicherheitsniveau (assurance level, (2.2.2.2)), d.h. welche Schutzziele die beteiligten Parteien (Sender, Empfänger, Fachverfahren) vorgeben und mit welchen Mitteln die geforderte Verfügbarkeit, ⓘ Authentifizierung, Authentizität, Vertraulichkeit und Integrität erreicht werden kann.

Welches Sicherheitsniveau angemessen ist, ergibt sich wiederum aus einer Risikobetrachtung und -bewertung möglicher Schadensfälle in finanzieller und/oder gesellschaftlicher Hinsicht. Zu untersuchen ist, welchem Risiko ein Teilnehmer bereits beim Registrierungsprozess ausgesetzt ist bzw. beim laufenden Betrieb in der jeweiligen Rolle als fachlicher/logischer/physikalischer Sender/Empfänger, wenn z.B. ein Angreifer die Schutzmaßnahmen außer Kraft gesetzt hat und die Identität eines Teilnehmers missbraucht, Daten oder Sicherungsmittel in falsche Hände geraten oder wenn die Daten verfälscht wurden. Daraus kann man die erforderliche Qualität von Sicherheitsverfahren und Sicherungsmitteln ableiten, die auf dem Weg der fachlichen Daten vom erzeugenden bis zum verwertenden Fachverfahren zum Einsatz kommen sollten.

Ist das geforderte Sicherheitsniveau gering, kann ein elektronischer Registrierungsprozess genügen und ein Klick auf einen Button „neuer Teilnehmer“, sowie der Eingabe eines Benutzernamens mit Passwort schon ausreichend sein. Im Gegensatz zu einem sehr hohen Si-

cherheitsniveau (assurance level 4, (2.2.2.2)), bei dem sich der Teilnehmer persönlich bei einer anerkannten Registrierungsstelle (Registration Authority) ausweisen und seine Identität mit entsprechenden Informationen/offiziellen Dokumenten nachweisen muss.

Das geforderte Sicherheitsniveau bestimmt weiterhin, welches Sicherungsmittels adäquat ist. Bei einem geringen Sicherheitsniveau kann bereits Benutzername/Passwort ausreichend sein, bei einem mittleren Sicherheitsniveau kann es z.B. ein Software-Zertifikat sein, beim höchsten Sicherheitsniveau muss es gemäß ISO [ISO29115-11] bzw. NIST [NIST_SP800 63] jedoch anerkannt sicher sein, z.B. eine SmartCard, die nach der Identitätsprüfung durch eine anerkannte Registrierungsstelle (Registration Authority) von einer anerkannten Zertifizierungsstelle (Credential Service Provider) ausgegeben wird.

Findet der Registrierungsprozess bzw. der laufende Betrieb über öffentliche Netze statt, z.B. über das Internet, und werden dabei personenspezifische Daten ausgetauscht, ist das Bedrohungspotential und die Missbrauchsgefahr aller Kommunikationsteilnehmer auf Sender- wie auf Empfängerseite gegenüber Angriffen aus dem Internet besonders hoch. Diesem Risiko und den Datenschutzerfordernissen muss auf allen drei Ebenen entsprechend begegnet werden.

Dem Schutzbedarf insbesondere der Empfängerseite gegenüber Angriffen aus dem Internet, gegenüber Regressforderungen wegen Missbrauch, Verlust oder nicht eingehaltenen qualitativen Zusagen z.B. von Verfügbarkeit sollte entsprochen werden. In diesem Sinn ist es ratsam die Verantwortlichkeiten und Zuständigkeiten der einzelnen Parteien (Sender, Empfänger, Fachverfahren) klar zu regeln und qualitative Zusagen explizit zu formulieren. Dies geschieht am besten nach einer sorgfältigen Risikoanalyse mit einem sog. Service-Level-Agreement (SLA) und entsprechenden Quality-Of-Service Zusagen (QOS).

2.2.2.2. Die internationale Standardisierung und die elektronische Authentifizierung

Die internationale Standardisierung gibt Hilfestellung u.a. bei der Frage welche Kriterien relevant sind bei der Bestimmung des erforderlichen Sicherheitsniveaus beim Registrierungsprozess und im laufenden Betrieb, der Wahl des geeigneten Sicherungsmittels und der Abwehr spezifischer Bedrohungen.

ISO/IEC hat im November 2011 mit ihrem „Entity authentication assurance framework“ [ISO29115-11] bzw. das National Institute of Standards and Technology der USA mit ihrem im August 2013 überarbeiteten „Electronic Authentication Guideline“ in [NIST_SP800 63] Richtlinien für den gesamten Komplex der elektronischen Authentifizierung über offene

Netze formuliert. Die Betrachtung erfolgt im Kontext einer allgemeinen Topologie (die über die bei eXTra betrachtete Topologie hinausgeht), in der das Identity Management vom Dienste-Anbieter getrennt ist und für mehrere Dienste-Anbieter zur Verfügung steht, so dass für einen Anwender bei der Inanspruchnahme mehrerer Dienste innerhalb einer Sitzung lediglich eine einmalige Anmeldung – ein sog. single-sign-on – genügt.

Der gesamte Komplex der elektronischen Authentifizierung wird bei ISO untergliedert in drei Phasen: Der „Enrolment Phase[1]“ u.a. mit der Prüfung der Identität eines Teilnehmers (siehe [ISO29115-11#8.1]), der „Credential Management Phase“ u.a. mit der Erzeugung und Ausgabe von Sicherungsmitteln (Credentials) (siehe [ISO29115-11#8.2]), und der „Entity Authentication Phase“ mit der eigentlichen Authentifizierung siehe [ISO29115-11#8.3]). Ausgehend von einer Risikoanalyse – wie hoch sind die möglichen Schäden wegen Missbrauchs und/oder auf Grund einer fehlerhaften Authentifizierung – werden Sicherheitsniveaus in 4 Stufen, den sog. assurance levels, festgelegt. Beim niedrigsten assurance level 1 genügt z.B. als Sicherungsmittel Benutzername/ Passwort, beim assurance level 3 muss es mindestens ein Software-Zertifikat sein mit multi-factor authentication, beim assurance level 4 jedoch ein hardware device, z.B. eine Smartcard mit multi-factor authentication (siehe [ISO29115-11#6] und [NIST_SP800 63#9.3.2].

Anhand von Tabellen werden die Beziehungen und das Zusammenspiel zwischen Sicherheitsniveau, Typus des Sicherungsmittels, den erforderlichen Schutzmaßnahmen gegenüber Angriffen aus dem Internet bei den drei unterschiedlichen Phasen (siehe auch [ISO29115-11#10], dem Protokolltyp und weiteren Anforderungen (z.B. Multi-Faktor Authentifizierung) einprägsam dargestellt.

Diese Richtlinien adressieren zwar primär offizielle Stellen der Verwaltung, Behörden und dergleichen (bei NIST diejenigen der USA), lassen es jedoch im Belieben eines Wirkungskreises/ einer Domäne eigene Kriterien bei der Definition ihrer Sicherheitsniveaus festzulegen, die jedoch exakt definiert und kommuniziert werden müssen. Gleichwohl bieten sie ein ausgezeichnetes Anschauungsmaterial für die Problemstellungen, aber auch für Lösungsmöglichkeiten im Bereich der elektronischen Authentifizierung, deren Kenntnisse auch bei Datenübermittlungsverbünden mit einer einfacheren Topologie sehr nützlich sind.

[1] In dem ISO Dokument ist die „Enrolment Phase“ (enrolment engl. für Anmeldung) für den Teilnehmer ein hochwahrscheinlich einmaliger Vorgang, während die „Registration“ jedes Mal stattfindet, wenn der Teilnehmer Zugriff auf eine Ressource oder den Zugang zu einem Dienst anfordert. Im deutschen Sprachgebrauch, wie auch im NIST-Dokument ist es genau umgekehrt, die Registrierung ist nur einmal erforderlich, die Anmeldung bei jedem Vorgang.

2.2.2.3. Sicherheit und Verfügbarkeit in eXTra

Eine mehr auf eXTra bezogene spezifische Betrachtung liefert das Dokument Sicherheit und Verfügbarkeit in eXTra [EXSEC], in dem u.a. das Zusammenwirken der unterschiedlichen Sicherheitsbereiche (security domains) bei eXTra verdeutlicht wird, aber auch Hinweise gegeben werden, wo man aktuelle Unterstützung findet bei der Abwehr und möglichen Vorkehrungen gegenüber Angriffen aus dem Internet.

Eine für jede eXTra-Ebene spezifische Betrachtung zum Themenbereich Sicherheits- und Effizienzverfahren findet man in den Design Guidelines [DSIG#5.11], [DSIG#6.11], [DSIG#7.11].

2.2.3. Die DFÜ-Ebene und DFÜ-Protokolle

Ausschlaggebend für die Gestaltung der ⓘ DFÜ-Ebene und der Wahl des DFÜ-Protokolls sollten, neben den charakteristischen Eigenschaften und dem Betriebsmodell der angebundenen Fachverfahren, insbesondere das von den angebundenen Fachverfahren geforderte Sicherheitsniveau sein.

In der folgenden Tabelle werden die aus Sicht von eXTra relevanten Eigenschaften verbreiteter DFÜ-Protokolle aufgelistet. Die Betrachtung beschränkt sich einerseits auf store-and-forward Protokolle – exemplarisch das SMTP-Protokoll für E-Mail-Verfahren – und andererseits auf DFÜ-Protokolle auf Basis von Punkt-zu-Punkt Verbindungen – exemplarisch http(s), ftp(s) und SOAP auf der Basis von http(s).

Hinweis: Einen unmittelbaren Vergleich mit den wichtigsten Unterschieden der beiden DFÜ-Protokolle ftp und http findet man unter [FTPVSHTTP].

2.2.3.1. Eigenschaften typischer DFÜ-Protokolle

	Punkt-zu-Punkt Verbindung		store&forward Protokoll
Eigenschaften typischer DFÜ-Protokolle	**ftp(s)**	**http(s) + SOAP/http(s)**	**SMTP**
Beide Kommunikationspartner (physikalischer Sender und physikalischer Empfänger) müssen nicht gleichzeitig verfügbar (online) sein.			X
In welchem Zustand (online/offline) sich der Kommunikationspartner (physikalischer Empfänger) befindet, ist irrelevant.			X
Der Transport der Daten erfolgt i.d.R. über mehrere Zwischenstationen mit entsprechender Zwischenspeicherung und nachfolgender zeitlich versetzter Weiterleitung.			X
Der Weg der Daten ist, was die Zwischenstationen angeht, unbestimmt. Dies gilt sowohl für den Ort als auch für die Anzahl der Zwischenstationen.			X
Das DFÜ-Protokoll garantiert weder, dass die Daten in einer bestimmten Zeitstrecke beim physikalischen Empfänger ankommen, noch dass sie dort korrekt, vollständig oder überhaupt ankommen.			X
Beide Kommunikationspartner (physikalischer Sender und physikalischer Empfänger) müssen immer gleichzeitig verfügbar (online) sein.	X	X	
Der Transport der Daten erfolgt ohne Zwischenstation und ohne Zwischenspeicherung direkt an den physikalischen Empfänger.	X	X	
Das DFÜ-Protokoll stellt einen garantierten Dienst zur Verfügung. Nach Abschluss der Übertragung weiß der physikalische Sender, ob die Übertragung erfolgreich war oder nicht. Die Zeitstrecke der Datenübermittlung ist vorhersehbar: Sie ist abhängig von der Übertragungsrate der Verbindung und dem Datenvolumen.	X	X	
Das DFÜ-Protokoll ermöglicht auf Empfängerseite eine Weiterleitung an eine Anwendung, sowie die Rückmeldung der Anwendung an den physikalischen Sender in der gleichen Verbindung. Allerdings muss die Rückmeldung der Antwort durch die Anwendung innerhalb einer vorgegebenen Zeitstrecke (definiert durch den time-out der DFÜ-Verbindung) erfolgen.		X	
Das DFÜ-Protokoll ermöglicht die Datenübermittlung in vertraulicher, verschlüsselter Form – Sicherheit auf Transportebene	ftps	https	

2.2.3.2. DFÜ-technische Ausgestaltung der relevanten Prozesse

Die Ausgestaltung der Prozesse, des Dialogprozesses, bzw. der drei relevanten Prozesse Sende-, Hol- bzw. Bestätigungsprozess kann mit Hilfe der genannten DFÜ-Protokolle in folgender Weise realisiert werden:

	Punkt-zu-Punkt Verbindung		store&forward Protokoll
Ausgestaltung der Prozesse	**ftp(s)**	**http(s)**	**SMTP**
Dialogprozess D mit **Scenario=Request-with-Response (R1)**: Der physikalische Sender fordert eine Rückmeldung (eXTra-Response) des Fachverfahrens (im eXTra Element Procedure angegeben) in der gleichen Verbindung.		X	
Sendeprozess S1 mit **Scenario=Fire-and-Forget (FF)**: Der physikalische Sender erwartet keine Rückmeldung (eXTra-Response) des eXTra-Empfangssystems.	X	X	X
Sendeprozess S2 mit **Scenario=Request-with-Acknowledgement (A1)**: Der physikalische Sender fordert eine Rückmeldung (eXTra-Response) des eXTra-Empfangssystems in der gleichen Verbindung.		X	
Sendeprozess S3 mit **Scenario=Request-with-Acknowledgement (A2)**: Der physikalische Sender fordert eine Rückmeldung des eXTra-Empfangssystems. Die Rückmeldung (eXTra-Response) erfolgt als Sendevorgang in einer nachfolgenden Verbindung.	X		X
Holprozess H1 mit **Scenario=Request-with-Response (R1)**: Der physikalische Sender fordert eine Rückmeldung (eXTra-Response) des Fachverfahrens (im eXTra Element Procedure angegeben) in der gleichen Verbindung.		X	
Holprozess H2 mit **Scenario=Request-with-Response (R2)**: Der physikalische Sender fordert eine Rückmeldung des Fachverfahrens (im eXTra Element Procedure angegeben). Die Rückmeldung (eXTra-Response) erfolgt als Sendevorgang in einer nachfolgenden Verbindung.	X		X
Bestätigungsprozess B1 mit **Scenario= Request-with-Acknowledgement (A1)**: Der physikalische Sender fordert eine Rückmeldung (eXTra-Response) des eXTra-Empfangssystems in der gleichen Verbindung.		X	
Bestätigungsprozess B2 mit **Scenario= Request-with-Acknowledgement (A2)**: Der physikalische Sender fordert eine Rückmeldung des eXTra-Empfangssystems. Die Rückmeldung (eXTra-Response) erfolgt als Sendevorgang in einer nachfolgenden Verbindung.	X		X

Anmerkungen zum Dialogprozess

Ein Dialog der miteinander kooperierenden Fachverfahren ist eine Folge von Dialogschritten, von jeweils atomaren Vorgängen, klassischerweise von Frage-Antwort Vorgängen. Ein Dialogbetrieb setzt somit voraus, dass es für jeden dieser atomaren Vorgänge eine direkte Verbindung zwischen dem physikalischen Sender und dem physikalischen Empfänger gibt, über die das verwertende Fachverfahren sofort antworten kann, dass also DFÜ-technisch eine Punkt-zu-Punkt Verbindung besteht.

⇨ Damit scheiden die store-and-forward Verfahren, wie z.B. das E-Mail Verfahren aus.

Bei einem Dialogschritt muss die Rückmeldung/Antwort des Fachverfahrens in der gleichen Anschaltung erfolgen wie die Anfrage.

⇨ Damit scheiden reine File-Transfer-Protokolle wie z.B. ftp(s) aus. Zwar könnten die Rückmeldungen/Antworten mittels ftp(s) zurückgesendet bzw. im (Teilnehmer-) spezifischen Filestore bereitgestellt werden, aber dann wäre es kein Dialog, sondern ein beidseitiger Sendebetrieb oder ein Sende- Holbetrieb.

⇨ Diesen Kriterien genügen die DFÜ-Protokolle http(s) und darauf aufbauend SOAP, sowie je nach Umsetzung WebServices auf Basis von SOAP/http(s).

Anmerkungen zum Holprozess

Der Holvorgang als solcher ist puristisch betrachtet ein atomarer Vorgang, der in zwei Schritten abläuft: Der Anforderung von spezifizierten Paketen / fachlichen Nachrichten mittels eXTra-Request durch den Sender und deren Auslieferung mittels eXTra-Response durch den Empfänger. Damit ist der Holprozess in DFÜ-technischer Hinsicht ein Dialogprozess.

Eine weniger puristische Einordnung des Holprozesses lässt zu, dass der Holprozess kein atomarer Vorgang ist und in zwei Prozessschritten abläuft, nämlich in einem ersten Sende- = Anforderungsprozess und einem folgenden Holprozess bzw. einem folgenden Sende- = Auslieferungsprozess. Damit gelten die Aussagen zum Sende- Holbetrieb bzw. des beiderseitigen Sendebetriebs.

Anmerkungen zum Bestätigungsprozess

DFÜ-technisch bewirkt der Bestätigungsprozess mittels Standardnachricht ConfirmationOfReceipt[2] keine neuen Anforderungen, da beim Bestätigungsprozess lediglich der eXTra-Request - wie beim Sendeprozess - mit Scenario=request-with-acknowledgement formuliert wird, also keine qualitativ zusätzliche Anforderung darstellt.

Allgemeine Anmerkungen

Liegt eine Bringschuld des Senders vor, möglicherweise gekoppelt mit einem fest vorgegebenen spätesten Eingangstermin beim Empfänger, so ist hierfür das E-Mail-Verfahren weniger geeignet, weil das E-Mail Verfahren DFÜ-technisch als nicht garantierter Dienst definiert ist und somit weder garantiert ist, dass die Sendung innerhalb vorgegebener Zeit beim physikalischen Empfänger ankommt, noch dass die Sendung dort überhaupt ankommt.

Beim E-Mail-Verfahren werden die fachlichen Nachrichten in der Regel als E-Mail-Attach gesendet, die gegebenenfalls wegen des Datenschutzes zu verschlüsseln sind (Sicherheit auf der Anwendungsebene; Sicherheit auf der Transportebene ist jedoch nicht möglich). In der Wirkung verlagert sich beim E-Mail-Verfahren die Ebene des physikalischen Senders auf den Auslieferungsdienst für E-Mails auf Empfängerseite.

Müssen die fachlichen Nachrichten bzw. die Rückmeldungen wegen des Datenschutzes verschlüsselt werden, sollte bei Verwendung des E-Mail-Verfahrens beachtet werden, dass insbesondere die Schlüsselverwaltung eine gewisse Vertrautheit mit technischen Vorgängen voraussetzt.

Wenn die Datenübermittlung zum verwertenden Fachverfahren über öffentliche Netze oder über Unternehmensgrenzen hinweg erfolgt, ist es empfehlenswert für entsprechende Sicherheit auf der Transportebene zu sorgen indem https bzw. SOAP/https verwendet wird (beim E-Mail-Verfahren gibt es das Äquivalent leider nicht).

eXTra und Webservices

Unterstützung für weitere detailliertere Fragestellungen, die sich aus der Kombination von Webservices mit eXTra ergeben findet man in eXTra und Webservices [EXWS].

[2] Hinweis: auf der DFÜ-Ebene gibt es natürlich auch Bestätigungen (z.B. Verbindung korrekt aufgebaut, Session korrekt beendet). Diese sind hier nicht gemeint. ConfirmationOfReceipt ist als fachliche Nachricht nicht auf der DFÜ-Ebene, sondern auf der Anwendungsebene angesiedelt. Kommunikationspartner ist das eXTra-Empfangssystem.

2.2.3.3. Die Betriebsmodelle und deren Ausgestaltung

Welche Prozesse mit welcher Ausgestaltung bei welchem Betriebsmodell zum Einsatz kommen, kann der folgenden Tabelle entnommen werden.

Betriebsmodell	**Dialogprozess**	**Sendeprozess S1**	**Sendeprozess S2**	**Sendeprozess S3**	**Holprozess H1**	**Holprozess H2**	**Bestätigungsprozess B1**	**Bestätigungsprozess B2**
Dialogbetrieb	X							
Einfacher Sendebetrieb		X	X					
Beiderseitiger einfacher Sendebetrieb		X		X		X		X
Einfacher Holbetrieb					X			
Sende- Holbetrieb			X		X			
Hol- Bestätigungsbetrieb					X		X	
Sende- Hol- Bestätigungsbetrieb			X		X		X	

Hinweis: Ist die eXTra-Response des Sende-, Hol- und/oder des Bestätigungsprozesses als Sendevorgang in einer nachfolgenden Verbindung realisiert, so liegt ebenfalls das Betriebsmodell des beiderseitigen Sendebetriebs vor. In diesem Fall haben die verschiedenen Sendevorgänge unterschiedliche logische Bedeutungen (als Empfangsbestätigung eines Sendevorgangs (Sendeprozess S3), als Antwort auf eine Hol-Anforderung (Holprozess H2) bzw. als Rückmeldung auf eine Bestätigung (Bestätigungsprozess B2)), die als solche das eXTra-System jedoch nicht erkennen kann.

2.2.4. Das Ebenenkonzept und die Anzahl erforderlicher Ebenen

Je nach Komplexität der Prozesse gibt es unterschiedliche Aufgabestellungen und damit verbundene Rollen beim Erstellen oder beim Auswerten einer Nachricht. Der eXTra Kommunikationsstandard unterstützt die Verteilung der Arbeitsschritte auf bis zu drei am Prozess beteiligte Instanzen, die jeweils auf ihrer Ebene miteinander kommunizieren (Allgemeines siehe auch Kompendium [KOMP#4], detaillierte Betrachtung siehe Design Guidelines [DSIG#3]):

Der eXTra Kommunikationsstandard erlaubt es, die Aufgabengebiete des Transports mehrerer Nachrichten-Pakete, des Bündelns mehrerer Einzelnachrichten zu einem Paket und des Verarbeitens einer Einzelnachricht auf physikalisch getrennte Organisationseinheiten zu verteilen, schreibt dies jedoch nicht vor. Jeder dieser Einzelschritte findet sich im Aufbau der Beschreibungsstruktur in einer sog. Ebene wieder.

eXTra kennt drei Ebenen (siehe auch Bild 1):

- Die eigentliche ⓘ Fach-Nachrichtenebene,
- die ⓘ Paket-Ebene und
- die ⓘ Transport-Ebene.

Eine Nachricht wird erstellt, indem jede damit befasste Instanz ihre bereitgestellten fachlichen Daten (in einem sog. ⓘ Body) zusammenfasst und eine Beschreibung dieses Arbeitsschritts - der Meta-Daten - (in Form eines sog. ⓘ Header) hinzufügt. Auf der Gegenseite wird die Beschreibung der entgegengenommenen Nachricht von der verarbeitenden Instanz interpretiert. Auf Basis dieser Beschreibung werden die zugehörigen fachlichen Daten entsprechend der Verarbeitungsregeln behandelt.

Je nach gegebener Topologie sind viele mögliche Varianten bei der Gestaltung der eXTra-Ebenen denkbar. Entscheidend für die Anzahl erforderlicher Ebenen sind folgende Fragen:

- Welche Topologie liegt auf Empfängerseite (Datenannahmestelle) vor?
- Wird in einem verteilten Szenario eine End-zu-End-Sicherheit vom erzeugenden bis zum verwertenden Fachverfahren angestrebt?
- Müssen die fachlichen Nachrichten jeweils getrennt in einem eigenen Übermittlungsvorgang übermittelt werden, oder – sofern das Fachverfahren auf Empfängerseite „batchfähig“ ist – können sie zu einem eXTra ⓘ Package bzw. zu einer eXTra-ⓘ Message gebündelt werden?
- Können die fachlichen Nachrichten zu einem Fachverfahren – sofern dieses mandantenfähig ist – von mehreren Unternehmen zu einem eXTra-Package gebündelt werden?
- Können mehrere logische Empfänger bzw. Fachverfahren in einer Übertragung an den physikalischen Empfänger adressiert werden?
- Wie viele unterschiedliche Fachverfahren (jeweils spezifiziert im eXTra-Element Procedure) bedient das eXTra-Empfangssystem? Muss das eXTra-Empfangssystem deshalb multimandantenfähig sein?

- Können mehrere Datentypen (jeweils spezifiziert im eXTra-Element DataType) in einem Übermittlungsvorgang übermittelt werden?

Kriterien für die Notwendigkeit nur einer Ebene

Eine einzige Ebene – die Transport-Ebene – genügt zumeist, wenn das eXTra-Empfangssystem nur ein einziges Fachverfahren bedient, oder wenn eine Sendung immer nur Daten für ein einziges Fachverfahren enthält.

Kriterien für die Notwendigkeit mehrerer Ebenen

Kriterien für die Notwendigkeit der Paket-Ebene findet man in Design Guidelines [DSIG#6] und Kriterien für die Notwendigkeit der ⓘ Nachrichten-Ebene in Design Guidelines [DSIG#7].

Eine Diskussion zusammen mit Beispielen über die Frage der Gestaltung der Ebenen findet man in den Best Practices [BEST#3.2].

2.2.5. Identifikation und Identifikatoren

Für den ordnungsgemäßen Betrieb eines Datenübermittlungsverbundes ist die Identifikation der Teilnehmer / Akteure aber auch der einzelnen Übermittlungsvorgänge essentiell. In diesem Zusammenhang sind folgende Fragestellungen relevant:

1) Welche Regeln hat ein Datenübermittlungsverbund in Bezug auf die verschiedenen Teilnehmer auf Sender- wie auf Empfängerseite definiert? Muss sich ein Teilnehmer registrieren und wenn bei wem? Gibt es eine oder mehrere Stellen, die einen Teilnehmer registrieren, die den Identifikator des Teilnehmers vergeben und verwalten und die Mechanismen festlegen bzw. die Sicherungsmittel ausgeben, mit denen die Identifikation erfolgen kann?
   - → Im eXTra Kommunikationsstandard ist die Frage der Registrierung, die Wahl des geeigneten Sicherungsmittels und die Identifikation eines Teilnehmers auf DFÜ-Ebene nicht Gegenstand der Betrachtung. Hilfestellung in diesem Bereich findet man beim „Entity authentication assurance framework“ von ISO/IEC [ISO29115-11] oder bei NIST im „Electronic Authentication Guideline“ [NIST_SP800 63].
   - → In einem eXTra-spezifischen Datenübermittlungsverbund ist für das eXTra-System der Identifikator eines Teilnehmers in der Rolle des physikalischen, logischen oder fachlichen Senders die ⓘ SenderID. bzw. die ⓘ ReceiverID bei einem Teilnehmer auf der Empfängerseite. Sinnvollerweise ist die SenderID und die ReceiverID ein

Begriff, der bereits auf der DFÜ-Ebene überprüft werden kann, z.B. dadurch, dass er im verwendeten Zertifikat enthalten ist.

2) Wie hoch ist der Schutzbedarf der Teilnehmer gegenüber Missbrauch ihrer Identifikatoren? Müssen die Identifikatoren SenderID und ReceiverID signiert werden?
   → Ab einem bestimmten (höheren) Schutzbedarf, sollte der Transport der Daten verschlüsselt erfolgen, jedoch in einer Form, dass der eXTra-TransportHeader auf Empfängerseite ausgewertet werden kann. Der erforderliche Schutz kann bei Punkt-zu-Punkt Protokollen z.B. mit einer Verschlüsselung auf Transportebene mittels SSL/TLS erreicht werden.

3) Besteht die Notwendigkeit im Datenübermittlungsverfahren auch das Fachverfahren und den Datentyp explizit zu benennen?
   → Wenn es im gesamten Datenübermittlungsverbund nur ein einziges Fachverfahren gibt bzw. wenn das/die Fachverfahren immer nur einen Datentyp kennen, dann könnte man auf die Nennung des Fachverfahrens (im eXTra-Element Procedure) bzw. des Datentyps (im eXTra-Element DataType) verzichten. Will man jedoch die Erweiterung um zusätzliche Fachverfahren oder Datentypen von vornherein bedenken, so empfiehlt sich entweder die explizite Nennung in den eXTra-Headern oder dessen Festlegung als Default-Verfahren bzw. Default-Datentyp.

4) Welchen Stellenwert hat der Nachvollzug von Datenübermittlungsvorgängen, bzw. welche Prozesssicherheit, welcher Komfort soll der Senderseite geboten werden bzw. welcher Automatisierungsgrad wird auf Empfängerseite angestrebt (und damit die Hotline entlastet)?
   → Der eXTra-Standard führt im Header jeder Ebene Identifikatoren für jeden einzelnen Übermittlungsvorgang mit: Die ⓘ RequestID und einen Zeitstempel, welche die Senderseite bei einem eXTra-Request vergibt und die ⓘ ResponseID ebenfalls mit einem Zeitstempel, die analog die Empfängerseite bei einer eXTra-Response vergibt. Die Verantwortung für die jeweils eindeutige Vergabe der Identifikatoren RequestID und ResponseID hat die jeweilige Seite. Sie sollten unbedingt jeweils eineindeutig vergeben werden. Denn nur so können diese beiden Begriffe einen Bezugspunkt für den nächsten Prozessschritt einer Prozesskette bilden, z.B. für den Holprozess oder den Bestätigungsprozess. Und nur so kann ein Nachvollzug im Störungsfall effizient bearbeitet werden, im Idealfall ohne menschliche Interaktion. Weitere Informationen zur Vergabe der RequestID und der ResponseID siehe Best Practices [BEST#4.2.4].

→ Der Wunsch bzw. die Notwendigkeit Datenübermittlungsvorgänge nachvollziehen zu können, ist z.T. abhängig vom Betriebsmodell des entsprechenden Fachverfahrens. Beim Betriebsmodell einfacher Sendebetrieb oder einfacher Holbetrieb ist die Notwendigkeit per se nicht gegeben (der Erfolg des Übermittlungsvorgangs interessiert nicht). Liegt jedoch eine Prozesskette vor, möglicherweise mit einer Bring- oder Holschuld, dann ist die Notwendigkeit sehr wohl gegeben.

Weitere Ausführungen findet man in den Design Guidelines spezifisch für jede Ebene unter [DSIG#Transport-Ebene, DSIG#Paket-Ebene und DSIG#Nachrichten-Ebene)]

2.2.6. Handhabung von Fehlern und Störungen

Fehler und Störungen gehören zum Alltag eines jeden EDV-Systems im laufenden Betrieb, so auch eines Datenübermittlungssystems. Der Umgang damit entscheidet darüber, wie hoch die Prozesssicherheit der Kommunikationspartner sein kann. Insofern lautet die prinzipielle Fragestellung, welches Maß an Prozesssicherheit die Sender- und die Empfängerseite haben sollen. Wenn für ein angeschlossenes Fachverfahren z.B. eine Bringschuld vorliegt, wird dieses Fachverfahren hohes Interesse an einer möglichst hohen Prozesssicherheit haben, um nachweisen zu können, dass es seiner Bringschuld auch Folge geleistet hat.

Die höchste Prozesssicherheit für die Senderseite ist dann gegeben, wenn für jeden Sendevorgang eine zugehörige Antwort der Empfängerseite garantiert ist, sei sie positiv oder negativ. Falls die Antwort negativ ist, ist die Instanz, die die Fehlermeldung ausgibt zunächst weniger wichtig (egal ob sie durch das DFÜ-System, die Middleware wie beim eXTra-System oder das verwertende Fachverfahren erzeugt wurde). Einzig wichtig ist jedoch die Frage, ob jeder Fehler bzw. jede Störung gemeldet werden kann, egal von welcher Instanz. Analoges gilt für die Empfängerseite, bei der die höchste Prozesssicherheit dann vorliegt, wenn zu jedem Holvorgang eine Antwort – positiv oder negativ – der Senderseite garantiert ist.

Ein eXTra-spezifisches Datenübermittlungssystem vermittelt zwischen den beteiligten Fachverfahren unter Verwendung des DFÜ-Systems. Jedes dieser Systeme hat eigene Mechanismen um mit Fehlern und Störungen umzugehen und diese dem jeweiligen Kommunikationspartner mitzuteilen. Bei einem eXTra-spezifischen Datenübermittlungssystem sind Fehler und Störungen auf DFÜ-Ebene für das eXTra-System nur daran erkennbar, dass der physikalische Sender keinen Sendevorgang erfolgreich abschließen kann, bzw. dass der physikalische Empfänger keine Sendungen mehr annehmen kann. Die Aufgabe eine entsprechende Fehlermeldung abzugeben verbleibt beim DFÜ-System.

Fehler, die das verwertende Fachverfahren bei der Verarbeitung der fachlichen Nachricht feststellt, sind für das eXTra-System als Fehler nicht erkennbar, da sie beim Betriebsmodell Sende-Hol-Betrieb oder beiderseitigem Sende-Betrieb Gegenstand einer fachlichen Nachricht/ Rückmeldung sind und das eXTra-System den Inhalt fachlicher Nachrichten nicht auswerten kann. Das eXTra-System kann lediglich feststellen, dass Rückmeldungen vorliegen bzw. auch abgeholt wurden. Die Aufgabe und die Verantwortung eine entsprechende Fehlermeldung abzugeben verbleibt also beim verwertenden Fachverfahren.

Für Fehler und Störungen, die innerhalb bzw. im Umfeld des eXTra-Systems erfolgen, bietet der eXTra-Standard mehrere spezifische Mechanismen an, die in ihrer Gesamtwirkung höchste Prozesssicherheit des eXTra-Systems bieten:

1) Für den Fall (Szenario 1), dass das eXTra-System auf Empfängerseite nicht mehr verfügbar ist (aus welchem Grund auch immer) gibt es die eXTra-Standardnachricht ExtraError, in der der Grund der Nichtverfügbarkeit in verständlicher, lesbarer Form mitgeteilt werden kann (siehe BestPractices [BEST#4.1] und eXTra-Transport-Spezifikation 1.4.0 [IFACE#7].
2) Für den Fall (Szenario 2), dass beim Sendeprozess aus Sicht des physikalischen Senders zwar der eXTra-Request gesendet werden konnte, die zugehörige eXTra-Response jedoch ausblieb, kann der physikalische Sender den physikalischen Empfänger mit der eXTra-StandardNachricht RepeatResponse oder alternativ RepeatResponseRequest auffordern, die ausgebliebene eXTra-Response erneut zu senden (siehe Design Guidelines [DSIG#8.1.4] und eXTra-Standardnachrichten [UMSG]).
3) Für den Fall (Szenario 3), dass sich der Sendeprozess aus Sendersicht mit einer positiven Empfangsbestätigung mittels eXTra-Response zunächst positiv darstellt, aber im Nachgang jedoch Fehler auf Empfängerseite (z.B. Fehler beim Entschlüsseln oder Dekomprimieren) auf dem Weg vom physikalischen Empfänger hin zum logischen Empfänger und dessen Fachverfahren erfolgten, gibt es das sog. Acknowledgement Update (siehe BestPractices [BEST#4.2.1]).

Die drei Szenarien reflektieren die Tatsache, dass das Gesamtsystem auf Empfängerseite in mehrere Domänen untergliedert ist, in das DFÜ-System, den potentiell drei Ebenen des eXTra-Empfangssystems und den Fachverfahren. Bei der Behandlung eines eXTra-Request wird auf Empfängerseite in den verschiedenen Domänen eine Folge von Prozessschritten mit entsprechenden Checkpoints durchlaufen, die sich der Transaktionslogik unterordnen. So war beim Szenario 1 zwar das DFÜ-System verfügbar, das eXTra-Empfangssystem jedoch nicht. Beim Szenario 2 konnte die Transaktion eXTra-Request-Response nicht abgeschlos-

sen werden und beim Szenario 3 ist die Transaktion nicht bis zur Auslieferung an das Fachverfahren vorangekommen.
Eine weitergehende Diskussion über Fehler und dem Umgang damit findet man in den Design Guidelines spezifisch für jede Ebene unter [DSIG#Transport-Ebene, DSIG#Paket-Ebene und DSIG#Nachrichten-Ebene].

2.2.7. Testunterstützung

Bei der Entwicklung von Software sollten frühzeitig Testszenarien überlegt und vorbereitet werden. Wird ein Datenübermittlungsverfahren implementiert, muss in der Regel für die Sender- wie für die Empfängerseite jeweils ein dediziertes System entwickelt werden – ein Client-System für die Senderseite und ein Server-System für die Empfängerseite. Beide Seiten setzen unterschiedliche Software ein, die in der Regel von verschiedenen Softwareerstellern stammt. Damit diese beiden Systeme bei Inbetriebnahme reibungslos zusammenpassen, sollten von Anfang an Testmöglichkeiten vorgesehen werden. Damit kann die Effizienz der Entwicklung deutlich gesteigert werden, u.a. dadurch dass die beiden Realisierungsteams sich auf technische Fakten stützen können und nicht permanent miteinander kommunizieren/telefonieren müssen, um Fehlerkonstellationen zu klären.

Neben diesem Szenario einer für beide Seiten initialen Inbetriebnahme des Datenübermittlungssystems, gibt es ähnliche Argumente für den Fall, dass ein Softwareersteller ein Produkt entwickelt oder erweitert, das als Neuerung das Datenübermittlungssystem unterstützt, oder dass ein neuer Teilnehmer dem Datenübermittlungsverbund beitritt. Wichtig ist dabei, dass es die Möglichkeit gibt mit Testteilnehmern zu testen, um zu verhindern, dass Echtdaten von produktiven Teilnehmern zum Test verwendet werden. Letztendlich bewirken Testmöglichkeiten für die Senderseite eine relevante Erleichterung und für die Empfängerseite eine deutliche Entlastung ihrer Hotline.

Darüber hinaus gibt es noch einen weiteren guten Grund für eine Testunterstützung: Damit kann ein Datenübermittlungsverbund die Teilnahme am Verbund von der erfolgreichen Verarbeitung definierter, vorgegebener Testfälle abhängig machen und so die Stabilität des Gesamtsystems befördern.

Die Relevanz und die Komplexität einer Testunterstützung sind abhängig vom Betriebsmodell der angebundenen Fachverfahren. Wenn lediglich das Betriebsmodell des einfachen Sende- oder Holbetriebs, bzw. des einfachen beiderseitigen Sendebetriebs zu bedienen ist, ist die Komplexität relativ gering. Ganz im Gegenteil, wenn Fachverfahren mit einem Betriebsmodell angebunden sind, die eine Prozesskette unterstützen, z.B. dem Sende-Hol-Bestätigungsbetrieb. Dann wäre die Relevanz, aber auch die Komplexität hoch.

Wenn nun feststeht, dass das Datenübermittlungsverfahren eine Testunterstützung bieten soll, weil Fachverfahren mit Prozessketten angebunden sind, dann stellt sich die Frage wie diese Testunterstützung aussehen soll. Mehrere Möglichkeiten sind bekannt:

1) Neben dem Produktivsystem, in dem die Echtdaten übermittelt werden, wird ein eigenständiges Testsystem zur Verfügung gestellt, das nur Testfälle bearbeitet. Die Frage, ob die Daten Echtdaten oder Testdaten sind, wird über die Zieladresse der Übermittlung beantwortet. Diese Lösung ist unabhängig vom eXTra Kommunikationsstandard.
   → Die getrennte Infrastruktur für Produktion und Test stellt sicher, dass die Produktionsumgebung durch Tests nicht in Mitleidenschaft gezogen werden kann. Andererseits erfordert die getrennte Infrastruktur eine sehr sorgfältige Implementierung, um sicherzustellen, dass beide Systeme die gleichen Eigenschaften aufweisen. Große Vorteile bietet diese Variante beim Übergang auf eine neue Version mit größeren Änderungen auf Empfängerseite, die sich auch auf die Senderseite auswirken. Die Senderseite kann dadurch mithelfen, diesen Übergang vorab mit Tests abzusichern.

2) Das Produktivsystem kann sowohl mit Echtdaten als auch mit Testdaten umgehen. Die Unterscheidung ob Echt- oder Testdaten wird über den Datentyp getroffen. Auch diese Lösung ist unabhängig vom eXTra-Standard.
   → Diese Lösung ist eine pragmatische Vorgehensweise, die vom Produktionssystem eine sehr sorgfältige Implementierung erfordert, die nicht nur die üblichen Fehlerfälle beherrscht, sondern auch seltene und exotische Fehlerkonstellationen behandeln kann. Allerdings kann der Übergang auf eine neue Version des Empfangssystems hiermit nicht abgesichert werden.

3) Das Produktivsystem kann sowohl mit Echtdaten als auch mit Testdaten umgehen. Die Unterscheidung ob die Übermittlung ein Testfall oder ein Echtfall ist, wird durch ein spezifisches Merkmal in den Metadaten getroffen. Dies ist beim eXTra-Standard das Merkmal TestIndicator im eXTra-Header der jeweiligen Ebene. Darüber hinaus bietet der eXTra-Standard drei Niveaus an: Soll der Testfall lediglich empfangen, vom eXTra-Empfangssystem bearbeitet oder sogar vom verwertenden Fachverfahren verarbeitet werden?
   → Für diese Lösung gelten zusätzlich auch die Aussagen zur 2. Variante.

Für ein eXTra-spezifisches Datenübermittlungssystem stehen im Idealfall für Tests sowohl eine getrennte Test-Infrastruktur zur Verfügung als auch die Möglichkeit im Produktionssystem Testfälle mit dem Merkmal TestIndicator zu markieren – zugegeben eine aufwändige Lösung. Bei einem eXTra-spezifischem Datenübermittlungsverbund mit Tausenden von Teil-

nehmern und mehreren Hundert oder Tausend physikalischen Sendern, die wiederum viele unterschiedliche Produkte einsetzen, ist diese Ideallösung dennoch bedenkenswert, denn sie entlastet die Hotline der Empfängerseite insgesamt betrachtet erheblich. Für jede Konstellation bietet sie die passenden Mechanismen an, insbesondere beim Übergang auf eine neue Version des eXTra-Empfangssystems.

Eine weitergehende Diskussion zum Themenbereich Testunterstützung findet man in den Design Guidelines spezifisch für jede Ebene unter [DSIG#5.1], [DSIG#6.1] und [DSIG#7.1].

2.2.8. Nachvollzug und Auskunftsfunktionen

Die Möglichkeit Datenübermittlungsvorgänge nachvollziehen zu können ist essentiell, um deren Existenz, die Korrektheit oder die Rechtzeitigkeit beweisen zu können. Wie relevant die Möglichkeit einer Beweisführung ist, hängt u.a. am Betriebsmodell des jeweiligen Fachverfahrens. Beim Betriebsmodell einfacher Sendebetrieb oder einfacher Holbetrieb ist die Relevanz gering (der Erfolg des Übermittlungsvorgangs interessiert nicht). Liegt jedoch eine Prozesskette vor, möglicherweise mit einer Bring- oder Holschuld, dann ist die Relevanz entsprechend hoch.

Wenn vereinbart ist, dass das verwertende Fachverfahren auf Empfängerseite zu jeder erhaltenen Lieferung fachlicher Nachrichten auch eine Rückmeldung erzeugen soll, diese aber aus Sicht des Senders über längere Zeit ausbleibt, benötigt er ein Mittel, den aktuellen Stand seiner ursprünglichen Lieferung zu erfragen. Zu diesem Zweck gibt es die eXTra-Standardnachricht StatusRequest, die es erlaubt in standardisierter Weise mit verschiedenen Selektionskriterien eine oder mehrere vergangene Sendungen zu benennen und deren aktuellen Bearbeitungsstand zu erfahren. Mittels einer Fachnachricht StatusResponse wird der aktuelle Status in standardisierter Form zurückgegeben. StatusRequest und StatusResponse realisieren somit eine Auskunftsfunktion über den Sendebetrieb der jüngsten Vergangenheit.

Die ergänzende Auskunftsfunktion über den Hol- und Bestätigungsbetrieb der jüngsten Vergangenheit wird über die beiden Standardnachrichten ListRequest und ListResponse zur Verfügung gestellt. Da die Auskunft auch den Status der Rückmeldungen bzw. Fachnachrichten enthält (Status=“bereitgestellt“, „ausgeliefert“ oder „abgeholt und bestätigt“) kann der Sender im Zusammenspiel mit der Standardnachricht DataRequest gezielt auf die bereitgestellten Rückmeldungen/Fachnachrichten zugreifen, oder bereits abgeholte oder bereits bestätigte Rückmeldungen/Fachnachrichten erneut abholen.

Weitere Informationen zu diesen Standardnachrichten findet man in den BestPractices [BEST#4.2.4.1], sowie zusammen mit Beispielen in den eXTra-Standardnachrichten [UMSG].

2.2.9. Die Profilierung

Am Ende der Analysen und spezifischen Betrachtungen der verschiedenen Themenbereiche sowie deren gegenseitige Beeinflussung steht der Vollzug der Design-Entscheidungen und deren Verfeinerung für die Implementierungsphase. Dieser Akt ist beim eXTra-Standard die Profilierung, die aus dem eXTra-Basisstandard einen verbundspezifischen eXTra-Standard mit entsprechenden verbundspezifischen Schemadateien formt.

Die Profilierung ist zum einen eine Maßschneiderung, ein Auswahlprozess aus dem Fundus des eXTra-Basisstandards. Mittels Profilierung wird z.B. ausgewählt, dass nicht alle drei eXTra-Ebenen notwendig sind, sondern z.B. nur zwei Ebenen, die Transport- und die Paket-Ebene. Und es wird u.a. ausgewählt, welche eXTra-Standardnachrichten notwendig sind und wie diese gestaltet sein sollen.

Zum anderen kann die Profilierung auch eine Anreicherung um bestimmte Konstrukte, den ⓘ PlugIns vornehmen, die für den verbundspezifischen eXTra-Standard relevant sind. Derzeit (eXTra der Version V1.5) bietet der eXTra-Basisstandard fünf PlugIns an: Zur ⓘ Migration und Weiterverwendung von Sicherheits- und Effizienzverfahren das PlugIn DataTransforms, zur Benennung des jeweiligen Ausgabestands fachlicher Nachrichten das PlugIn DataSource, zur Weitergabe von Zertifikaten das PlugIn Certificates, zur Bekanntgabe von Ansprechpartnern auf Senderseite das PlugIn Contacts und ab eXTra V1.5 zur Bekanntgabe weiterer Metadaten z.B. eines Dokumentes oder einer Prozesskette das PlugIn BusinessProcess.. Zu PlugIns siehe auch Design Guidelines [DSIG#5.10].

Weitere Hinweise und Details zur Gestaltung eines verbundspezifischen eXTra-Standards, z.B. zu der Frage ob prozessübergreifende Schemadateien oder prozessspezifische Schemadateien angebracht sind, findet man in den Best Practices [BEST#3.]

Weitere Details zur Profilierung spezifisch für jede Ebene findet man in den Design Guidelines unter [DSIG#6,7,8].

Zu beachten ist bei der Profilierung, dass bestimmte Regeln einzuhalten sind, um zu erreichen, dass der verbundspezifische eXTra-Standard auch eXTra-konform ist. Die wichtigste

Vorgabe ist, dass der verbundspezifische eXTra-Standard ein syntaktisch korrekter eXTra-Basisstandard sein muss: Eine verbundspezifische eXTra-Nachricht muss mit den Schemadateien des eXTra-Basisstandards verarbeitet werden können. Das impliziert, dass der verbundspezifische eXTra-Standard zwar eine Einschränkung, aber keine Erweiterung des eXTra-Basisstandards sein darf. Weitere Details zu den Regeln der Profilierung findet man im Dokument Profilierung [PROF].

2.2.10. Dynamische Aspekte im laufenden Betrieb eines Datenübermittlungsstandards

In den vorangegangenen Kapiteln wurde überwiegend die Statik des Datenübermittlungsverbundes betrachtet. Im laufenden Betrieb gibt es darüber hinaus noch weitere Aspekte, die ebenfalls zu bedenken sind. Eine Zusammenstellung darüber findet man in den Best Practices [BEST#4] mit Hinweisen, Klarstellungen und Empfehlungen, die insbesondere für die Betriebsmodelle nützlich sind, die Prozessketten unterstützen:

2.2.10.1. Zu Zeitstempeln

siehe [BEST#4.2]

2.2.10.2. Zum Sendeprozess

siehe [BEST#4.2.1]

- Grenzen der Parallelität bzw. der Notwendigkeit der Serialisierung des Sendeprozesses
- Annahmetransaktion oder teilweise Annahme des Sendeprozesses
- Zusammenspiel des eXTra-Request mit dem eXTra-Response, spezifiziert mit dem Element Scenario
- Wiederholtes Senden bei einem Sendeprozess mit scenario=request-with-acknowledgement
- Wiederholtes Senden bei einem Sendeprozess mit scenario=request-with-response
- Technische Fehler auf Empfängerseite (AcknowledgementUpdate)

2.2.10.3. Zum Holprozess

Siehe [BEST#4.2.2]

- Vorbereitungen zum Holprozess mit der Auskunftsfunktion ListRequest und ListResponse

- Zusammenspiel des eXTra-Servers auf Empfängerseite mit dem verarbeitenden Fachverfahren
- Der Holprozess: Abholtransaktion oder teilweise Auslieferung
- Parametrierung der Standardnachricht DataRequest
- Antwort der Empfängerseite (eXTra-Response) auf einen DataRequest
- Gestaltung des PackageHeader in der eXTra-Response auf einen DataRequest
- Wiederholtes Abholen einer erfolgreich abgeholten und evtl. bereits bestätigten Rückmeldung bzw. fachlichen Nachricht

2.2.10.4. Der Bestätigungsprozess

Siehe [BEST#4.2.3]

- Transaktionssicherheit
- Automatische Bestätigung

2.2.10.5. Zusammenspiel der beiden Fachverfahren auf Sender- und Empfängerseite

Siehe [BEST#4.3]

- Allgemeines zu Rückmeldungen und Verarbeitungsquittungen
- Die semantische Qualität einer Rückmeldung

3. Beispiele existierender eXTra-spezifischer Datenübermittlungsverbünde

Im Folgenden werden als Anschauungsmaterial Beispiele existierender ⓘ verbundspezifischer eXTra Datenübermittlungsverbünde gegeben. Dies ist der Datenübermittlungsverbund der gesetzlichen Krankenkassen GKV mit Arbeitgebern und Zahlstellen, die Datenübermittlungsverbünde der Deutschen Rentenversicherung DRV (mit Arbeitgebern und mit weiteren Behörden, z.B. dem Deutschen Post Rentenservice DPRS) und der XUV-Datenübermittlungsverbund der Unfallversicherung. Pro Datenübermittlungsverbund werden die charakteristischen Merkmale in fünf Bereichen dargelegt:

- Wichtige Gründe, die für die Wahl von eXTra ausschlaggebend waren,
- eine graphische Darstellung der Topologie des Datenübermittlungsverbundes,
- der Steckbrief,
- Festlegungen von Betriebsparametern und eXTra-spezifischen Merkmalen,
- Visualisierung der eXTra-Strukturen des Sende- und Holprozesses.

Als weiteres Anschauungsmaterial dienen XML-Beispiele auf Basis von eXTra V1.3 (siehe [XBSP13]) und eXTra V1.4 (siehe [XBSP14]) sowohl nach dem Muster der GKV als auch nach dem Muster der Sofortmeldungen der Rentenversicherung

- für die Prozesse des Betriebsmodells des einfachen Sendebetriebs,
- für die Prozesse des Betriebsmodells des Sende- Hol- und Bestätigungsbetriebs,
- für das AcknowledgementUpdate Szenario,
- für die eXTra-Standardnachrichten.

Der Steckbrief des jeweiligen Datenübermittlungsverbundes und die Festlegungen von Betriebsparametern und Merkmalen der DFÜ-Ebene des Empfangssystems und des eXTra-Empfangssystems erfolgt in Form von Muster-Tabellen in [MTAB].

3.1. Datenübermittlungsverbund der gesetzlichen Krankenkassen GKV

3.1.1. Die Wahl von eXTra als Datenübermittlungsverfahren

2010 sollte das DEÜV-Fachverfahren um zusätzliche Meldegründe, die der Arbeitgeber z.T. in seine Stammdaten übernehmen und auswerten musste, erweitert werden. Diese erforderten als Neuerung den Rückfluss von Informationen vom verwertenden hin zum ursprünglich erzeugenden Fachverfahren. Das bisherige KKS Datenübermittlungsverfahren mit den DFÜ-Protokollen E-Mail und FTAM eignete sich (aus unterschiedlichen Gründen) nur bedingt für diesen Zweck und musste überarbeitet werden. Ganz entscheidend war dabei, wie aufwändig und komplex die Migration zum neuen Datenübermittlungsverfahren sein würde bzw. wie viele der bisher verwendeten Verfahren weiterhin eingesetzt werden könnten und ob auch Änderungen in den bisherigen Fachverfahren erforderlich sein würden. Das Sicherheitsverfahren PKCS#7 konnte unverändert weiterverwendet werden. Ebenso mussten die Fachverfahren, sowie deren Datentypen und Datenformate nicht geändert werden. Genauso wichtig für das künftige Datenübermittlungsverfahren war außerdem neben der Bekanntgabe von eXTra als Bundesstandard im Bundesanzeiger dessen Eignung als Massendatenverfahren mit hoher Transaktionsrate, u.a. wegen der Teilnahme aller Unternehmen (direkt oder indirekt über ihre Meldestellen). Das auszuwählende DFÜ-Protokoll sollte eine Punkt-zu-Punkt Verbindung unterstützen, international standardisiert und weit verbreitet sein, sowie nur geringe Anforderungen an die Entwicklung, Einbindung und den laufenden Betrieb stellen – sowohl für Softwareersteller als auch für die Bediener der Lohnabrechnungsprogramme. Entlastend für die Arbeitgeberseite sollte die bisherige Rollenverteilung zwischen der Arbeitgeberseite und der Verwaltung beibehalten werden. Die Arbeitgeberseite sollte nicht gezwungen werden Server bereit zu stellen. Die Initiative für alle Übermittlungsvorgänge sollte weiterhin nur von der Arbeitgeberseite und dem physikalischen Sender ausgehen.

3.1.2. Die Topologie des Datenübermittlungsverbundes der GKV

Die schematische Darstellung der Topologie des Datenübermittlungsverbundes der GKV mit Arbeitgebern und Zahlstellen auf Sender- wie auf Empfängerseite ergibt folgendes Bild:

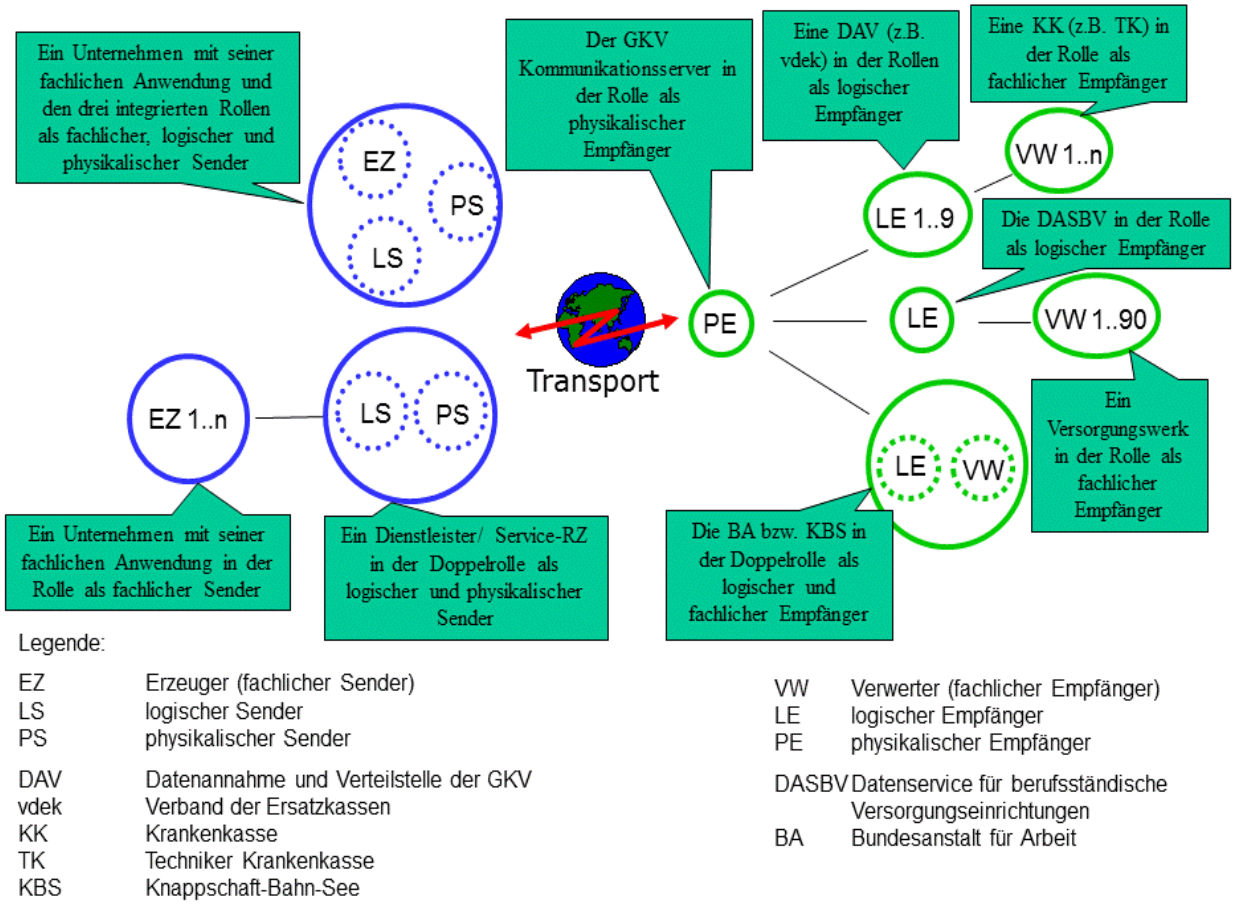

Bild 2: Die Topologie des Datenübermittlungsverbundes der GKV

3.1.3. Steckbrief

Der Datenübermittlungsverbund der gesetzlichen Krankenkassen GKV mit Arbeitgebern und Zahlstellen hat die in den folgenden Tabellen aufgelisteten charakteristischen Merkmale, die auf der Basis der zum 1.1.2016 gültigen Version V1.4 des GKV-Kommunikationsservers beruhen.

Merkmal	**Ausprägung**
Maßgebliches Gremium	Das Gremium zu Erstellung der „Gemeinsamen Grundsätze Technik“ gemäß §95 SGB IV.
Typus für den Einsatz von eXTra	• Migration des bestehenden Datenübermittlungsverbundes der GKV • Beibehaltung des Sicherheitsverfahrens PKCS#7 mit X.509 Zertifikat (Aussteller sind die zugelassenen Trustcenter im Gesundheits- und Sozialwesen) für die Authentifizierung und Verschlüsselung • Beibehaltung der ⓘ Komprimierungsverfahren • Beibehaltung der bestehenden Fachverfahren samt Datentypen und Datenformat
Auslösendes Moment für eXTra	Erweiterung des Fachverfahrens um Meldegründe, die den Rückfluss von Informationen vom verwertenden hin zum ursprünglich erzeugenden Fachverfahren erfordern und dort in die Stammdaten eingearbeitet werden müssen. Die bisherigen DFÜ-Verfahren E-Mail und FTAM waren dafür weniger geeignet. Für eXTra sprachen neben der einfachen Migration die konfliktfreie Nutzung weiterer Standards (z.B. http und https) und die relativ einfache Realisierung des offiziellen Bundesstandards eXTra (veröffentlicht im Bundesanzeiger).
Authentifizierung und Identifizierung der Senderseite	• Identifizierung des logischen und des physikalischen Senders mittels Betriebsnummer • Authentifizierung des physikalischen Senders mittels X.509 Zertifikat

Merkmal	**Ausprägung**
Benennung und Identifizierung der Empfängerseite	Identifizierung des physikalischen und des logischen Empfängers mittels Betriebsnummer
Datenschutz, Vertraulichkeit und Integrität	Die fachlichen Daten enthalten personenspezifische Informationen, deshalb ist eine Ende-zu-Ende Verschlüsselung erforderlich. **Datenfluss vom Sender zum Empfänger**: Verschlüsselung durch den physikalischen Sender (Arbeitgeber/Zahlstelle oder deren Dienstleister) für den logischen Empfänger (DAV). **Datenfluss vom Empfänger zum Sender:** Verschlüsselung durch den logischen Empfänger (DAV) für den physikalischen Sender. Als Verschlüsselungsverfahren wird PKCS#7 verwendet, zusätzlich erzeugt die verschlüsselnde Instanz eine ⓘ Signatur.
Rollenverteilung	Für alle Prozesse ist die Rollenverteilung zwischen Arbeitgeber/Zahlstelle und Verwaltung, der Sender- und Empfängerseite einheitlich: Die Arbeitgeber/Zahlstellen haben immer die Rolle eines Senders - technisch eines Clients, die Verwaltung immer die Rolle eines Empfängers - technisch eines Servers.
Klassifizierung der Teilnehmer	Auf Senderseite sind die Teilnehmer Unternehmen, die sozialversicherungspflichtige Meldungen abgeben müssen, bzw. deren Dienstleister oder ein Service-RZ. Auf Empfängerseite sind es die Sozialversicherungsträger mit ihren Dienstleistern.
Registrierung der Teilnehmer	Ein teilnehmendes Unternehmen muss bei der Bundesagentur für Arbeit eine Betriebsnummer erwerben, eine zertifizierte Entgeltabrechnungssoftware besitzen und – sofern es die Rolle eines physikalischen Senders einnimmt – bei einem registrierten Trustcenter ein X.509 Zertifikat besitzen.

Merkmal	Ausprägung
Anzahl Teilnehmer auf Senderseite	ca. 3,5 Millionen Unternehmen
Anzahl Teilnehmer auf Empfängerseite	• 1 physikalischer Empfänger: GKV-Kommunikationsserver • 11 logische Empfänger: 9 DAVn der GKV, Bundesagentur für Arbeit, Datenservice für berufsständische Versorgungseinrichtungen GmbH (DASBV) • ca. 220 fachliche Empfänger mit ihren verwertenden Fachverfahren: 130 Krankenkassen, ca. 90 berufsständische Versorgungseinrichtungen, ein zentrales Fachverfahren bei der Bundesagentur für Arbeit
Größe und Rolle der Teilnehmer auf Senderseite	Unternehmen jeder Größe; a) Ein Unternehmen kann zugleich Erzeuger der Meldungen und ⓘ physikalischer Sender sein. b) Die Rollen können verteilt werden zwischen erzeugendem Unternehmen und einem Dienstleister oder einem Service-RZ, das als logischer und physikalischer Sender für viele Unternehmen fungiert.
Zulässige Transaktionsrate und Datenvolumen	Spitzenwerte werden sowohl bei der Transaktionsrate als auch dem Datenvolumen um den Stichtag, dem 5. letzten Bankarbeitstag eines Monats erzielt. Pro Übermittlungsvorgang ist ein maximales Datenvolumen von 20 MB gestattet. Pro Jahr werden ca. 80 Millionen Dateien über den GKV-Kommunikationsserver ausgetauscht.
Topologie auf Empfängerseite	Der GKV-Kommunikationsserver (betrieben durch die ITSG) fungiert als physikalischer Empfänger, der die Pakete an die logischen Empfänger (die DAVn) weiterleitet bzw. von dort die Rückmeldungen/Verarbeitungsergebnisse erhält (Sternarchitektur). ITSG und die DAVn sind eigenständige Unternehmen, jeweils an geographisch unterschiedlichen Orten.
Unterstützung der ExtraError Nachricht V1.0	ab 1.1.2016 mit Version V1.4

Merkmal	Ausprägung
Übertragung großer Dateien, z.B. Unterstützung der MTOM-Funktionalität	(derzeit) keine Unterstützung von MTOM
Verwendete PlugIns	Contacts, DataTransforms, DataSource
Empfangsquittung	Ja, wegen scenario=request-with-acknowledgement
Unterstützung der eXTra AcknowledgementUpdate Funktion	ab 1.1.2016 mit Version V1.4 und dem Bezugspunkt ResponseID (der sog. Tracking ID) der ursprünglichen Sendung von Meldungen
Unterstützung der eXTra RepeatResponse Funktion	nein
Grundlage der Fachverfahren	gesetzliche Grundlagen für die Fachverfahren (SGB)
Anzahl angebundener Fachverfahren	12 Fachverfahren: Sozialversicherungsmelde-Verfahren (DUA, VSA, SAG), Beitragsnachweise für Arbeitgeber (BNA), Mitteilungen zu Entgeltersatzleistungen (EEL, ab 2016 zusätzlich EEK), AAG-Erstattungsverfahren (AAG, ab 2016 zusätzlich AAK), Zahlstellenmeldeverfahren (ZAV, ZAK), Beitragsnachweise für Zahlstellen (BNZ), Beitragserhebungen berufsständischer Versorgungseinrichtungen (BEA), Bescheinigungen zum Arbeitslosengeld für die Bundesagentur für Arbeit (ALG)
Betriebsmodell der Fachverfahren	Betriebsmodell für alle Verfahren: Sende-Hol-Bestätigungsbetrieb
Prozesse der Fachverfahren	• Sendeprozess (2 Ebenen, Transport- und Paket-Ebene) • Holprozess (1 Ebene mit Standardnachricht DataRequest, Antwort auf 2 Ebenen, Transport- und Paketebene) • Bestätigungsprozess (1 Ebene mit Standardnachricht ConfirmationOfRceipt)

Merkmal	**Ausprägung**
Typus der Profilierung: prozessübergreifende Profilierung (die profilierten Schemadateien gelten für alle Prozesse) oder prozessspezifische Profilierung (die profilierten Schemadateien gelten jeweils nur für einen Prozess)	Prozessspezifische Profilierung: Für den Sende-, Hol- und Bestätigungsprozess gibt es jeweils einen eigenen Satz von Schemadateien
Abgabereihenfolge der Meldungen	Pro Fachverfahren müssen die Meldungen streng seriell und aufsteigend abgegeben werden
Meldepflicht der erzeugenden Teilnehmer	Ja, bei Beitragsnachweisen für Arbeitgeber einmal im Monat spätestens am 5. letzten Bankarbeitstag, ja bei den DUA-Jahresmeldungen mit der ersten Entgeltabrechnung des Folgejahres, spätestens zum 15.2., alle anderen Verfahren und Meldegründe anlassbezogen.
Holpflicht der Verarbeitungsergebnisse, bzw. der einzuarbeitenden Stammdaten	Ja, ab 1.1.2016 hat der Arbeitgeber/die Zahlstelle die Verpflichtung, mindestens einmal pro Woche die Daten vom GKV-Kommunikationsserver abzurufen.
Verwendete eXTra-Standardnachrichten	DataRequest V1.3, ConfirmationOfRequest V1.3, ExtraError V1.0

3.1.4. Festlegung von Betriebsparametern und Merkmalen

Allgemeine Betriebsparameter und Merkmale der DFÜ-Ebene des Empfangssystems – Gegenstand der Festlegung	**Festlegung**
Verfügbarkeit des eXTra-Empfangssystems (z.B. 7 x 24 Stunden)	7 x 24 Stunden
Wartungszeitfenster des eXTra Empfangssystems	
DFÜ-Protokoll	http und https mit dem X.509 Zertifikat eines im Verfahren registrierten Trustcenters (clientseitig) und einem Standard-X.509 Zertifikat (serverseitig)
Die maßgebliche Uhr – welche Uhr ist maßgeblich, wenn die Uhren des Senders und Empfängers auseinander laufen?	keine, da die Meldung erst mit der Erstellung der Verarbeitungsbestätigung durch die DAV als eingegangen gilt

Spezifische Betriebsparameter und Merkmale des eXTra Systems – Gegenstand der Festlegung	**Festlegung**
Sendebetrieb: Realisierung als Annahmetransaktion (alles oder nichts) oder als teilweise Annahme?	Teilweise Annahme von Paketen möglich. Bedingung: Wenn ein Paket als angenommen markiert wird, dann konnte es auch vollständig (und nicht nur teilweise) übernommen werden. Bei der inhaltlichen Prüfung des Pakets durch die DAV ist ebenfalls eine teilweise Annahme möglich.
Bedeutung eines Acknowledgements beim Sendeprozess. Welche Prozessschritte im eXTra-Empfangssystem werden damit bestätigt?	Empfang der Lieferung und Übernahme in die lokale Datenhaltung

Spezifische Betriebsparameter und Merkmale des eXTra Systems – Gegenstand der Festlegung	**Festlegung**
Sendebetrieb: Festlegung der maximalen Größe einer Lieferung (in MB bzw. Anzahl Pakete), eines Paketes (in MB bzw. Anzahl Nachrichten) und einer Nachricht (in MB oder KB)	Die maximale Größe einer Lieferung und eines Paketes beträgt 20 MB.
Sendebetrieb: Toleranzzeit, innerhalb derer Lücken in der Belieferung vom Sender geschlossen werden müssen (z.B. bei laufender Dateinummer)	eine Stunde
Sende-Holbetrieb: Zeitspanne nach der der Sender das Verarbeitungsprotokoll (die Rückmeldung) des verwertenden Fachverfahrens abholen kann	ein Tag nach der Prüfung der Datei (§97 SGB IV)
Parametrierung des Holprozesses, der Standardnachricht DataRequest V1.3:	Query mit Element Argument und @property=ReceiverID bzw. @property=Procedure Element Control wird nicht unterstützt
Holbetrieb: Festlegung der maximalen Größe einer Auslieferung (in MB bzw. Anzahl Paketen), eines bereitgestellten Paketes (in MB bzw. Anzahl von Nachrichten) bzw. Nachricht (in MB oder KB)	Die Größe einer Auslieferung wird vom GKV-Kommunikationsserver begrenzt.
Parametrierung des Bestätigungsprozesses, der Standardnachricht ConfirmationOfReceipt V1.3:	ab 1.1.2016: nur Element PropertySet mit @name=ResponseID zulässig
Kann der Sender bereits abgeholte und ggfls. bereits bestätigte fachliche Nachrichten/Pakete erneut abholen?	Bereits abgeholte Pakete können erneut abgeholt werden, sofern der Empfang noch nicht bestätigt wurde. Nach erfolgreicher Empfangsbestätigung können sie nicht erneut abgeholt werden.

Spezifische Betriebsparameter und Merkmale des eXTra Systems – Gegenstand der Festlegung	Festlegung
Bis zu welcher Instanz kann der Sender den Status seiner Nachrichten auf Empfängerseite mit der Standardnachricht StatusRequest nachverfolgen?	nicht unterstützt
Empfängerseite: Vorhaltezeitraum für bereitgestellte fachliche Nachrichten/Pakete. Wann muss der Sender spätestens abholen?	Spätestens nach 30 Tagen, danach werden die Daten gelöscht
Empfängerseite: Vorhaltezeitraum für bereits abgeholte und bestätigte fachliche Nachrichten/Pakete. Wie lange kann der Sender erneut abholen?	nicht unterstützt

3.1.5. Visualisierung der eXTra-Strukturen

Exemplarisch werden aus Sicht des physikalischen Senders der Sendeprozess fachlicher Daten zum GKV-Kommunikationsserver (mit zwei eXTra-Ebenen) und der Anforderungs-/ Holprozess von fachlichen Rückmeldungen (mit einer eXTra-Ebene) veranschaulicht. Basis ist die ab 1.1.2016 gültige Version V1.4.

Der Bestätigungsprozess wird auf Grund seiner einfachen Struktur nicht explizit gezeigt.

Die unten gezeigten eXTra-Strukturen gelten für alle Fachverfahren der GKV; explizit aufgeführt ist das Fachverfahren DUA.

Sendeprozess Teil 1: eXTra-Request

Für den Sendeprozess fachlicher Daten ergeben sich folgende schematische Bilder der eXTra-Strukturen: Der Transport- und der Paketebene, sowie der zugehörigen Header:

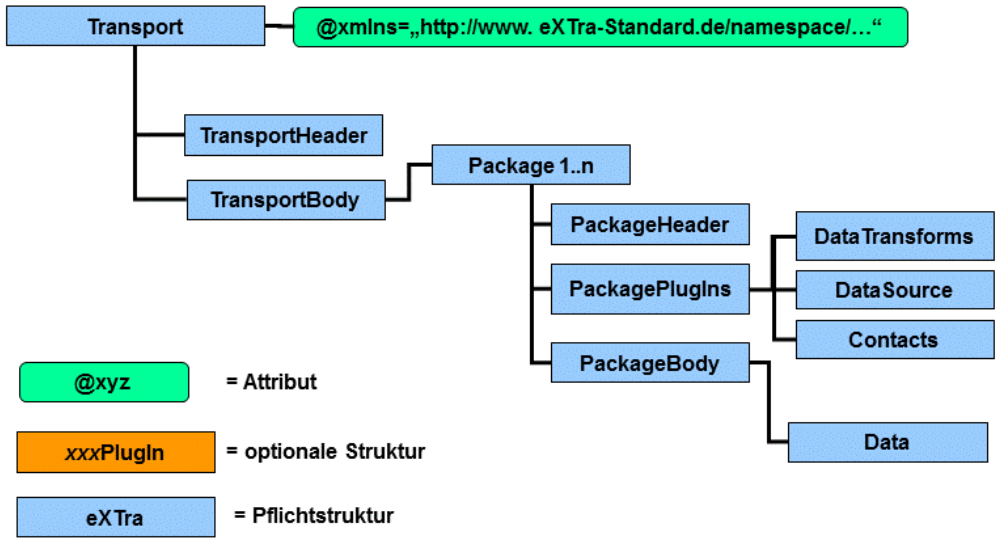

Bild 3: Die Ebenenstruktur des Sendeprozesses (eXTra-Request) beim GKV-Kommunikationsserver

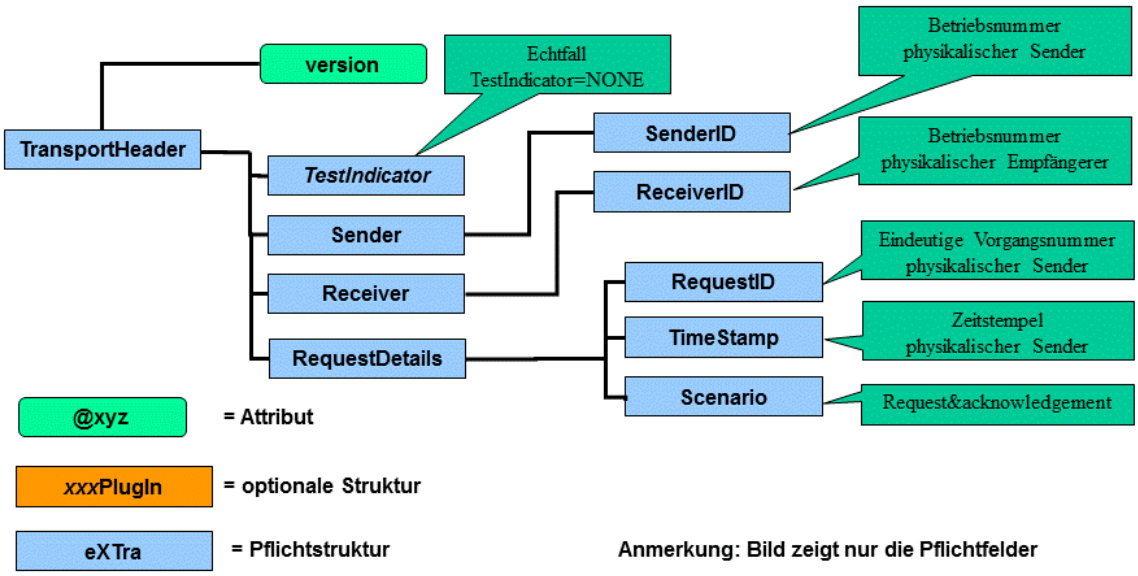

Bild 4: Der Transportheader des Sendeprozesses (eXTra-Request) beim GKV-Kommunikationsserver

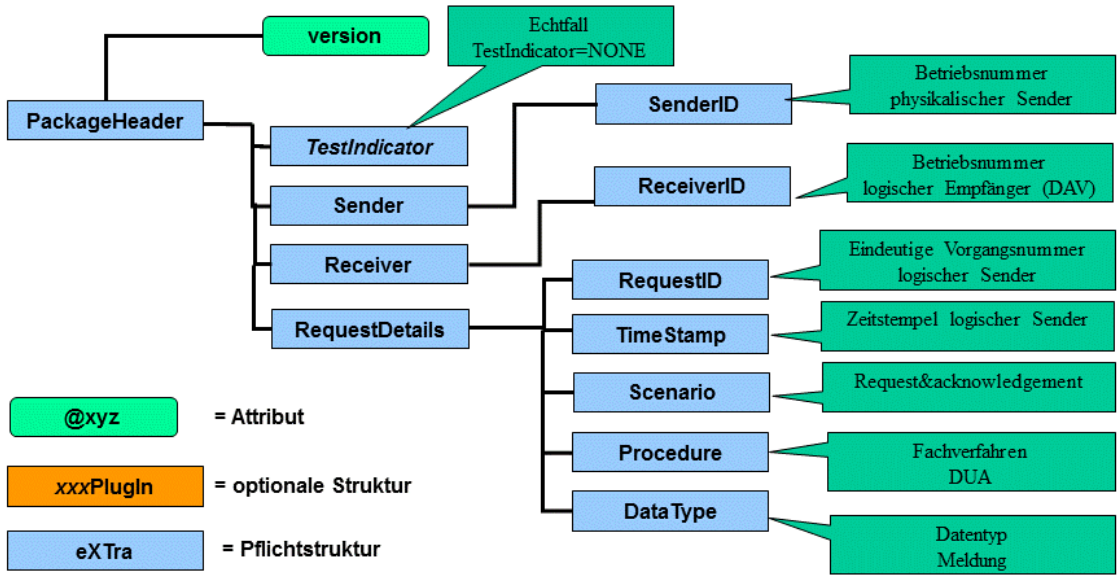

Bild 5: Der PackageHeader des Sendeprozesses (eXTra-Request) beim GKV-Kommunikationsserver

Hinweis: In der eXTra-Philosophie erzeugt der logische Sender die Pakete. Kommt auf Senderseite jedoch eine integrierte Anwendung mit der dreifachen Rolle als fachlicher, logischer und physikalischer Sender zum Einsatz, ist diese Trennschärfe nicht mehr gegeben. Analoges gilt bei Dienstleistern/ Service-RZs, die eine Doppelrolle als logischer und physikalischer Sender wahrnehmen.

Beim GKV-Kommunikationsserver wurde festgelegt, dass die SenderID auf Transport- wie auf Paket-Ebene jeweils die Betriebsnummer des physikalischen Senders sein muss.

Sendeprozess Teil 2: eXTra-Response

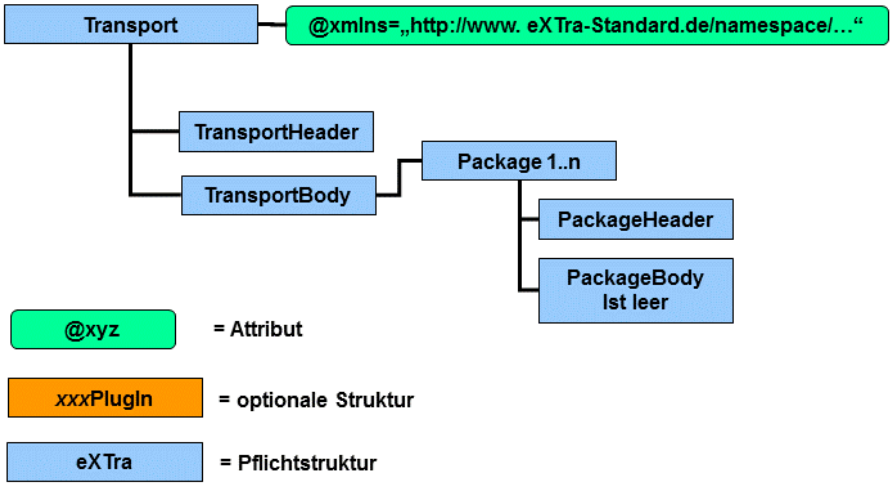

Bild 6: Die Ebenenstruktur des Sendeprozesses (eXTra-Response) beim GKV-Kommunikationsserver

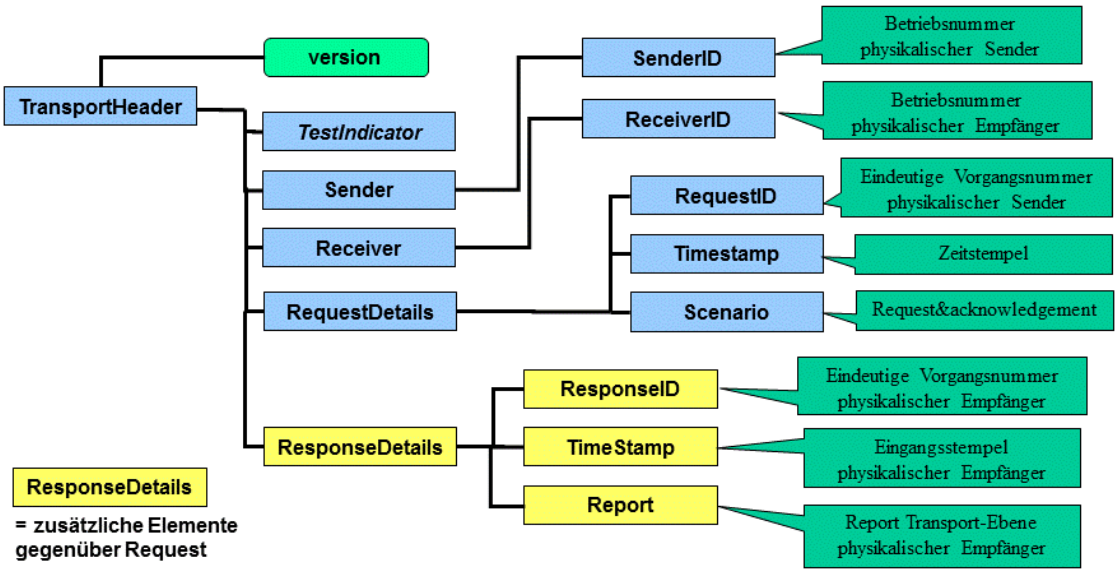

Bild 7: Der TransportHeader des Sendeprozesses (eXTra-Response) beim GKV-Kommunikationsserver

Bild 8:

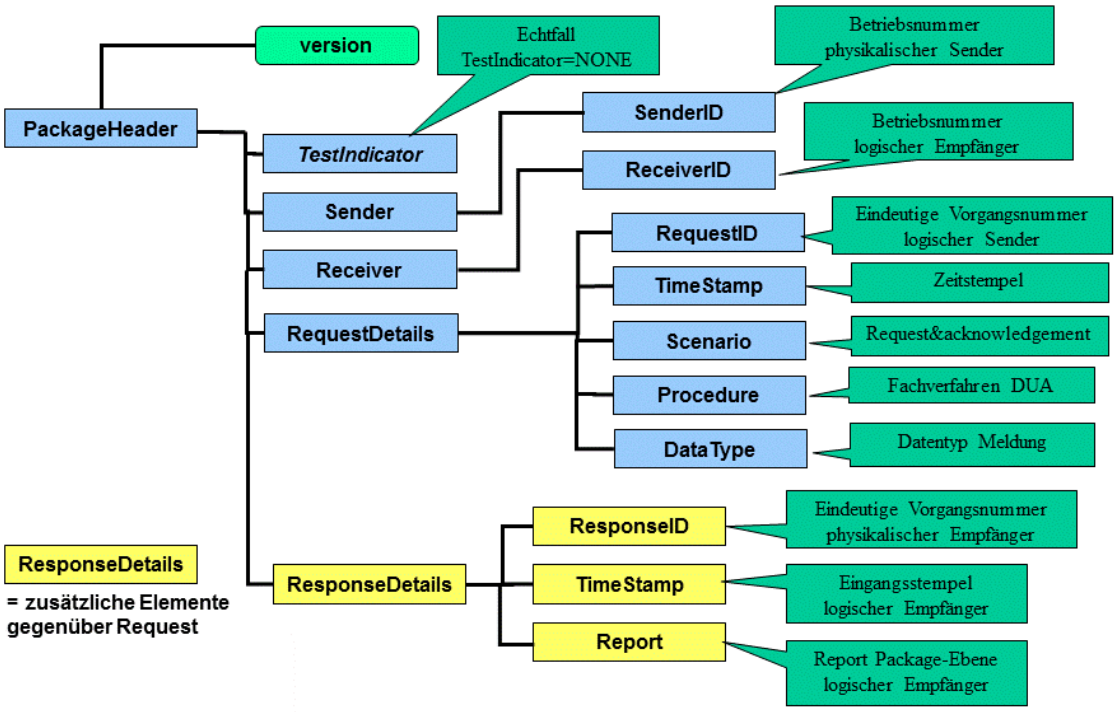

Bild 9: Der PackageHeader des Sendeprozesses (eXTra-Response) beim GKV-Kommunikationsserver

Holprozess Teil 1: eXTra-Request

Für den Anforderungs-/Holprozess fachlicher Daten (Verarbeitungsergebnisse bzw. einzuarbeitende Stammdaten) ergeben sich folgende schematische Bilder der eXTra-Strukturen: Der eXTra-Ebene, der eXTra-Header, sowie der eXTra-Standardnachricht DataRequest:

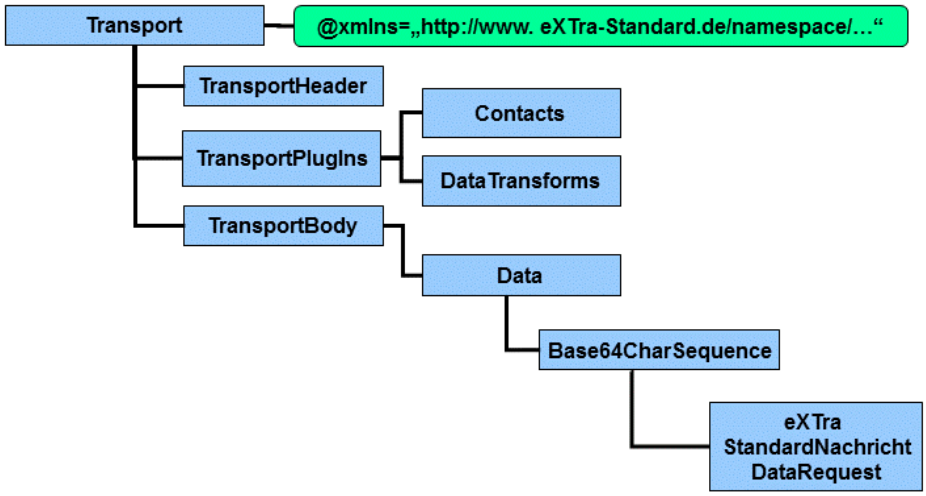

Bild 10: Die Ebenenstruktur des Holprozesses Request beim GKV-Kommunikationsserver

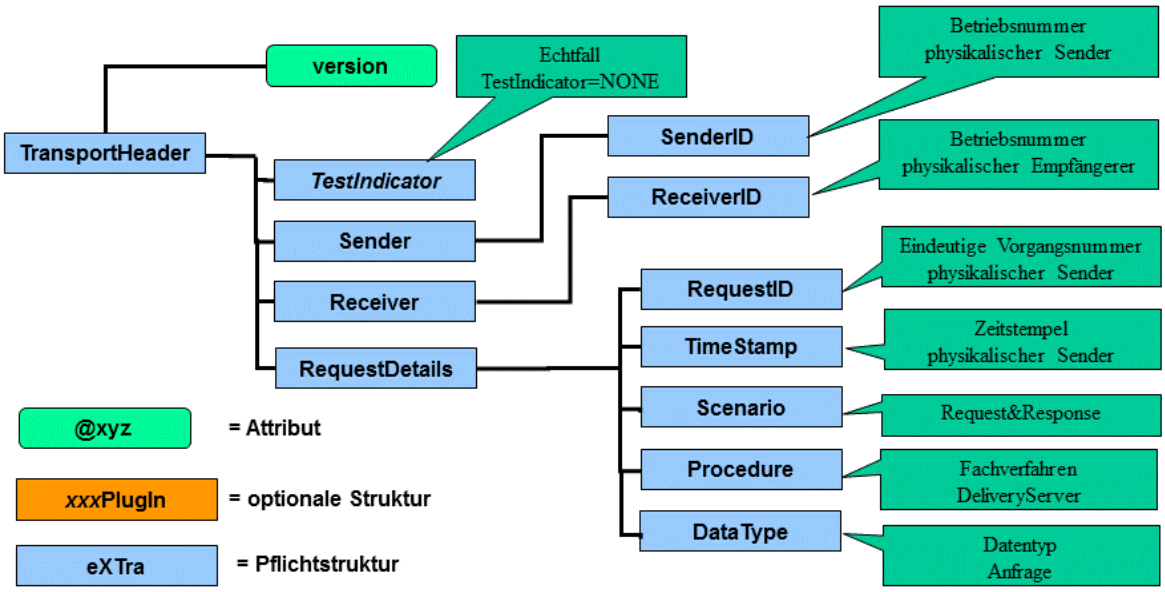

Bild 11: Der TransportHeader des Holprozesses: eXTra-Request „Holen von n Rückmeldungen in n Paketen“ beim GKV-Kommunikationsserver

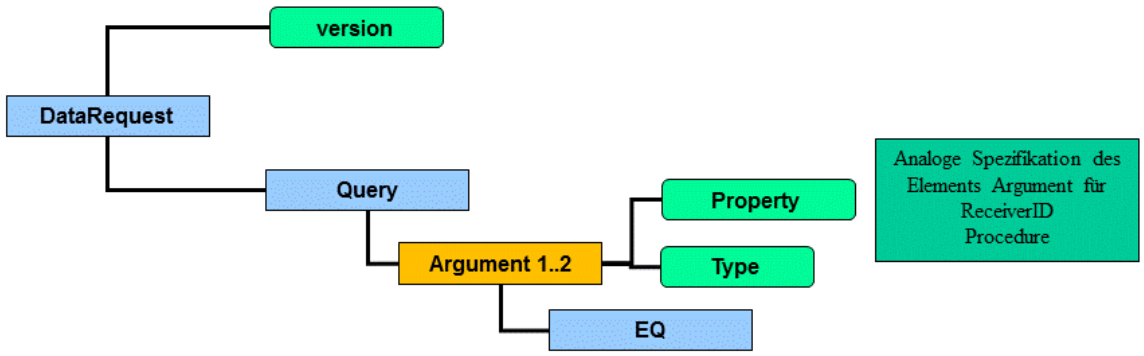

Bild 12: Die eXTra-Standardnachricht DataRequest beim GKV-Kommunikationsserver

Hinweis:

Die Standardnachricht DataRequest wurde im Sinne einer einfachen Ausprägung profiliert, sinngemäß: „gib mir alles vom Receiver X (ReceiverID) und dem Fachverfahren Y (Procedure), was Du hast“ oder noch einfacher: „gib mir von allen Receivern und allen Fachverfahren (Procedure), was Du hast“.

Die Selektion nur nach ReceiverID oder nur nach Procedure ist ebenfalls möglich („gib mir alles vom Receiver X, was Du hast“ oder „gib mir alles zum Fachverfahren Y, was Du hast“).

Der Umfang/ das Datenvolumen, der so ausgelieferten fachlichen Daten kann vom Sender her nicht eingeschränkt werden, sondern wird durch den GKV-Kommunikationsserver beschränkt.

Holprozess Teil 2: eXTra-Response

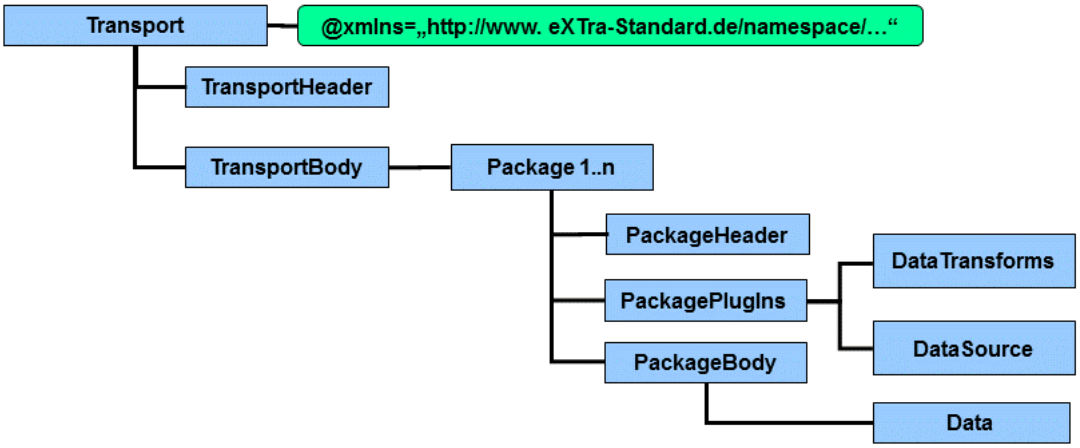

Bild 13: Die Ebenenstruktur des Holprozesses: eXTra-Response beim GKV-Kommunikationsserver „Holen von n Rückmeldungen in n Paketen“

Hinweis:

Im Falle eines AcknowledgementUpdate ist der PackageBody leer (gilt ab 1.1.2016).

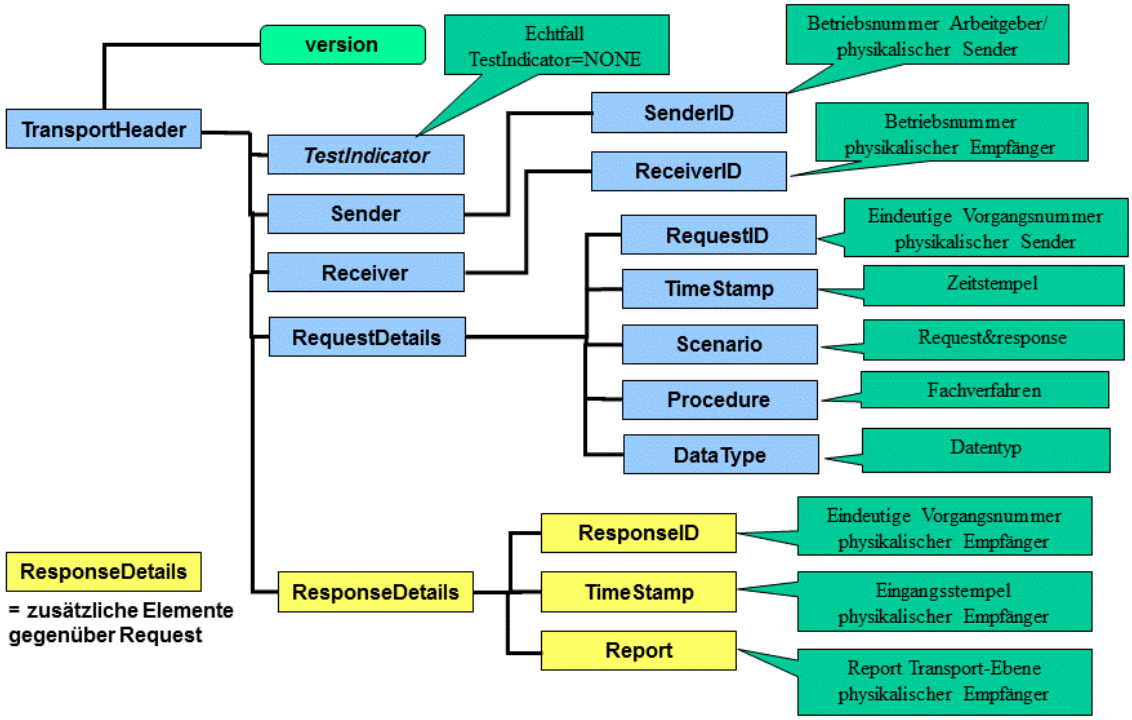

Bild 14: TransportHeader des Holprozesses: eXTra-Response beim GKV-Kommunikationsserver „Holen von n Rückmeldungen in m Paketen“

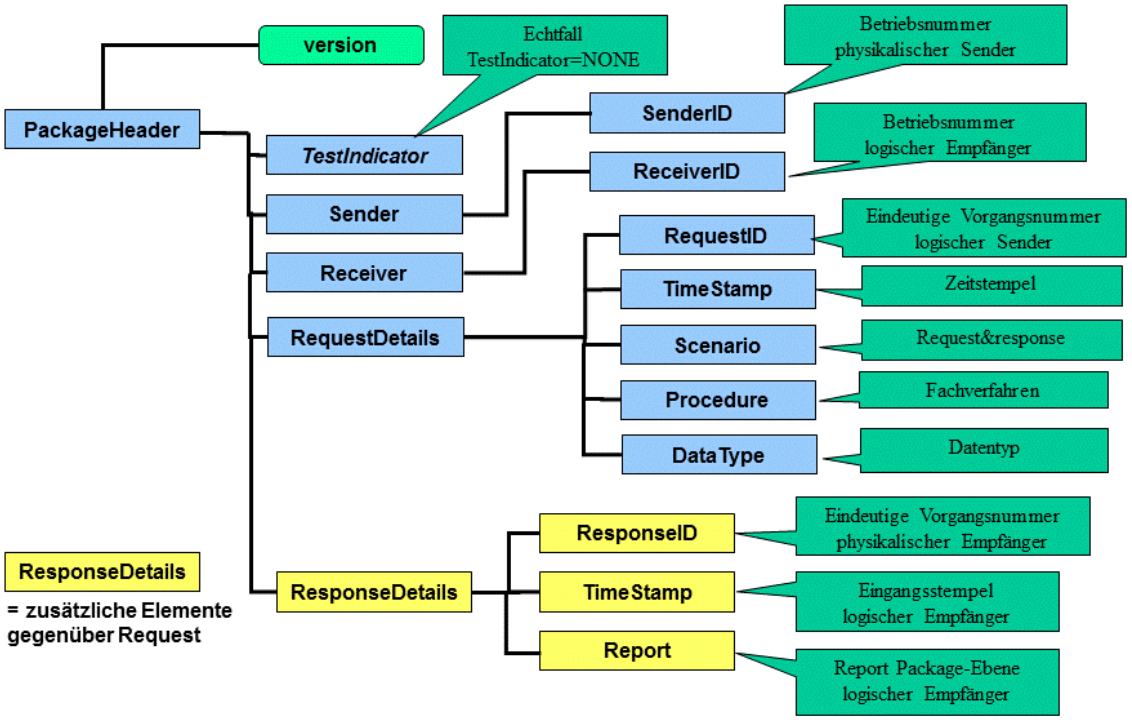

Bild 15: PackageHeader des Holprozesses: eXTra-Response beim GKV-Kommunikationsserver „Holen von n Rückmeldungen in m Paketen“

3.2. Die Datenübermittlungsverbünde der deutschen Rentenversicherung DRV

3.2.1. Der Datenübermittlungsverbund der DRV mit Arbeitgebern

3.2.1.1. Die Wahl von eXTra als Datenübermittlungsverfahren

Da einerseits auf Senderseite das Sofortmeldungen erzeugende Fachverfahren ein Lohnabrechnungsprogramm ist (genau wie bei DUA-Meldungen und Beitragsnachweisen der GKV) und andererseits den Arbeitgebern und deren Softwareherstellern die beim Datenübermittlungsverbund der GKV eingesetzten Sicherheitsverfahren (PKCS#7 und das X.509 Zertifikat der ITSG) bereits bekannt waren, war es für eine möglichst einfache Einführung der Sofortmeldungen in 2009 naheliegend, dass die Deutsche Rentenversicherung diese Verfahren auch für die Sofortmeldung einsetzt.

Um den meldepflichtigen Unternehmen eine möglichst hohe Prozesssicherheit bieten zu können (im Zuge des Meldevorgangs soll der Sender eine Empfangsbestätigung der RV erhalten), wählte man in Kombination mit eXTra als DFÜ-Protokoll ein standardisiertes, sicheres und weit verbreitetes Protokoll, das einfach zu implementieren ist: Das https-Protokoll. Durch https werden die Daten auf dem Transportweg verschlüsselt übertragen und damit die Vertraulichkeit der Sofortmeldungen mit ihren personenspezifischen Daten sichergestellt.

3.2.1.2. Die Topologie des Datenübermittlungsverbundes der DRV

Die schematische Darstellung der Topologie des Datenübermittlungsverbundes der Deutschen Rentenversicherung DRV mit Arbeitgebern auf Sender- wie auf Empfängerseite ergibt folgendes Bild:

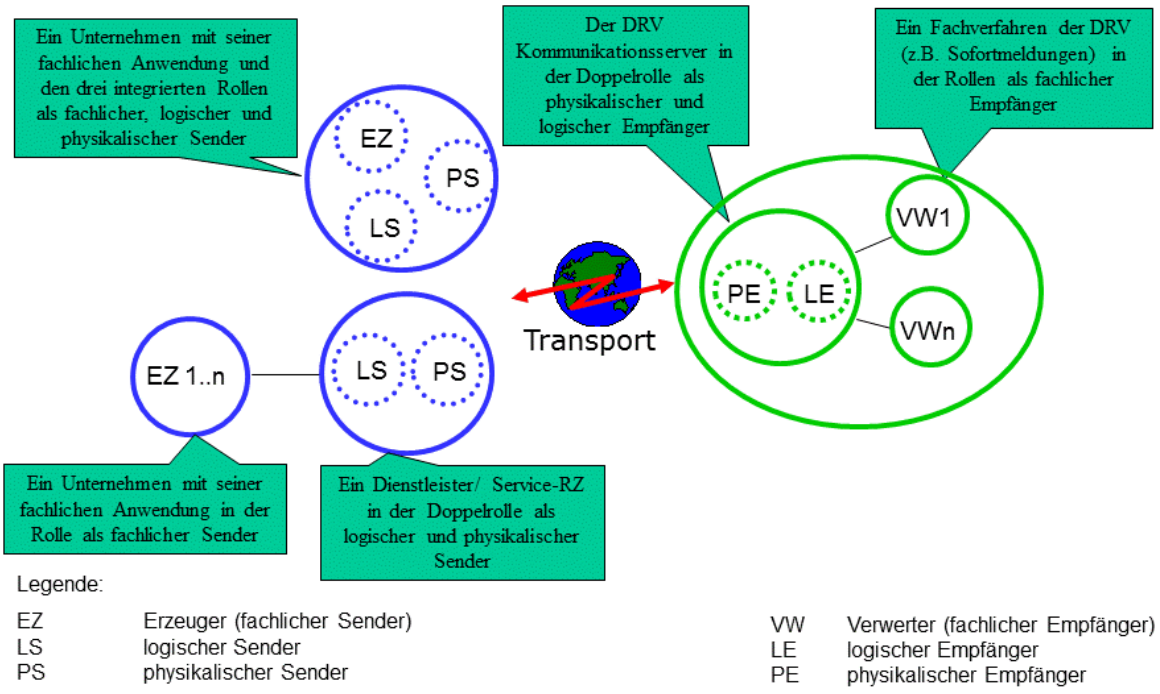

Bild 16: Die Topologie des Datenübermittlungsverbundes der DRV mit Arbeitgebern

3.2.1.3. Steckbrief

Der Datenübermittlungsverbund der deutschen Rentenversicherung DRV mit Arbeitgebern hat die in den folgenden Tabellen aufgelisteten charakteristischen Merkmale. Bei den Sofortmeldungen beruhen sie auf der zum 1.1.2016 gültigen Version V1.4 des DSRV Kommunikationsservers, bei den euBP-Meldungen ist es die Version V1.3.

Merkmal	Ausprägung
Maßgebliches Gremium	Sofortmeldungen und elektronisch unterstützte Betriebsprüfung euBP: Die DSRV selbst und das Bundesministerium für Arbeit und Soziales BMAS.
Typus für den Einsatz von eXTra	Neuer Datenübermittlungsverbund der DRV mit Arbeitgebern: Zielsetzung ist eine weitgehende Konformität mit dem Datenübermittlungsverbund der GKV, um für Arbeitgeber einen leichten Einstieg bzw. um für Softwareersteller einen geringen Realisierungsaufwand zu ermöglichen. Übernahme des Sicherheitsverfahrens mit X.509 Zertifikat (Aussteller ist die ITSG) für die Authentifizierung und Verschlüsselung; Übernahme der Komprimierungsverfahren; Anschluss neuer Fachverfahren (Sofortmeldungen und elektronisch unterstützte Betriebsprüfung euBP)
Auslösendes Moment für eXTra	• Leistungsfähigkeit für den Betrieb mit sehr hohen Teilnehmerzahlen mit Massendaten und hoher Transaktionsrate, • Adaptionsfähigkeit an die eigenen Bedürfnisse, • Nutzungsmöglichkeit bestehender Sicherheits- und Komprimierungsverfahren, • konfliktfreie Nutzung weiterer Standards (z.B. http und https), • relativ einfache Realisierung des offiziellen Bundesstandards (veröffentlicht im Bundesanzeiger)
Authentifizierung und Identifizierung der Senderseite	• Identifizierung des Teilnehmers und des physikalischen Senders mittels Betriebsnummer; • Authentifizierung des physikalischen und logischen Senders mittels Client-Authentifizierung (https) und X.509 Zertifikat der ITSG
Benennung und Identifizierung der Empfängerseite	Identifizierung des physikalischen und des logischen Empfängers mittels Betriebsnummer

Merkmal	Ausprägung
Datenschutz, Vertraulichkeit und Integrität	• Die fachlichen Daten enthalten personenspezifische Informationen, deshalb ist eine End-zu-Ende Verschlüsselung erforderlich. • Datenfluss vom Sender zum Empfänger: Verschlüsselung durch den logischen Sender für den logischen Empfänger (DSRV). • Datenfluss vom Empfänger zum Sender: Verschlüsselung durch den logischen Empfänger (DSRV) für den logischen Sender. • Als Verschlüsselungsverfahren wird PKCS#7 verwendet, zusätzlich erzeugt die verschlüsselnde Instanz eine Signatur. • Dokumentation nach BSI Grundschutz.
Rollenverteilung	Für alle Prozesse ist die Rollenverteilung zwischen Arbeitgeber und DSRV, der Sender- und Empfängerseite einheitlich: Die Arbeitgeber haben immer die Rolle eines Senders, technisch eines Client, die DSRV immer die Rolle eines Empfängers, technisch eines Servers.
Klassifizierung der Teilnehmer	Auf Senderseite sind die Teilnehmer Unternehmen, die Sofortmeldungen abgeben müssen (gesetzliche Vorschrift nach Sozialgesetzbuch SGB), bzw. Dienstleister/Service-RZ im Auftrag der meldepflichtigen Unternehmen. Auf Empfängerseite ist es die Datenstelle der Rentenversicherung DSRV.
Registrierung der Teilnehmer	Ein teilnehmendes Unternehmen muss bei der Bundesagentur für Arbeit eine Betriebsnummer erwerben und – sofern es die Rolle eines physikalischen Senders einnimmt – bei der ITSG ein X.509 Zertifikat
Anzahl Teilnehmer auf Senderseite	**Sofortmeldungen**: Verpflichtende Teilnahme von Unternehmen bestimmter Branchen, insgesamt ca. 900.000 Arbeitgeber. **euBP**: Optionale Teilnahme

Merkmal	**Ausprägung**
Anzahl Teilnehmer auf Empfängerseite	1 physikalischer und logischer Empfänger: DSRV, 2 verwertende Fachverfahren (im Element Procedure der untersten eXTra-Ebene erkennbar)
Größe und Rolle der Teilnehmer auf Senderseite	Unternehmen jeder Größe; a) Unternehmen kann zugleich Erzeuger der Meldungen und physikalischer Sender sein. b) Rollen können verteilt werden zwischen erzeugendem Unternehmen und einem Service-RZ, das als logischer und physikalischer Sender für viele Unternehmen fungiert
Zulässige Transaktionsrate und Datenvolumen	Spitzenwerte werden um den Stichtag, sechstletzter Bankarbeitstag eines Monats erzielt, sowohl bei der Transaktionsrate als auch dem Datenvolumen. Pro Übermittlungsvorgang ist ein maximales Datenvolumen von 20 MB gestattet.
Topologie des Datenübermittlungsverbundes	Der Kommunikationsserver der DRV, die DSRV fungiert als physikalischer und logischer Empfänger, der die Nachrichten bzw. Daten an das entsprechende Fachverfahren weiterleitet bzw. von diesen die Verarbeitungsergebnisse erhält (Sternarchitektur). Alle Instanzen der Empfängerseite gehören der Rentenversicherung an.
Unterstützung der ExtraError Nachricht	Sofortmeldungen: nein euBP-Meldungen: ja
Übertragung großer Dateien, z.B. Unterstützung der MTOM-Funktionalität	nein
Verwendete PlugIns	Contacts, DataTransforms, DataSource
Empfangsquittung	ja, wegen scenario=request-with-acknowledgement
Unterstützung der eXTra AcknowledgementUpdate Funktion	Sofortmeldungen: Ja, Bezugspunkt ist die ResponseID der ursprünglichen Sendung von Sofortmeldungen euBP-Meldungen: nein
Unterstützung der eXTra RepeatResponse Funktion	Sofortmeldungen: nein euBP-Meldungen: ja

Merkmal	**Ausprägung**
Grundlage der Fachverfahren	Gesetzliche Grundlagen für die Sofortmeldungen für Unternehmen bestimmter Branchen gemäß Sozialgesetzbuch. Gesetzliche Grundlagen für die Betriebsprüfung; die Teilnahme am elektronischen Meldeverfahren euBP ist für Unternehmen freiwillig.
Anzahl Fachverfahren	2 Fachverfahren: Sofortmeldungen, elektronisch unterstützte Betriebsprüfung (euBP)
Betriebsmodell der Fachverfahren	Betriebsmodell der Sofortmeldungen und euBP: Sende-Hol-Bestätigungsbetrieb
Prozesse der beiden Fachverfahren	• Sendeprozess (1 Ebene bei Sofortmeldungen, 2 Ebenen bei euBP: Transport- und Nachrichten-Ebene) • Holprozess (1 Ebene mit der Standardnachricht DataRequest V1.3) • Bestätigungsprozess (1 Ebene mit der Standardnachricht ConfirmationOfRceipt V1.3)
Typus der Profilierung: Prozessübergreifende Profilierung (Schemadateien gelten für alle Prozesse) oder prozessspezifische Profilierung (Schemadateien gelten jeweils nur für einen Prozess)	Prozessspezifische Profilierung: Für den Sende-, Hol- und Bestätigungsprozess gibt es jeweils einen eigenen Satz von Schemadateien
Abgabereihenfolge der Meldungen	Pro Fachverfahren müssen die Meldungen lückenlos und streng aufsteigend abgegeben werden.
Meldepflicht der erzeugenden Teilnehmer	**Sofortmeldungen**: ja, für Unternehmen bestimmter Branchen, ereignisabhängig sofort zu melden (kein Stichtag für die Abgabe); **euBP**: nein
Holpflicht der Verarbeitungsergebnisse	ja, innerhalb von 40 Tagen
Verwendete eXTra-Standardnachrichten	DataRequest V1.3, ConfirmationOfRequest V1,3, ExtraError V1.0 (nur euBP)

3.2.1.4. Festlegung von Betriebsparametern und Merkmalen

Allgemeine Betriebsparameter und Merkmale der DFÜ-Ebene des Empfangssystems – Gegenstand der Festlegung	**Festlegung**
Verfügbarkeit des eXTra-Empfangssystems (z.B. 7 x 24 Stunden)	7 x 24 Stunden
Wartungszeitfenster des eXTra-Empfangssystems	Systemwartungen werden angekündigt
DFÜ-Protokoll	ab 1.1.2016 nur https mit dem X.509 Zertifikat der ITSG (clientseitig) und einem Standard-X.509 Zertifikat (serverseitig)
Zeitspanne (Wert des Timeout der DFÜ-Ebene) innerhalb der eine Empfangsbestätigung des Empfangssystems in der gleichen Anschaltung erfolgen muss (bei eXTra die eXTra-Response aufgrund eines eXTra-Request mit Scenario=Request-with-Acknowledgement)	Systemeinstellungen
Zeitspanne (Wert des Timeout der DFÜ-Ebene) innerhalb der eine Antwort des Fachverfahrens in der gleichen Anschaltung erfolgen muss (bei eXTra die eXTra-Response aufgrund eines eXTra-Request mit Scenario=Request-with-Response)	Systemeinstellungen
Die maßgebliche Uhr – welche Uhr ist maßgeblich, wenn die Uhren des Senders und Empfängers auseinander laufen?	die Uhr des DRV Kommunikationsservers

spezifische Betriebsparameter und Merkmale des eXTra Systems – Gegenstand der Festlegung	**Festlegung**
Sendebetrieb: Realisierung als Annahmetransaktion (alles oder nichts) oder als teilweise Annahme?	Realisierung als Annahmetransaktion (alles oder nichts)
Bedeutung eines Acknowledgements beim Sendeprozess. Welche Prozessschritte im eXTra-Empfangssystem werden damit bestätigt?	Empfang der Lieferung und Übernahme in die lokale Datenhaltung
Sendebetrieb: Zulässiges Maß an parallelen Sendeprozessen	nein
Sendebetrieb: Festlegung der maximalen Größe einer Lieferung (in MB bzw. Anzahl Paketen), eines Paketes (in MB bzw. in Anzahl Nachrichten) und einer Nachricht (in MB oder KB)	Ohne Einsatz von MTOM beträgt die maximale Größe einer Lieferung und eines Paketes 20 MB.
Sendebetrieb: Toleranzzeit, innerhalb derer Lücken in der Belieferung vom Sender geschlossen werden müssen (z.B. bei laufender Dateinummer)	keine
Sende- Holbetrieb: Zeitspanne nach der der Sender das Verarbeitungsprotokoll (die Rückmeldung) des verwertenden Fachverfahrens abholen kann	laufend
Parametrierung des Holprozesses, der Standardnachricht DataRequest V1.3:	**Sofortmeldungen**: Query mit den Elementen Argument und Control Argument mit @property=Procedure bzw @property=ResponseID und @event=SendData Control mit Kindelement MaximumPackages **euBP**: Query mit den Elementen Argument und Control Argument mit @property=Procedure bzw @property=ResponseID und @event=SendData oder RequestData Control mit Kindelement MaximumMessages

spezifische Betriebsparameter und Merkmale des eXTra Systems – Gegenstand der Festlegung	**Festlegung**
Holbetrieb: Zulässiges Maß an parallelen Holprozessen	nein
Holbetrieb: Festlegung der maximalen Größe einer Auslieferung (in MB bzw. Anzahl Paketen), eines bereitgestellten Paketes (in MB bzw. Anzahl von Nachrichten) bzw. Nachricht (in MB oder KB)	Die Rückmeldung – und damit der Umfang – bezieht sich immer auf das ursprüngliche Datenpaket des Sende-prozesses
Parametrierung des Bestätigungsprozesses, der Standardnachricht ConfirmationOfReceipt V1.3:	**Sofortmeldungen**: Nur Element PropertySet mit @name=ResponseID zulässig **euBP** kennt 2 Methoden der Bestätigung, die Einzelbestätigung jeder abgeholten Message (mittels Element PropertySet mit @name=ResponseID und 1-n ResponseIDs der 1-n Response MessageHeader) oder die Bulk-Bestätigung eines gesamten Abholvorgangs (mittels Element Property mit @name=ResponseID und der ResponseID des Response TransportHeaders, sowie dem Element Property)
Kann der Sender bereits abgeholte und ggfls. bereits bestätigte fachliche Nachrichten/Pakete erneut abholen?	bereits abgeholt: ja bereits bestätigt: nein
Bis zu welcher Instanz kann der Sender den Status seiner Nachrichten auf Empfängerseite mit der Standardnachricht StatusRequest nachverfolgen?	nicht unterstützt
Empfängerseite: Vorhaltezeitraum für bereitgestellte fachliche Nachrichten/Pakete. Wann muss der Sender spätestens abholen?	spätestens nach 40 Tagen, danach erfolgt Zustellung per E-Mail
Empfängerseite: Vorhaltezeitraum für bereits abgeholte und bestätigte fachliche Nachrichten/Pakete. Wie lange kann der Sender erneut abholen?	nicht unterstützt

3.2.1.5. Visualisierung der eXTra-Strukturen

Exemplarisch werden aus Sicht des physikalischen Senders der Sendeprozess fachlicher Daten zum DRV Kommunikationsserver (eine eXTra-Ebene bei den Sofortmeldungen, zwei eXTra-Ebenen bei euBP) und der Anforderungs/Holprozess von fachlichen Rückmeldungen (eine eXTra-Ebene) veranschaulicht. Basis ist die ab 1.1.2016 gültige Version V1.4.

Der Bestätigungsprozess wird auf Grund seiner einfachen Struktur nicht explizit gezeigt.

Sendeprozess Teil 1: eXTra-Request

Für den Sendeprozess von Sofortmeldungen bzw. euBP Meldungen ergeben sich folgende schematische Bilder der eXTra-Strukturen: Der Transport- und der Nachrichtenebene (nur bei euBP), sowie der zugehörigen Header:

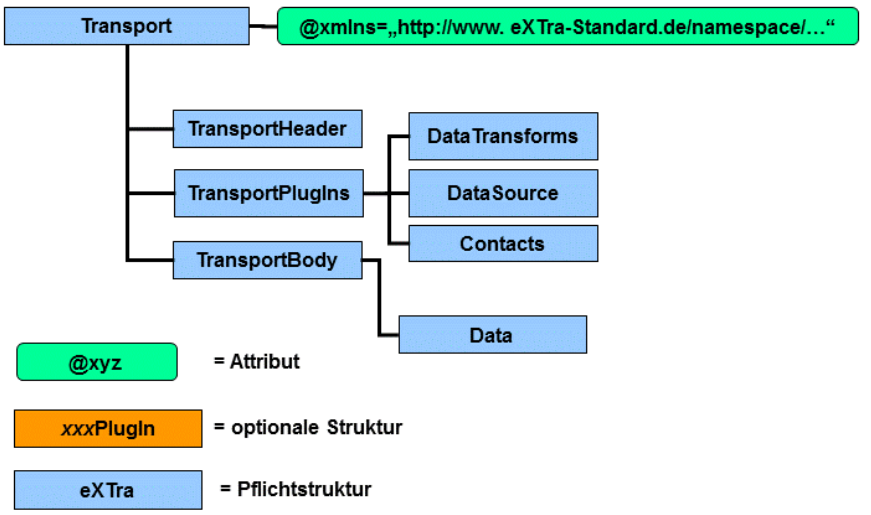

Bild 17: Die Ebenenstruktur des Sendeprozesses (eXTra-Request) mit Sofortmeldungen beim DRV Kommunikationsserver (eine Ebene, die Transportebene)

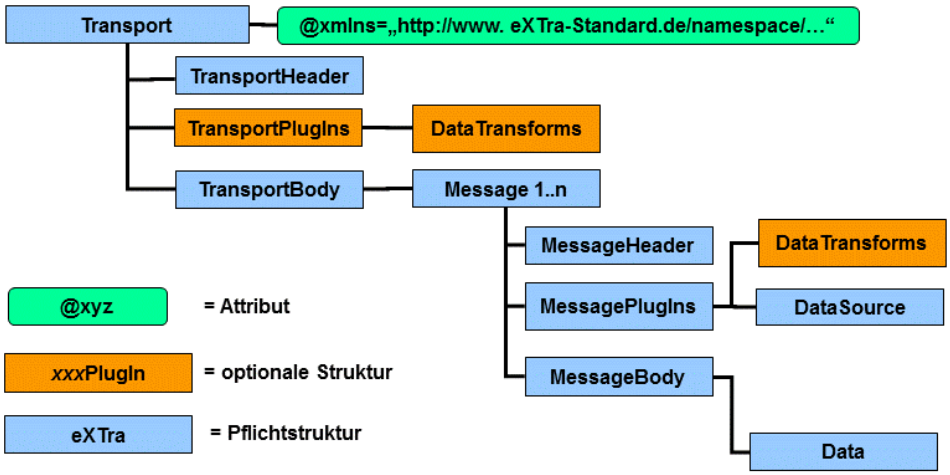

Bild 18: Die Ebenenstruktur des Sendeprozesses (eXTra-Request) mit euBP Meldungen beim DRV Kommunikationsserver (zwei Ebenen: Transport- und Nachrichtenebene)

Der Grund für die Nachrichtenebene ist der Wunsch des Fachverfahrens euBP, dass in einem Übermittlungsvorgang zwar die euBP Meldungen mehrerer Unternehmen gesendet werden können, aber dass die euBP Meldungen eines jeden Unternehmens in getrennten eXTra-Nachrichten – in eXTra Messages – unterschieden werden können.

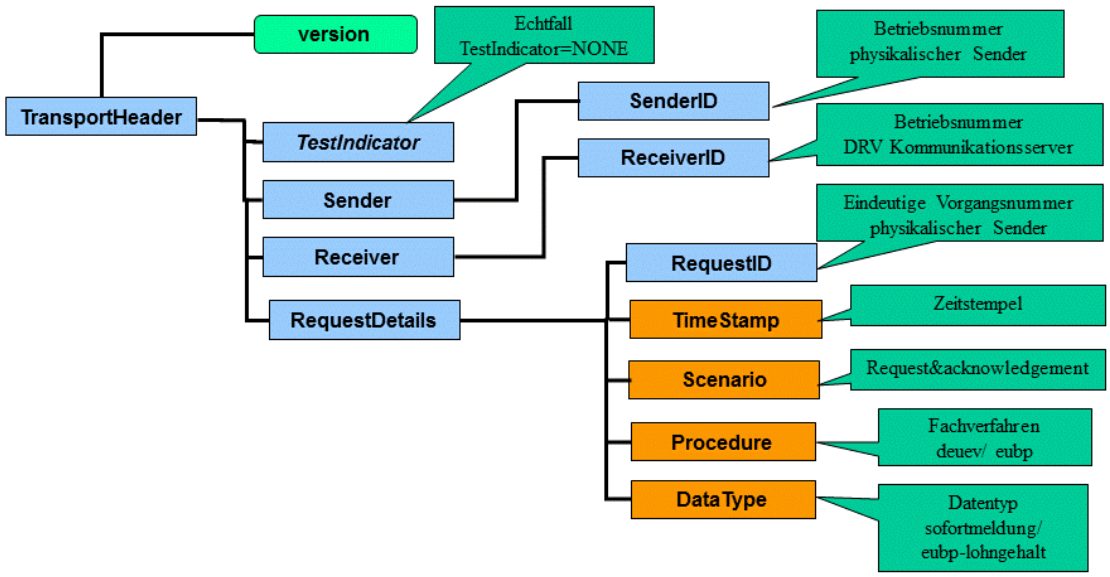

Bild 19: Der TransportHeader des Sendeprozesses (eXTra-Request) mit Sofortmeldungen oder euBP Meldungen beim DRV Kommunikationsserver (gilt für beide Fachverfahren)

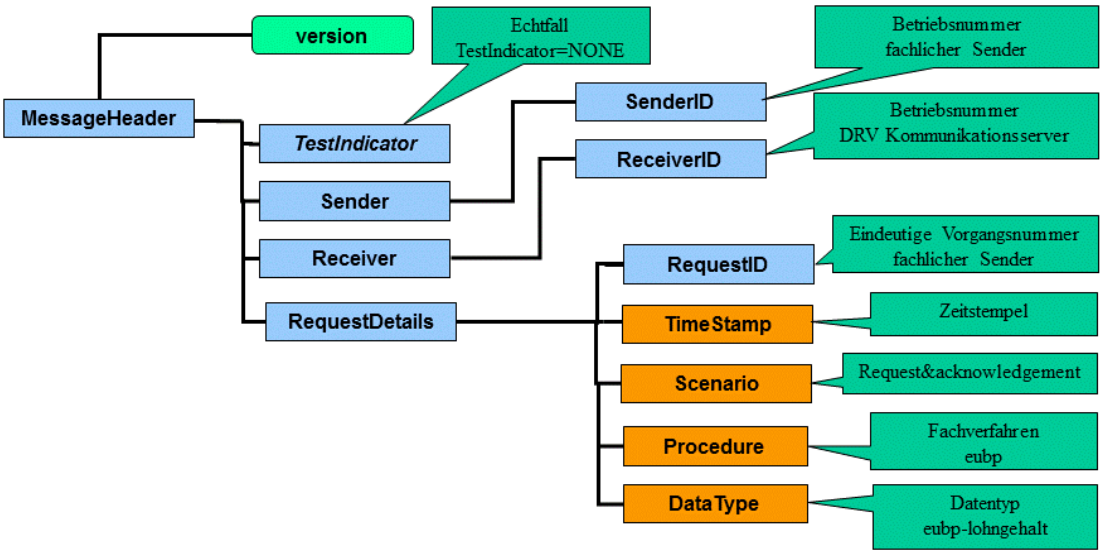

Bild 20: Der MessageHeader des Sendeprozesses (eXTra-Request), der nur bei den euBP Meldungen erforderlich ist (zwei Ebenen: Transport- und Nachrichtenebene).

Sendeprozess Teil 2: eXTra-Response

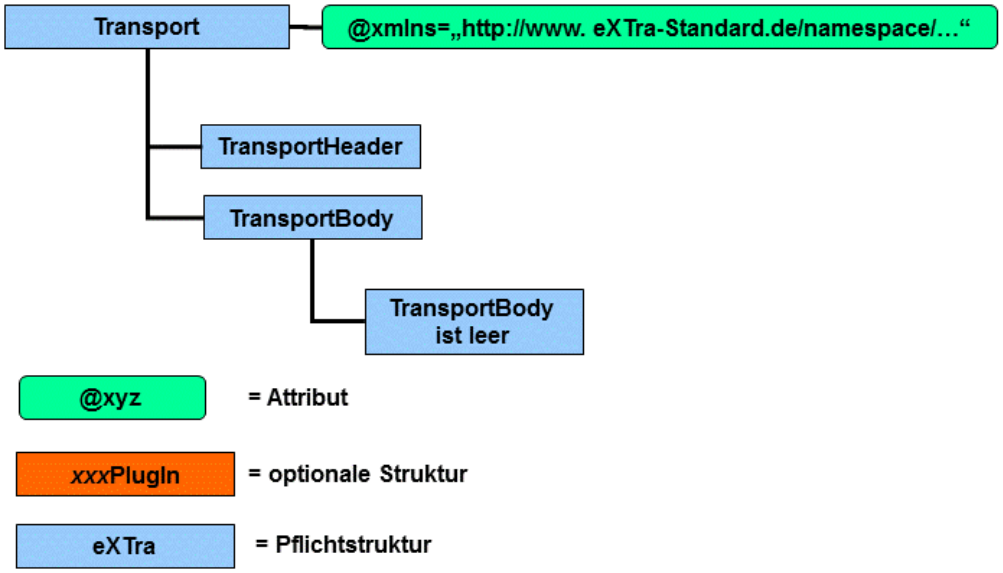

Bild 21: Die Ebenenstruktur des Sendeprozesses (eXTra-Response) beim DRV Kommunikationsserver „Senden von Sofortmeldungen“

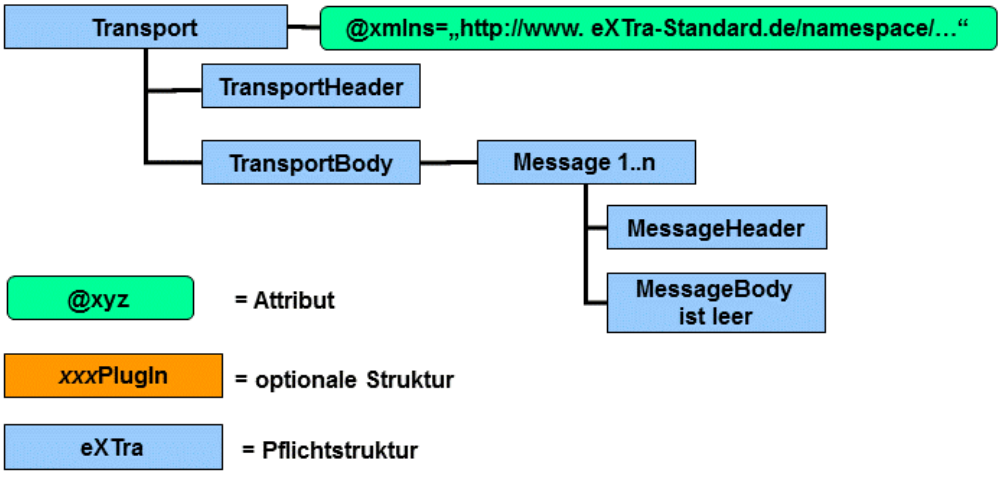

Bild 22: Die Ebenenstruktur des Sendeprozesses (eXTra-Response) beim DRV Kommunikationsserver „Senden von euBP-Meldungen“

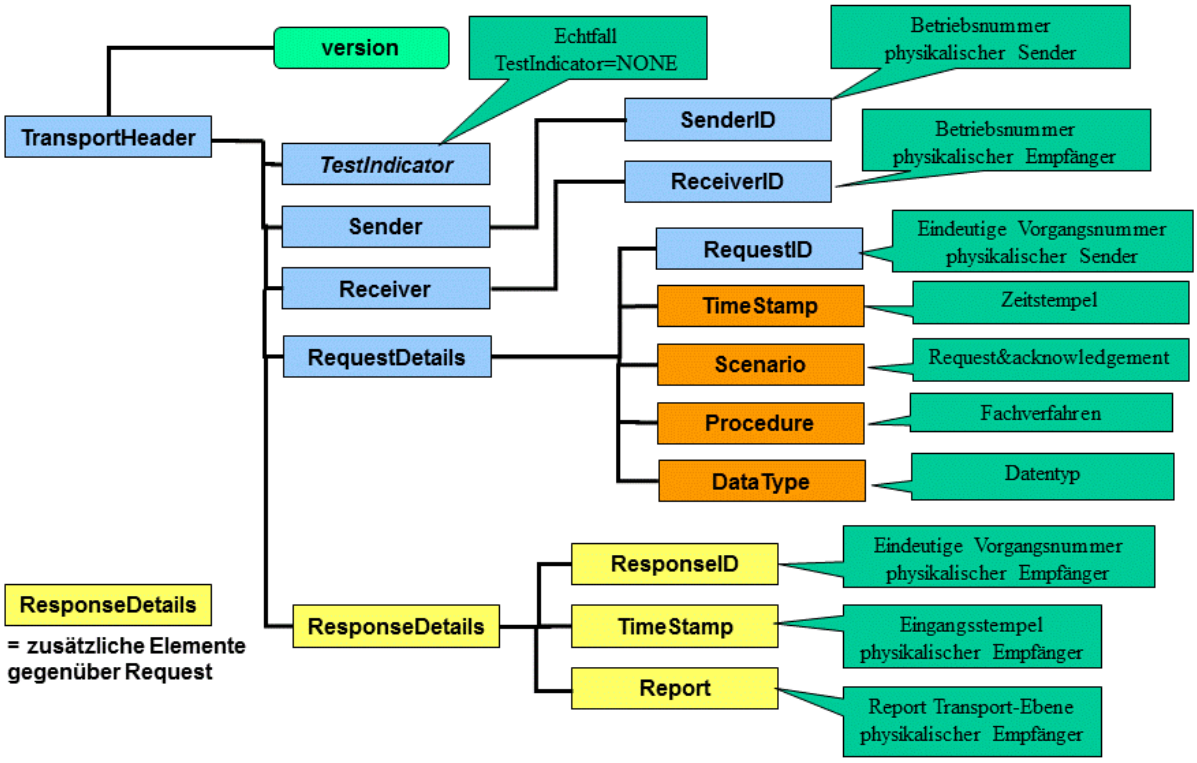

Bild 23: Der TransportHeader des Sendeprozesses (eXTra-Response) beim DRV Kommunikationsserver „Senden von Sofortmeldungen bzw. von euBP-Meldungen“

Der eXTra-Response MessageHeader des Sendeprozesses „Senden von euBP-Meldungen“ ist strukturell identisch zum eXTra-Response TransportHeader aufgebaut; die Angaben zu den einzelnen Elementen sind dem fachlichen Sender bzw. fachlichen Empfänger zugeordnet. Die relevanten Aussagen der Response sind in den ResponseDetails zu finden, insbesondere im Element Report (der Transport der Nachrichten war erfolgreich oder es trat ein Fehler auf).

Holprozess Teil 1: eXTra-Request

Für den Anforderungs-/Holprozess fachlicher Daten (Verarbeitungsergebnisse) ergeben sich folgende schematische Bilder der eXTra-Strukturen: Der eXTra-Ebene, der eXTra-Header, sowie der eXTra-Standardnachricht DataRequest der Version V1.3:

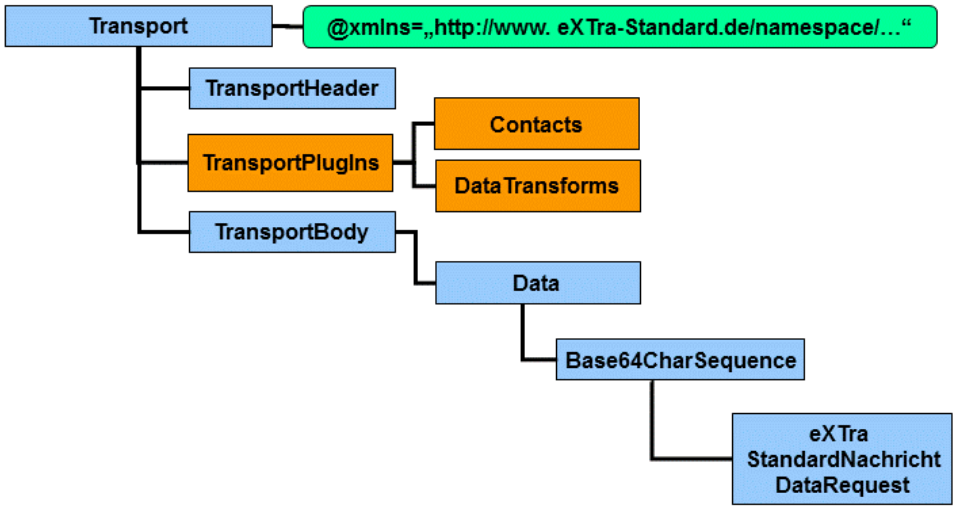

Bild 24: Die Ebenenstruktur des Holprozesses (eXTra-Request) beim DSRV Kommunikationsserver für beide Fachverfahren Sofortmeldungen und euBP-Meldungen.

Hinweis: Die Ebenenstruktur des Holprozesses ist analog zum GKV Kommunikationsserver ausgebildet.

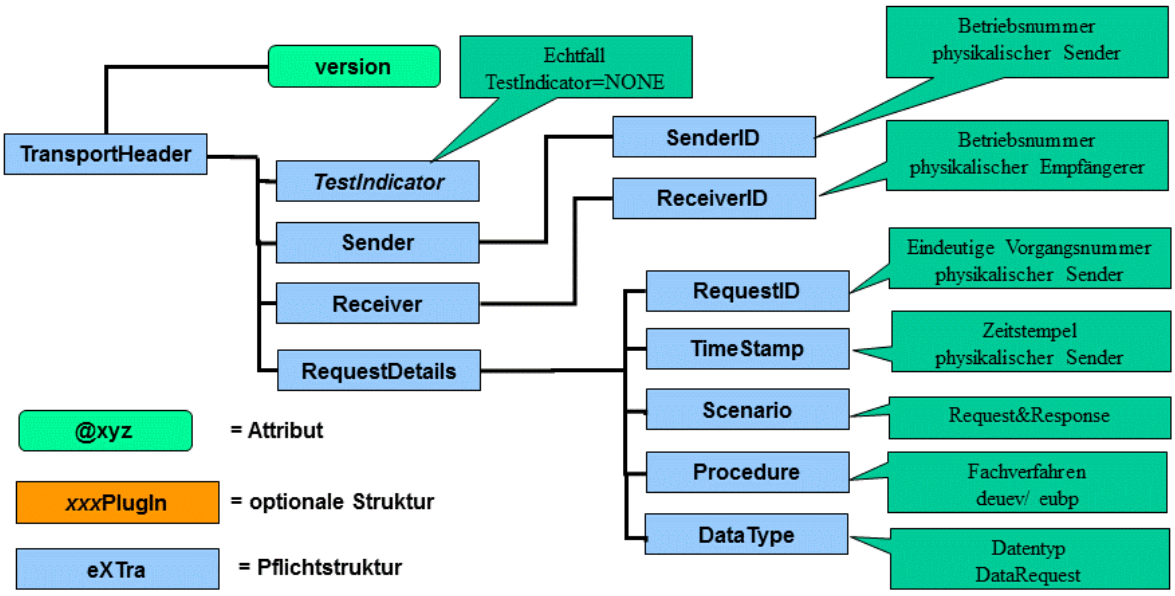

Bild 25: Der TransportHeader des Holprozesses (eXTra-Request) von Rückmeldungen zu Sofortmeldungen oder euBP Meldungen beim DSRV Kommunikationsserver

Hinweis: Der TransportHeader ist für beide Fachverfahren strukturell identisch.

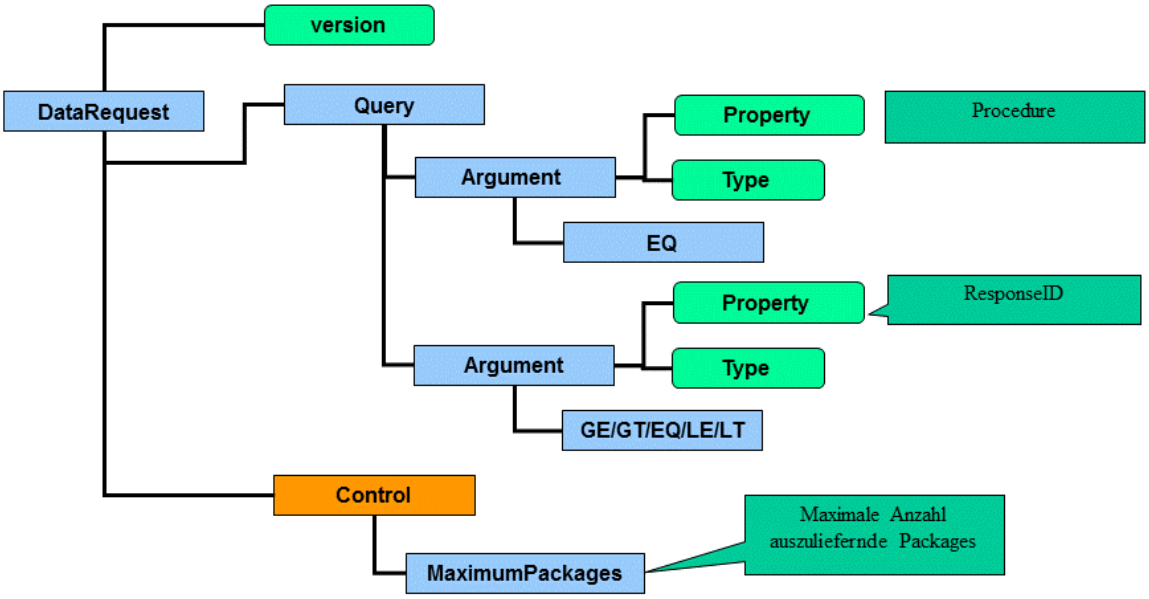

Bild 26: Die eXTra-Standardnachricht DataRequest beim DSRV-Kommunikationsserver Komfortable Ausprägung, weil die gewünschten Rückmeldungen genau spezifiziert bzw. eingegrenzt werden können (über die Folge von Arguments, sowie dem Property der ResponseID) und weil das Datenvolumen der so ausgelieferten fachlichen Daten vom Sender her (mit dem Element Control) eingeschränkt werden kann.

Holprozess Teil 2: eXTra-Response

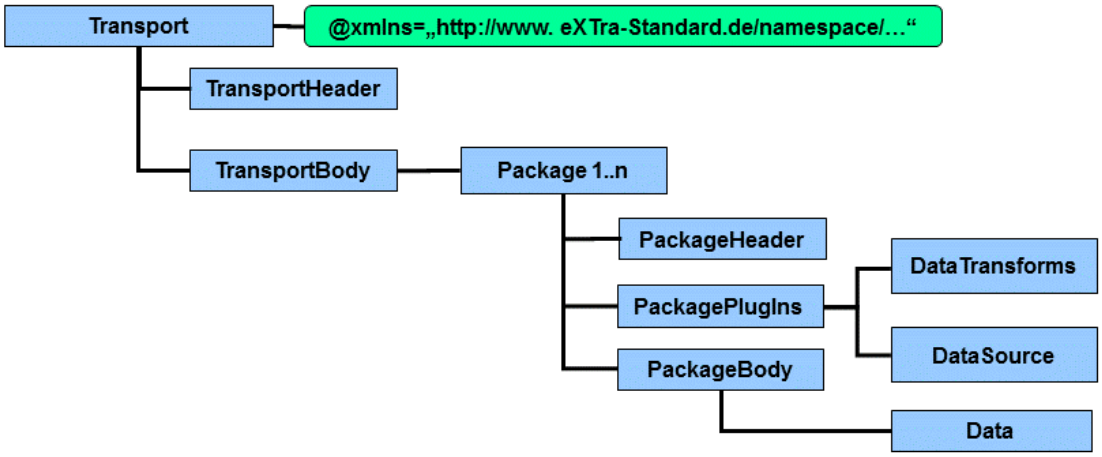

Bild 27: Die Ebenenstruktur des Holprozesses (eXTra-Response) beim DSRV Kommunikationsserver für das Fachverfahren Sofortmeldungen

Die fachlichen Rückmeldungen werden auf der Paket-Ebene zurückgegeben.

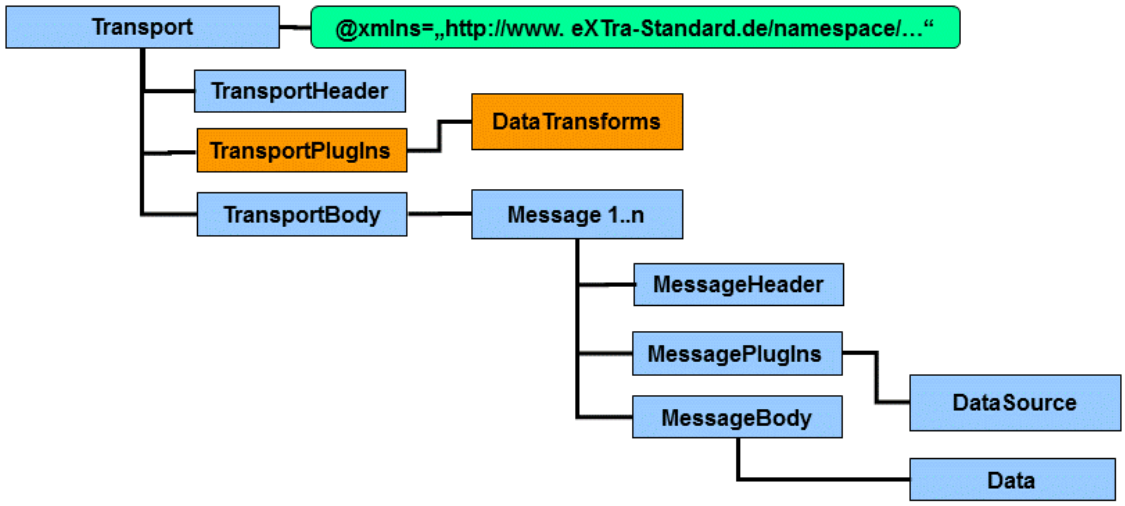

Bild 28: Die Ebenenstruktur des Holprozesses (eXTra-Response) beim DSRV Kommunikationsserver für das Fachverfahren euBP

Die fachlichen Rückmeldungen werden beim Fachverfahren euBP analog zum Sendeprozess auf der Nachrichten-Ebene zurückgegeben.

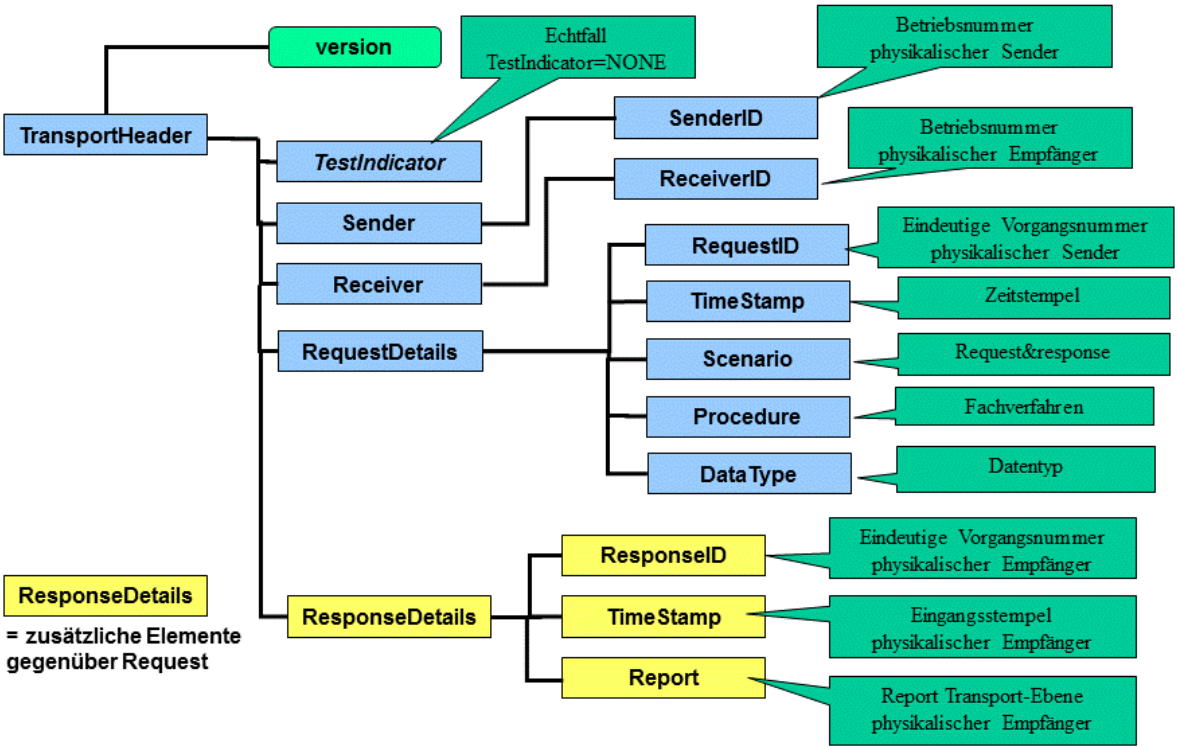

Bild 29: Der TransportHeader des Holprozesses (eXTra-Response) von fachlichen Rückmeldungen zu Sofortmeldungen oder euBP Meldungen beim DSRV Kommunikationsserver (gilt für beide Fachverfahren)

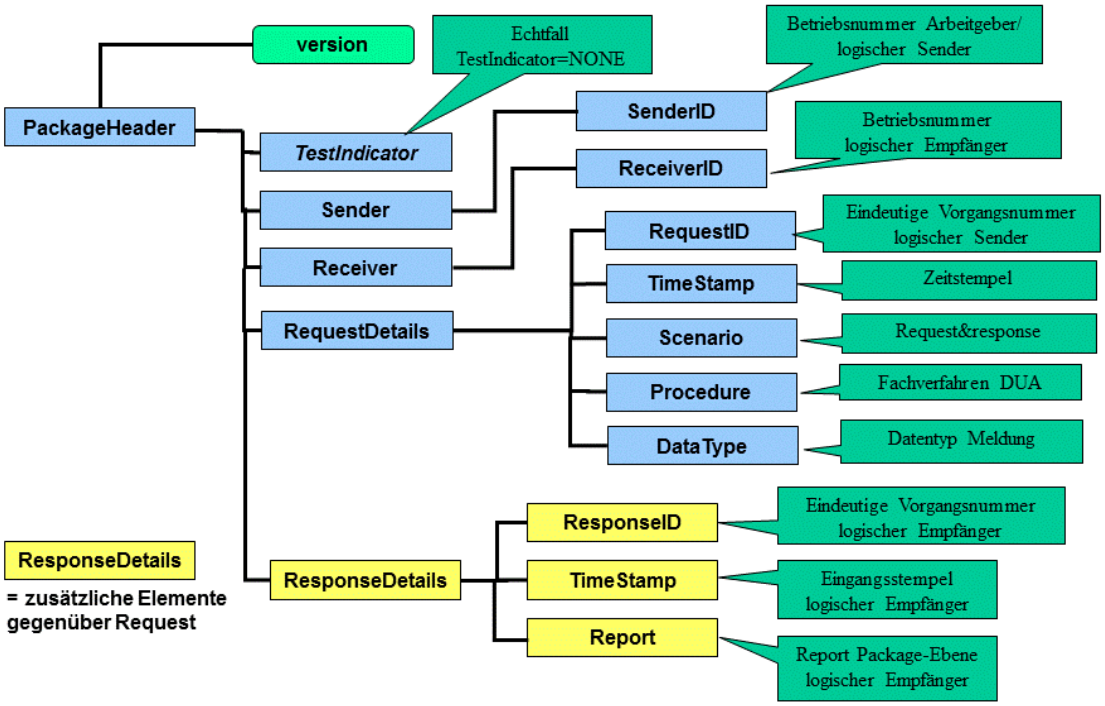

Bild 30: Der PackageHeader des Holprozesses (eXTra-Response) von Rückmeldungen zu Sofortmeldungen beim DSRV Kommunikationsserver

Beim Fachverfahren der elektronisch unterstützten Betriebsprüfung euBP ist der eXTra-Response MessageHeader strukturell identisch zum eXTra-Response PackageHeader der Sofortmeldungen. Die Angaben zu den einzelnen Elementen sind beim MessageHeader dem fachlichen Sender bzw. fachlichen Empfänger zugeordnet.

3.2.2. Der objektbasierte Datenaustausch der Rentenversicherung

3.2.2.1. Die zentrale Annahmestelle der DSRV, das System SPoC

Aufgrund der positiven Erfahrungen, die seit Einführung der Sofortmeldungen in 2009 inzwischen beim Betrieb mit eXTra-spezifischen Datenübermittlungsverfahren gewonnen werden konnten (u.a. mit den Sofortmeldungen, ELENA und der elektronisch unterstützten Betriebsmeldung), wurde bei der Rentenversicherung das System „Single Point of Contact“ (SPoC) für die eXTra-Annahme als zentrale Annahmestelle (Enterprise Service Bus) realisiert.

Als Zielsetzung soll das System SPoC generell für den objektbasierten Datentausch der verschiedenen Fachdienste dienen, sowohl innerhalb der Rentenversicherung als auch außerhalb mit externen Partnern.

Technische Details

Auf der DFÜ-Ebene kommen Webservices auf Basis von SOAP mit https zum Einsatz, die zur Kommunikation und Steuerung der Fachdienste mit dem eXTra-Standard verknüpft werden.

Die SPoC Applikation ist lauffähig auf den Web-Applikation-Servern WAS 8 bzw. JBoss 6.2. Als Datenhaltungssysteme werden wahlweise die Datenbanken Oracle V11, DB2/ZOs V10 und DB2/LUW V10.5 eingesetzt.

Als Basis wurde aufgrund der Unterstützung von MTOM eXTra der Version V1.3.1 verwendet[3].

Konsolidierung

Die bisherige Dialogisierung (Host-zu-Host-Kommunikation) bei der DSRV mit ca. 10 Fachverfahren soll im Zuge einer schrittweisen Konsolidierung sukzessive mit eXTra-Nachrichten und SPoC abgelöst werden, da die aktuelle Form der Dialogisierung verschiedene technologische Einschränkungen besitzt und für große Nachrichten nur bedingt geeignet ist. Als Beispiel für Fachdienste, welche mit großen Nachrichten umgehen müssen, wurden eAntrag und eAkte genannt.

3.2.2.2. Vorteile des Systems Single Point of Contacts SPoC

Durch die Webservice orientierte Architektur der eXTra Kommunikation des SPoC eXTra-Servers ist eine einfache Einbindung weiterer Fachdienste in den SPoC eXTra-Server bei der DSRV möglich. Bei neuen Fachdiensten ist keine Neuinstallation notwendig. Eine standardisierte Kommunikation und Steuerung der Fachdienste anhand des Bundesstandards eXTra ist gegeben. Hierdurch wird eine performante und objektbasierte Kommunikation ermöglicht. Die Host-Host Kommunikation der Dialogisierung innerhalb der Rentenversicherung kann im Zuge einer schrittweisen Konsolidierung auf die Webservice orientierte Architektur und damit auf den SPoC eXTra-Server umgestellt werden.

Das eXTra-Nachrichten-Schema lässt seit eXTra V1.3.1 mittlerweile MTOM-Attachments zu, die bei großen Nachrichten verwendet werden sollten.

[3] eXTra V1.3.1 ist inhaltsgleich zu eXTra V1.4. eXTra V1.3.1 musste formal deshalb verwendet werden, weil zum Realisierungszeitpunkt des SPoC eXTra V1.4 noch nicht freigegeben war.

3.2.2.3. Die Topologie der Datenübermittlungsverbünde der DRV

Die Topologie der Datenübermittlungsverbünde der Deutschen Rentenversicherung DRV innerhalb der Rentenversicherung sowie mit externen Partnern unter Einbezug des SPoC ist gegenüber der Topologie der Sofortmeldungen (3.2.1.2) unverändert.

3.2.2.4. Das Beispiel des Sterbedatenaustauschs Ausland

Aktuell werden von deutscher Seite ein elektronischer Sterbedatenabgleich mit Israel, Italien, Luxemburg, Österreich, den Niederlanden, der Schweiz und Spanien durchgeführt. Im Verhältnis zu diesen Staaten wird daher auf die jährliche Lebensbescheinigung verzichtet. Dies ist einerseits eine Erleichterung für die Rentner, andererseits verringert sich der Verwaltungsaufwand. Ferner wird das Risiko der Überzahlung verringert, da der Abgleich zeitnah zur Rentenauszahlung vorgenommen wird.
Durch § 119 Sozialgesetzbuch -Gesetzliche Rentenversicherung- (SGB VI) ist die Deutsche Post AG vom Gesetzgeber ausdrücklich ermächtigt, die Renten der gesetzlichen Rentenversicherung auszuzahlen. Darüber hinaus bietet sich der Renten Service als kompetentes Dienstleistungsunternehmen an. Der „Deutsche Post Renten Service“ führt über die Datenstelle der Träger der Rentenversicherung (DSRV) den Sterbedatenabgleich mit dem Ausland über den eXTra-Standard durch.

3.2.2.4.1. Steckbrief

Der Datenübermittlungsverbund der deutschen Rentenversicherung DRV mit dem Deutschen Post Rentenservice (DPRS) hat folgende charakteristische Merkmale:

Merkmal	**Ausprägung**
Maßgebliches Gremium	Gremien der DRV
Typus für den Einsatz von eXTra	Datenübermittlungsverbund der DRV mit DPRS; Übernahme des Sicherheitsverfahrens mit X.509 Zertifikat (Aussteller ist die ITSG) für die Authentifizierung und Verschlüsselung; Übernahme der Komprimierungsverfahren, SPoC Enterprice Bus eXTra mit Fachdiensten
Auslösendes Moment für eXTra	standardisierte Kommunikation mit Webservice und SPoC Enterprice Bus bei der DSRV; einfacher automatischer Betrieb

Merkmal	**Ausprägung**
Authentifizierung und Identifizierung der Senderseite	Identifizierung des Teilnehmers und des physikalischen Senders mittels Betriebsnummer; Authentifizierung des physikalischen und logischen Senders mittels Client-Authentifizierung (https) und X.509 Zertifikat der ITSG
Benennung und Identifizierung der Empfängerseite	Identifizierung des physikalischen und des logischen Empfängers mittels Betriebsnummer
Datenschutz; Vertraulichkeit und Integrität	Die fachlichen Daten enthalten personenspezifische Informationen, deshalb ist eine End-zu-Ende Verschlüsselung erforderlich. Datenfluss vom Sender zum Empfänger: Verschlüsselung durch den logischen Sender für den logischen Empfänger (DSRV). Datenfluss vom Empfänger zum Sender: Verschlüsselung durch den logischen Empfänger (DSRV) für den logischen Sender. Gemäß spezifischer Vereinbarung mit DPRS wird als Verschlüsselungsverfahren per Default PKCS#7 verwendet (deshalb ist das PlugIn DataTransforms explizit nicht erforderlich), zusätzlich erzeugt die verschlüsselnde Instanz eine Signatur. Dokumentation nach BSI Grundschutz.
Rollenverteilung	Für alle Prozesse ist die Rollenverteilung zwischen DPRS und DSRV, der Sender- und Empfängerseite einheitlich: Der DPRS hat immer die Rolle eines Senders, technisch eines Client, die DSRV immer die Rolle eines Empfängers, technisch eines Servers.
Klassifizierung der Teilnehmer	auf Senderseite DPRS; als Empfänger die DSRV
Registrierung der Teilnehmer	spezifische Vereinbarung mit der DSRV
Anzahl Teilnehmer auf Senderseite	1 Teilnehmer, der DPRS. Perspektivisch die 7 ausländischen Fachverfahren

Merkmal	Ausprägung
Anzahl Teilnehmer auf Empfängerseite	1 physikalischer und logischer Empfänger: DSRV, 2 verwertende Fachverfahren (im Element Procedure der untersten eXTra-Ebene erkennbar)
Größe und Rolle der Teilnehmer auf Senderseite	DPRS
Zulässige Transaktionsrate und Datenvolumen	Vereinbarung DSRV mit DPRS. Durch MTOM Technologie Massendaten in einer fachlichen Nachricht möglich (bis ca. 140 MB)
Topologie des Datenübermittlungsverbundes	Der Kommunikationsserver der DRV, die DSRV fungiert als physikalischer und logischer Empfänger, der die Nachrichten/ Daten an das entsprechende Fachverfahren weiterleitet bzw. von diesen die Verarbeitungsergebnisse erhält (Sternarchitektur). Alle Instanzen der Empfängerseite gehören der Rentenversicherung an.
Unterstützung der ExtraError Nachricht	ja
Übertragung großer Dateien, z.B. Unterstützung der MTOM-Funktionalität	ja, Unterstützung von MTOM
Verwendete PlugIns	DataSource
Empfangsquittung	ja, wegen scenario=request-with-acknowledgement
Unterstützung der eXTra AcknowledgementUpdate Funktion	ja, in den ResponseDetails, Kindelement Report, Kindelement Flag, Kindelement Originator wird die ResponseID als Bezugspunkt des ursprünglichen Acknowledgements zurückgegeben
Unterstützung der eXTra RepeatResponse Funktion	nein
Grundlage der Fachverfahren	spezifische Vereinbarung DSRV mit DPRS
Anzahl Fachverfahren	zurzeit 2 Fachverfahren: Sterbedatenabgleich und Sterbequartalsvorschuss
Betriebsmodell der Fachverfahren	Sende-Hol-Bestätigungsbetrieb

Merkmal	**Ausprägung**
Prozesse der beiden Fachverfahren	Sendeprozess (1 Ebene) Holprozess (1 Ebene mit der Standardnachricht DataRequest) Bestätigungsprozess (1 Ebene mit der Standardnachricht ConfirmationOfRceipt)
Typus der Profilierung: prozessübergreifende Profilierung (die Schemadateien gelten für alle Prozesse) oder prozessspezifische Profilierung (die Schemadateien gelten jeweils nur für einen Prozess)	Prozessspezifische Profilierung: Für den Sende-, Hol- und Bestätigungsprozess gibt es jeweils einen eigenen Satz von Schemadateien
Abgabereihenfolge der Meldungen	Pro Fachverfahren müssen die Meldungen lückenlos und streng aufsteigend abgegeben werden (mittels PlugIn DataSource).
Meldepflicht der erzeugenden Teilnehmer	spezifische Vereinbarung DSRV mit DPRS
Holpflicht der Verarbeitungsergebnisse	ja, 3 mal am Tag (Vereinbarung DSRV mit DPRS)
Verwendete eXTra Standardnachrichten	DataRequest V1.3, ConfirmationOfRequest V1.3, ExtraError V1.0

3.2.2.4.2. Festlegung von Betriebsparametern und Merkmalen

Allgemeine Betriebsparameter und Merkmale der DFÜ-Ebene des Empfangssystems – Gegenstand der Festlegung	**Festlegung**
Verfügbarkeit des eXTra-Empfangssystems (z.B. 7 x 24 Stunden)	7 x 24 Stunden
Wartungszeitfenster des eXTra-Empfangssystems	Systemwartungen werden angekündigt
DFÜ-Protokoll	Webservice auf Basis von SOAP mit https und dem X.509 Zertifikat der ITSG (clientseitig)

Allgemeine Betriebsparameter und Merkmale der DFÜ-Ebene des Empfangssystems – Gegenstand der Festlegung	**Festlegung**
Zeitspanne (Wert des Timeout der DFÜ-Ebene) innerhalb der eine Empfangsbestätigung des Empfangssystems in der gleichen Anschaltung erfolgen muss (bei eXTra die eXTra-Response aufgrund eines eXTra-Request mit Scenario=Request-with-Acknowledgement)	Systemeinstellungen
Zeitspanne (Wert des Timeout der DFÜ-Ebene) innerhalb der eine Antwort des Fachverfahrens in der gleichen Anschaltung erfolgen muss (bei eXTra die eXTra-Response aufgrund eines eXTra-Request mit Scenario=Request-with-Response)	Systemeinstellungen
Die maßgebliche Uhr – welche Uhr ist maßgeblich, wenn die Uhren des Senders und Empfängers auseinander laufen?	die Uhr des DRV Kommunikationsservers

spezifische Betriebsparameter und Merkmale des eXTra Systems – Gegenstand der Festlegung	**Festlegung**
Sendebetrieb: Realisierung als Annahmetransaktion (alles oder nichts) oder als teilweise Annahme?	alles oder nichts
Bedeutung eines Acknowledgements beim Sendeprozess. Welche Prozessschritte im eXTra-Empfangssystem werden damit bestätigt?	Empfang der Lieferung und Übernahme in die lokale Datenhaltung
Sendebetrieb: Zulässiges Maß an parallelen Sendeprozessen	nein
Sendebetrieb: Festlegung der maximalen Größe einer Lieferung (in MB bzw. Anzahl Paketen), eines Paketes (in MB bzw. in Anzahl Nachrichten) und einer Nachricht (in MB oder KB)	Einsatz von MTOM beträgt die maximale Größe einer Lieferung und eines Paketes 140 MB
Sendebetrieb: Toleranzzeit, innerhalb derer Lücken in der Belieferung vom Sender geschlossen werden müssen (z.B. bei laufender Dateinummer)	keine

spezifische Betriebsparameter und Merkmale des eXTra Systems – Gegenstand der Festlegung	**Festlegung**
Sende- Holbetrieb: Zeitspanne nach der der Sender das Verarbeitungsprotokoll (die Rückmeldung) des verwertenden Fachverfahrens abholen kann	laufend
Holbetrieb: Zulässiges Maß an parallelen Holprozessen	nein
Holbetrieb: Festlegung der maximalen Größe einer Auslieferung (in MB bzw. Anzahl Paketen), eines bereitgestellten Paketes (in MB bzw. Anzahl von Nachrichten) bzw. Nachricht (in MB oder KB)	Rückmeldung bezieht sich immer auf das Datenpaket des Senders
Kann der Sender bereits abgeholte und ggfls. bereits bestätigte fachliche Nachrichten/Pakete erneut abholen?	nein
Bis zu welcher Instanz kann der Sender den Status seiner Nachrichten auf Empfängerseite mit der Standardnachricht StatusRequest nachverfolgen?	nicht unterstützt
Empfängerseite: Vorhaltezeitraum für bereitgestellte fachliche Nachrichten/Pakete. Wann muss der Sender spätestens abholen?	nach Vereinbarung
Empfängerseite: Vorhaltezeitraum für bereits abgeholte und bestätigte fachliche Nachrichten/Pakete. Wie lange kann der Sender erneut abholen?	nicht unterstützt

3.2.2.4.3. Visualisierung der eXTra-Strukturen

Die Ebenen-Struktur des Sende-, Hol- und Bestätigungsprozesses ist identisch zur Ebenen-Struktur der Sofortmeldungen; ebenso die Struktur der Transport-Ebene (mit der Ausnahme, dass die PlugIns DataTransforms und Contacts nicht verwendet werden) und des TransportHeaders (3.2.1.5).

3.3. Datenübermittlungsverbund der Unfallversicherung

3.3.1. Die Wahl von eXTra als Standard

Dem Problem vielfältiger und unterschiedlicher Datenübermittlungsverfahren in der Unfallversicherung soll durch Standardisierung und Harmonisierung begegnet werden. Im Zuge der Weiterentwicklung einer übergreifenden Software-Architektur auf Basis eines gemeinsamen Architekturmodells, dem sog. „Tempelmodell“ mit ihrer Integrationsschicht, ist das Ziel die Standardisierung der Übertragungswege und die Harmonisierung von Daten sicher zu stellen, sodass der Transportmechanismus für beliebige Fachverfahren unter Einhaltung von Sicherheitsaspekten vereinheitlicht wird. Beim XUV-Datenübermittlungsverbund kommen XUV-konforme Webservices zum Einsatz, wobei der Nachrichtenaufbau durch die Verwendung des Webservice SOAP Protokolls weitgehend vorgegeben und standardisiert ist. Beim Nachrichtenaustausch gibt es für den Nachrichtenaufbau jedoch keine vergleichbar etablierten Standards, so dass ohne Vorgabe jedes Verfahren seinen eigenen Nachrichtenaufbau definieren kann. Um dies zu verhindern und den Nachrichtenaufbau zu standardisieren wurde der eXTra-Standard ausgewählt und eigens profiliert. Der eXTra-Standard hat bereits weite Verbreitung in der Sozialversicherung, so dass auch im zukünftigen Nachrichtenaustausch innerhalb der Sozialversicherung Synergieeffekte erzielt werden können. Er definiert neben dem eigentlichen Nachrichtenaufbau auch die Kommunikationsmuster und die Transporteigenschaften.

3.3.2. Die Topologie des XUV-Datenübermittlungsverbundes

Die Topologie des XUV-Datenübermittlungsverbundes der Unfallversicherung wird mit einem sog. UV-Bus in der Rolle als zentrale Vermittlungsstelle zwischen allen Teilnehmern realisiert.

Die schematische Darstellung des XUV-Datenübermittlungsverbundes ergibt folgendes Bild:

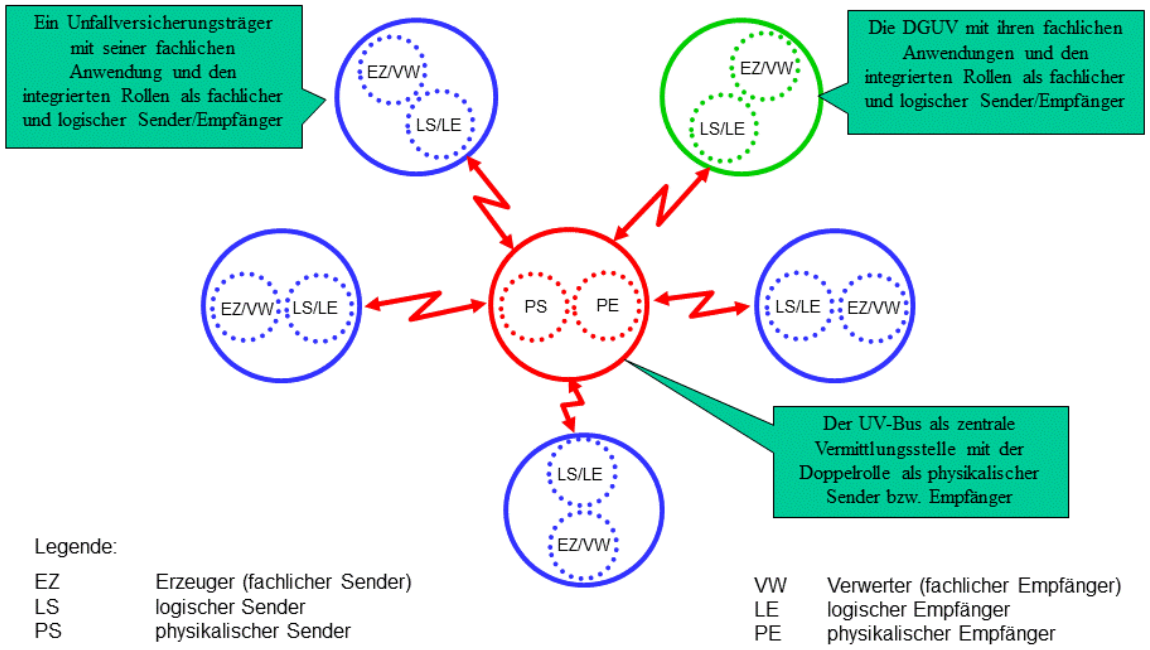

Bild 31: Die Topologie des XUV-Datenübermittlungsverbundes der Unfallversicherung mit UV-Bus

3.3.3. Das Vorgehensmodell des XUV-Datenübermittlungsverbundes

Der XUV-Datenübermittlungsverbund hat ein differenziertes Vorgehensmodell entwickelt, das in drei Dokumenten unter [VMXUV] anschaulich niedergelegt ist: Die organisatorischen Rahmenbedingungen sind dort im Begleitdokument zum XUV Standard 1.0 zu finden; zudem eine Anleitung, wie man XUV-Webservices von der Planung bis zur Implementierung gestaltet sowie eine Darstellung des Nachrichtenaustauschs mit den Anforderungen und Aufgaben beim Sender und beim Empfänger.

3.3.4. Steckbrief

Der Datenübermittlungsverbund der Unfallversicherung, der XUV-Standard hat folgende charakteristische Merkmale:

Merkmal	Ausprägung
Maßgebliches Gremium	XUV-Board, u.a. zuständig für die Registrierung von Teilnehmern, Pflege und Weiterentwicklung des XUV-Standards und der Codelisten, Prüfung von Fachverfahren und Diensten auf XUV-Konformität
Typus für den Einsatz von eXTra	Neuentwicklung eines eXTra-spezifischen Datenübermittlungsstandards, des XUV-Standards; z.T. Migration bestehender Datenübermittlungsverfahren hin zu eXTra
Auslösendes Moment für eXTra	Derzeit gibt es keinen international etablierten Standard für den Nachrichtenaufbau beim Nachrichtenaustausch. Dies leistet jedoch der eXTra-Standard, der zudem mit weiteren internationalen Standards, z.B. den WS-* Standards gekoppelt werden kann. Weiterhin ist eXTra in der Sozialversicherung weit verbreitet, was Synergieeffekte ermöglicht.
Authentifizierung und Identifizierung der Senderseite	Authentifizierung: Mittels Signatur und X.509 Zertifikaten Identifizierung: SenderID/ReceiverID mittels vollqualifiziertem Domain-Namen des Teilnehmers (Sender wie Empfänger)
Datenschutz; Vertraulichkeit und Integrität der fachlichen Nachrichten	Datenschutz ist geboten, da die fachlichen Nachrichten personenspezifische Informationen enthalten; Vertraulichkeit: Verschlüsselung der fachlichen Nachrichten im eXTra TransportBody gemäß XML-Encryption, asymmetrisch mittels RSA V1.5 und X.509-Zertifikaten und symmetrisch mit AES 256 Bit Integrität: TransportHeader wie auch TransportBody werden gemäß XML-Signature signiert, mit RSA-SHA512
Rollenverteilung	Bedingt durch das Betriebsmodell des beiderseitigen einfachen Sendebetriebs kann ein Teilnehmer beide Rollen einnehmen, die des Client und die des Servers
Klassifizierung der Teilnehmer	Teilnehmer des XUV-Verbundes können primär aus der Unfallversicherung kommen, aus den Unfallversicherungsträgern und der DGUV. Die Ausweitung auf externe Teilnehmer ist geplant.
Registrierung der Teilnehmer	Die Registrierung der Teilnehmer muss beim XUV Board erfolgen, u.a. mit seinem X.509-Zertifikat.

Merkmal	Ausprägung
Anzahl Teilnehmer des XUV-Verbundes	In der Unfallversicherung gibt es neben der DGUV 38 Unfallversicherungsträger und beliebig viele externe Teilnehmer.
Größe und Rolle der Teilnehmer	Der Sender hat immer die Client-Rolle, der Empfänger immer die Server-Rolle. Ein Teilnehmer kann beide Rollen einnehmen.
Topologie des XUV-Datenübermittlungsverbundes	Ein UV-Bus als zentrale Vermittlungsstelle ist geplant.
Unterstützung der ExtraError Nachricht	ja
Übertragung großer Dateien, z.B. Unterstützung der MTOM-Funktionalität	nein
Verwendete eXTra PlugIns	keine Verwendung von PlugIns
Unterstützung der eXTra AcknowledgementUpdate Funktion	nicht relevant wegen scenario=fire-and-forget im eXTra TransportHeader
Empfangsquittung	Die positive Empfangsquittung erfolgt auf DFÜ-Ebene mittels http-Response 200, die negative mittels ExtraError und spezifischem Statuscode.
Betriebsmodell der Fachverfahren	Je nach Fachverfahren das Betriebsmodell des „einfachen Sendebetriebs“, oder des „beiderseitigen einfachen Sendebetriebs“
Prozesse der Fachverfahren	nur Sendeprozess
Verwendete eXTra-Standardnachrichten	keine Verwendung von Standardnachrichten
Typus der Profilierung: Prozessübergreifende Profilierung (die Schemadateien gelten für alle Prozesse) oder prozessspezifische Profilierung (die Schemadateien gelten jeweils nur für einen Prozess)	Da es nur einen Prozess, den Sendeprozess gibt, ist die Frage irrelevant.

Merkmal	**Ausprägung**
Abgabereihenfolge der Meldungen: Muss die Belieferung eines Fachverfahrens in einer bestimmten Reihenfolge, z.B. lückenlos in streng aufsteigender Reihenfolge erfolgen?	fachverfahrensspezifisch
Meldepflicht der erzeugenden Teilnehmer	Meldepflicht für alle angebundenen Fachverfahren: ja beim XUV-Board
Bringpflicht der Antwort des verwertenden Teilnehmers	Bringpflicht für alle angebundenen Fachverfahren: nein (Nachrichtenaustausch), ja (Webservice)

3.3.5. Festlegung von Betriebsparametern und Merkmalen

Allgemeine Betriebsparameter und Merkmale der DFÜ-Ebene des Empfangssystems – Gegenstand der Festlegung	**Festlegung**
Mindest-Verfügbarkeit eines eXTra-Empfangssystems eines Teilnehmers (z.B. 5 x 12 Stunden) Verfügbarkeit des UV-Busses, (z.B. 7 x 24 Stunden)	Bei Webservice sehr hoch. Bei Nachrichtenaustausch werden die Nachrichten auf dem UV-BUS dem Empfangssystem zur Abholung bereitgestellt. Der UV-BUS: 7x24 Stunden
Wartungszeitfenster, individuelle Regelung pro Teilnehmer oder gemeinsame Regelung Wartungszeitfenster des UV-Busses	Gemeinsame Regelung: In Summe 8h pro Quartal.
DFÜ-Protokoll	Webservice auf Basis von SOAP und REST mit https
Zeitspanne des DFÜ-Systems (Wert des Timeout auf https-Ebene) innerhalb der eine Response erfolgen muss, z.B. eine http-response 200	

spezifische Betriebsparameter und Merkmale des eXTra Systems – Gegenstand der Festlegung	**Festlegung**
Sendebetrieb: Realisierung als Annahmetransaktion (alles oder nichts) oder als teilweise Annahme?	Alles oder nichts.
Bedeutung eines Acknowledgements beim Sendeprozess. Welche Prozessschritte im eXTra-Empfangssystem werden damit bestätigt?	Nicht relevant wegen scenario=fire-and-forget. Durch den http-response 200 wird bestätigt, dass die Nachricht signiert und XUV-konform ist, der Sender/ Empfänger registriert sind und die Nachricht dem Empfänger bereitgestellt wird.
Sendebetrieb: Zulässiges Maß an parallelen Sendeprozessen an einen physikalischen Empfänger	Aktuell keine Einschränkung
Sendebetrieb: Festlegung der maximalen Größe einer Lieferung	Der Sendeprozess beinhaltet immer nur eine einzige fachliche Nachricht an ein spezifisches Fachverfahren; die maximale Größe einer fachlichen Nachricht beträgt je nach Fachverfahren 20 MB
Beiderseitiger Sendebetrieb: Zeitspanne nach der das verwertende Fachverfahren spätestens seine Antwort, z.B. das Verarbeitungsprotokoll an den ursprünglichen Sender versendet	Nicht relevant wegen scenario=fire-and-forget.

3.3.6. Visualisierung der eXTra-Strukturen

Exemplarisch wird aus Sicht des physikalischen Senders der Sendeprozess fachlicher Daten (eine eXTra-Ebene) mit seinen eXTra-Strukturen zum physikalischen Empfänger, bzw. zum UV-Bus veranschaulicht.

Sendeprozess einer XUV-Nachricht: eXTra-Request

Für den Sendeprozess von XUV-Nachrichten ergeben sich folgende schematische Bilder der eXTra-Strukturen: Beim eXTra-Request der Transportebene, sowie des zugehörigen TransportHeader und der Fehlernachricht ExtraError:

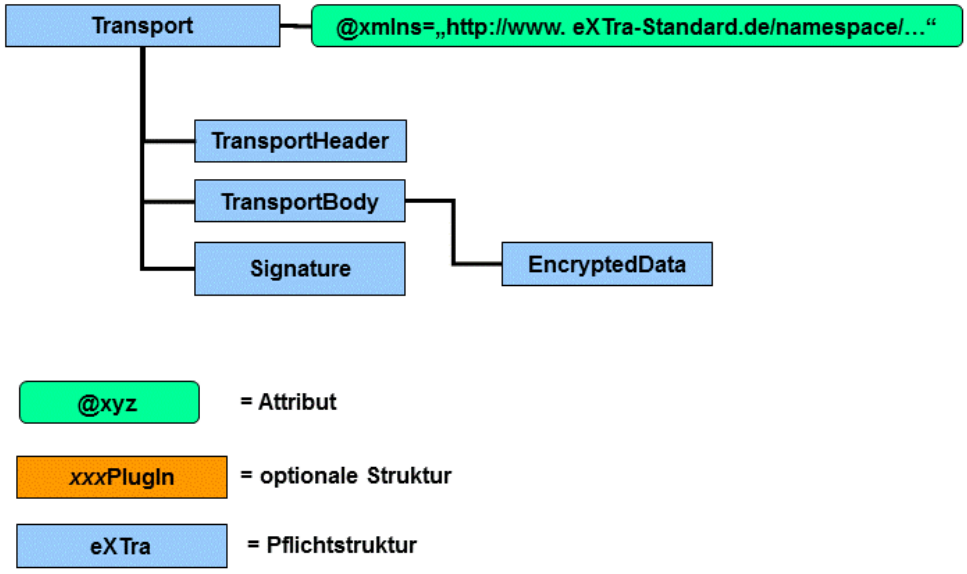

Bild 32: Die Ebenenstruktur des Sendeprozesses (eXTra-Request) mit XUV-Nachrichten (eine Ebene, die Transportebene)

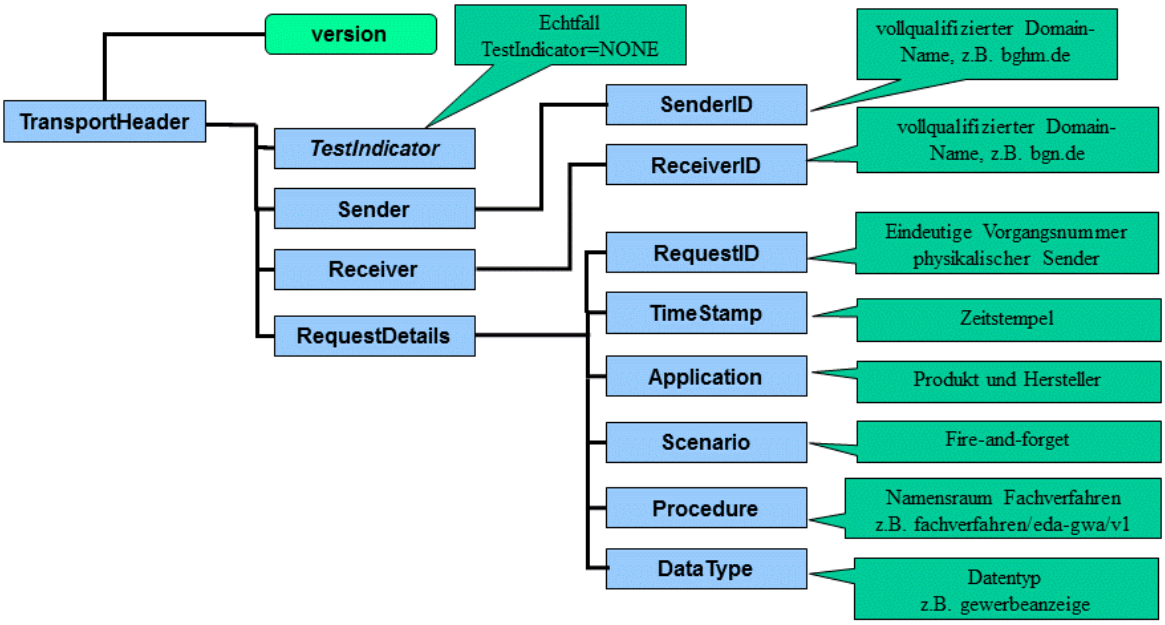

Bild 33: Der TransportHeader des Sendeprozesses (eXTra-Request) mit XUV-Nachrichten

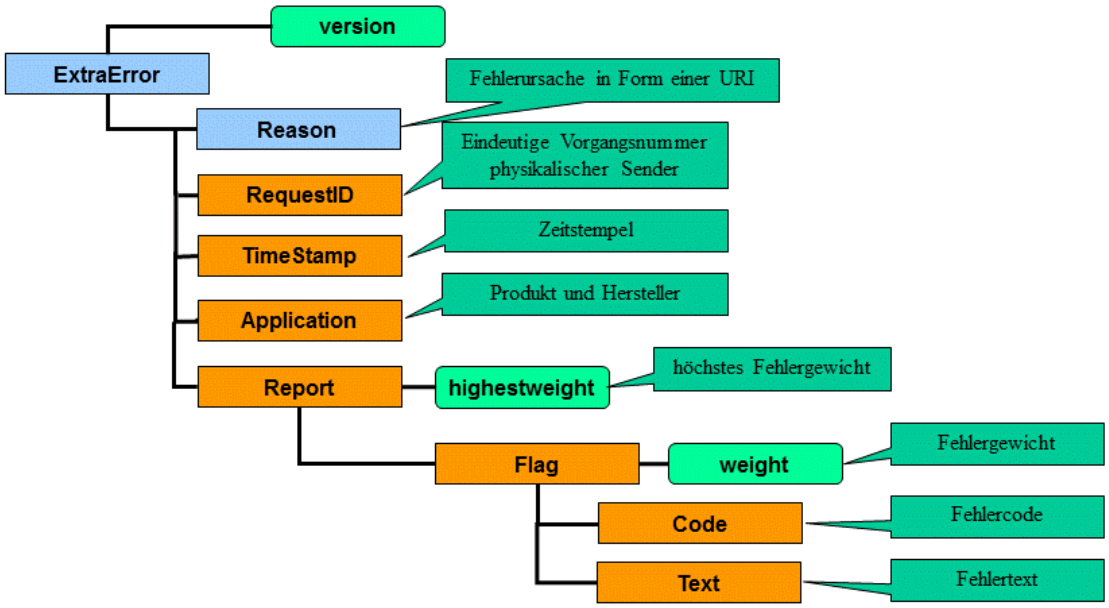

Bild 34: Die Fehlernachricht ExtraError

Sendeprozess einer Antwort auf eine XUV-Nachricht: eXTra-Response

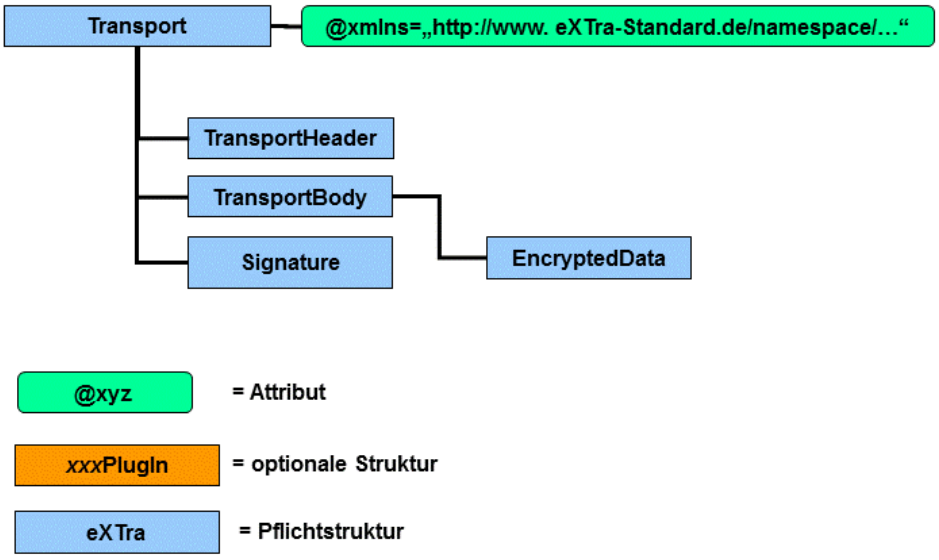

Bild 35: Die identische Ebenenstruktur des Sendeprozesses (eXTra-Request) mit XUV-Nachrichten bzw. deren Antwort (eXTra-Response) (eine Ebene, die Transportebene)

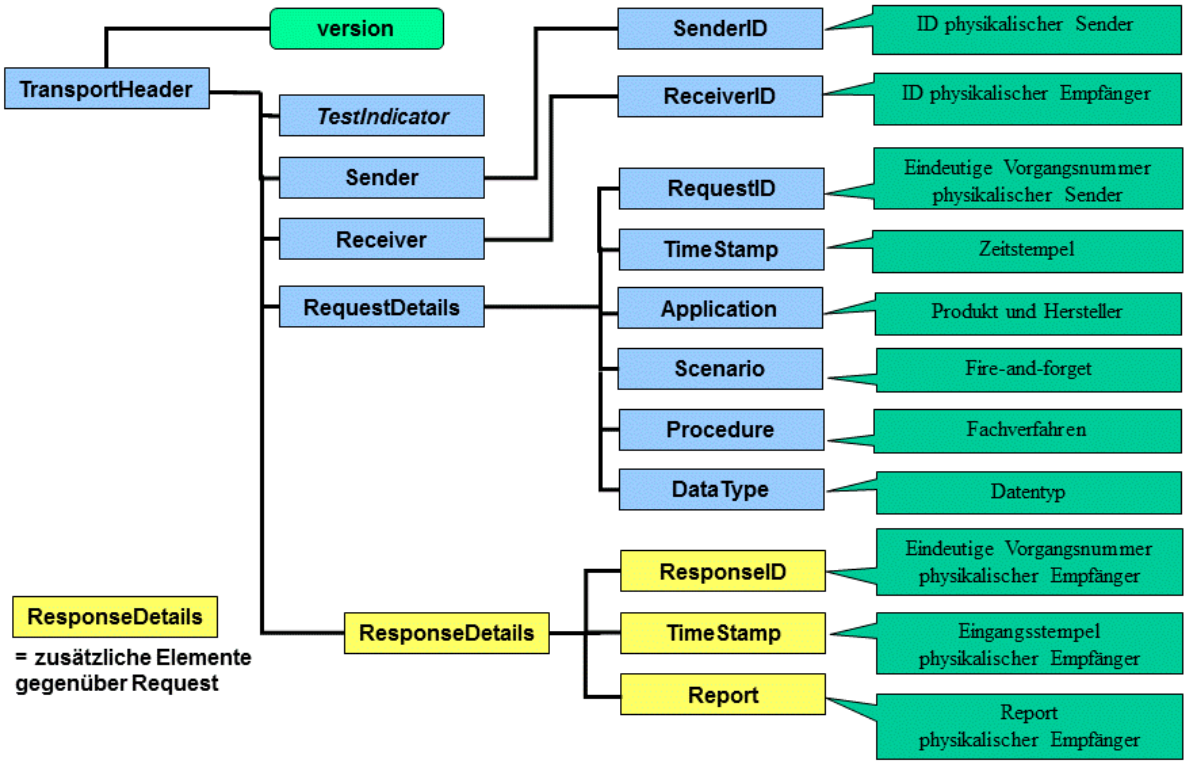

Bild 36: Der TransportHeader des Sendeprozesses (eXTra-Response), semantisch die Antwort des verwertenden Fachverfahrens auf eine XUV-Nachricht

4. Anhang

4.1. Referenzen

Kurzname	Quelle
ANWLF	*eXTra Anwenderleitfaden mit Beispielen aus der Praxis,* zu finden unter http://www.extra-standard.de
BEST	*eXTra Best Practices,* zu finden unter http://www.extra-standard.de
DSIG	*eXTra Design Guidelines*, zu finden unter http://www.extra-standard.de
EINF	*Einführung in den eXTra-Standard,* zu finden unter http://www.extra-standard.de
EMSG	*eXTra-Standardnachrichten, Schnittstellenbeschreibung,* zu finden unter http://www.extra-standard.de
EXSEC	*Sicherheit und Verfügbarkeit in einem eXTra-spezifischen Datenübermittlungsverbund,* zu finden unter http://www.extra-standard.de
EXWS	*eXTra und Webservices,* zu finden unter http://www.extra-standard.de
FTPVSHTTP	*ftp vs http,* Daniel Haxx, zu finden unter http://daniel.haxx.se/docs/ftp-vs-http.html
ISO29115-11	*Entity authentication assurance framework,* ISO/IEC 29115, ursprüngliche Fassung November 2011, zu finden unter https://www.oasis-open.org/committees/download.php/44751/285-17Attach1.pdf aktuelle Fassung vom April 2013, zu finden unter https://www.iso.org/obp/ui/#iso:std:iso-iec:29115:ed-1:v1:en
IFACE	*eXTra Transport Schnittstellenbeschreibung,* zu finden unter http://www.extra-standard.de
KOMP	*eXTra Kompendium,* zu finden unter http://www.extra-standard.de
MTAB	*eXTra Mustertabellen,* zu finden unter http://www.extra-standard.de
NIST_SP80063	*Electronic Authentication Guideline*, National Institute of Standards and Technology, USA NIST Special Publication 800-63-2, 26. August 2013: Überarbeitete Fassung, zu finden unter http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf NIST Special Publication 800-63 Version 1.0.2, April 2006: ursprüngliche Fassung zu finden unter http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

RFC2119	*Request for Comments: 2119*, S. Bradner, Harvard University, March 1997, http://www.ietf.org/rfc/rfc2119.txt
PROF	*eXTra Profilierung,* zu finden unter http://www.extra-standard.de
UMSG	*eXTra-Standardnachrichten, Überblick,* zu finden unter http://www.extra-standard.de
VERS	*eXTra Versionierung,* zu finden unter http://www.extra-standard.de
VMXUV	Drei Dokumente, die das Vorgehensmodell des XUV-Standards zeigen: *XUV_Standard_1.0_Begleitdokument.pdf* *Webservices.pptx* *Nachrichtenaustausch.pptx* zu finden unter http://www.extra-standard.de
XBSP13	*XML-Beispiele auf Basis von eXTra V1.3,* zu finden unter http://www.extra-standard.de
XBSP14	*XML-Beispiele auf Basis von eXTra V1.4,* zu finden unter http://www.extra-standard.de
XENC	*XML Encryption*, http://www.w3.org/TR/xmlenc-core/
XML	*XML Recommendation 1.0, 3rd Edition*, http://www.w3.org/XML
XSD	*XML Schema Definition*, http://www.w3.org/TR/xmlschema-0/
XSIG	*XML Signature*, http://www.w3.org/TR/xmldsig-core/
XSL	*XML Stylesheet Language*, http://www.w3.org/TR/1999/REC-xslt-19991116, http://www.w3.org/TR/xslt20/

4.2. Glossar

Begriff	Erklärung
Authentifizierung	Authentifizierung ist der Nachweis (Verifizierung) einer behaupteten Eigenschaft eines Systems, eines Dokumentes oder einer Information. Bei einer Authentifizierung zwischen zwei Parteien authentisiert sich die Eine (z.B. der Sender), während die Andere (z.B. der Empfänger) die Erstere authentifiziert. Eine in der EDV weit verbreitete Form ist die Authentifizierung des Senders durch den Empfänger mittels UserID, Passwort, oder auch mittels Zertifikat und Signatur
Authentisierung	Authentisierung ist das Aufstellen einer Behauptung (engl. claim) über eine partielle Identität. Der Anwender (z.B. der Sender) authentisiert sich durch Vorlage von Behauptungen (synonym Attribute oder claims) mit Hilfe eines Sicherungsmittels (z.B. mit Benutzername/Passwort, oder Zertifikat oder mittels SmartCard).
Betriebsmodell	Das Betriebsmodell eines *Fachverfahrens* beschreibt ob das *Fachverfahren* nur einen (z.B. einen Sende- oder einen Holprozess) oder mehrere Prozesse in einer *Prozesskette* (z.B. einen Sende- einen Hol und einen Bestätigungsprozess) unterstützt. DFÜ-technisch sind die Prozesse der Anwendungsebene zugeordnet.
Body	Im eXTra Datenmodell enthält dieser Bereich entweder die gesamte nächsttiefere Ebene oder im Fall der untersten Ebene die fachlichen Nutzdaten.
Clearing Stelle	Zentrale annehmende Stelle von Daten, welche die Funktion eines Bindegliedes zwischen fachlichem Sender und fachlichem Empfänger darstellt und für beide Seiten in der Regel für Rechtssicherheit und einen geordneten Betrieb sorgt.

Begriff	Erklärung
Client Client-Server Modell	In einem Client-Server Modell ist der Client der aktive Teil, der einen Dienst vom *Server* anfordert und konsumiert. Der Client ist also der Dienstkonsument. Der Server ist der passive Teil, der dem Client einen Dienst zur Verfügung stellt. Der Server ist also der Dienstanbieter.
Datenübermitt-lungsverbund	Heute können in einem Datenübermittlungsverbund definierte Nachrichten über ein konkretes Datenübermittlungsverfahren ausgetauscht werden. In der Regel definiert der Empfänger der Daten (zumeist eine Behörde, ein Verband oder eine Institution) sowohl das Datenübermittlungsverfahren als auch die Nachrichten. Die Teilnehmer, die Datenlieferanten, müssen üblicherweise beim Empfänger registriert sein. Die Idee von eXTra ist es für beliebige Datenübermittlungsverbünde ein einheitliches Datenübermittlungsverfahren, bzw. über ein generisches Konzept – der *Profilierung* – eine Familie verwandter Datenübermittlungsverfahren zur Verfügung zu stellen. Das Ergebnis der Profilierung ist ein *verbundspezifischer eXTra-Standard*.
DFÜ Ebene	Die DFÜ Ebene repräsentiert innerhalb des abstrakten Architekturmodells eines Datenübermittlungssystems, sowie bei eXTra eine Ebene, bei der ein *DFÜ Sender* Daten mit einem *DFÜ Protokoll* an einen *DFÜ Empfänger* sendet. Weiterhin sind in der DFÜ Ebene in der Regel Sicherheitsmaßnahmen integriert, die insbesondere Angriffen aus der Internet-Welt entgegen wirken sollen. In eXTra wird die Ausgestaltung der DFÜ Ebene nicht behandelt; insofern trifft eXTra keinerlei Aussagen zum DFÜ-Protokoll oder zu den dort angesiedelten Sicherheitsmaßnahmen.
Fachverfahren	Mit Hilfe von eXTra kann ein Fachverfahren auf Senderseite (fachlicher Sender) fachliche Daten an das zugeordnete Fachverfahren auf Empfängerseite (fachlicher Empfänger) übermitteln. In umgekehrter Datenflussrichtung kann ein erzeugendes Fachverfahren auf Empfängerseite dem anfordernden Fachverfahren auf Senderseite fachliche Daten zum Abholen bereitstellen.

Begriff	Erklärung
Header	In der Informationstechnik werden Metadaten am Anfang einer Datei oder eines Datenblocks als Header (auch: Dateikopf) bezeichnet. Diese können verwendet werden, um beispielsweise das Dateiformat zu beschreiben oder weitere Angaben zu den Daten zu machen.
Kommunikationsszenario	Ein Kommunikationsszenario definiert das erwartete Verhalten eines Empfängers auf einer Ebene.
Kommunikationsvorgang	Ein Kommunikationsvorgang definiert den Ablauf der Kommunikation zwischen Sender und Empfänger auf einer Ebene des eXTra Kommunikationsmodells. Er legt fest, wie die Rollen Sender und Empfänger verteilt werden und ob eine synchrone Response möglich ist.
Komprimierung	Datenkompression oder Datenkomprimierung ist die Anwendung von Verfahren zur Reduktion des Speicherbedarfs von Daten.
logischer Empfänger	Der logische Empfänger ist ein Akteur, der auf Empfänger-Seite der *Logistikebene* zugeordnet ist.
logischer Sender	Der logische Sender ist ein Akteur, der auf Sender-Seite der *Logistikebene* zugeordnet ist.
Logistikebene	Die Logistik- oder auch Paketebene repräsentiert bei eXTra eine Ebene, die auf Senderseite durch den *logischen Sender* für die Bündelung mehrerer fachlichen Nachrichten für einen Endempfänger zu einem Paket zuständig ist, bzw. auf Empfängerseite durch den *logischen Empfänger* die Verteilung der Paketinhalte auf die Endempfänger/ Verwerter übernimmt.
Logging	Eine Logdatei beinhaltet das automatisch erstellte Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem. Das Fortschreiben dieser Datei nennt man Logging.

Begriff	Erklärung
Message	(Fach-)Nachricht, die ein Erzeuger mithilfe eines Fachverfahrens generiert und die ein Verwerter verarbeiten soll. Eine eXTra Message enthält im MessageBody in der Regel eine einzige Fachnachricht. Dadurch ist eine Fachnachricht für eXTra sicht- und greifbar.
Migration	Unter Migration versteht man im Rahmen der Informationstechnik den Umstieg eines wesentlichen Teils der eingesetzten Software beziehungsweise den Transfer von Daten aus einer Umgebung in eine andere, sowie die Umstellung von Hardware einer alten Technologie in neue Technologien unter weitgehender Nutzung vorhandener Infrastrukturen.
Nachrichtenebene	Die Nachrichtenebene repräsentiert bei eXTra eine Ebene, bei der z.B. auf Senderseite ein Erzeuger durch ein Fachverfahren eine fachliche Nachricht generiert, die in Form einer eXTra Message übermittelt wird.. Auf der Empfängerseite verarbeitet das korrespondierende Fachverfahren als Endempfänger und Verwerter die fachliche Nachricht.
Package	Ein Paket, das z.B. ein *logischer Sender* an einen *logischen Empfänger* übermittelt. Ein Package enthält im PackageBody entweder die fachlichen Daten oder die nächsttiefere Ebene, die Nachrichtenebene. Sind im PackageBody fachliche Daten enthalten, so ist es für eXTra nicht erkennbar, aus wie vielen fachlichen Nachrichten der PackageBody zusammengesetzt ist.
Paketebene	Die Paket- oder Logistikebene erlaubt es, Einzelnachrichten zu Paketen zusammenzufassen und damit in verschiedener Hinsicht einheitlich zu behandeln. Sie unterstützt damit insbesondere die Massendatenverarbeitung. Ein derartiges Paket wird in Form eines eXTra *Package* übermittelt.

Begriff	Erklärung
physikalischer Empfänger	Der physikalische Empfänger ist ein Akteur, der auf Empfänger-Seite der *Transportebene* zugeordnet ist. Physikalischer Sender und –Empfänger stehen über ein konkretes Kommunikationssystem direkt miteinander in Verbindung und tauschen darüber eXTra-Dokumente aus. Die Ausgestaltung des konkreten Kommunikationssystems (und damit der verwendeten DFÜ-Protokolle und Netze) ist in eXTra nicht vorgegeben.
physikalischer Sender	Der physikalische Sender ist ein Akteur, der auf Sender-Seite der *Transportebene* zugeordnet ist. Physikalischer Sender und Empfänger stehen über ein konkretes Kommunikationssystem direkt miteinander in Verbindung und tauschen darüber eXTra-Dokumente aus. Die Ausgestaltung des konkreten Kommunikationssystems (und damit der verwendeten DFÜ-Protokolle und Netze) ist in eXTra nicht vorgegeben.
PlugIns	Softwarehersteller definieren Schnittstellen zu ihren Produkten, mit deren Hilfe Dritte Funktionserweiterungen (Plug-Ins) für diese Softwareprodukte programmieren können. In eXTra sind Plug-Ins optionale Erweiterungen des Datenmodells, die aber nicht unabhängig entwickelt werden können, sondern dem Standardisierungsprozess unterliegen.
Profilkonfiguration Profilierung	Die Profilkonfiguration ist bei eXTra eine XML-Datei, die dazu dient aus dem allgemeinen eXTra-Basisschema für ein konkretes Fachverfahren bzw. einen konkreten *Datenübermittlungsverbund* auf formale Weise eine spezifische Schemadatei – ein eXTra Subschema - zu generieren. Diesen Generierungsvorgang – die Profilierung - kann jedes Fachverfahren bzw. jeder Datenübermittlungsverbund selbst durchführen.

Begriff	Erklärung
Prozesskette	Eine Prozesskette ist eine zusammengehörige Folge mehrerer Prozesse, d.h. mehrerer Kommunikationsvorgänge kooperierender Fachverfahren, die aus einer beliebigen Kombination von Sende- Hol- und/oder Bestätigungsprozessen bestehen kann.
RequestID	Anfragekennung. In der eXTra Terminologie ist die RequestID ein vom Sender vergebener eindeutiger Identifikator einer Anfrage.
ResponseID	Antwortkennung In der eXTra Terminologie ist die ResponseID ein vom Empfänger vergebener eindeutiger Identifikator einer Antwort auf eine Anforderung mit einer eindeutigen RequestID.
Server Client-Server Modell	Der Server ist der passive Teil in einem Client-Server Modell, der auf Anforderung eines *Client* diesem einen Dienst zur Verfügung stellt. Der Server ist also der Dienstanbieter, der Client der Dienstkonsument.
Signatur Signierung	Unter einer elektronischen Signatur versteht man Daten, mit denen man den Unterzeichner bzw. Signaturersteller identifizieren kann und sich die Integrität der signierten, elektronischen Daten prüfen lässt. Die elektronische Signatur erfüllt somit technisch gesehen unter bestimmten Bedingungen den gleichen Zweck wie eine eigenhändige Unterschrift auf Papierdokumenten. Den Vorgang nennt man Signierung.
Standardnachricht	Eine eXTra-Standardnachricht ist formal eine fachliche Nachricht. Sie bietet ein optionales Sprachmittel an, das für einen bestimmten Standardvorgang eingesetzt werden kann. Mit der Standardnachricht DataRequest kann man z.B. einen Holvorgang formulieren, in dem man aus der Menge der bereitgestellten fachlichen Nachrichten die gewünschten auswählen und abholen kann.

Begriff	Erklärung
Topologie	Die Topologie bezeichnet bei einem Computernetz die Struktur der Verbindungen mehrerer Geräte untereinander, um einen gemeinsamen Datenaustausch zu gewährleisten. Bei einem Datenübermittlungsverbund stellt die Topologie die Struktur der Verbindungen der einzelnen Teilnehmer bzw. Systeme des Datenübermittlungsverbundes dar.
Transportebene	Die Transportebene repräsentiert bei eXTra eine Ebene, bei der ein *physikalischer Sender* vollständige eXTra-Dokumente an einen *physikalischen Empfänger* sendet. Im TransportBody sind entweder die fachlichen Daten oder die nächsttiefere Ebene, die Paket- oder Nachrichtenebene enthalten. Sind im TransportBody fachliche Daten enthalten, so ist es für eXTra nicht erkennbar, aus wie vielen fachlichen Nachrichten der TransportBody zusammengesetzt ist.
URL	Als Uniform Resource Locator (URL, engl. „einheitlicher Quellenanzeiger“) bezeichnet man eine Unterart von Uniform Resource Identifiern (URIs). URLs identifizieren eine Ressource über das verwendete Netzwerkprotokoll (beispielsweise http oder ftp) und den Ort (engl. location) der Ressource in Computernetzwerken.
Validierung	In der Softwaretechnik bezeichnet Validierung (auch Plausibilisierung, als Test auf Plausibilität, oder engl. Sanity Check genannt) die Kontrolle eines konkreten Wertes darauf, ob er zu einem bestimmten Datentyp gehört oder in einem vorgegebenen Wertebereich oder einer vorgegebenen Wertemenge liegt.
Verbund-spezifischer eXTra-Standard	Die Idee von eXTra ist es für beliebige Datenübermittlungsverbünde ein einheitliches Datenübermittlungsverfahren, bzw. über ein generisches Konzept – der *Profilierung* - eine Familie verwandter Datenübermittlungsverfahren zur Verfügung zu stellen. Das Ergebnis der Profilierung ist ein verbundspezifischer eXTra-Standard.

Begriff	Erklärung
Verschlüsselung	Verschlüsselung nennt man den Vorgang, bei dem die Repräsentation einer Informationseinheit wie etwa ein Text oder eine Bilddatei aus einer unverschlüsselten Form, dem sogenannten Klartext, in eine verschlüsselte Form, dem sogenannten Geheimtext, überführt wird. In der Regel erfolgen Ver- und Entschlüsselung mit Hilfe mathematischer Verfahren, die hierzu ein oder mehrere extern zugeführte Schlüssel verwenden.
W3C	Das World Wide Web Consortium (W3C, http:www.w3.org) entwickelt Standards und Technologien für das Internet.
XSLT Stylesheet	XSL Transformation, kurz XSLT, ist eine XML-basierte Sprache für die Transformation von XML-Dokumenten. Sie ist Teil des W3C-Standards Extensible Stylesheet Language (XSL).