einheitliches XML-basiertes Transportverfahren

eXTra Basis-Standard

Design Guidelines
Version 1.2.0

FINAL

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.

Änderungsprotokoll

Änderungsprotokoll für Ausgabestand 1.2.0

Autor[en]	Datum	Beschreibung
[gelöscht]	16.08.2010	Ersterstellung, Basis ist Ausgabestand 1.1.1 Aufnahme neue Nachricht ExtraError, neue Standardnachrichten ListOfDataRequest und ListOfConfirmationOfReceipt, neues Plug-In Contacts

Änderungsprotokoll für Ausgabestand 1.1.0 bis 1.1.1

Autor[en]	Datum	Beschreibung
[gelöscht]	06.07.2009	Ersterstellung
	08.03.2010	Freigabe

Inhaltsverzeichnis

1 Einleitung und Übersicht

Hinweis zum Gebrauch: Bibliographische Referenzen stehen in eckigen Klammern ([*bibref*]) und sind am Ende dieser Spezifikation beschrieben.

eXTra, das *Einheitliche XML-basierte Transportverfahren*, ist ein gemeinschaftlich von Unternehmen und Behörden entwickelter, offener Standard für die Datenübermittlung. Eine kurze Einführung sowie eine detaillierte Beschreibung finden sich in [EINF] bzw. [KOMP]. Diese Dokumente und sämtliche öffentlichen Informationen über eXTra sind im Internet unter der Adresse http://www.extra-standard.de abrufbar.

Das Verfahren eXTra definiert ein allgemein gültiges Format einer Beschreibungsstruktur zum Zwecke des Austauschs von Fachnachrichten zwischen zwei Kommunikationspartnern und deren Prozessbeteiligten. Für die Strukturdefinition wird XML verwendet. Entstanden ist das eXTra-Verfahren aus dem Wunsch heraus, den Austausch von fachlichen Nachrichten zwischen Arbeitgebern und der Verwaltung einheitlich zu gestalten. Dabei wurden bereits bestehende Verfahren, wie z.B. Elster an die Finanzverwaltung, statistische Meldungen an das Statische Bundesamt oder das DEÜV-Verfahren an die gesetzlichen Krankenkassen GKV, betrachtet und deren Belange berücksichtigt. Des Weiteren wurde in der Entstehung dieses Verfahrens darauf geachtet, dass sowohl einzelne Nachrichten als auch eine Sammlung vieler Nachrichten und sogar verschiedener Nachrichtentypen gleichzeitig übertragen werden können, so dass das eXTra Verfahren prinzipiell für jede Form des Nachrichtenaustauschs verwendet werden kann. Darüber hinaus ist das eXTra Verfahren geeignet einen Datenübermittlungsverbund zu unterstützen, d.h. eine beliebige Menge von Sendern mit einer Menge von Empfängern miteinander zu verbinden, wie dies z.B. beim Elster-Verfahren der Finanzverwaltung oder dem DEÜV-Verfahren der gesetzlichen Krankenkassen der Fall ist.
Ergebnis dieser Betrachtung ist das sogenannte eXTra Basis-Verfahren, das zugleich einer Zusammenfassung wie auch Verallgemeinerung der bestehenden Verfahren entspricht. Es obliegt dem jeweiligen Datenübermittlungsverbund, bzw. Fachverfahren, ausgehend vom eXTra Basis-Verfahren, eine auf dessen Belange zugeschnittene Ausprägung – sein spezifisches eXTra-Verfahren - zu definieren. Dieser Vorgang des Zuschnitts heißt Profilierung des eXTra Basis-Standards, das Ergebnis einer Profilierung ist ein verbund- bzw. fachspezifischer eXTra Standard.

Die formale Syntaxbeschreibung des eXTra Basis-Standards ist in XSD-Schemadateien hinterlegt. Im Zuge der Profilierung des eXTra Basis-Standards hin zu einem verbund- bzw. fachspezifischen eXTra Standard werden deshalb die Schemadateien des eXTra Basis-Standards profiliert, d.h. im wesentlichen eingeschränkt und genauer spezifiziert. Ergebnis des Profilier-Vorgangs ist somit ein weiteres XSD-Schema, welches die zu verwendenden Strukturen des neugebildeten verbund- bzw. fachspezifischen eXTra-Standards beschreibt. Jede Nachricht an das zu bedienende Fachverfahren muss sowohl dem allgemein gültigen eXTra Basis-Schema als auch dem neuen verbund- bzw. fachspezifischen eXTra Standard entsprechen.

2 Verwendung dieses Dokumentes

Dieses Dokument richtet sich an Projektleiter, technisch orientierte Gremien und Arbeitsgruppen von Datenübermittlungsverbünden bzw. an Verantwortliche eines Fachverfahrens, die einen elektronischen Nachrichtenaustausch für zu übertragenden Fachnachrichten definieren wollen.

Insbesondere will dieses Dokument Hilfestellung bei der Profilierung und Definition der auf die Bedürfnisse des jeweiligen Datenübermittlungsverbundes bzw. Fachverfahrens zugeschnittenen eXTra-Strukturen geben.

3 Analyse des bestehenden Fachverfahrens

In den meisten Fällen, in denen eine Datenübermittlung über eXTra eingeführt werden soll, existiert bereits ein Fachverfahren. Möglicherweise werden die im Rahmen des Verfahrens zu übertragenden Daten bisher in Form von Papier oder E-Mail ausgetauscht, oder ein existierendes elektronisches Datenübermittlungsverfahren soll modernisiert werden.
Eine Analyse des bestehenden Fachverfahrens, des gegebenenfalls bereits bestehenden Datenübermittlungsverfahrens, der daran beteiligten Personen und Instanzen und der auszutauschenden Daten ist Voraussetzung, um die passenden Strukturen für ein neues verbund- bzw. fachspezifisches eXTra-Verfahren zu definieren.
In den folgenden Kapiteln werden mögliche entscheidende Fragestellungen genannt, die Einfluss auf die Profilierung der eXTra-Struktur haben.

4 Ebenenkonzept

4.1 Analyse der Rollen

Fragestellung:
- Wer ist an der Übertragung der fachlichen Daten beteiligt?

Je nach Komplexität der Prozesse gibt es unterschiedliche Aufgabestellungen und damit verbundene Rollen beim Erstellen oder beim Auswerten einer Nachricht. Das eXTra-Verfahren unterstützt die Verteilung der Arbeitsschritte auf bis zu drei am Prozess beteiligte Instanzen, die jeweils auf ihrer Ebene miteinander kommunizieren:

1. Erstellen und Verarbeiten einer einzelnen fachlichen Nachricht durch z.B. eine meldende Person bzw. einen bearbeitenden Sachbearbeiter.
2. Sammeln und Zusammenfassen mehrerer Einzelnachrichten eines Nachrichtentyps zu einem Paket durch einen Dienstleister bzw. Trennen eines solchen Paketes und Verteilung der Einzelnachrichten an die verarbeitende Instanz von einer hierfür beauftragten Stelle.
3. Sammeln und Zusammenfassen mehrere Pakete für einen Kommunikationspartner zu einer Transporteinheit, die an eine entsprechende Gegenstelle übertragen wird.

Dort wird die Transportnachricht entgegengenommen und die einzelnen Pakete an die hierfür vorgesehene Stelle weitergegeben.

Es dürfen nicht nur die den Verantwortlichen bekannten Rollen auf Empfängerseite betrachtet werden. In vielen Datenübermittlungsverfahren steht dem Server auf Empfängerseite eine Vielzahl von Software-Lösungen gegenüber, die unterschiedliche Voraussetzungen und damit Anforderungen an das Verfahren haben. In Fachverfahren, die Meldungen von Arbeitgebern an Behörden oder gesetzliche Institutionen zum Gegenstand haben, gibt es auf der Senderseite neben Client-Lösungen, die den einzelnen Meldenden als Bediener voraussetzen, auch Service-Provider und Service Rechenzentren, die die Daten tausender Meldender sammeln und in großen Einheiten an den Empfänger übertragen. Die Anzahl der Rollen, also der am Prozess der Datenzusammenstellung Beteiligten, ist daher unterschiedlich, und sollte in allen möglichen Varianten betrachtet werden.

Das eXTra-Verfahren 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:

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

Eine Nachricht wird erstellt, indem jede damit befasste Instanz ihre bereitgestellten Daten (in einem sog. Body) zusammenfasst und eine Beschreibung dieses Arbeitsschritts (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 Daten entsprechend behandelt.

Die Weitergabe der Daten von einem Ersteller einer Einzelnachricht hin zu einem Sender der Transportnachricht bzw. von einem Empfänger der Transportnachricht hin zu einem Bearbeiter der Einzelnachricht ist nicht Gegenstand der Spezifikation von eXTra. Eine mögliche und naheliegende Variante ist es auf der Erzeugerseite die jeweilige Ebene zuzufügen und diese auf der Empfängerseite wieder zu entfernen.

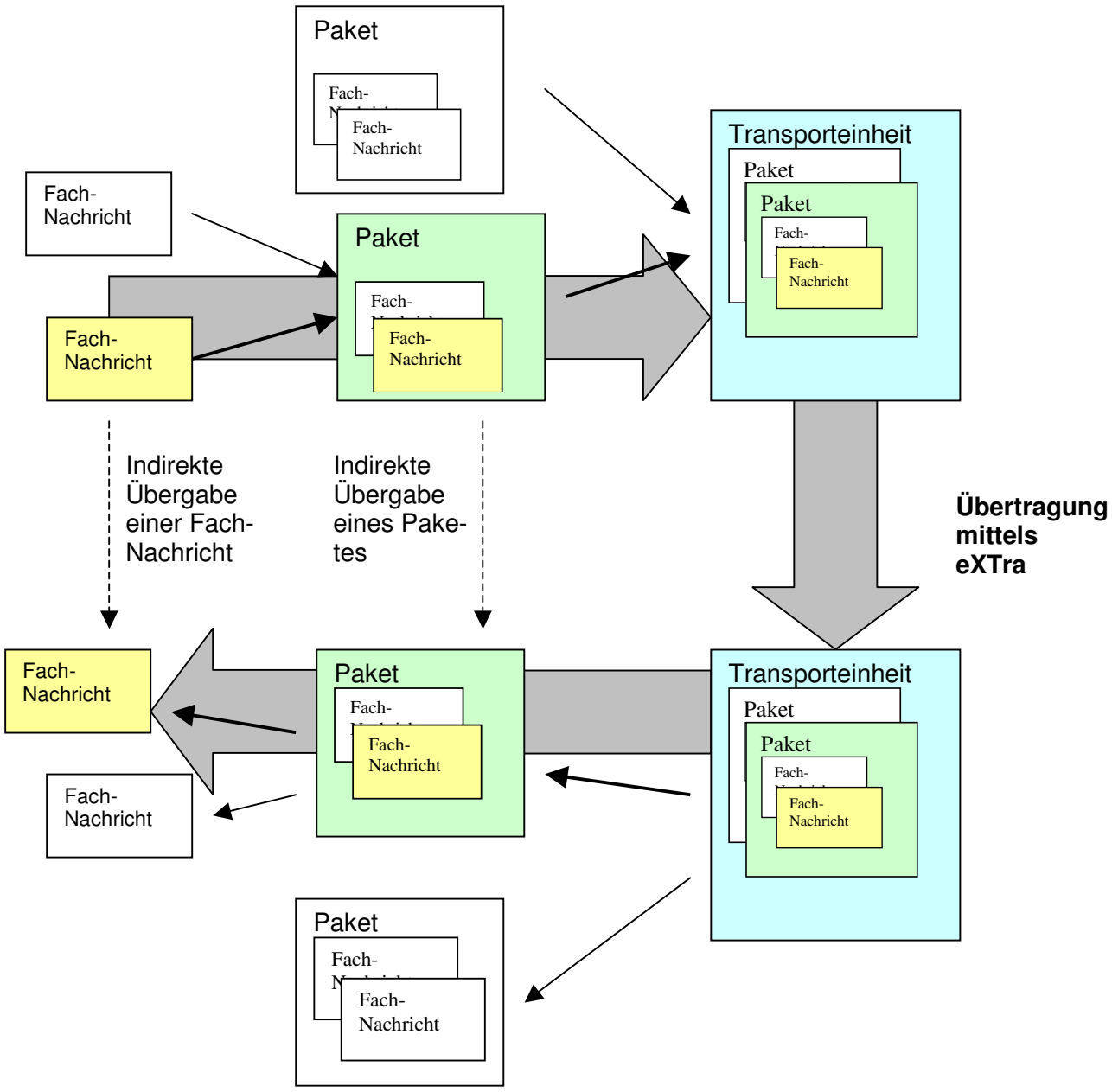


Bild1: Lebenszyklus einer eXTra-Nachricht

4.2 Erforderliche Ebenen

Nicht in jedem Fall ist es erforderlich, die genannten Aufgabengebiete differenziert auf mehrere Organisationseinheiten aufzuteilen. Im einfachsten Fall gibt es genau eine Instanz, die eine übertragene Einzelnachricht entgegennimmt und an das Fachverfahren weiterleitet. Auch diese einfache Topologie wird unterstützt. Hier genügt es statt alle drei Ebenen nur eine Ebene, nämlich die verpflichtende Transport-Ebene zu definieren. Zwischen diesen beiden Topologien sind viele mögliche Varianten denkbar.

Entscheidend für die Anzahl erforderlicher Ebenen sind folgende Fragen:

- welche Topologie liegt auf Empfängerseite (Datenannahmestelle) vor
- wie viele unterschiedliche Fachverfahren bedient das eXTra-Empfangssystem
- wie viele unterschiedliche Datentypen kann ein angeschlossenes Fachverfahren verarbeiten

Kriterien für die Notwendigkeit nur einer Ebene

Eine einzige Ebene – die Transport-Ebene - genügt, 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 von 2 Ebenen werden im Kapitel 6 behandelt.

4.3 Erforderliche Komponenten

Die Struktur der Beschreibung ist für jede eXTra-Ebene gleich aufgebaut. Jede Instanz einer Ebene bekommt mit Hilfe der in gleicher Weise enthaltenen Elemente die Möglichkeit, die gleichen Teilaufgaben auszuführen. Typische Aufgaben können z.B. auf der Empfängerseite sein:

- Prüfen der Berechtigung der Gegenstelle, den entsprechenden Nachrichtentyp zu erstellen oder zu senden.
- Prüfen, ob die Nachricht für einen selbst bestimmt war.

- Entschlüsseln und Dekomprimieren des Datenbereichs der eigenen Ebene.
- Aussteuern von Testnachrichten
- Weitergabe der Nachricht an die Instanz der nächsten Ebene.
- Mitschreiben der durchgeführten Arbeitsschritte für den späteren Nachvollzug (Logging)
- Rückmeldung an die zugehörige Gegenstelle über die erfolgreiche Entgegennahme der zugeordneten Ebene und Weitergabe der Daten an die nächste Ebene.

Jede Ebene bietet die Möglichkeit, Logging-Informationen anzufügen und diese an die nächste Ebene weiterzureichen. Hiermit kann ein Nachweis über erfolgreiche Prüfungen weitergegeben werden oder z.B. ein Laufzettel erstellt werden.
Die Bestimmung der beteiligten Instanzen und die Zuteilung der durchzuführenden Teilaufgaben ist die Aufgabe des mit der Definition des verbund- bzw. fachspezifischen eXTra Verfahrens beauftragten Verantwortlichen. Um ihn dabei zu unterstützen, werden in der Folge Entscheidungshilfen an die Hand gegeben.

4.4 Profilierung

Bevor auf die einzelnen Ebenen eingegangen wird, soll der Vorgang des Profilierens allgemein betrachtet werden.
Ausgangspunkt ist die jeweils gültige Beschreibung des eXTra-Verfahrens. Hierzu gehören Schema-Dateien des eXTra Basis-Standards, die die Syntax einer gültigen eXTra-Nachricht definieren. Eine Profilierung dieser Schema-Dateien bedeutet, sie so zu modifizieren, dass eine damit geprüfte XML-Datei sowohl dem eXTra-Basis-Standard, als auch den Regeln des so erzeugten verbund- bzw. fachspezifischen eXTra Standards genügt.

Es gelten für die Profilierung folgende Regeln:

- im Rahmen der Profilierung kann die Anzahl der zulässigen Ebenen festgelegt werden. Die Transport-Ebene ist Pflicht, die Paket- wie die Nachrichtenebene sind optional.
- Eine Ebene besteht mindestens aus Header und Body. PlugIns, Signatures und Logging sind optional. Die Festlegungen bzgl. der optionalen Strukturelemente können ebenenspezifisch unterschiedlich sein.

- im Rahmen der Profilierung kann festgelegt werden, wie bzgl. der optionalen Elemente der Header auf Transport-, Paket- und Fachnachrichten-Ebene zu verfahren ist. Die Festlegungen können ebenenspezifisch unterschiedlich sein.
- Es kann festgelegt werden, dass ein optionales Element zum Pflichtelement wird, oder dass ein optionales Element nicht unterstützt und somit ignoriert wird.
- Es kann nicht festgelegt werden, dass ein Pflichtelement zum optionalen Element wird oder nicht unterstützt wird.

5 Profilierung der Transport-Ebene

Gegenstand des eXTra-Verfahrens ist der elektronische Transport von Nachrichten von einem physikalischen Sender zu einem physikalischen Empfänger. Daher sind Informationen zum Transportvorgang notwendig. Die Rolle eines physikalischen Senders und eines physikalischen Empfängers der Nachricht ist immer definiert. Eine Beschreibung des Vorgangs in Form eines TransportHeader muss immer erstellt werden.

Im Rahmen des Verfahrens muss von der Annahmestelle entschieden werden, welche Möglichkeiten und Freiheiten der Sender der Nachricht erhalten soll. Hieraus können sich folgende Fragestellungen ergeben:
Wird ihm die Möglichkeit gegeben, Testdaten zu senden? Kann er unterscheiden, ob nur der Transport getestet werden soll, oder ob er auch die Qualität der Daten geprüft haben möchte? Ggf. müssen Testdaten an die nächste Ebene bzw. bis zum verarbeitenden Fachverfahren weitergereicht werden.
Der TransportHeader enthält Angaben zum Sender in Form einer Identifikation, möglicherweise die Art der Identifikation sowie des Namens des Senders als Person oder als Organisation. Im Rahmen der Definition des verbund- bzw. fachspezifischen eXTra Verfahrens ist zu entscheiden, ob alle möglichen Sender der annehmenden Stelle bekannt sein müssen. In diesem Fall muss eine Infrastruktur zur Verwaltung der Sende-Identifikationen geschaffen werden. Ist ein Nachweis der Identität nötig, so muss ggf. eine Sicherheits-Infrastruktur aufgebaut werden.
Auch die Bezeichnung des Empfängers kann, wenn es mehrere mögliche Empfänger gibt, die die Nachrichten entgegen nehmen dürfen, eine Verwaltung der Empfänger-Identifikationen bzw. Sicherheits-Infrastruktur notwendig machen.
Der Dateninhalt wird durch die Angabe des Verfahrens und des Datentyps gekennzeichnet. Es kann im Rahmen der Anbindung eines Fachverfahrens notwendig sein mehrere Datenty-

pen zu definieren. Bereits bei einem Fachverfahren, welches Nachrichten entgegennimmt und verarbeitet, und das auf Anforderung Quittungen oder Protokolle ausliefert, sind mehrere Datentypen zu verwenden, nämlich der Datentyp der zu sendenden Daten, der Datentyp der Protokollanforderung und der Bestätigung.

Bei der Definition des verbund- bzw. fachspezifischen eXTra Verfahrens muss festgelegt werden, auf welche Art die Kommunikation durchgeführt werden soll. Bekommt der Sender der Nachricht eine Information, dass die Entgegennahme der Daten funktioniert hat? Bekommt er evtl. auf seine Anfrage Daten zurück? Der Sender formuliert die gewünschte Vorgehensweise im Element. Scenario. Die möglichen Szenarien je Datentyp müssen festgelegt werden.

Die ausgetauschten Sendungen und Antworten müssen nachvollziehbar sein. Eine eindeutige Identifikation der Nachricht aus Sicht des Senders und des Empfängers ist daher notwendig. Beide Seiten des Transportvorgangs sollten Sorge dafür tragen, dass die Identifikationen gespeichert, zugeordnet und nachvollzogen werden können.

Ist eine Antwort als unmittelbare Reaktion auf die Übertragung vorgesehen, so muss sich der Empfänger Gedanken über die Menge der möglichen Fehlercodes machen. Er hat die Möglichkeit Informationen, Warnungen und Fehler zurückzumelden. Bei aufgetretenem Fehler sollte die gesamte Nachricht abgelehnt werden. Eine teilweise Verarbeitung der Daten wird nicht empfohlen, da in diesem Fall der Sender die u. U. schwierige Aufgabe hat, die noch nicht verarbeiteten Daten neu zu bündeln und eine neue Sendung zu erstellen.

Sind für die Entgegennahme der Daten weitere Informationen nötig, die der TransportHeader nicht anbietet, gibt es die Möglichkeit, Erweiterungen, sog. Plugins, zu definieren. Im eXTra Basis-Standard sind bereits einige Plugins definiert, die auf jeder Ebene Verwendung finden können. Weitere notwendige Plugins müssen für den Standard beantragt werden.

5.1 Testszenarien

Fragestellung:

- Welche Testmöglichkeiten soll der physikalische Sender erhalten?

Bei der Entwicklung von Software sollten frühzeitig Testszenarien überlegt und vorbereitet werden. Wird ein Datenübermittlungsverfahren implementiert, gibt es zwei Prozess-Beteiligte, die jeder für sich eine Datenschnittstelle mit allen Komplexitäten realisieren. Damit diese Implementierungen bei Inbetriebnahme reibungslos zusammenpassen, müssen von Anfang an Testmöglichkeiten vorgesehen werden.

Die im Rahmen von eXTra untersuchten Verfahren kennen für die Festlegung, welche Übertragung eine Testübertragung ist, drei wesentliche Varianten:

- Manche Verfahren bieten neben einer Empfangsstelle für echte Daten auch eine Empfangsstelle für Testdaten an. Das kann bei Übertragungen im Internet eine eigene URL sein. Das kann bei Mail-Verfahren eine eigene Mail-Adresse sein. Kurz: Die Adresse, wohin die Daten gesendet werden, bestimmt deren Bedeutung.
- Andere Verfahren kennzeichnen Testdaten und Echtdaten mit verschiedenen Datentypen.
- In der Beschreibung der Daten wird ein Testvorgang als solcher gekennzeichnet.

Letztere Variante ist die in eXTra empfohlene. Das eXTra-Verfahren sieht in den Headern der jeweiligen Ebenen einen Testmerker vor, mit dem ein Test gekennzeichnet werden kann, und darüber hinaus auch noch der Umfang des Tests festgelegt werden kann.
Standardmäßig werden in eXTra auf der Transport-Ebene folgende Testvarianten unterschieden:

- „receive“: Test des Übertragungsvorgangs, einschließlich Validierung des erhaltenen eXTra-Dokumentes gegenüber dem profilierten Schema; die empfangenen Daten werden ignoriert.

  Dieser Testmerker eignet sich u.a. für die ersten Tests im Rahmen der Realisierung und Inbetriebnahme eines neuen Datenübermittlungssystems, um die formale Korrektheit der übermittelten eXTra-Dokumente zu verifizieren.
- „accept“: Test des Übertragungsvorgangs und der bei der Entgegennahme der Daten notwendigen Arbeitsschritte, wie z.B. Validierung des erhaltenen eXTra-Dokumentes gegenüber dem profilierten Schema, Übernahme in die lokale Datenhaltung, Komprimieren/Dekomprimieren, Verschlüsseln/Entschlüsseln, Signieren/Signatur prüfen usw. Die Daten werden nicht weitergereicht.
- „process“: Weiterreichen der als Testdaten gekennzeichneten Daten an die nächste Ebene bzw. an das Fachverfahren. Diese Möglichkeit kann dann sinnvoll sein, wenn als Folge der Verarbeitung weitere asynchron abzuholende Informationen, wie z.B. Protokolle oder Bescheide, erstellt werden, die ja ebenfalls getestet werden sollten.

Ein Testmerker wird in einer eXTra-Struktur in der Form eines URIs dargestellt. Dabei ist der Pfad der vom Standard definierten Varianten des Testmerkers vorgegeben, z.B.:

<TestIndicator>http://www.extra-standard.de/test/PROCESS</TestIndicator>

Sind im Rahmen des zu definierenden Fachverfahrens weitere Testmerker sinnvoll, so werden diese mit einer URI des entsprechenden Fachverfahrens gekennzeichnet:

<TestIndicator>http://www.fachverfahren-xy.de/test/EIGENE-VARIANTE</TestIndicator>

Wurden die möglichen Testvarianten für den Transport der Daten festgelegt, so gilt es, sich Gedanken über die Behandlung der Daten und die Weitergabe derselben an die nächste Ebenen-Instanz zu machen. Die einfachste Variante wurde bereits benannt. Ein reiner Übertragungstest führt dazu, dass die Daten ignoriert werden. Für die anderen Testvarianten muss die Art der Weiterverarbeitung der Daten festgelegt werden.
Es ist möglich, dass die auf einer tieferen Ebene enthaltenen Daten nicht durchgängig als Testdaten gekennzeichnet sind. Wenngleich es nicht empfehlenswert ist, könnte der Sender Echtdaten zum Zwecke der Test-Verarbeitung zweckentfremden. Ein auf Transport-Ebene als Test gekennzeichneter Vorgang darf natürlich nicht dazu führen, dass die Information vergessen wird, und ein später beteiligter Sachbearbeiter eine Test-Nachricht für echt hält.
Da die Art der Weitergabe der Daten von einer Ebene zu einer nächsten nicht Gegenstand des eXTra-Verfahrens ist, bleibt es dem Prozessverantwortlichen überlassen, wie er die Information, dass es sich um einen Test handelt, bzw. um welche Art eines Tests es sich handelt, an die folgenden Prozess-Beteiligten weitergibt.
Es ist auch möglich, dass eine Sendung auf der Transport-Ebene als echte Lieferung gekennzeichnet ist, dass aber auf einer tieferen Ebene ein Paket oder eine einzelne Fachnachricht als Testfall gekennzeichnet wurde. Der physikalische Sender und der physikalische Empfänger der Lieferung müssen über den Inhalt der Daten ja nicht Bescheid wissen. Es ist legitim, dass ein Prozessbeteiligter auf der Erzeugerseite seine Daten an den Prozessbeteiligten der gleichen Ebene auf der Empfängerseite als Test kennzeichnet.

5.2 Identifikation des physikalischen Senders

Fragestellung:
- Wie kann der Sender der Nachricht identifiziert werden?

Handelt es sich um ein verbund- bzw. fachspezifisches eXTra Verfahren, in dem die empfangende Stelle ihre jeweilige sendende Gegenstelle kennen muss, kann es notwendig sein, dass eine Verwaltung der zugelassenen Beteiligten vorgesehen werden muss. Muss die

Identität der Gegenstelle dabei sichergestellt werden, so sind entsprechende Nachweisverfahren vorzusehen. Ein zeitgemäßes Mittel hierfür ist die elektronische Signatur.
Denkbar sind auch Alternativen im Rahmen der Vergabe von User-IDs und Passwort je berechtigter Sender. Der Einsatz dieser Mittel ist nur dann sinnvoll, wenn gleichzeitig durch entsprechende Sicherheitsverfahren ein Ausspähen dieser Merkmale verhindert werden kann, z.B. Transportsicherung mittels SSL.
Im eXTra-Verfahren ist die Sender-ID als ein Muss-Element vorgesehen, da alle gängigen Fachverfahren sich dieses Begriffs bedienen.
Zusätzlich zur Sender-ID kann der Name des Beteiligten in den TransportHeader eingetragen werden.

5.3 Identifikation des physikalischen Empfängers

Fragestellung:
- Wie kann sichergestellt werden, dass die Nachricht für den Empfänger bestimmt ist?

Es sollte im Rahmen der Benennung aller Beteiligten des Verfahrens jeder Empfänger seine Identifizierung erhalten, um mit der Nachricht zu dokumentieren, für wen sie bestimmt ist. Die Benennung des Empfängers ist auch dann sinnvoll, wenn es nur einen möglichen Empfänger für die Daten geben sollte. Für die Identifikation des physikalischen Empfängers wird die ReceiverID vorgesehen, die im eXTra-Standard als verpflichtend definiert wurde.
Die Identifikation des Empfängers in einem unverschlüsselten Bereich der transportierten Nachricht ist nur dokumentarisch. Für eine zweifelsfreie Adressierung müssen darüber hinaus entsprechende Sicherheitsverfahren verwendet werden, z.B. eine Authentifizierung mittels Zertifikat.

5.4 Identifikation des Transports

Fragestellung:
- Wie kann ein Transportvorgang identifiziert werden?

Ein Transportvorgang muss für jeden der Beteiligten jederzeit nachvollziehbar sein. Jeder hat seine Datenbasis mit seinen eigenen Sprachmitteln definiert. Deshalb müssen bei der Identifizierung eines Transportvorgangs beide Seiten unabhängig voneinander dem Vorgang

einen Namen geben können. Bei eXTra werden diese Identifikatoren als RequestID für den Sender und als ResponseID für den Empfänger bezeichnet.
Idealerweise hebt sich jede Seite beide IDs auf, um jeweils mit den Sprachmitteln der Gegenseite umgehen zu können und eine Zuordnung zu den eigenen Sprachmitteln durchführen zu können. Für die Annahmestelle eines verbund- bzw. fachspezifischen eXTra Verfahrens, die mit vielen sendenden Beteiligten zu tun hat, die für sie vielleicht sogar anonyme Beteiligte sind, bedeutet die Verwaltung der RequestIDs und deren Zugehörigkeit zu den eigenen vergebenen ResponseIDs einen hohen Verwaltungsaufwand. Sinnvollerweise wird daher im Allgemeinen seitens der Annahmestelle nur die ResponseID zum gemeinsamen Sprachmittel erklärt, mit dem die Abstimmung im Problemfall zu erfolgen hat. Der Sender einer Nachricht hat demnach immer dafür Sorge zu tragen, dass er dem Empfänger den Transportvorgang mit dessen ID benennen kann.
Unabhängig davon haben beide Seite Sorge dafür zu tragen, dass sie dem Transportvorgang eine eindeutige Identifikationsbezeichnung zuordnen. Bei Wiederholung einer erfolgreichen Sendung wird eine neue ID sowohl auf Sender- als auch auf Empfänger-Seite empfohlen.
Zusätzlich zur ID der jeweiligen Seite ist jeweils ein Zeitstempel definiert, der zu Beginn des Sendvorgangs vom Sender (RequestDetails-TimeStamp) bzw. beim Ende des Empfangsvorgangs vom Empfänger (ResponseDetails-TimeStamp) belegt wird. Diese Zeitstempel sind zusätzlich ein hilfreiches Mittel, um einen Transportvorgang zu identifizieren.
Sieht das Fachverfahren für die Übertragung der Daten verpflichtende Termine vor, so ist die korrekte Belegung der Zeitstempel empfohlen. Es muss berücksichtigt werden, dass Sendungen, die von PCs von Privatpersonen ausgehen, nicht notwendigerweise mit einer korrekten Zeiteinstellung versehen sind. Deshalb ist üblicherweise der Zeitstempel der Annahmestelle maßgeblich dafür, ob die Abgabe termingerecht erfolgt ist und deshalb ist dieser Zeitstempel des Empfängers eine Pflichtangabe.

5.5 Software des physikalischen Senders

Fragestellung:
- welche Software setzt der physikalische Sender ein?

Das eXTra-Verfahren ist eine offene Schnittstelle. Aus Sicht des Verfahrens darf jedermann ein Programm entwickeln, um diese Schnittstelle zu bedienen.

Aus Sicht des Fachverfahrens können die Anforderungen an die verwendete Software höher sein. Im solchen Fall kann das Fachverfahren zur Sicherstellung der Datenqualität fordern, dass nur ausgewählte oder Qualitäts-geprüfte Programme am Verfahren teilnehmen dürfen.
Um solche Programme zu identifizieren, kann ein Registrierungsverfahren der zugelassenen Software notwendig werden. Registrierte Software erhalten hierbei eine Identifizierungsnummer (RegistrationID), die vom Fachverfahren vergeben werden. Muss die Registrierung bereits auf der Transport-Ebene nachgewiesen werden, so sollte mittels Sicherungsverfahren sichergestellt werden, dass das Merkmal nicht ausgespäht und von unbefugter Seite verwendet werden kann. Da der TransportHeader nicht verschlüsselt wird, bietet sich hierfür die Verwendung einer Transport-Verschlüsselung, wie z.B. SSL, an.
Zusätzlich zur Registrierungs-Identifikation bietet das eXTra-Verfahren Elemente für die Bezeichnung der Software (Product) sowie für deren Hersteller (Manufacturer).
Das Element Application, das die genannten Angaben zur verwendeten Software enthält, ist in der Definition des eXTra-Verfahrens optional.

5.6 Bezeichnung des Fachverfahrens

Eine Bezeichnung für das Fachverfahren (Procedure) ist aus eXTra-Sicht eine optional verwendbare Information. Nimmt ein physikalischer Empfänger die Daten im Auftrag mehrerer Fachverfahren entgegen, so sollte ein Name für das Verfahren vorgegeben werden.
Werden mehrere Pakete oder Fachnachrichten für unterschiedliche Fachverfahren in einer Sendung transportiert, sollte die Bezeichnung des Fachverfahrens auf der Transport-Ebene leer bleiben.

5.7 Bezeichnung des Datentyps

Die für die Bezeichnung des Fachverfahrens aufgeführten Kriterien gelten auch für die Verwendung der Bezeichnung des Datentyps (Datatype).
Werden mehrere Pakete oder Fachnachrichten unterschiedlichen Datentyps in einer Sendung transportiert, sollte der Datentyp auf der Transport-Ebene leer bleiben.

5.8 Art der Kommunikation

Fragestellung:
- Wie soll die Kommunikation zwischen Sender und Empfänger geregelt werden?

Eine Übertragung von Daten kann sich in der Art der Reaktion des Empfängers unterscheiden.

- Er kann die Daten ohne Reaktion entgegennehmen (fire-and-forget).
- Er kann dem Sender mitteilen, ob die Daten korrekt entgegengenommen werden konnten. Bestandteil dieser Antwort ist u. a. die oben beschriebene ResponseID (response-with-acknowledgement).
- Wenn es sich bei der gesendeten Nachricht um eine entsprechende Anforderung handelt, reagiert der Empfänger mit der Rückgabe der angeforderten Daten, wenn vorhanden (request-with-response).

Die Art der Kommunikation (Scenario) ist abhängig von Fachverfahren und Datentyp. Die drei Begriffe „Bezeichnung des Fachverfahrens“, „Bezeichnung des Datentyps“ und „Art der Kommunikation“ hängen eng zusammen und bedingen oft einander. Das Fachverfahren gibt vor, welche sinnvollen Kombinationen erlaubt sind.
Sollte das Verfahren für einen Datentyp mehrere Kommunikationsarten erlauben, hat der Sender der Nachricht die Wahl, welche Art der Kommunikation er verwenden möchte.

Die Art der Kommunikation wird in einer eXTra-Struktur in der Form einer URI dargestellt. Dabei ist der Pfad der vom Standard definierten Varianten vorgegeben, z.B.:

<Scenario>http://www.extra-standard.de/scenario/request-with-response</Scenario>

Sind im Rahmen des zu definierenden Verbund- bzw. fachspezifischen eXTra-Verfahrens weitere Kommunikationsarten sinnvoll, so werden diese mit einer URI des entsprechenden Fachverfahrens gekennzeichnet:

<Scenario>http://www.fachspezifisches_eXTra-verfahren-xy.de/scenario/NEUES
- SCENARIO</Scenario>

In der eXTra-Spezifikation sind folgende Kommunikationsarten vorgesehen:

- http://www.extra-standard.de/scenario/fire-and-forget
  Die Nachricht wird nach Empfang nicht beantwortet. Der physikalische Sender bleibt über den Erfolg seiner Übertragung im Unklaren.
- http://www.extra-standard.de/scenario/resquest-with-acknowledgement
  Der physikalische Sender erhält eine sofortige Antwort über den Erfolg seiner Lieferung. Über die Qualität der Antwort, d.h. welche Arbeitsschritte wurden bis zur Antwort ausgeführt, bestimmt das jeweilige verbund- bzw. fachspezifischen eXTra Verfahren.
- http://www.extra-standard.de/scenario/request-with-response
  Der physikalische Sender erwartet Daten in der Antwortstruktur.

Je Fachverfahren und Datenart unter Berücksichtigung des Transportverfahrens wird eine Auswahl der genannten Kommunikationsarten zugelassen.

Fragestellung:
- Wie kann der Sender damit umgehen, wenn der Empfänger nicht erreichbar ist, bzw. was kann der Empfänger tun, wenn er eine undefinierte Nachrichten erhält?

Wenn der physikalische Empfänger nicht erreichbar ist, oder die eXTra-Instanz auf Empfängerseite nicht antworten kann, sei es temporär z.B. wegen Wartungsarbeiten oder über längere Zeit, weil z.B. die Maßnahmen zur Wiederherstellung der Betriebsbereitschaft nach Fehlern noch nicht zu Ende sind, dann gibt es für derartige Fälle die eXTra-Nachricht ExtraError. Der physikalische Empfänger kann in solchen Fällen wenigstens eine kurze Rückmeldung, z.B. „service temporarily unavailable“ abgeben. Falls ein eXTra Request teilweise auswertbar war, können darüber hinaus auch noch einige wichtige eXTra spezifische Informationen wie RequestID, ResponseID, TimeStamp oder Report mitgegeben werden.
Die ExtraError Nachricht leistet auch dann gute Dienste, wenn die eXTra-Instanz auf Empfängerseite zwar beriebsbereit ist, aber undefinierte Nachrichten, möglicherweise nicht einmal XML-Dokumente erhält. Je nachdem wie weit die empfangene Nachricht überhaupt auswertbar ist, kann die ExtraError Nachricht neben der simplen Information „invalid request“ auch die oben erwähnten eXTra spezifische Informationen wie RequestID, ResponseID, TimeStamp oder Report enthalten.

5.9 Datenbereich

Neben dem TransportHeader gehört der TransportBody zu den notwendigen Bestandteilen einer eXTra-Nachricht. Wenn die Aussage der Nachricht nicht allein schon durch ihren Header klar ist, enthält der Body fachliche Daten, die es zu transportieren gilt.

Die fachlichen Daten der Transport-Ebene können eXTra-Strukturen der tieferen Ebenen sein, also Pakete oder Nachrichten im eXTra-Format, oder bereits die reinen Fachstrukturen.

Der Datenbereich kann im Auftrag (Request) mit den genannten Daten gefüllt sein. Es kann aber auch je nach Verfahren, Datentyp und Art der Kommunikation die Antwort (Response) mit einem gefüllten Datenbereich an den Sender zurückgegeben werden.

5.10 Individuelle Erweiterungen

Fragestellung:
- Das Verfahren benötigt Steuerungsparameter, die im Basis eXTra-Verfahren nicht vorgesehen sind.

Die Gestalter des eXTra-Verfahrens haben darauf geachtet, dass in die Header-Strukturen keine Elemente aufgenommen werden, die nur für einzelne wenige Verfahren relevant sind. Die Header sollen in kompakter Form die relevanten Informationen enthalten, wer an wen mit welchem Ergebnis Daten weitergibt.
Es hat sich aber gezeigt, dass bestehende Datenübermittlungsverfahren auf bestimmte Informationen außerhalb der Nutzdatenstrukturen nicht verzichten können. Für diese wurden Erweiterungen definiert. Im Sprachgebrauch von eXTra heißen diese Erweiterungen „Plug-Ins“.

Die bisher definierten Plug-Ins werden hier vorgestellt. Anregungen für weitere Erweiterungen im Zuge der Neugestaltung eines Fachverfahrens werden von der Arbeitsgruppe eXTra des AWV entgegengenommen.

5.10.1 Das Plug-In „DataTransforms“

Dieser Baustein ist zur Unterstützung der Migration von bestehenden Fachverfahren gedacht. Ziel ist es bestehenden Datenübermittlungsverfahren einen erleichterten Einstieg in eXTra zu ermöglichen, indem diese die verwendeten Verschlüsselungs-, Komprimierungs- und Signaturverfahren weiterhin nutzen können und sie nicht zu einem Wechsel dieser Verfahren zu zwingen.
Im Plug-In „DataTransforms“ kann einerseits jedes dieser drei Verfahren in einer Kurzform benannt werden, andererseits kann die Reihenfolge ihrer Nutzung festgelegt werden, z.B. bei gleichzeitiger Verschlüsselung und Komprimierung eines Bereiches. Über die drei Angaben „ID“, „Name“ und „Version“ kann ein Datenübermittlungsverbund das bei ihm aktuell verwendete Verfahren benennen. Die genaue Spezifikation, was sich hinter dieser Benennung verbirgt, muss der jeweilige Datenübermittlungsverbund, z.B. der gesetzlichen Krankenkassen GKV, an anderer Stelle hinterlegen, z.B. auf den eigenen Web-Seiten.

5.10.2 Das Plug-In „DataSource“

Zweck dieses Bausteins ist ebenso wie beim Plug-In „DataTransforms“ die Unterstützung bei der Migration bestehender Fachverfahren.
Mit diesem Plug-In können für ein bestehendes Datenübermittlungsverfahren mit angeschlossenem Fachverfahren unverzichtbare Informationen ausgetauscht werden, so dass das Fachverfahren beim Übergang auf den eXTra-Standard nicht geändert werden muss. Bei einem bestehenden Datenübermittlungsverbund, z.B. der Rentenversicherung (DRV) oder der gesetzlichen Krankenkassen (GKV) können diese unverzichtbaren Informationen wie der Name und der Ausgabestand einer Datensammlung, sowie dessen Erzeugungsdatum oder der verwendete Zeichensatz sein.

5.10.3 Das Plug-In „Certificates“

Auch dieser Baustein dient der Migration bestehender Fachverfahren in eXTra.
Mit diesem Plug-In kann der Sender dem Empfänger sein Verschlüsselungszertifikat mitgeben. Dadurch kann der Empfänger dem Sender später eine für ihn verschlüsselte Information, z.B. eine Rückantwort oder das Verarbeitungsergebnis zur Verfügung stellen. Ein Fachverfahren, das diesen Baustein benötigt, ist das Verfahren Elster der Finanzbehörden.

5.10.4 Das Plug-In „Contacts“

Dieses Plug-In dient dazu, dass der Sender gegenüber dem Empfänger einen zusätzlichen Informationskanal definieren kann. Hiermit kann der Empfänger dem Sender - derzeit nur über e-mail - eine Information zustellen. Wer beim Sender von welchen Ereignissen benachrichtigt werden soll, können die beiden Kommunikationspartner frei festlegen. Z.B. kann man mit diesem Mittel eine Erinnerungsfunktion realisieren, um den Sender daran zu erinnern, dass vor längerer Zeit Nachrichten bereitgestellt wurden, die noch nicht abgeholt wurden.

5.11 Sicherheits- und Effizienzverfahren

Fragestellung:
- Welche Maßnahmen optimieren den Übertragungsvorgang?
- Wie kann eine sichere Übertragung gewährleistet werden?

Zur Steigerung der Effizienz (kurze Übertragungszeiten) und zur Abwehr von Sicherheitsangriffen von Dritten bieten sich verschiedene Verfahren an.
Welche Verfahren möglich sein sollen und wie genau sie anzuwenden sind, muss in einer Verfahrensdokumentation beschrieben werden. Das Profilierungsergebnis in Form eines eigenen Schemas des verbund- bzw. fachspezifischen eXTra Verfahrens ist für diese Zwecke nicht ausreichend.
Bei mehreren hintereinander auszuführenden Sicherheits- und Effizienzverfahren muss festgelegt werden, in welcher Reihenfolge diese angewendet werden sollen. So macht es sicherlich Sinn umfangreiche Daten erst zu komprimieren bevor sie verschlüsselt werden.

5.11.1 Optimierung der Übertragung

Ein Transport der Daten soll schnell erfolgen. Besonders bei umfangreichen Datenmengen ist es sinnvoll über Optimierungsmaßnahmen nachzudenken.

- Schon durch die Wahl des zu verwendenden Transportprotokolls wird eine Vorentscheidung über die Geschwindigkeit der Übertragung getroffen. Bei entsprechender Leistung ist ein Internet-Protokoll deutlich schneller als z.B. ein ISDN-Protokoll.
- Die Leistung der installierten Hard- und Software beeinflusst die Effizienz des Verfahrens.

- Besonders bei umfangreichen zu übertragenden Datenmengen kann eine Komprimierung sinnvoll sein. Komprimiert wird in eXTra der gesamte Inhalt des Transport-Body.

5.11.2 Sicherung gegen unbefugtes Mitlesen

Die meisten Übertragungsverfahren bedienen sich heute eines Transport-Protokolls im Internet. Das hat zur Folge, dass prinzipiell jede Nachricht wie ein offenes Buch von unberufener Seite mitgelesen oder verändert werden kann.

- Eine Möglichkeit, dieses zu verhindern, ist die Verwendung eines Transport-Protokolls mit integrierter Verschlüsselung (SSL, TLS). Hierfür benötigt der Empfänger der Nachricht, der Server, ein von autorisierter Stelle (z.B. Verisign) beglaubigtes Zertifikat.
- Alternativ hierzu kann die Verschlüsselung einzelner Bausteine der eXTra-Nachricht vorgesehen werden. Verschlüsselt werden kann der Datenbereich als Ganzes und verschiedene Plugins mit sensiblen Inhalten, wie z.B. Öffentliche Schlüssel für spätere Rückmeldung, Adressangaben usw. Der TransportHeader oder Teile davon dürfen nicht verschlüsselt werden. Es sollten gängige ausreichend sichere Verschlüsselungsverfahren gewählt werden.

5.11.3 Sicherung gegen unbefugte Sender

Handelt es sich um ein Verfahren, bei dem jedermann eine Datei an den Empfänger übertragen darf, ist eine Sicherung gegen unbefugte Sender nicht notwendig.
Soll aber sichergestellt werden, dass nur autorisierte Partner eine Verbindung aufbauen, gibt es unterschiedliche Möglichkeiten:

- Bei Nutzung einer Transport-Verschlüsselung (SSL, TLS) kann die Verwendung eines Client-Zertifikats gefordert werden. Hierzu muss sich der Sender ein entsprechendes beglaubigtes Zertifikat besorgen.
- Ebenfalls auf Transport-Ebene können Zugangsberechtigungen mit Benutzerkennung und Passwort eingerichtet werden.

- Mit Hilfe einer elektronischen Signatur kann sich der Sender identifizieren und nebenbei noch die Unveränderbarkeit der Nachricht sicherstellen.

In allen Fällen muss auf Empfängerseite eine Datenbank gepflegt werden, in der gegen unerlaubten Zugriff gesichert die öffentlichen Schlüssel oder die Benutzerkennungen der autorisierten Sender eingetragen werden.

5.11.4 Sicherung gegen Verfälschung

Wie schon erwähnt, können ungesicherte Nachrichten von unbefugten Dritten nicht nur gelesen, sondern auch verändert werden. Um dies zu erkennen, bietet sich die schon beschriebene elektronische Unterschrift (Signatur) an.
Die Signatur auf Transport-Ebene wird auf der gleichen Ebene wie TransportHeader und TransportBody abgelegt. Welche Elemente der Transport-Ebene signiert werden, muss in der Beschreibung des verbund- bzw. fachspezifischen eXTra Verfahrens festgelegt werden. Alternativ sehen Sicherheitsverfahren wie z.B. die XML-Signatur Beschreibungen der signierten Bereiche vor.

5.11.5 Sicherstellung der Korrektheit der Daten

Das eXTra-Verfahren definiert eine XML-Struktur, in denen die fachlichen Nutzdaten eingebettet werden. Sowohl dem Sender der Nachricht als auch dem Empfänger wird empfohlen diese vor dem Senden bzw. nach dem Empfang zu validieren.
Bei manchen Datentypen, z.B. Protokollabholungen oder Quittungen, können von eXTra definierte Fachnachrichten verwendet werden. So kann bei Verwendung entsprechender Sicherheitsverfahren erst nach der Entschlüsselung und Dekomprimierung eine komplette Validierung der übertragenen Daten mit dem eXTra-Schema stattfinden.
Darüber hinaus kann es sich bei den Fachnachrichten natürlich ebenfalls um XML-Nachrichten oder einer Syntax folgenden strukturierten Datensätzen handeln. Auch hier kann die Korrektheit der Daten im Allgemeinen erst an späterer Stelle nach Abbau der Verbindung geprüft werden.

5.12 Ergebnis des Transports

Fragestellung:

- Welche Informationen erhält der physikalische Sender zurück?
- Welche Information müssen nachträglich bereitgestellt werden?

Der physikalische Sender der Nachricht möchte so weit möglich wissen, ob die transportierten Daten den Empfänger erreicht haben, ob sie erfolgreich entschlüsselt und geprüft wurden, und ob sie an die nächste Ebeneninstanz auf Empfängerseite weitergegeben werden konnten.

Die Art des Transports, die Größe der Daten sowie der Aufwand beim Transformieren und Validieren bestimmt, welche Informationen sofort zurückgegeben werden können. Wie in Kapitel „Art der Kommunikation“ beschrieben, bestimmt das Verfahren welche Anforderungen an die Reaktion auf den Transport zulässig sind.

Hat der physikalische Sender im Rahmen der zulässigen Kommunikationsarten ein Acknowledgement oder ein Response angefordert, erhält er notwendigerweise neben der vom Empfänger vergebenen Transportidentifikation und des Empfangs-Zeitstempels mindestens auch einen Status zurück.

Wesentlich bei der Rückgabe von Informationen im TransportHeader ist, dass sämtliche gesendeten Inhalte des Header in der Antwort unverändert an den Sender zurückgegeben werden. Ergänzt wird der Header um ein Struktur-Element ResponseDetails, welches die mindestens notwendigen Ergebnisinformationen enthält.

Weitere mögliche Informationen sind ein dedizierter Statuscode mit Statustext, sowie ergänzende Angaben, die bei einem Fehler zu Diagnosezwecken mitgeteilt werden können, wie z.B. ein Stack bei Verarbeitungsabbrüchen, Pfade von XML-Elementen bei Validierungsfehlern oder Angaben über das verursachende oder meldende Teil-System des Empfängers.

Sind Statuscodes vorgesehen, so sollten diese maschinell auswertbar sein. Ein flankierender beschreibender Text je Statuscode wird empfohlen.

Wird bei bestimmten Statuscodes eine Reaktion des Senders erwartet, z.B. wenn er aufgefordert wird, die Lieferung wiederholt zu senden, dann sollte eine Liste der möglichen Statuscodes mit Beschreibung der erwarteten Reaktion veröffentlicht werden.

Antworten auf einen Transport setzen ein Transportverfahren voraus, bei dem die Verbindung erhalten bleibt bis die Antwort zurückgegeben werden konnte. Im Idealfall ist in dieser Zeitspanne die Fachnachricht komplett elektronisch verarbeitet worden. Die Antwort enthält eine komplette Information über den Erfolg der Sendung. Dieser Idealfall ist im Allgemeinen

nicht gegeben. Je mehr Ebenen eingesetzt werden, je größer die Daten sind, bzw. wenn manuelle Arbeitsschritte einer Person notwendig sind, muss die Qualität der Antwort eingeschränkt werden.
Die Mindestanforderung an die Aussage einer Antwort ist, dass der Empfänger die Daten entgegennehmen und speichern konnte. Je mehr Arbeitsschritte im Zeitraum bis zur Antwort durchgeführt werden können, desto hochwertiger ist die Qualität der Aussage.
Wenn es nach einer positiven Antwort an den physikalischen Sender noch dazu kommen kann, dass die Fachnachricht ausgesteuert und nicht verarbeitet wird, muss sich das Fachverfahren Gedanken darüber machen, wie der Sender über den Misserfolg informiert werden soll. Möglichkeiten gibt es außerhalb des maschinellen Übermittlungsverfahrens durch Wechsel des Mediums (Anruf, Schreiben an den Sender der Nachricht). Soll aber die Mitteilung über einen Misserfolg ebenfalls maschinell erfolgen, so ist das verbund- bzw. fachspezifische eXTra Verfahren gezwungen über weitere Nachrichtentypen nachzudenken. Es sollte hierfür eine Abholung von Protokollen vorgesehen werden, im Rahmen deren solchen nachträgliche Fehlermeldungen zur Abholung bereitgestellt werden können (Stichwort Acknowledgement 2).

5.13 Logging

Fragestellung:
- Wie können eigene Informationen in der Verarbeitungskette weitergegeben werden?
- Welche Unterstützung bietet eXTra für ein Auskunftssystem?

Jede Ebene kann neben ihren obersten Strukturelementen Header, Body, Plug-Ins und Signatur noch einen Bereich für Protokollierung der Vorgänge beim Erstellen oder beim Verarbeiten der Nachricht nutzen.
Logging-Informationen sind geeignet, Informationen über die Ebenen hinweg in einer Art Laufzettel weiterzugeben. Relevante Informationen könnten z.B. der Hinweis auf den Zeitpunkt des Eingangs, auf erfolgreiche Signaturprüfungen, verwendete Schlüssel oder Komprimierverfahren sein, die bei Entfernen der Informationen der eigenen Ebene sonst verloren gehen würden.
Sieht das verbund- bzw. fachspezifische eXTra Verfahren eine Auskunftsmöglichkeit für Teilnehmer der erstellenden Seite vor, so kann bei entsprechender Architektur mit sofortigem Zugriff auf derartige Protokolle mitgeteilt werden, in welchem Verarbeitungsstand sich die jeweilige Lieferung aktuell befindet.

Auf der Transport-Ebene werden die typischen Aufgabengebiete des physikalischen Senders und des physikalischen Empfängers protokolliert.

6 Profilierung der Paket-Ebene

Fragestellung:

- Wann benötigt ein Fachverfahren eine Paket-Ebene?

Die Paket-Ebene befindet sich direkt innerhalb des TransportBody. Mit den auf dieser Ebene ausgetauschten Paketen kommunizieren zwei Instanzen auf Sender- und Empfängerseite miteinander, die möglicherweise mehrere einzelne Fachnachrichten zu einer logischen Einheit zusammenfassen und an die für den Transport zuständige Instanz weitergeben, bzw. die auf der Gegenseite ein Paket von der physikalisch empfangenden Stelle entgegennehmen und in einzelne Fachnachrichten trennen.

Die betreffenden Instanzen werden „logischer Sender“ und „logischer Empfänger“ genannt.

Gründe für das Definieren einer Paket-Ebene kann es mehrere geben:

- Die für den Transport zuständige Empfänger-Instanz ist in der Lage, mehrere Pakete gleichzeitig entgegenzunehmen und diese an verschiedene logische Empfänger zu verteilen. Hierbei müssen Empfänger und Datentyp der Pakete nicht notwendigerweise identisch sein. Eine derartige Lösung erhöht die Effizienz bei der Übertragung. Sie kann z.B. Service-Providern auf der Sender-Seite angeboten werden.
- Physikalischer Empfänger und logischer Empfänger dürfen nicht die gleichen Informationen erhalten. Die Daten müssen ggf. für den logischen Empfänger verschlüsselt werden. Der physikalische Empfänger muss zwar den PackageHeader sehen, um die Verteilung durchführen zu können, darf aber den Inhalt des Body nicht lesen. Das ist eine typische Situation bei Beauftragung eines Service-Providers auf der Empfänger-Seite.
- Der logische Empfänger benötigt Header-Informationen, die beim Transport verschlüsselt sein müssen, um nicht von unbefugten Dritten eingesehen zu werden. Wird kein entsprechendes Transport-Protokoll gewählt, so kann das Problem auf Transport-Ebene nur durch Verschlüsseln des TransportBody gelöst werden. Da der TransportHeader in diesem Fall die sensiblen Daten nicht enthalten darf, muss es einen PackageHeader geben, in dem diese Informationen eingetragen werden.
- Der logische Sender wird verpflichtet sein zusammengestelltes Paket zu signieren. Die Signatur wird parallel zum Header und Body in der Paket-Ebene abgelegt.

Die Entscheidung, ob eine Paket-Ebene benötigt wird, ist nicht nur abhängig von den Vorbedingungen der Empfängerseite, sondern richtet sich auch nach den Gegebenheiten typischer Sender.

- Die Sender-Seite bedient sich einen Service-Providers, der einzelne Nachrichten seiner Kunden erst sammelt, bevor er sie zu einem Paket für einen logischen Empfänger zusammenfasst.
- Wenn der Zusammenbau der Pakete und der Transport der Nachricht von unterschiedlichen Stellen durchgeführt werden, kann es notwendig sein, ein Paket bereits verschlüsselt an den Transporteur weiterzugeben.

Neben der Frage, ob einzelne Personen/Firmen ihre Daten übertragen, sollte daher auch immer betrachtet werden, ob es Service-Provider auf der Senderseite gibt, die gewöhnlich erhöhte Anforderungen an eine Transport-Schnittstelle haben.
Wird ein Auftrag, der Pakete enthält, gesendet, so sollte die Antwort nach Möglichkeit immer auch eins zu eins Pakete mit Ergebniswerten (fachliche Quittungen) zurückgeben. Sollte der physikalische Empfänger zeitlich oder organisatorisch nicht dazu in der Lage sein, die Entgegennahme der Pakete einzeln zu bestätigen, so kann dies ein Indiz dafür sein, dass eine weitere Fachnachricht notwendig wird, mit der die Ergebnisse der Paket-Ebene nachträglich erfragt werden können.
Ein Anfrage-Auftrag, der in der Antwort Pakete zurückgeliefert bekommt, muss nicht notwendigerweise selbst ein Paket gesendet haben. Ein typisches Beispiel hierfür ist das Senden einer Protokollanforderung, die allein aus einem TransportHeader mit entsprechenden Datentyp und leerem TransportBody besteht, oder nur eine steuernde Nachricht im TransportBody enthält. Auf Senderseite ist hierfür keine Paket-Ebene notwendig.

6.1 Testszenarien

Fragestellung:
- Welche Testmöglichkeiten soll es auf der logischen Ebene geben?

Über die Varianten der Testumgebungen wurde bereits im Kapitel 5.1 geschrieben. Auf der Paket-Ebene sind vom Prinzip her die gleichen Varianten möglich.

- Ein logischer Empfänger kann neben einer Empfangsstelle für echte Daten auch eine Empfangsstelle für Testdaten anbieten. Bei dieser Lösung muss der physikalische Empfänger Kenntnis dieser Vorgehensweise haben und das Testpaket an die richtige

Stelle weiterleiten. Der logische Sender steuert bei dieser Variante die Testdaten über die Identifikation des logischen Empfängers.

- Manche Verfahren kennzeichnen Testdaten mit einem eigenen Datentyp. Echtdaten werden anders bezeichnet als Testdaten. In diesem Fall muss der logische Sender für die Versorgung des richtigen Datentyps sorgen.
- In der Beschreibung der Daten wird ein Testvorgang als solcher gekennzeichnet. Auch bei dieser Lösung muss der logische Sender die gewünschte Variante eintragen.

Standardmäßig werden in eXTra auf der Paket-Ebene folgende Testvarianten unterschieden:

- Test der Entgegennahme des Paketes durch den logischen Empfänger; die empfangenen Daten werden ignoriert. Diese Variante macht für die Sender-Seite wenig Sinn, da hier speziell die Verbindung des physikalischen zum logischen Empfänger getestet wird.
- Test der bei Erstellung oder der Entgegennahme der Daten notwendigen Arbeitsschritte, wie z.B. Erstellen/ Validieren der Beschreibungsdaten, Komprimieren/ Dekomprimieren, Verschlüsseln/ Entschlüsseln, Signieren/ Signatur prüfen usw. Die Daten werden nicht weitergereicht.
- Verarbeiten der als Testdaten gekennzeichneten Daten. Diese Möglichkeit kann dann sinnvoll sein, wenn als Folge der Verarbeitung weitere asynchron abzuholende Informationen, wie z.B. Protokolle oder Bescheide, erstellt werden, die ja ebenfalls getestet werden sollten.

Wie bereits ausführlich beschrieben, ist die Behandlung der Daten über die Ebenengrenzen hinweg sorgfältig zu bedenken.
Grundsätzlich steuert der logische Sender, welche Daten er als Testdatei betrachtet. Echtdaten müssen vom physikalischen Sender korrekt gekennzeichnet transportiert werden. Sie dürfen technisch zwar zusätzlich auch zu Testzwecken verwendet werden. Allerdings haben hier alle Beteiligte eine besondere Verantwortung zur sorgfältigen und vertraulichen Behandlung der Testdaten.
Ein zu Testzwecken gekennzeichnetes Paket kann unterhalb eines als Echtdaten gekennzeichneten TransportHeader parallel zu echten Paketen gesendet werden.
Alle Daten unterhalb eines Testpaketes sind als Testdaten zu betrachten und müssen vom logischen Empfänger vor der Weitergabe an die Endempfänger als solche gekennzeichnet werden.

6.2 Identifikation des logischen Senders

Fragestellung:

- Wie kann der logische Sender der Nachricht identifiziert werden?

Prinzipiell gelten die in Kapitel 5.2 gemachten Anmerkungen auch für den logischen Sender. Ein logischer Sender muss lediglich dem logischen Empfänger bekannt sein.

6.3 Identifikation des logischen Empfängers

Fragestellung:

- Wie kann sichergestellt werden, dass die Nachricht für den logischen Empfänger bestimmt ist?

Prinzipiell gelten die in Kapitel 5.3 gemachten Anmerkungen auch für den logischen Empfänger.
Ein logischer Empfänger muss folgenden Instanzen bekannt sein: Der logische Sender adressiert ihn. Der physikalische Sender muss zuordnen können, an wen die Nachricht gesendet werden soll. Der physikalische Empfänger muss beim Trennen Pakete zuordnen können, an wen er das Paket weitergeben muss.

6.4 Identifikation des Paketes

Fragestellung:

- Wie kann ein Datenpaket identifiziert werden?

Die Erstellung und der Empfang eines Paketes müssen für jeden der Beteiligten jederzeit nachvollziehbar sein. Jeder hat seine Datenbasis mit seinen eigenen Sprachmitteln definiert. Deshalb müssen bei der Identifizierung eines Paketes beide Seiten unabhängig voneinander dem Vorgang einen Namen geben können. Bei eXTra werden diese Identifikatoren als RequestID für den Sender und als ResponseID für den Empfänger bezeichnet.
Die Anforderungen an eine Identifikation auf Sender- und auf Empfänger-Seite gelten in gleicher Weise wie in Kapitel 5.4.

Auf Empfängerseite macht die Vergabe eine Paket-Identifikation nur dann Sinn, wenn im Rahmen des Verfahrens mindestens eine Übertragung mit Bestätigung (acknowledgement) auf der Paket-Ebene vorgesehen ist.

6.5 Software des logischen Senders

Fragestellung:
- welche Software setzt der logische Sender ein?

Wie auf der Transport-Ebene in Kapitel 5.5 beschrieben, kann es auch auf der Paket-Ebene zu besonderen Anforderungen an die verwendete Software kommen. Hierbei ist es nicht notwendig, dass die Software, die die Sender-Seite auf der Paket-Ebene nutzt, identisch ist zu der Software, die der physikalische Sender zum Transport verwendet.
Konsequenterweise sollten Anforderungen an die Software, die ein logischer Empfänger vorgibt, sich nur auf die Komponenten beschränken, die auf der Sender-Seite für das Zusammenbauen der Pakete und, falls es keine Nutzdaten-Ebene gibt, für das Erstellen der Nutzdaten verantwortlich ist.

6.6 Bezeichnung des Fachverfahrens

Eine Bezeichnung für das Fachverfahren (Procedure) ist aus eXTra-Sicht eine optional verwendbare Information. Nimmt ein logischer Empfänger die Daten im Auftrag mehrerer Fachverfahren entgegen, so sollte ein Name für das Verfahren auf Paket-Ebene vorgegeben werden.

6.7 Bezeichnung des Datentyps

Die für die Bezeichnung des Fachverfahrens aufgeführten Kriterien gelten auch für die Verwendung der Bezeichnung des Datentyps (Datatype).
Werden allerdings mehrere Fachnachrichten unterschiedlichen Datentyps in einem Paket übertragen, sollte der Datentyp auf der Paket-Ebene und auf der Transport-Ebene leer bleiben.

6.8 Art der Kommunikation

Fragestellung:
- Wie soll die Kommunikation auf der Paket-Ebene geregelt werden?

Die in Kapitel 5.8 beschriebenen möglichen Reaktion des Empfängers gelten gleichermaßen auch für die Paket-Ebene. Je nach Fachverfahren muss untersucht werden, welche unmittelbaren Antworten auf der Paket-Ebene zum Sender zurück erfolgen können.
Der physikalische Empfänger hat die Aufgabe, die Pakete an die richtigen logischen Empfänger weiterzuleiten. Bei dieser Aktion sieht er die Einträge des PackageHeader. Wenn er nun selbst dem Sender der Daten eine Bestätigung (acknowledgement) zurückgibt, kann er immer auch eine Bestätigung je Paket zurückgeben, dass er den PackageHeader interpretieren konnte, und dass er das Paket zur Weitergabe gespeichert oder sofort an den logischen Empfänger weitergegeben hat. Weitergehende Informationen auf Paket-Ebene sind nur dann möglich, wenn eine Online-Verbindung zwischen physikalischen Sender und Empfänger so lange geöffnet bleibt, bis der logische Empfänger die Entgegennahme oder Verarbeitung des Paketes selbst bestätigen konnte.
In Kapitel 9.1 werden Szenarien der unterschiedlichen Kommunikationsarten über die Ebenen hinweg dargestellt.

6.9 Datenbereich

Die fachlichen Daten der Paket-Ebene können eXTra-Strukturen der tieferen Ebenen sein, also Nachrichten im eXTra-Format, oder bereits reine Fachstrukturen.

Der Datenbereich kann im Auftrag (Request) mit den genannten Daten gefüllt sein. Es kann aber auch je nach Verfahren, Datentyp und Art der Kommunikation die Antwort (Response) mit einem gefüllten Datenbereich an den Sender zurückgegeben werden.

6.10 Individuelle Erweiterungen

Die Unterbringung von individuellen Merkmalen, die nicht in den Header-Strukturen enthalten sind, wurden bereits in Kapitel 5.10 vorgestellt. Die vier bisher bekannten Plug-Ins sind dort beschrieben. Die Nutzung der Plug-Ins ist auf jeder Ebene gleich möglich.

6.11 Sicherheits- und Effizienzverfahren

Fragestellung:
- Welche Maßnahmen optimieren die Paketübergabe?
- Wie kann eine sichere Übertragung gewährleistet werden?

Auch auf der Paket-Ebene bieten sich verschiedene Verfahren zur Steigerung der Effizienz (kurze Übertragungszeiten) und zur Abwehr von Sicherheitsangriffen von Dritten an.
Welche Verfahren möglich sein sollen und wie genau sie anzuwenden sind, muss in einer Verfahrensdokumentation beschrieben werden. Das Profilierungsergebnis in Form eines eigenen Schemas des verbund- bzw. fachspezifischen eXTra Verfahrens ist für diese Zwecke nicht ausreichend.
Bei mehreren hintereinander auszuführenden Sicherheits- und Effizienzverfahren muss festgelegt werden, in welcher Reihenfolge diese angewendet werden sollen. So macht es sicherlich Sinn umfangreiche Daten erst zu komprimieren bevor sie verschlüsselt werden.
In den folgenden Unterkapiteln werden Sende-Aufträge mit enthaltenen Paketen beschrieben. Die dort beschriebenen Maßnahmen sind jedoch auch für den umgekehrten Weg bei Hol-Aufträgen mit im Response enthaltenen Paketen gültig.

6.11.1 Optimierung der Übertragung

Ein Transport der Daten soll schnell erfolgen. Besonders bei umfangreichen Datenmengen ist es sinnvoll über Optimierungsmaßnahmen nachzudenken. Das verwendete Transport-Protokoll spielt dabei für die Paket-Ebene keine Rolle.
Soll die Transport-Ebene sich nicht mit Komprimierverfahren beschäftigen müssen, so bietet sich eine Komprimierung unterhalb des PackageBody an.

6.11.2 Sicherung gegen unbefugtes Mitlesen

Wenn die Transport-Ebene nicht schon durch Auswahl eines entsprechenden Transport-Protokolls ihren Datenbereich vor unbefugtem Lesen schützt, oder wenn die Daten der Paket-Ebene nicht für den Transporteur lesbar sein sollen, oder dieser sich nicht im Besitz der

notwendigen Schlüssel befindet, sollte eine Verschlüsselung des PackageBody vorgesehen werden.
Ebenso wie auf der Transport-Ebene können auch hier einzelne Erweiterungs-Bausteine gesondert verschlüsselt werden.
Sollte der PackageHeader schützenswerte Angaben enthalten, wie z.B. Identifikatoren oder persönlich Angaben, so kann die Sicherung dieser Inhalte nur durch eine Verschlüsselung der gesamten Paket-Ebene einschließlich Header und Body erreicht werden. Eine derartige Verschlüsselung kann nur der Transporteur durchführen.
Der logische Sender einer Nachricht kann seinen eigenen Header nicht verschlüsseln.

6.11.3 Sicherung gegen unbefugte Sender

Handelt es sich um ein Verfahren, bei dem jedermann ein Paket an den Empfänger übertragen darf, ist eine Sicherung gegen unbefugte Sender nicht notwendig.
Soll aber sichergestellt werden, dass nur von autorisierten Partnern ein Paket gesendet wird, bieten sich auf der Paket-Ebene folgende Maßnahmen an:

- Es können Zugangsberechtigungen mit Benutzerkennung und Passwort eingerichtet werden. In diesem Fall ist eine Verschlüsselung auf Transport-Ebene notwendig, da unverschlüsselte Benutzerkennungen keine Sicherheit bieten, sondern nur beschreibender Natur sind.
- Mit Hilfe einer elektronischen Signatur kann sich der logische Sender identifizieren und nebenbei noch die Unveränderbarkeit der Nachricht sicherstellen.

Auf der Empfängerseite muss hierfür eine Datenbank gepflegt werden, in der gegen unerlaubten Zugriff gesichert die öffentlichen Schlüssel oder die Benutzerkennungen der autorisierten logischen Sender eingetragen werden.

6.11.4 Sicherung gegen Verfälschung

Zur Sicherstellung der Unverfälschtheit eines Paketes bietet sich die schon beschriebene elektronische Unterschrift (Signatur) an.
Die Signatur auf Paket-Ebene wird auf der gleichen Ebene wie PackageHeader und PackageBody abgelegt. Welche Elemente der Paket-Ebene signiert werden, muss in der Beschrei-

bung des verbund- bzw. fachspezifischen eXTra Verfahrens festgelegt werden. Alternativ sehen Sicherheitsverfahren wie z.B. die XML-Signatur Beschreibungen der signierten Bereiche vor.

6.11.5 Sicherstellung der Korrektheit der Daten

Wird auf Verwendung von Sicherheitsverfahren auf der Paket-Ebene verzichtet, so umfasst eine Validierung durch den physikalischen Empfänger bereits die XML-Elemente der Paket-Ebene. Wird jedoch der PackageBody gesondert verschlüsselt, so ist eine Validierung bzw. syntaktische Prüfung der Daten erst nach Entschlüsselung durch den logischen Empfänger möglich.

6.12 Ergebnis des Transports

Fragestellung:
- Welche Informationen erhält der logische Sender zurück?

Besteht zwischen dem Bündeln eines Paketes durch den logischen Sender und dem Senden desselben Paketes oder mehrerer Pakete durch den physikalischen Sender ein zeitlicher Versatz, so kann der logische Sender nicht davon ausgehen, dass er sofort eine Reaktion zum Erfolg seiner Lieferung von der Gegenseite erhält. In der inneren Kommunikation zwischen logischem und physikalischem Sender muss ein nachträglicher Abruf der erhaltenen Response-Daten vorgesehen werden.

Werden Pakete in einer Transporteinheit gesendet, so sollte jedes Verfahren eine Antwort je Paket vorsehen.
Wesentlich bei der Rückgabe von Informationen im PackageHeader ist, dass sämtliche gesendeten Inhalte des Header in der Antwort unverändert an den Sender zurückgegeben werden. Ergänzt wird der Header um ein Struktur-Element ResponseDetails, welches die mindestens notwendigen Ergebnisinformationen enthält.
Wenn die Sende-Struktur keine Paket-Ebene enthält, so kann trotzdem in der Antwort-Struktur eine Paket-Ebene enthalten sein. In diesem Fall wird empfohlen in den Package-Headern die RequestDetails der ursprünglichen Lieferung einzutragen, falls es sich um Ergebnisse einer ursprünglichen Lieferung handelt. Wenn nicht, sollten die PackageHeader die RequestDetails des TransportHeader der aktuellen Anfrage zurückgeben.

ResponseDetails zu einem gesendeten Paket, die bei bestehender Verbindung erzeugt werden, beschreiben im Allgemeinen nicht die komplette Verarbeitung eines Paketes, sondern nur das Ergebnis der bei geöffneter Verbindung möglichen Arbeitsschritte. Weitere Arbeitsschritte, die zu einem Abbruch der Verarbeitung führen können, wie z.B. eine asynchrone Validierung der Nutzdaten, sollten nachträglich in einem bereits erwähnten Acknowledgment 2 protokolliert werden.

7 Profilierung der Nachrichtenebene

Fragestellung:
- Wann benötigt ein Fachverfahren eine Nachrichten-Ebene?

Die Nachrichten-Ebene befindet sich direkt innerhalb des TransportBody oder des PackageBody. Mit den auf dieser Ebene ausgetauschten Nachrichten kommunizieren zwei Instanzen, möglicherweise Personen, auf Sender- und Empfängerseite miteinander, die genau eine Nachricht erstellen und an die für das Sammeln oder den Transport zuständige Instanz weitergeben, bzw. die auf der Gegenseite ein Einzelnachricht von der physikalisch empfangenden Stelle oder dem logischen Empfänger entgegennehmen verarbeiten.

Die betreffenden Instanzen werden Ersteller und Verarbeiter genannt.

Gegenstand des Verfahrens ist es Fachnachrichten auszutauschen. Von einer vorhandenen Nachrichtenebene spricht man dann, wenn die einzelne Nachricht in eine eXTra-Struktur mit MessageHeader, MessageBody und ggf. zusätzlich die Erweiterungen (Plugins), Protokollierungen (Logging) und Unterschriften (Signatures) enthält.

Gründe für das Definieren einer Nachrichten-Ebene kann es mehrere geben:

- Die Daten sind derart sensibel, dass nur der Verarbeiter der Nachricht diese lesen darf. Der physikalische oder der logische Empfänger müssen zwar den MessageHeader sehen, um die Verteilung durchführen zu können, dürfen aber den Inhalt des Body nicht lesen.
- Der Verarbeiter benötigt Header-Informationen, die beim Transport verschlüsselt sein müssen, um nicht von unbefugten Dritten eingesehen zu werden. Wird kein entspre-

chendes Transport-Protokoll gewählt, so kann das Problem auf Transport-Ebene durch Verschlüsseln des TransportBody oder des PackageBody gelöst werden.

- Der Ersteller wird verpflichtet seine Nachricht zu signieren. Die Signatur wird parallel zum Header und Body in der Nachrichten-Ebene abgelegt.

Wird ein Auftrag, der mehrere Nachrichten enthält, gesendet, so sollte die Antwort nach Möglichkeit immer auch eins zu eins Nachrichten mit Ergebniswerten zurückgeben. Sollte der physikalische oder der logische Empfänger zeitlich oder organisatorisch nicht dazu in der Lage sein, die Entgegennahme der Nachricht einzeln zu bestätigen, so kann dies ein Indiz dafür sein, dass eine weitere Fachnachricht notwendig wird, mit der die Ergebnisse der Nachrichten-Ebene nachträglich erfragt werden können.
Ein Auftrag, der in der Antwort Nachrichten zurückgeliefert bekommt, muss nicht notwendigerweise selbst ein Nachricht gesendet haben. Ein typisches Beispiel hierfür ist das Senden einer Protokollanforderung, die allein aus einem TransportHeader mit entsprechenden Datentyp und leerem TransportBody besteht, oder nur eine steuernde Nachricht im TransportBody enthält. Auf Senderseite ist hierfür keine Paket- oder Nachrichten-Ebene notwendig. Sehr wohl kann die Antwort aber Pakete und/oder mehrere Nachrichten mit ergebniswerten enthalten.

Bei der Entscheidung für oder gegen eine Nachrichtenebene muss berücksichtigt werden, dass sich die Größe der transportierten Datei in Verfahren mit vielen ausgetauschten Nachrichten in einer Paket- oder Transport-Einheit durch das Vorhandensein zusätzlicher XML-Strukturen vor allem der MessageHeader deutlich erhöht. Sind die oben genannten Kriterien nicht gegeben, kann dies auch zu der Entscheidung führen, auf die Nachrichten-Ebene zu verzichten und die Fachnachrichten kompakt in strukturiertes Datenformat unterzubringen. Bei Verfahren, in denen lediglich Einzel-Nachrichten transportiert werden, spielt diese Überlegung eine geringere Rolle.

7.1 Testszenarien

Fragestellung:
- Welche Testmöglichkeiten soll es auf der Nachrichten-Ebene geben?

Über die Varianten der Testumgebungen wurde bereits im Kapitel 5.1 und 6.1 geschrieben. Auf der Nachrichten-Ebene sind vom Prinzip her die gleichen Varianten möglich, jedoch nicht unbedingt alle in gleicher Weise sinnvoll.

- Ein Verarbeiter wird aller Voraussicht nach keinen eigenen Testeingang besitzen. Bei Verfahren, in der eine hohe Anzahl Ersteller einer ebenfalls hohen Anzahl Verwerter gegenübersteht, z.B. Verfahren zwischen Bürger und Verwaltung, ist die Verwaltung einer doppelten Anzahl Eingangskanäle wohl wenig sinnvoll.
- Manche Verfahren kennzeichnen Testdaten mit einem eigenen Datentyp. Echtdaten werden anders bezeichnet als Testdaten. In diesem Fall muss der Ersteller für die Versorgung des richtigen Datentyps sorgen.
- In der Beschreibung der Nachricht wird ein Testvorgang als solcher gekennzeichnet. Auch bei dieser Lösung muss der Ersteller die gewünschte Variante eintragen.

Standardmäßig werden in eXTra auch auf der Nachrichten-Ebene folgende Testvarianten unterschieden:

- Test der Entgegennahme der Nachricht durch den Verwerter; die empfangenen Daten werden ignoriert. Diese Variante macht für die Ersteller-Seite wenig Sinn, da hier speziell die Verbindung des physikalischen oder logischen Empfängers zum Verwerter getestet wird. Sie kann aber durchaus in Integrationstests einer Server-Anwendung auf Empfängerseite eine Rolle spielen.
- Test der bei Erstellung oder der Entgegennahme der Daten notwendigen Arbeitsschritte, wie z.B. Validieren der Beschreibungsdaten, Komprimieren/Dekomprimieren, Verschlüsseln/Entschlüsseln, Signieren/Signatur prüfen usw. Die Daten werden nicht verarbeitet.
- Verarbeiten der als Testdaten gekennzeichneten Daten. Diese Möglichkeit kann dann sinnvoll sein, wenn die Endanwendung für die Verarbeiter getestet werden soll, oder wenn als Folge der Verarbeitung weitere asynchron abzuholende Informationen, wie z.B. Protokolle oder Bescheide, erstellt werden.

Wie bereits ausführlich beschrieben, ist die Behandlung der Daten über die Ebenengrenzen hinweg sorgfältig zu bedenken.
Grundsätzlich steuert der Ersteller, welche Nachricht er zu Testzwecken erstellt hat. Bei der Weitergabe der Nachrichten über die verschiedenen Ebenen darf diese ihren Testzweck nicht verlieren. Eine gekennzeichnete Test-Nachricht kann unterhalb eines als Echtdaten

gekennzeichneten TransportHeader oder PackageHeader parallel zu echten Nachrichten gesendet werden.

7.2 Identifikation des Erstellers

Fragestellung:

- Wie kann der Ersteller der Nachricht identifiziert werden?

Prinzipiell gelten die in Kapitel 5.2 und 6.2 gemachten Anmerkungen auch für den Nachrichten-Ersteller.
Ein Ersteller muss lediglich dem Verwerter der Nachricht bekannt sein. Bei Verfahren mit einem großen Teilnehmerkreis ist u. U. ein erheblicher Aufwand für die Verwaltung der Ersteller-Identifikationen notwendig.

7.3 Identifikation des Verwerters

Fragestellung:

- Wie kann sichergestellt werden, dass die Nachricht für den Verwerter bestimmt ist?

Die Fragestellung könnte auch heißen: Muss der Verwerter der Nachricht überhaupt bekannt sein?
Wenn die Verarbeitung der Nachricht mit einem manuellen Eingriff verbunden ist, und wenn der Verwerter eine Person, z.B. ein Sachbearbeiter im Auftrag einer Verwaltung ist, so ist er dem Ersteller der Nachricht sehr wahrscheinlich nicht bekannt. Der Ersteller wird also nicht die verarbeitende Person, sondern eine Organisationseinheit benennen, die für die Verarbeitung der Nachricht zuständig ist. Eine Zuteilung auf Personen findet dann auf Empfängerseite statt. Der Vorgang der Zuteilung gehört zum Aufgabengebiet des logischen Empfängers.

7.4 Identifikation der Nachricht

Fragestellung:

- Wie kann eine Nachricht identifiziert werden?

Die Anforderungen an eine Identifikation auf Sender- und auf Empfänger-Seite gelten in gleicher Weise wie in Kapitel 5.4 und 6.4 beschrieben.
Auf Empfängerseite ist die Vergabe eine Nachrichten-Identifikation im Rahmen des Übertragungsverbundes nur dann notwendig, wenn mindestens eine Übertragung mit Bestätigung (acknowledgement) auf der Nachrichten-Ebene vorgesehen ist.

7.5 Software des Erstellers

Fragestellung:
- welche Software setzt der Ersteller der Nachricht ein?

So wie in den anderen benannten Ebenen, kann es auch auf der Nachrichten-Ebene zu besonderen Anforderungen an die verwendete Software kommen. Hierbei ist es nicht notwendig, dass die Software, die die Sender-Seite auf der Nachrichten-Ebene nutzt, identisch ist zu der Software, die der logische Sender zur Bündelung oder der physikalische Sender zum Transport verwendet.
Es kommt darauf an, was die Intention hinter der Vergabe von Software-Identifikationen ist und auf welcher Ebene der Empfänger ggf. ungenehmigte Software-Produkte abwehren möchte. Während die Aufgabengebiete der Transport- und der Paket-Ebene eher Querschnittsthemen behandeln, dürften die Qualitäts-Anforderungen an die Software, mit der die eigentliche fachliche Nachricht erstellt wird, am höchsten sein.
Ein weiterer Grund für die Vergabe von Software-Identifikationen kann es sein, dass lediglich eine Übersicht mit statistischen Auswertungen der im Einsatz befindlichen Produkte erreicht werden soll.

7.6 Bezeichnung des Fachverfahrens

Eine Bezeichnung für das Fachverfahren (Procedure) ist aus eXTra-Sicht eine optional verwendbare Information. Während die Querschnittsthemen Transport und Bündelung u. U. mehrere Fachverfahren bedienen, und daher u. U. keine eindeutige Bezeichnung festgelegt werden kann, gibt es auf der Nachrichten-Ebene keinen Grund, darauf zu verzichten. Eine Nachricht wird im Rahmen genau eines Fachverfahrens erstellt und übertragen. Das Verfahren sollte daher benannt werden.

7.7 Bezeichnung des Datentyps

Wie die Bezeichnung des Fachverfahrens ist auf der Nachrichten-Ebene jeder Nachricht ein eindeutiger Datentyp zuordenbar. Ein Datentyp sollte, auch wenn zwischen den beiden Partnern immer nur ein Datentyp ausgetauscht wird, eingetragen werden.

7.8 Art der Kommunikation

Fragestellung:
- Wie soll die Kommunikation auf der Nachrichten-Ebene geregelt werden?

Wird das eXTra-Verfahren in der Vollausbaustufe mit drei Ebenen über mehrere unterschiedliche Instanzen genutzt, so ist eine direkte Antwort des Verwerters auf die Nachricht des Erstellers eher unwahrscheinlich. Gänzlich unmöglich ist diese, wenn die Bearbeitung der Nachricht manuell erfolgt, denn es müsste in dieser Zeit ja die Leitung offen gehalten werden.
Im Allgemeinen wird eine auf die Nachricht bezogene Rückmeldung asynchron in einer eigenen Anforderung abgeholt werden müssen. Zur Verarbeitung einer Rückmeldungsanforderung darf kein manueller Handgriff auf Empfänger-Seite notwendig sein. Die Rückmeldungen müssen vom System des Verwerters bereitgestellt werden und auf Anfrage automatisch übergeben werden können.
In einem Dialog-Verfahren kann diese Anforderung durch den Ersteller direkt gestellt werden. Sind jedoch Prozesse wie Paketbildung und Transport durch einen beauftragten Provider vorgesehen, so ist es günstig, die bereitstehenden Rückmeldungen durch den Provider abholen zu lassen. Dieser kann dann die Rückmeldungen auf der Sender-Seite für den Abruf durch den Ersteller der ursprünglichen Nachricht bereithalten.

7.9 Datenbereich

Als unterste Ebene sind die eigentlichen Fach-Nachrichten jeweils im MessageBody untergebracht. Es kann sich hierbei um XML-Nachrichten handeln oder um beliebige andere Strukturen.

Der Datenbereich kann im Auftrag (Request) mit den genannten Daten gefüllt sein. Es kann aber auch je nach Verfahren, Datentyp und Art der Kommunikation die Antwort (Response) mit einem gefüllten Datenbereich an den Sender zurückgegeben werden.

7.10 Individuelle Erweiterungen

Die Unterbringung von individuellen Merkmalen, die nicht in den Header-Strukturen enthalten sind, wurden bereits in Kapitel 5.10 vorgestellt. Die vier bisher bekannten Plug-Ins sind dort beschrieben. Die Nutzung der Plug-Ins ist auf jeder Ebene gleich möglich.

7.11 Sicherheits- und Effizienzverfahren

Die in Kapitel 6.11 beschrieben Effizienz- und Sicherungsverfahren für ein Paket gelten prinzipiell auch für die Nachrichten-Ebene – jedoch mit einer Einschränkung.
Lediglich bei der Übertragung einer einzelnen Nachricht macht es Sinn, diese zu komprimieren und zu verschlüsseln. Handelt es sich um viele Nachrichten unterhalb eines Paketes, so ist die Komprimierung und Verschlüsselung der Einzelnachrichten eher unwirtschaftlich. Hier sollten die Verfahren eher auf die Paket-Ebene verlagert werden.

Sind die Nachrichten von verschiedenen Erstellern erzeugt worden, so kann es im Rahmen des Verfahrens durchaus notwendig sein, dass jeder Ersteller die Nachricht signiert. Die Prüfung vieler Signaturen in einer großen Sammeldatei ist dann trotz der damit verbundenen Performance-Problematik notwendig.

7.12 Ergebnis des Transports

Fragestellung:
- Welche Informationen erhält der Ersteller zurück?

Es kann bei Verwendung mehrerer Ebenen davon ausgegangen werden, dass zwischen dem Erstellen der Nachricht und dem Entgegennahme durch den Verwerter eine längere Zeit vergeht. Eine direkte Antwort des Erstellers auf seinen Auftrag kann in solchen Fällen nicht sofort zurückgegeben werden. Der physikalische Sender erhält im besten Fall die Antworten

zu den enthaltenen Paketen zurück. In der indirekten Kommunikation zwischen Ersteller und Verwerter muss ein nachträglicher Abruf der Response-Daten vorgesehen werden.

Im Falle, dass nur eine Einzelnachricht, vielleicht sogar ohne vorhandene Paket-Ebene übertragen wird, mag eine sofortige Antwort möglich sein, in der die syntaktische Korrektheit, Entschlüsselbarkeit und Speicherung der Nachricht zurückgemeldet wird.

8 Die Fachnachricht

Das eXTra-Verfahren ermöglicht das Senden oder Holen beliebig gestalteter Fachnachrichten.

- Bei den Nachrichten kann es sich um Strukturen im XML-Format handeln. Diese sollten zur Abgrenzung gegen die eXTra-spezifischen Strukturen in einem eigenen Namensraum definiert sein.
- Die Nachricht kann beliebige nicht in XML definierte Satz-Strukturen enthalten. Stimmt der verwendete Zeichensatz nicht mit dem Encoding der gesamten XML-Datei überein, so muss die Nachricht mindestens Base64-codiert in die XML-Datei des eXTra-Verfahrens eingefügt werden.
- Für einige in verschiedenen Fachverfahren wiederkehrende Prozessschritte, wie z.B. Protokollanforderungen bzw. das holen bereitgestellter fachlicher Daten oder Bestätigungen abgeholter Daten, wurden im Rahmen des eXTra-Verfahrens eigene formalisierte Nachrichtentypen definiert, sogenannte eXTra Standardnachrichten.

8.1 eXTra Standard-Nachrichten

8.1.1 Anfordern bereitgestellter Daten

Beim Senden von fachlichen Nachrichten ist die Nachricht selbst der Gegenstand, den der Sender an den Empfänger übergeben möchte.

Beim Holen von fachlichen Nachrichten wird eine Anforderung gesendet, die im einfachsten Fall einen leeren Datenteil enthält und nur mit den Inhalten der Header die Anforderung beschreibt. Eine Anforderung mit leerem Datenteil bedeutet mangels vorhandener Parametrisierung soviel wie „Gib mir alles, was du hast!“

Mit einer derartigen pauschalen Anforderung kann der Sender der Nachricht nicht steuern, wie umfangreich die Rückantwort ausfallen wird. Es gibt verschiedene Gründe, die es dem Sender ermöglichen sollten, den Abholvorgang feiner zu steuern und zu beeinflussen.

- Jedes System hat eine begrenzte Kapazität. Für das Abholen großer Datenmengen durch unterschiedlich dimensionierte Systeme sollte es möglich sein, die gewünschte Datenmenge zu begrenzen.
- Sind mehrere Anforderungen notwendig, um alle bereitgestellten Daten abzuholen, muss der Sender der Anforderung einen Aufsetzpunkt bezeichnen können, bis zu dem er die bereitgestellten Daten schon abgeholt hat.
- Kann eine bestimmte Datei nicht abgeholt werden, weil sie z.B. syntaktisch nicht korrekt ist, und wird sie aus diesem Grund später nicht als abgeholt bestätigt, so muss es eine Möglichkeit geben, ohne manuellen Aufwand, diese Datei bei weiteren Anforderungen zu übergehen.
- Kommt es bei der Folgeverarbeitung der Daten zu einer Fehlverarbeitung oder gehen die abgeholten Daten verloren, kann es notwendig werden, dass bereits abgeholte Daten noch einmal angefordert werden.

In eXTra wurde daher eine eXTra Standard-Nachricht „DataRequest“ definiert, die es über eine Folge von Kriterien ermöglicht, die Menge der angeforderten Daten bzw. Fachnachrichten einzuschränken bis hin zur Anforderung genau einer einzigen Fachnachricht. Zugleich kann damit ein Aufsetzpunkt definiert und ggf. auch eine obere Grenze für die Menge der abzuholenden Daten benannt werden. Es wird ermöglicht, die abzuholende Datenmenge zu begrenzen, indem die maximal gewünschte Größe der Daten in Bytes/Kilobytes/Megabytes oder die maximale gewünschte Anzahl der abzuholenden Pakete oder Nachrichten angegeben werden kann.
Für die Definition eines Aufsetzpunkts können verschiedene Attribute wie z.B. ResponseID, ResponseFileName oder ResponseCreationTime bestimmt werden.

Für den Fall, dass der Sender mehrere Anforderungen mit einem Kommunikationsvorgang stellen will, gibt es die eXTra Standard-Nachricht „ListOfDataRequest“, in der hintereinander mehrere „DataRequest“ Nachrichten enthalten sind.

8.1.2 Bestätigen abgeholter Daten

Die Annahmestelle, die Daten zur Abholung bereitstellt, ist daran interessiert, Resourcenschonend arbeiten zu können und die Menge der gespeicherten Daten gering zu halten. Deshalb ist oft der abschließende Schritt einer Bestätigung abgeholter Daten im Gesamtprozess vorgesehen.
Es handelt sich bei dabei um einen eigenen Sendevorgang. Die hierbei gesendeten Daten enthalten Angaben zu den abgeholten Daten, die vom Sender auf Seiten der Annahmestelle nicht mehr benötigt werden.

eXTra hat zu diesem Zweck eine weitere eXTra Standard-Nachricht „ConfirmationOfReceipt“ definiert. In dieser sind Angaben zu den geholten Daten enthalten. Bei den möglichen Angaben zur Identifikation der geholten Daten sollte es sich um Kennzeichen handeln, die sämtlich aus den Header- oder Plug-In-Bereichen der vorherigen Abholung gelesen werden können. Es bieten sich hierfür die vormals genannten Attribute ResponseID, ResponseFileName oder ResponseCreationTime an.
Sieht der Prozess die Abholung vieler einzelner Pakete oder Nachrichten vor, so ist es sinnvoll, eine Sammelbestätigung zu ermöglichen, d.h. das Bestätigen mehrerer abgeholter Daten in einem Sendevorgang.

Soll darüber hinaus der Sender die Möglichkeit erhalten, mehrere (Sammel-)Bestätigungen in einem Kommunikationsvorgang abzugeben, gibt es die eXTra Standard-Nachricht „ListOfConfirmationOfReceipt“, in der hintereinander mehrere „ConfirmationOfReceipt“ Nachrichten enthalten sind.

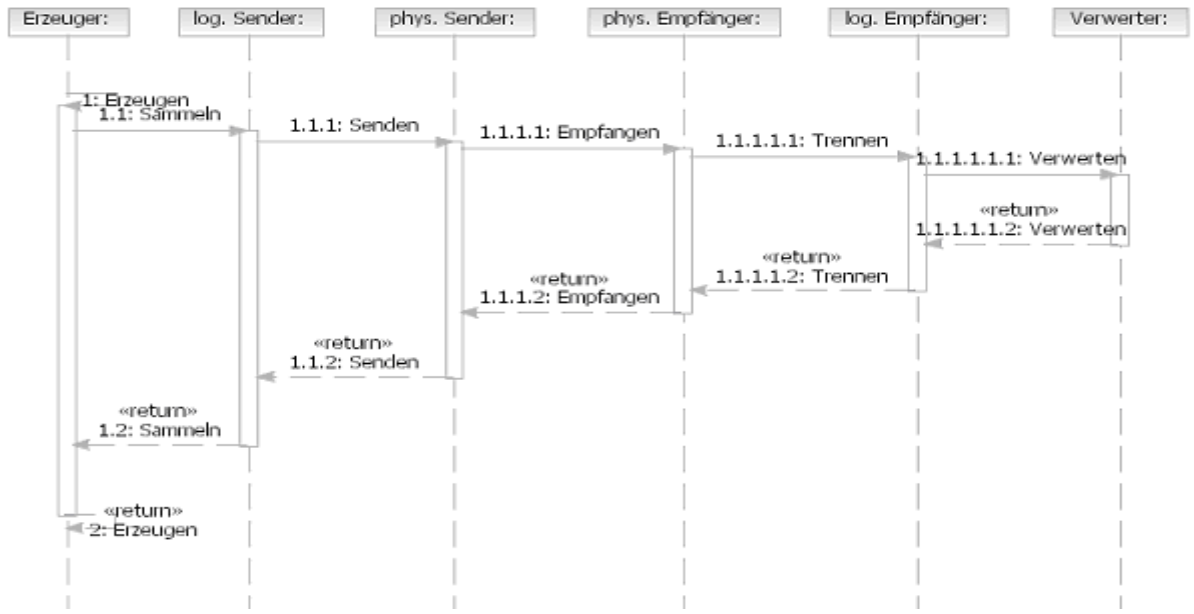
9 Ausgestaltung des Dialogs

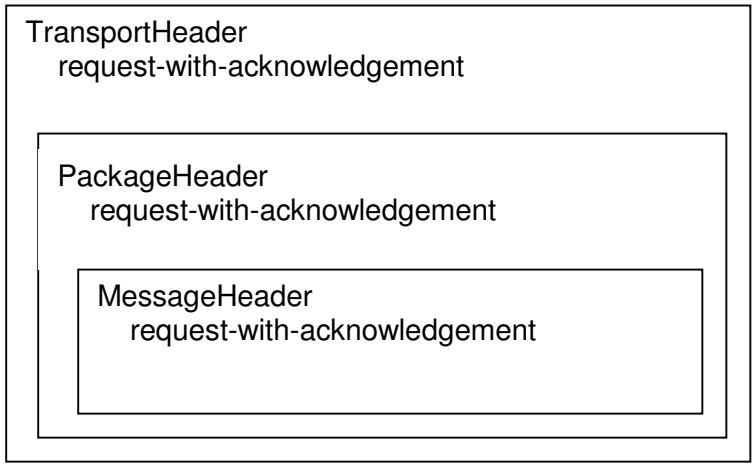
9.1 Zusammenspiel Request Response

Das Zusammenspiel der verschiedenen Instanzen im Zuge des Zusammenstellens, Transportierens und Auseinandernehmens einer eXTra-Nachricht hängt davon ab, wie eng die Instanzen auf der Empfänger-Ebene untereinander zusammen arbeiten. Je enger die Zusammenarbeit auf der Empfängerseite, desto mehr Information bekommt der Sender auf seinen Request zurück.

Im Moment der Datenübertragung vom physikalischen Sender an den physikalischen Empfänger bestimmt der Umfang der Antworten, die der Sender erwarten kann, welche Kommunikationsarten in den Header der verschiedenen Ebenen eingetragen werden können. Wenn der physikalische Sender in die Header der Paket- und Nachrichtenebene nicht selbst korrigierend eingreifen will, muss er die korrekte Versorgung des Feldes scenario von seinen ihn beliefernden Instanzen verlangen.

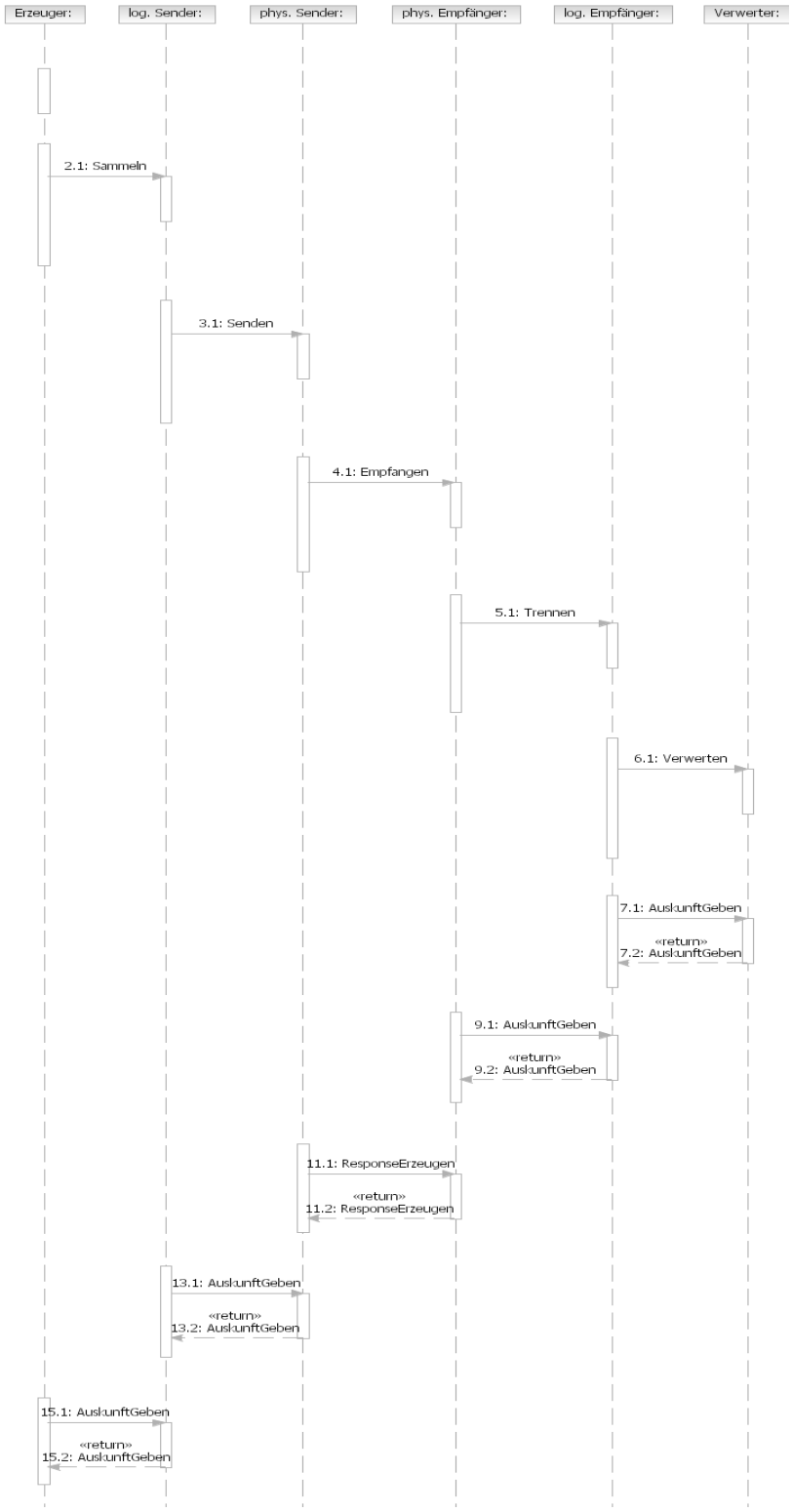
9.1.1 Beispiel 1: Komplette synchrone Verarbeitung





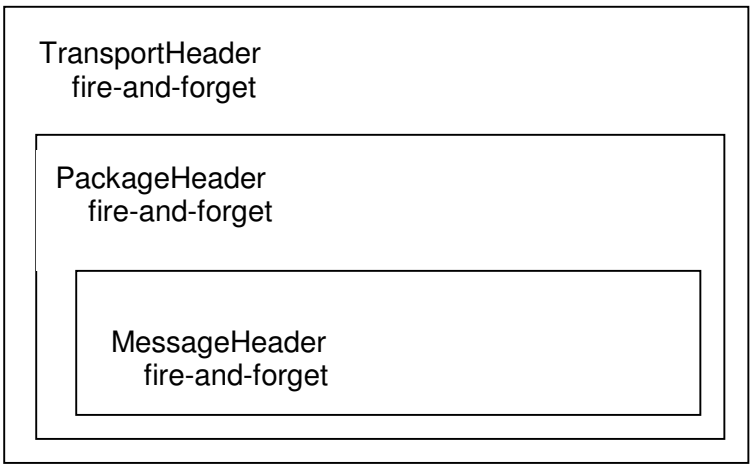
Obige Abbildung zeigt das Idealbild einer Kommunikation, in der über alle Ebenen hinweg die Leitungen bis zur Antwort an den Erzeuger einer Nachricht offen gehalten werden. Bei einer solchen Vorgehensweise, die in der Praxis selten anzutreffen sein wird, kann auf jeder Ebene durchgehend ein …/request-with-acknowledgement oder …/request-with-response eingetragen werden.

9.1.2 Beispiel 2: Komplett asynchrone Verarbeitung

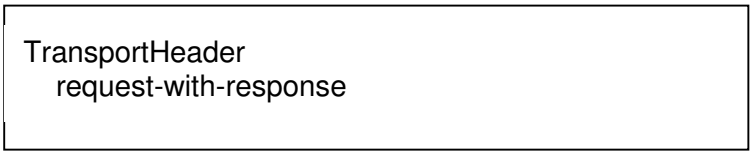


Im anderen Extrem werden sämtliche Weitergabe- und Transport-Aktionen sowie anschließende Statusabfragen, wenn das Fachverfahren diese vorsieht, asynchron aufgerufen. Obiges Bild zeigt die Idealfolge, bei der jeder Statusabfragender eine endgültige Meldung bekommt, da der Auskunft gebende bereits im Besitz der Informationen ist.
Hierfür können sämtliche Akteure in ihren Header eine Kommunikationsart „./fire-and-forget eintragen.

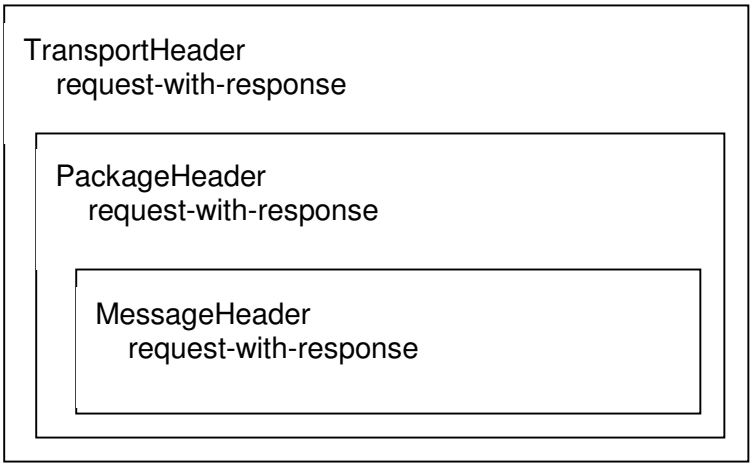
Header-Einträge für den ersten Request (Senden der Daten):



Header-Einträge für den zweiten Request (Statusabfrage)

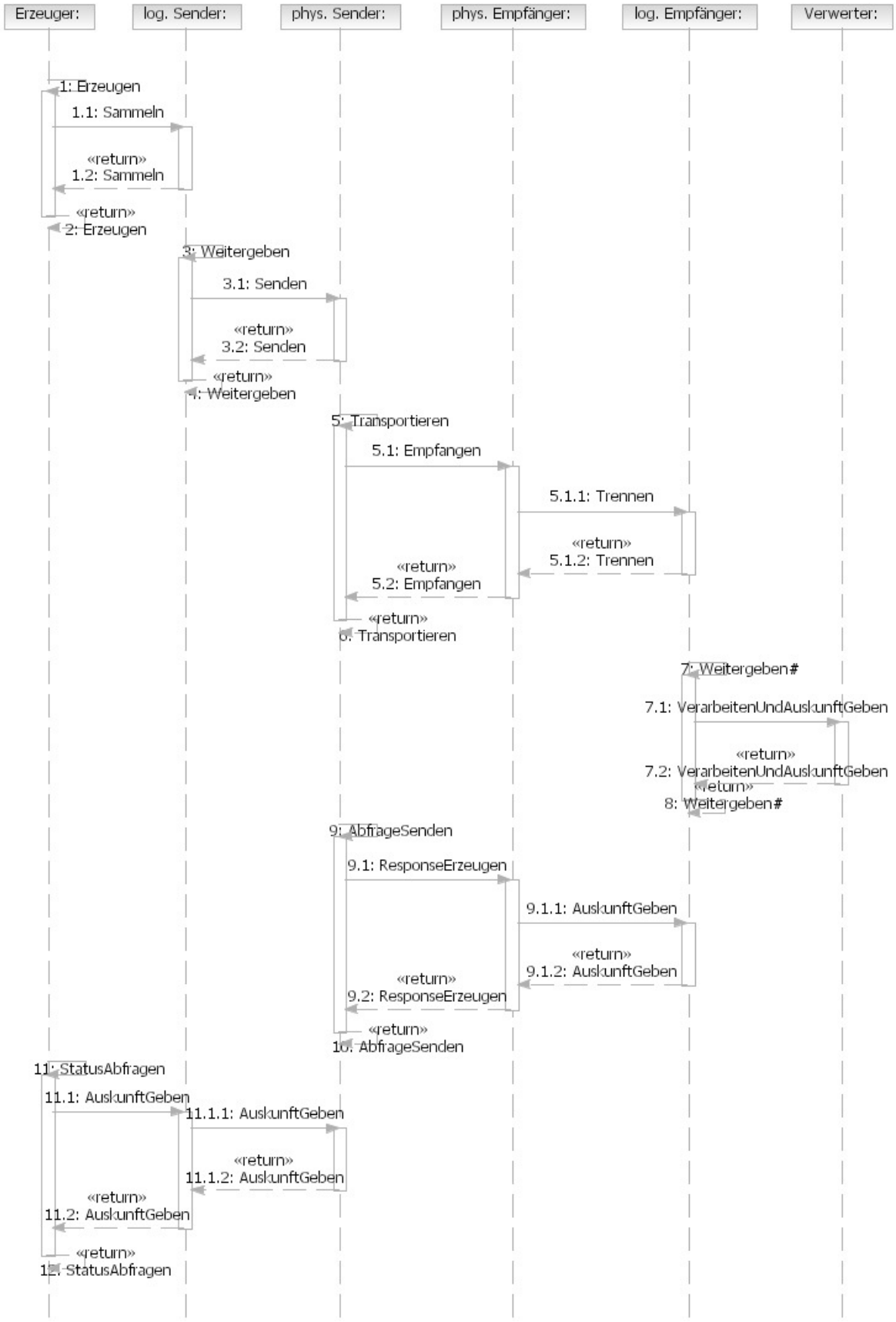


Und zugehöriger Response:

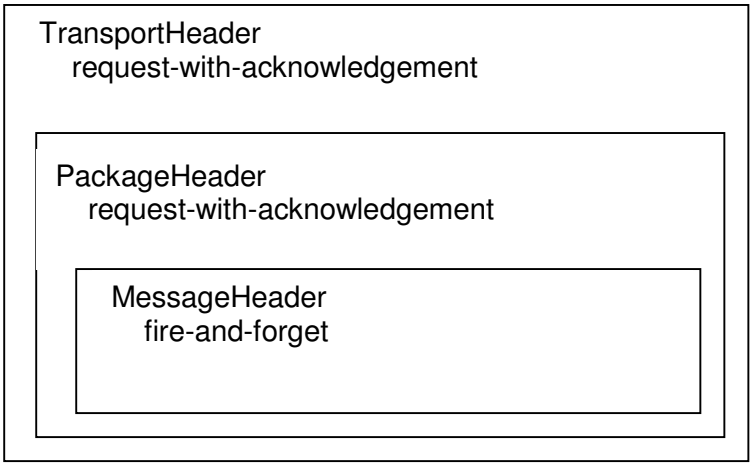


9.1.3 Beispiel 3: Teilweise synchrone/asynchrone Verarbeitung

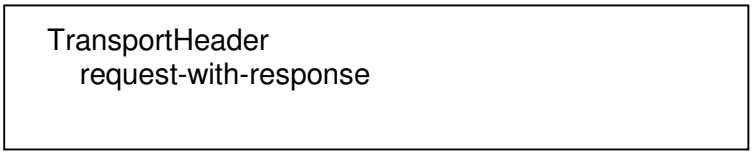
Der Normalfall in einem Fachverfahren wird sein, dass einige Schritte synchron, andere wiederum asynchron verarbeitet werden.
Wie schon erwähnt, sind die Gegebenheiten auf der Sender-Seite nicht relevant für die Versorgung der Kommunikationsarten. Es kommt auf die Gegebenheiten der Empfänger-Seite und auch auf das Transferprotokoll an, ob Informationen in einer Anschaltung zurückgegeben werden können.
Hier ein Beispiel für teilweise eng zusammen arbeitende Instanzen:


Erzeuger:
log. Sender:
phys. Sender:
phys. Empfänger:
log. Empfänger:
Verwerter:
1: Erzeugen
1.1: Sammeln
«return»
1.2: Sammeln
«return»
2: Erzeugen
3: Weitergeben
3.1: Senden
«return»
3.2: Senden
«return»
4: Weitergeben
5: Transportieren
5.1: Empfangen
5.1.1: Trennen
«return»
5.1.2: Trennen
«return»
5.2: Empfangen
«return»
6: Transportieren
7: Weitergeben#
7.1: VerarbeitenUndAuskunftGeben
«return»
7.2: VerarbeitenUndAuskunftGeben
«return»
8: Weitergeben#
9: AbfrageSenden
9.1: ResponseErzeugen
9.1.1: AuskunftGeben
«return»
9.1.2: AuskunftGeben
«return»
9.2: ResponseErzeugen
«return»
10: AbfrageSenden
11: StatusAbfragen
11.1: AuskunftGeben
11.1.1: AuskunftGeben
«return»
11.1.2: AuskunftGeben
«return»
11.2: AuskunftGeben
«return»
12: StatusAbfragen

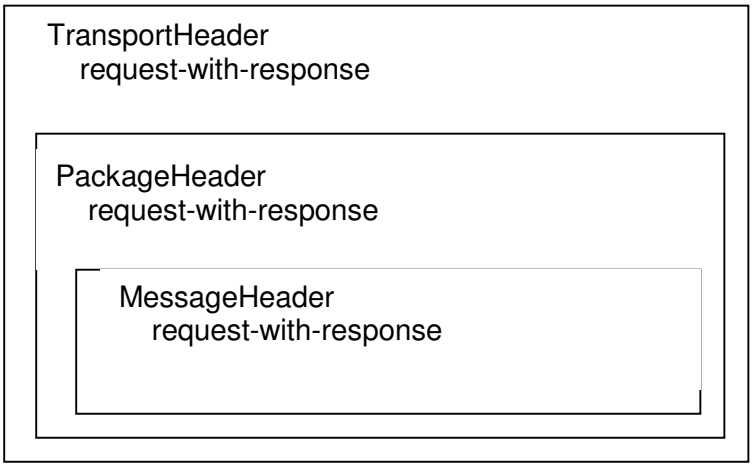
Header-Einträge für den ersten Request (Senden der Daten):



Header-Einträge für den zweiten Request (Statusabfrage)



Und zugehöriger Response:



10 Beispielhafte Modellierung eines eXTra Datenübermittlungsverfahrens

10.1 Allgemeines

Der Leistungsumfang eines verbundspezifischen Datenübermittlungsverfahrens[1] wird überwiegend durch die Topologie auf Empfängerseite, dem oder den geforderten Betriebsmodi Dialogbetrieb, Sende- und/ oder Holbetrieb, sowie dem auf Sender- und Empfängerseite gefordertem Automatisierungsgrad von Sende- und Rückmeldungsvorgängen bestimmt. Zusätzliche Aspekte werden durch die Massendatenverarbeitung hervorgerufen, sowohl durch die Sendung einer sehr umfangreichen Meldung eines Unternehmens als auch durch Bündelung der Meldungen vieler Unternehmen.

[1] Ein derartiges Datenübermittlungsverfahrens eines Datenübermittlungsverbundes ist z.B. das Elster-Verfahren der Finanzverwaltung, das Arbeitgeberverfahren der gesetzlichen Krankenkassen oder das Core Verfahren des statistischen Bundesamtes jeweils mit Meldepflichtigen aus der Wirtschaft

10.2 Das Modell eines eXTra-Servers auf Empfängerseite

Das folgende Bild gibt einen Überblick über die beispielhafte Architektur eines eXTra-Servers auf Empfängerseite und dessen Zusammenspiel mit den angegliederten Fachverfahren.

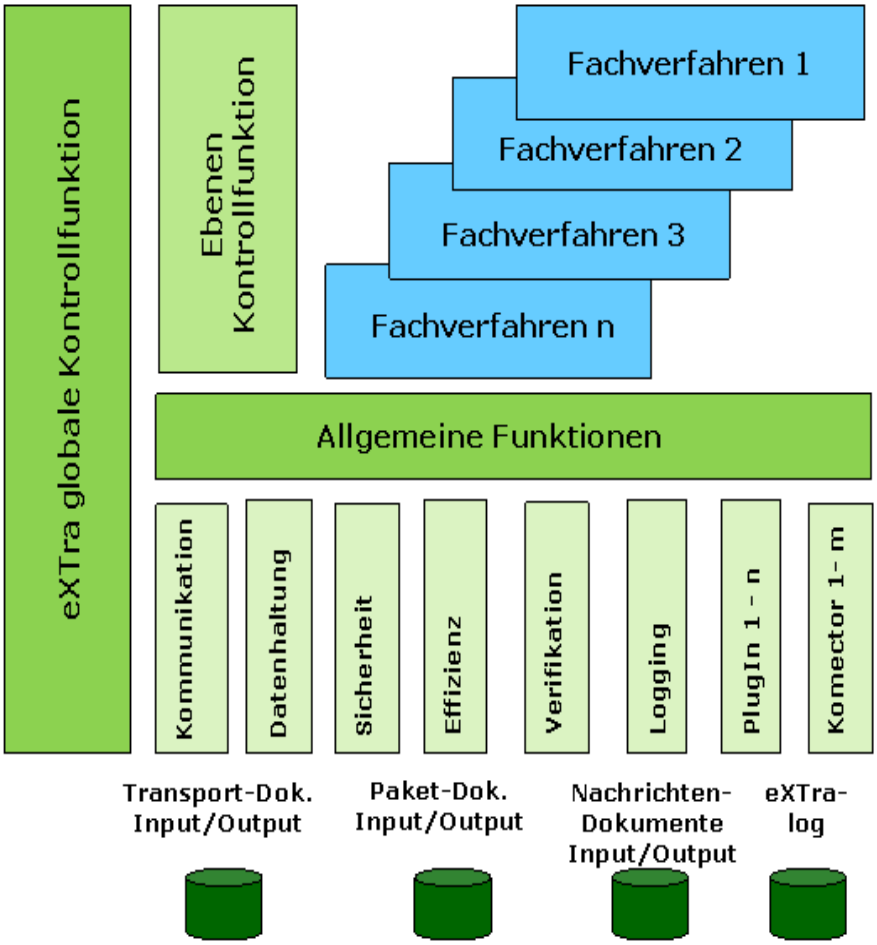


Bild 2: Das statische Modell eines eXTra-Servers, der mehrere Fachverfahren (blau hinterlegt) bedient, wobei die Fachverfahren beispielhaft lokal angesiedelt sind

Der eXTra Server ist nach diesem Modell untergliedert in

- eine Globale Kontrollfunktion
- eine Ebenen Kontrollfunktion
- allgemeine Funktionen, die von jeder Kontrollfunktion verwendet werden können

Die Globale Kontrollfunktion

Über diese Kontrollfunktion stellt der eXTra-Server die Verbindung mit der Außenwelt der Sender, d.h. der eXTra-Clients her. Andererseits gibt die globale Kontrollfunktion die Kontrolle weiter an die Transport-Ebene, sprich die Ebenenkontrollfunktion.

Die Ebenen Kontrollfunktion

Die Ebenen Kontrollfunktion steuert alle Vorgänge, die innerhalb einer eXTra-Ebene ablaufen und regelt den Übergang von einer eXTra-Ebene zur nächsten bzw. zum angeforderten Fachverfahren. Die Steuerung dieser Vorgänge ist auf jeder eXTra-Ebene weitgehend identisch, sodass eine gemeinsame Kontrollfunktion für alle eXTra-Ebenen ausreichend ist. Ebenenspezifische Kontrollfunktionen sind ebenso denkbar, sollte sich dies bei einer konkreten Realisierung als angemessen herausstellen.
Die Ebenen Kontrollfunktion bedient sich im Zuge der Vorgangssteuerung – wie auch die Globale Kontrollfunktion - einer Reihe von allgemeinen Funktionen, die schematisch als „allgemeine Funktionen“ zusammengefasst sind.

Die allgemeinen Funktionen

Diese Funktionen oder Funktionsgruppen sind ebenenunabhängig gestaltet, d.h. sie decken jeweils ein streng abgegrenztes Funktionsspektrum ab, das von jeder eXTra-Ebene genutzt werden kann. Hierin äußert sich u.a. auch der funktionale Gleichklang der eXTra-Ebenen.
Während die Globale Kontrollfunktion wie auch die Ebenenkontrollfunktion weitgehend unabhängig von der tatsächlichen Systemumgebung des eXTra-Servers ist, so abhängig sind die „allgemeinen Funktionen“ von der vorgegebenen Systemumgebung, z.B. vom Datenmanagementsystem, vom Sicherheitssystem und von den realen Schnittstellenbedingen der verschiedenen angegliederten Fachverfahren.
Einige dieser „allgemeinen Funktionen“ abstrahieren demgemäß die Systemumgebung, z.B. die allgemeine Funktion „Kommunikation“ und „Datenhaltung“, „Sicherheit“ und „Effizienz“ setzen die vom jeweiligen Datenübermittlungsverbund getroffene konkrete Auswahl um an Sicherheits- und Effizienzfunktionen, die ebenfalls eXTra-unabhängig sind. Die Funktionsgruppe „PlugIns“ dient zum einen dazu, die Migration eines bestehenden Datenübermittlungsverfahrens hin zu eXTra zu erleichtern, andererseits zur Ergänzung des eXTra-Standards um Aspekte, die dieser nicht bietet. „Logging“ hingegen ist eine pure eXtra-spezifische Funktion. Die wichtigste Aufgabe der Funktionsgruppe „Konnektoren“ ist es eine Brückenfunktion zwischen dem eXTra-Server und der Welt der Fachverfahren zu bilden.

„Kommunikation“
In dieser Funktion ist das Zusammenspiel mit den Remote-Partnern auf der DFÜ-Ebene, z.B. auf der Basis von http, https, ftp etc. angesiedelt

„Datenhaltung“
Die Thematik der Datenhaltung, ob mit einer Datenbank oder mit konventionellen System mitteln gearbeitet wird, ist hier angesiedelt.

„Sicherheit“ und „Effizienz“
Alle Verschlüsselungs-, Authentifizierungs- Signatur- sowie alle Komprimierungsfunktionen, die auf den eXTra-Ebenen zur Geltung kommen, sind in diesen beiden Funktionsgruppen zusammengefasst.

„Verifikation“
Die Verifizierung der eXTra-Dokumente findet hier statt, insbesondere die der eingehenden Dokumente auf Transport-Ebene.

„PlugIns“
In dieser eXTra-spezifischen Funktionsgruppe sind alle vom eXTra-Server unterstützten PlugIns angesiedelt. Sie können von jeder eXTra-Ebene verwendet werden.

„Logging“
Die eXTra Logging-Funktion steht ebenfalls allen eXTra-Ebenen zur Verfügung, um gegebenenfalls sehr detailliert die einzelnen Vorgänge mit zu protokollieren und damit bei Fehlfunktionen einen Nachvollzug zu gewährleisten. Zusätzlich kann man die Logging-Funktion auch dazu benutzen, um Informationen vom Eingang in den eXTra-Server bis hin zum Fachverfahren durchzuschleußen.

„Konnektoren“
In dieser Funktionsgruppe sind alle „Konnektoren“ des eXTra-Servers zusammengefasst. Über Konnektoren wird die Verbindung der eXTra-Ebenen untereinander, sowie vom eXTra-Server zu den einzelnen angebundenen Fachverfahren hergestellt. Da für die einzelnen Fachverfahren möglicherweise ganz unterschiedliche Schnittstellenbedingen (Aufruf, Versorgung) gelten, wird es in der Regel mehrere Konnektoren geben. Erst innerhalb des Konnektors wird sichtbar, ob das Fachverfahren z.B. lokal oder remote angesiedelt ist, ob es über eine Datei- oder eine prozedurale Schnittstelle angesprochen werden kann etc.

Fachverfahren

Die Fachverfahren wurden in das Bild 2 mit aufgenommen, um deren Anordnung im Zusammenspiel mit dem eXTra-Server darzustellen.

Eine besondere Rolle spielt der sog. eXTra-Auslieferungs-Server, der auf Grund seiner Charakteristik als Fachverfahren eingeordnet ist und somit ein eXTra-Fachverfahren darstellt.

10.3 Die dynamischen Abläufe im Modell eines eXTra-Servers auf Empfängerseite

Dynamisch laufen in jeder Ebene hintereinander vergleichbare Vorgänge ab, die beispielhaft folgendem Schema genügen:

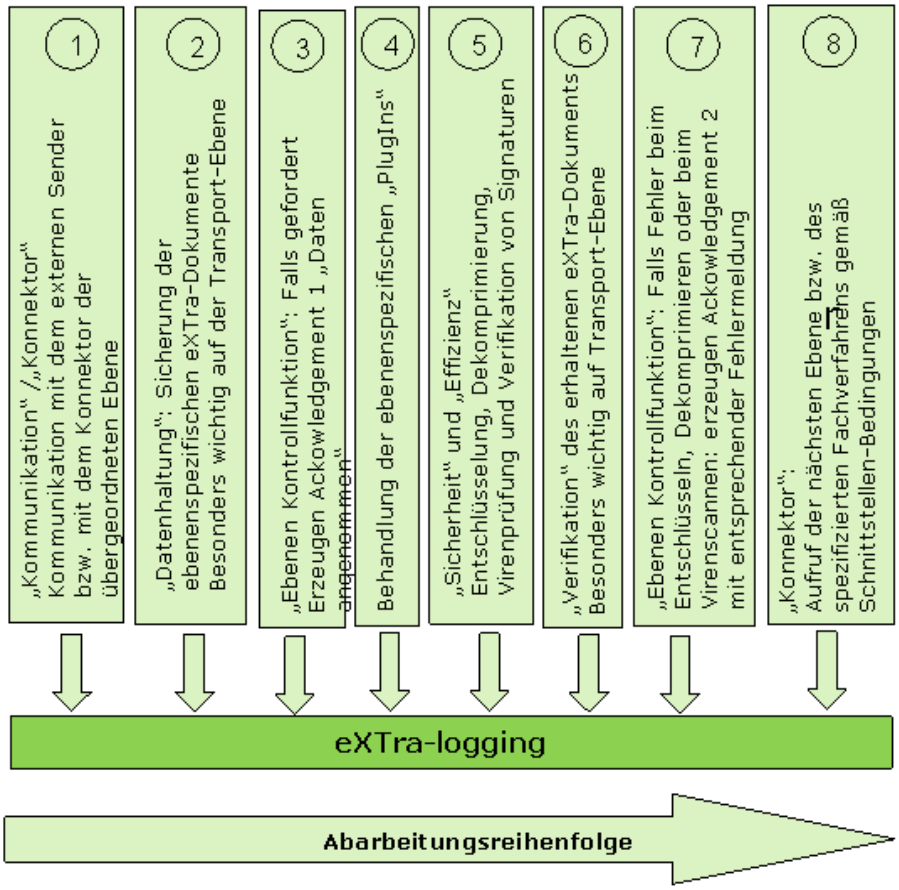


Bild 3: Dynamischer Ablauf bis zum Aufruf der nächsten Ebene bzw. des Fachverfahrens

Schritt 1: „Kommunikation“ auf Transportebene bzw. „Konnektor“
Diese Funktion erhält die Kontrolle vom externen Sender bzw. der übergeordneten Ebene, z.B. die TransporteEbene per DFÜ vom externen Sender oder z.B. die Paket-Ebene von der Transport-Ebene

Schritt 2: „Datenhaltung“: Sicherung der erhaltenen Strukturen in der lokalen Datenhaltung, z.B. in einer Datenbank. Bei der Transportebene ist es besonders wichtig zum frühest möglichen Zeitpunkt die erhaltenen eXTra-Dokumente im Orginal sicherzustellen, um so die Grundlage für einen evtl. notwendigen Nachvollzug aller Vorgänge zu schaffen.
Bei den anderen Ebenen, der Paket- und Nachrichtenebene ist dies nicht so bedeutend und kann oftmals entfallen, insbesondere wenn alle Ebenen lokal im selben eXTra-Server bearbeitet werden.

Schritt 3 „Ebenen Kontrollfunktion“: Erzeugung des acknowledgement falls vom Sender gefordert mittels scenario=request-with-acknowledgement
Die sematische Bedeutung eines acknowledgement ist die Bestätigung, dass eine Ebene die übergebenen Strukturen zumindest erhalten hat, also eine Empfangsbestätigung. Eine Aussage, dass die Strukturen und Daten auch korrekt waren und verarbeitet werden konnten, ist damit nicht notwendigerweise verbunden.

Ob ein acknowledgement für den Sender auch einen zusätzlichen Nutzen darstellt, hängt einerseits von der Charakteristik des gewünschten Fachverfahrens, andererseits von dem Datenvolumen und den Durchlaufs- und Bearbeitungszeiten der involvierten eXTra-Ebenen, sowie des Fachverfahrens ab.
Ist das Fachverfahren als Online-System ausgestaltet, dann muss es auch z.B. eine Anfrage, die mit scenario=request-with-response gestellt wurde, sofort mit einer response beantworten können. In diesem Kontext brächte ein scenario=request-with-acknowledgement keinen Nutzen, bzw. wäre verfehlt.
Wenn das Fachverfahren hingegen als Batch-System realisiert ist, oder wenn der Sender auch umfangreiche eXTra-Dokumente übermitteln kann, dann ist ein acknowledgement des Empfängers für den Sender eine wesentliche Information, insbesondere bei terminrelevanten Meldungen. Diese Empfangsbestätigung gibt dem Sender die erwünschte Rechtssicherheit für die rechtzeitige Abgabe seiner Meldung.

Diese Empfangsbestätigung sollte der Sender als Rückmeldung noch in der gleichen DFÜ-Anschaltung von der Transport-Ebene des Empfängers erhalten.

Schritt 4 „PlugIns“: Die ebenenspezifischen PlugIns müssen in der Regel schon an dieser Stelle behandelt werden, da in ihnen evtl. Informationen enthalten sind, die bei der weiteren Behandlung beachtet werden müssen. Ein Beispiel hierfür ist das PlugIn DataTransforms, welches u.a. das Verfahren benennt, mit dem die fachlichen Daten anschließend vom Empfänger entschlüsselt werden können.

Schritt 5 „Sicherheit“ und „Effizienz“: Aufbereitung der Daten, Entschlüsselung, Dekomprimierung, Virenprüfung und Verifikation von Signaturen
Erst nach der Aufbereitung des ebenenspezifischen Body, insbesondere des Header der nächsten Ebene bzw. der fachlichen Daten sind diese in einem lesbaren Zustand, dass die Virenprüfung erst sinnvoll ist und sie von der nächsten Ebene bzw. vom Fachverfahren verarbeitet werden können.
Die Verifikation von Signaturen stellt sicher, dass Verfälschungen innerhalb des signierten Bereichs erkannt werden.

Schritt 6 „Verifikation“: Verifikation des eXTra-Dokuments
Die Verifikation des aufbereiteten eXTra-Dokuments stellt sicher, dass das XML-Dokument formal „well-defined“ ist und dem entsprechenden Schema entspricht.

Schritt 7 „Ebenen Kontrollfunktion“: Erzeugung eines weiteren Acknowledgement, falls der Sender ein Acknowledgement gefordert hat und danach auf dem Weg der Daten bis zum Fachverfahren ein Fehler auftrat.

Der Kontext für dieses Szenario ist wie folgt: falls das Fachverfahren als Batch-System ausgestaltet ist oder umfangreiche eXTra-Dokumente übermittelt werden (siehe oben Schritt 3), kann der Empfänger dem Sender nur eine Empfangsbestätigung (ackowledgement) bei stehender Verbindung geben.
Tritt nach der Rückmeldung an den Sender jedoch beim Empfänger ein Fehler bei der weiteren Bearbeitung innerhalb der eXTra-Ebenen auf, z.B. beim Entschlüsseln, so können die

fachlichen Daten nicht an das Fachverfahren weitergereicht werden. Das Fachverfahren kann deshalb auch kein Verarbeitungsergebnis für eine nachfolgende Response-Anforderung des Senders bereitstellen – es hat ja gar keinen Daten erhalten. Wenn nun in einer derartigen Situation zwischen Sender und Empfänger für den Sendevorgang lediglich ein request-with-acknowledgement und für das Abholen der Verarbeitungsergebnisse ein request-with-response vereinbart wurde, dann gibt es keine technische Möglichkeit dem Sender den Fehler zurückzumelden – dem Empfänger bleibt nur eine manuelle, z.B. telefonische Benachrichtigung des Senders, eine sowohl kostenträchtige, zeitintensive wie auch fehleranfällige Methodik.
Soll jedoch ein Datenübermittlungsverfahren etabliert werden, das über die gesamte Verarbeitungsstrecke beim Empfänger eine vollständig automatisierbare Überwachung ermöglicht, so bietet sich bei eXTra das Konstrukt eines weiteren acknowledgement an (acknowledgement2).

Gestaltung des weiteren Acknowledgement:
Zum Zeitpunkt des Fehlers ist bereits die Verbindung zum Sender wieder abgebaut. Somit verbleibt nur die Möglichkeit ein weiteres Acknowledgement zu erzeugen. Wesentlich ist dabei, dass dieses Acknowledgement den Rückbezug zum ursprünglichen Sendevorgang ermöglicht.
Eine Möglichkeit dieses Acknowledgement zu gestalten ist ihm den identischen formalen Aufbau wie bei der Empfangsbestätigung zu geben, d.h. es erhält die gleiche RequestID des Senders (es gehört logisch zum gleichen Sendevorgang), aber gegenüber der Empfangsbestätigung eine unterschiedliche ResponseID und eine entsprechende Fehlermeldung im Report der ebenenspezifischen ResponseDetails. Evtl. ist es sinnvoll auch den Body und das oder die PlugIns mit zurückzugeben, z.B. dann, wenn nur über das ursprüngliche PlugIn ein Rückbezug möglich ist.
Dieses weitere Acknowledgement stellt der Empfänger- analog zu einer Anforderung des Senders mit request-with-response – für den Sender zum abholen bereit.

Schritt 8 und 9 „Konnektor“:
Je nachdem, ob die nächste eXTra-Ebene, bzw. das gewünschte Fachverfahren lokal oder remote an einem anderen Ort angesiedelt ist, sind unterschiedliche Kommunikationsverfahren erforderlich. Ebenso kann jetzt erkannt werden, ob ein gefordertes Fachverfahren überhaupt existiert, wie es aufgerufen und wie es mit Daten versorgt werden muss.

Aufruf der nächsten Ebene bzw. des geforderten Fachverfahrens

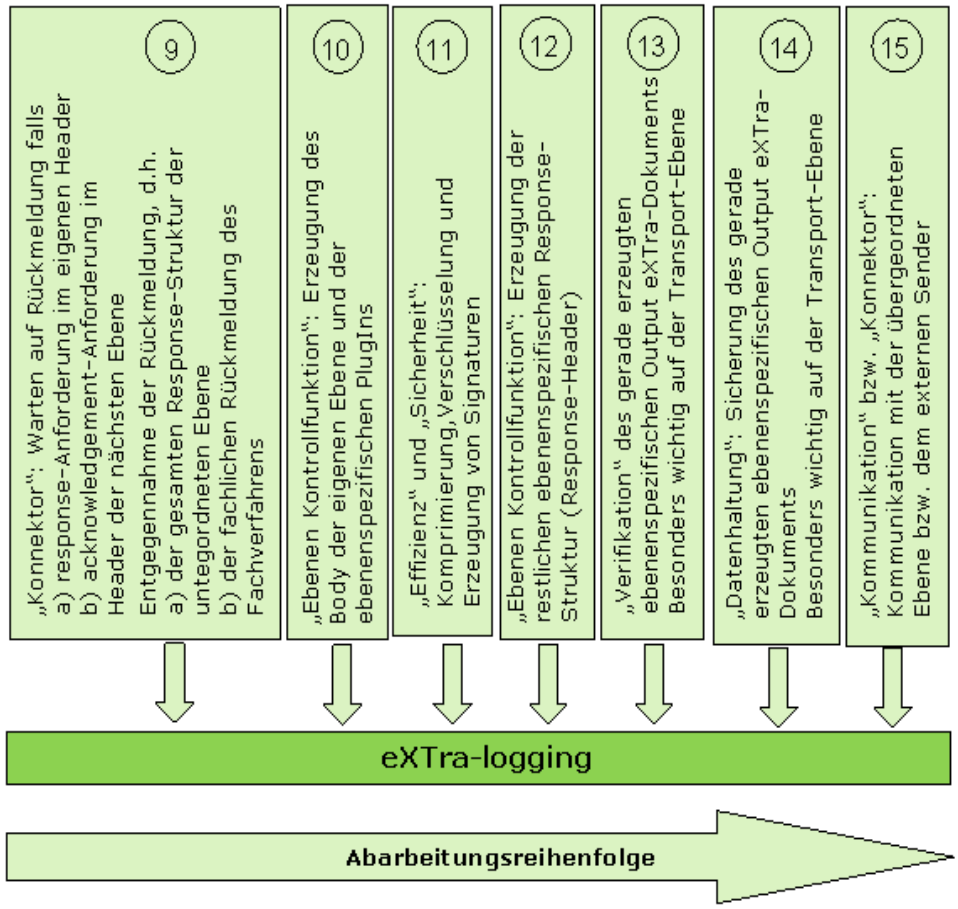


Bild 4: Dynamischer Ablauf von der Rückkehr vom Fachverfahren bzw. der unteren Ebene zurück zum Sender, falls eine Rückmeldung zum Sender gefordert ist

Warten auf die Rückmeldung der nächsten Ebene bzw. des aufgerufenen Fachverfahrens
Ein Warten ist immer dann erforderlich, wenn der Sender eine Rückmeldung mit einer Response-Anforderung oder im Header der nächsten Ebene ein Acknowledgement gewünscht hat. Ebenso kommen alle nachfolgenden Aktivitäten und Schritte nur dann zum tragen, wenn auf eine Rückmeldung gewartet werden muss.

Entgegennahme der Rückmeldung der untergeordneten Ebene, bzw. des aufgerufenen Fachverfahrens
Übergibt das Fachverfahren die Kontrolle wieder an die aufrufende eXTra-Ebene zusammen mit seiner Rückmeldung, so wird diese Rückmeldung (die fachlichen Daten) entgegengenommen und das Element Data gebildet.

Schritt 10 „Ebenen Kontrollfunktion“:

Hat eine untergeordnete eXTra-Ebene ihre Arbeit beendet und übergibt die Kontrolle wieder zurück, so muss deren gesamte Response-Struktur – ein Package oder eine Message – übernommen und nach der folgenden Aufbereitung der ebenenspezifische Body gebildet werden.

Erzeugung der ebenenspezifischen PlugIns

Die ebenenspezifischen PlugIns müssen schon an dieser Stelle erzeugt werden, da in ihnen evtl. Informationen enthalten sind, die bei der weiteren Behandlung beachtet werden müssen. Ein Beispiel hierfür ist das PlugIn DataTransforms, welches u.a. das Verfahren benennt, mit dem die zurück zuliefernden fachlichen Daten vom Empfänger verschlüsselt werden müssen.

Schritt 11 „Sicherheit“ und „Effizienz“. Erzeugung von Signaturen, Komprimierung und Verschlüsselung

Entsprechend der Vereinbarung zwischen Sender und Empfänger müssen die zu übermittelnden Strukturen und Daten aufbereitet werden. Durch die Komprimierung kann die Übertragungszeit erheblich reduziert werden, die Verschlüsselung sichert die Vertraulichkeit der Daten zu und mit Signaturen können Verfälschungen auf dem Weg der Übertragung erkannt werden.

Schritt 12 „Ebenen Kontrollfunktion“: Erzeugung der vollständigen ebenenspezifischen Response-Struktur

Nach der Aufbereitung der Daten im Schritt 11 kann der ebenenspezifische Body fertig gestellt werden. Danach kann der ebenenspezifische ResponseHeader erzeugt werden, wobei der ResponseHeader quasi eine Kopie des empfangenen RequestHeader ist, der lediglich um die <ResponseDetails> erweitert werden muss. Als letztes verbleibt noch das eine Ebene umschließende Element zu generieren, bei der Transport-Ebene ist dies das Element XMLTransport bei den anderen Ebenen das Element Package oder Message.

Schritt 13 „Verifikation“: Verifikation der erzeugten eXTra-Strukturen

Als abschließende qualitätssichernde Maßnahme kann das gerade erzeugte eXTra-Dokument mit Hilfe der zugeordneten Schema-Datei verifiziert werden.

Empfohlen wird diese Maßnahme für die Transport-Ebene, so dass beide Kommunikationspartner die Sicherheit verifizierter und gültiger eXTra-Dokumente haben. Bei den anderen Ebenen ist dies evtl. dann in Erwägung zu ziehen, wenn die Ebenen in verschiedenen Standorten bearbeitet werden.

Schritt 14 „Datenhaltung“: Sicherung der erzeugten eXTra-Strukturen
Insbesondere für die Transport-Ebene wird dringend empfohlen, das gerade erzeugte eXTra-Dokument als Nachweis für den ordnungsgemäßen Übermittlungsbetrieb z.B. in einer Datenbank zu sichern. Zugleich ist dies die Grundlage für die Reklamationsbearbeitung und für Recherchen im Fehlerfalle.

Schritt 15 „Kommunikation“ auf Transport-Ebene bzw. „Konnektor“
Als letzte Aktion einer eXTra-Ebene werden die gerade erzeugten eXTra-Strukturen an die nächst höhere eXTra-Ebene übergeben, bzw. das gerade erzeugte eXTra-Dokument dem ursprünglichen Sender per DFÜ durch den eXTra-Server übermittelt.

11 Literatur

Kurzname	Quelle
DSIG	*eXTra Design Guidelines*, zu finden unter www.extra-standard.de
EINF	*Einführung in den eXTra Standard,* zu finden unter www.extra-standard.de
EMSG	*eXTra Standardnachrichten, Schnittstellenbeschreibung,* zu finden unter www.extra-standard.de
IFACE	*eXTra Schnittstellenbeschreibung,* zu finden unter www.extra-standard.de
IMPL	*eXTra Implementierung*
KOMP	*eXTra Kompendium,* zu finden unter www.extra-standard.de
RFC2119	*Request for Comments: 2119*, S. Bradner, Harvard University, March 1997, http://www.ietf.org/rfc/rfc2119.txt
PROF	*eXTra Profilierung*
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/