




Elektronisches Datenmanagement - Umwelt

 **Bundesministerium**
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

BESCHREIBUNG DER WEBSERVICE-SCHNITTSTELLE FÜR ELEKTRONISCHE BEGLEITSCHIN-MELDUNGEN (EBSM)

SCHNITTSTELLEN-VERSION: v1.03
BESCHREIBUNGSDOKUMENT-VERSION: v1.00
DOKUMENTERSTELLUNGSDATUM: 26. APRIL 2023

Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und
Technologie (BMK)

Stubenbastei 5, 1010 Wien

INHALTSVERZEICHNIS

1	Einleitung.....	3
1.1	Inhalt und Zweck des Dokuments	3
1.2	Aufbau des Dokuments	3
1.3	Verwendung des Dokuments.....	3
1.4	Literaturhinweise.....	4
1.5	Kontakt.....	4
2	Beschreibung des Datenformats	5
2.1	Allgemeine Anmerkungen zum Datenformat.....	5
2.1.1	Zielsetzungen und Prinzipien der Datenmodellierung	5
2.1.2	XML.....	5
2.1.3	Zeichencodierung: UTF-8.....	6
2.1.4	XML Schema.....	6
2.1.5	Datenanforderungen und Datenprüfungen.....	6
2.1.6	Codelisten	8
2.1.7	Identifikationszeichenketten und natürlichsprachige Angaben	8
2.1.8	XML Schema Design Pattern: Venetian Blind	9
2.2	Zuordnung von Fachbegriffen zu Datenelementen.....	9
3	XML Beispieldaten	10
3.1	Einleitung.....	10
3.2	Beispieldaten	10
3.3	Erläuterungen	11
4	Webservice Beschreibung.....	12
4.1	Unterstützte Begleitscheinverfahren	12
4.1.1	Elektronische Begleitscheinmeldung (EBSM)	12
4.1.2	Vollelektronisches Begleitscheinverfahren (VEBSV 1.0)	12
4.2	Begleitschein-Identifikation: Begleitscheinnummer	12
4.3	Handhabung bestimmter Fälle von Abfallübergaben und Abfalltransporten	14
4.3.1	Streckengeschäft	14
4.3.2	Sammeltour	14
4.3.3	Begleitscheinsplitting	14
4.4	Korrektur und Stornierung.....	14
4.5	Zugriffsbeschränkungen	15
4.6	Prüfprotokolle	15
4.7	Authentifizierung.....	16
4.7.1	Varianten.....	16
4.7.2	Wahl der passenden Authentifizierungsvarianten	16
4.7.3	„Username/Passwort“ Authentifizierung	16
4.7.4	„Token“ („Session-ID“) Authentifizierung	16
4.8	Fehlerbehandlung	17
5	Vorgaben an Software mit Schnittstellenanbindung und an deren Benutzer	18
5.1	Allgemeines	18
5.2	Vorgaben, die ausschließlich die Software betreffen	18
5.2.1	Erstellung und Verarbeitung von Dateninstanzen	18
5.2.2	Persistierung und (De-)serialisierung	19
5.2.3	Umgang mit Codelisten.....	19
5.2.4	Fehlerbehandlung	20
5.2.5	Authentifizierung	20
5.3	Vorgaben, die auch den Benutzer der Software betreffen können.....	21
5.3.1	Authentifizierung	21
5.3.2	Fristen	21

1 EINLEITUNG

1.1 Inhalt und Zweck des Dokuments

Das EDM, das *Elektronische Daten-Management in der Umwelt- und Abfallwirtschaft*, ermöglicht es, Meldeverpflichtungen und Registrierungsverpflichtungen im Umwelt- und Abfallbereich elektronisch abzuwickeln.

Am EDM Anwendungsportal <http://edm.gv.at> steht neben zahlreichen weiteren Anwendungen die Teilanwendung *eBegleitschein* zur Verfügung: Diese ist das eGovernment-Werkzeug für Begleitschein-bezogene Prozesse und Meldungen, gemäß § 18 und § 19 des Abfallwirtschaftsgesetz 2002 und der Abfallnachweisverordnung 2012.

Das eBegleitschein Webservice ist dafür eingerichtet, direkt aus Unternehmenssoftware Begleitscheinmeldungen an die zuständige Behörde zu übermitteln, und unterstützt die **Elektronische Begleitscheinmeldung (EBSM)**. Dabei handelt es sich um die Meldung gemäß § 14 Abs. 1 Abfallnachweisverordnung 2012, d.h. um die Meldung von Begleitscheinen an den Landeshauptmann innerhalb von sechs Wochen nach der Übernahme.

Anmerkung: Das Webservice enthält Operationen für das Vollelektronische Begleitscheinverfahren 1.0 (VEBSV 1.0). Die Behörden bieten das Vollelektronische Begleitscheinverfahren 1.0 nicht mehr an. Das Webservice enthält die VEBSV 1.0 bezogenen Operationen nur noch aus Gründen der Abwärtskompatibilität.

Es gibt ein Nachfolge-Pilotprojekt VEBSV 2.0, zu welchem die Abteilung V/2 Abfall- und Altlastenrecht des BMK gerne Auskünfte erteilt.

Dieses Dokument beschreibt die EDM eBegleitschein Webservice Schnittstelle.

Das Dokument richtet sich in erster Linie an solche **IT-Analytiker** und **Entwickler**, die mit der Entwicklung der Anbindung von Software an die EDM eBegleitschein Webservice Schnittstelle befasst sind.

Zusätzlich kann das Dokument auch von Umwelt- und Abfallwirtschaft **Fachpersonal** genutzt werden, um genauen Aufschluss über Art und Struktur der über die Schnittstelle übermittelbaren Daten zu erlangen.

1.2 Aufbau des Dokuments

Das Dokument ist wie folgt strukturiert:

- Kapitel 1 enthält eine Einleitung, Hinweise zur Verwendung des Dokuments, eine Auflistung von Literaturhinweisen sowie Kontaktinformationen.
- Kapitel 2 enthält eine Beschreibung des XML-Formats für Verpackungs-bezogene Meldungen.
- Kapitel 3 enthält illustrative XML-Beispieldaten mit Erläuterungen.
- Kapitel 4 beschreibt das Webservice mit seinen Operationen.
- Kapitel 5 enthält Vorgaben an Software, für die eine Anbindung an die EDM eVerpackung Webservice-Schnittstelle implementiert wird

1.3 Verwendung des Dokuments

Zur Schnittstellenbeschreibung gibt es einen **Anhang im HTML-Format** innerhalb des Spezifikationspakets. Dieser Anhang enthält vorwiegend automatisiert generierte Teile der Schnittstellenbeschreibung, z.B. aus annotierten XSD-Dateien automatisiert generierte Beschreibungen der XML-Formate.

Das Spezifikationspaket enthält darüber hinaus eine Reihe weiterer Inhalte, insbesondere:

- **XML Schema Definition** für Begleitschein-Meldungen (Datei mit „xsd“-Endung), zweifach, einmal mit Beschreibungstexten, und einmal ohne.
Anmerkung: Nähere Informationen dazu, was eine XML Schema Definitions-Datei ist und wozu sie verwendet wird, ist in Abschnitt 2.1.4 auf Seite 6 beschrieben;
- **WSDL** (Web Services Description Language) **Beschreibung des Webservice** (Datei mit „wsdl“-Endung)
- **Datenanforderungen und Prüfregelein** (PDF-Datei)

Anmerkung: Nähere Informationen dazu, was Datenanforderungen und Prüfregelein sind, und wozu sie dienen, ist in Abschnitt 2.1.5 auf Seite 6 beschrieben;

1.4 Literaturhinweise

Zum Verständnis dieser Schnittstellenbeschreibung können die folgenden Dokumente hilfreich oder erforderlich sein:

RECHTSGRUNDLAGEN:

- [1] *Abfallwirtschaftsgesetz 2002, idgF;*
- [2] *Abfallnachweisverordnung 2012, idgF;*

TECHNISCHE STANDARDS:

- [1] *Extensible Markup Language (XML) 1.1 (Second Edition), W3C Recommendation 16 August 2006, edited in place 29 September 2006; <http://www.w3.org>;*
- [2] *ISO/IEC 10646:2003, Information technology – Universal Multiple-Octet Coded Character Set (UCS);*
- [3] *ISO/TS 15000-5:2005, Electronic Business Extensible Markup Language (ebXML) – Part 5: ebXML Core Components Technical Specification, Version 2.01 (ebCCTS);*
- [4] *ONR 192150: 2007 11 01: Datenstrukturen für den elektronischen Datenaustausch in der Abfallwirtschaft; Österreichisches Normungsinstitut;*
- [5] *XML Schema Part 1: Structures Second Edition, W3C Recommendation 28 October 2004; <http://www.w3.org>;*
- [6] *XML Schema Part 2: Datatypes Second Edition, W3C Recommendation 28 October 2004; <http://www.w3.org>;*
- [7] *UN/CEFACT Core Components Library (CCL) Version 07A; <http://www.unece.org>;*

1.5 Kontakt

Für Auskünfte zur Schnittstelle steht der **EDM Helpdesk** zur Verfügung.

Das EDM-Portal edm.gv.at/ enthält die detaillierten Kontaktinformationen zum EDM Helpdesk.

2 BESCHREIBUNG DES DATENFORMATS

2.1 Allgemeine Anmerkungen zum Datenformat

2.1.1 Zielsetzungen und Prinzipien der Datenmodellierung

Im Folgenden sind einige wichtige allgemeine Zielsetzungen und Prinzipien angeführt, die bei der Spezifikation des Datenformats angewendet wurden. In den Folgeabschnitten wird dann näher auf einzelne technische Standards und Modellierungsprinzipien eingegangen.

- **Zukunftstauglichkeit – Flexibilität in Bezug auf allfällig im Laufe der Zeit erforderliche Änderungen:** Das XML-Datenformat ist so konzipiert, dass es möglichst langfristig verwendet werden kann. Das Grundprinzip dabei ist jenes, dass Datenformat-Vorgaben, von denen nicht ausgeschlossen werden kann, dass sie sich im Laufe der Zeit ändern, als Codelisten abgebildet sind. Anwendungen, die das Lesen oder Schreiben eines Datenformats unterstützen, können so implementiert werden, dass ein Aktualisieren von lokalen Codelisten-Kopien automatisiert ohne die Notwendigkeit der Anpassung von Software (Um- oder Neuprogrammierungen) erfolgen kann.

Beispiel: Für die Angabe von Abfallarten kommen im Datenformat Codelisten zum Einsatz. Kommt es zukünftig zu Änderungen bei den Abfallarten, so gibt es lediglich eine Aktualisierung der entsprechenden am EDM Anwendungsportal abrufbaren Codeliste. Die XML Schema Definition hingegen bleibt gänzlich unverändert. Die Datenformat-Spezifikation ermöglicht es daher, Datenformat-lesende oder -schreibende Anwendungen so zu implementieren, dass die Berücksichtigung von Änderungen bei Abfallarten keinen Entwicklungsaufwand und auch keinen sonstigen Administratoren-Aufwand erfordert, sondern die Anwendungen einfach weiterverwendet werden können.

Bemerkung: Dem Datenformat wird durch die Verwendung von Codelisten eine Flexibilität in Bezug auf Anpassungen verliehen. Dies ist als Vorkehrung zu verstehen, und nicht als Absicht, die Codelisten tatsächlich häufig zu ändern. Stattdessen werden Codelisten, wie im EDM üblich, auch hinkünftig nur dann geändert, wenn dies unbedingt notwendig ist, etwa aus rechtlichen Gründen.

- **Kriterium Technische Verarbeitbarkeit; Nicht-Kriterien inhaltliche Richtigkeit und Vollständigkeit von Daten:** Das XML-Datenformat ist so spezifiziert, dass eine grundlegende technische Verarbeitbarkeit, insbesondere das Speichern in relationalen Datenbanken sichergestellt ist. Darüber hinausgehende Anforderungen an die inhaltliche Richtigkeit und Vollständigkeit von Daten werden durch das XML-Datenformat nicht generell berücksichtigt. Das ist bewusst so gehalten, um möglichst keine Barrieren für die Repräsentation von Daten, beispielsweise von bereits bestehenden Datensammlungen, in dem Datenformat zu schaffen: Es handelt sich um eine Anforderung an das Datenformat, dass damit auch die Übermittlung von unvollständigen oder unplausiblen Daten grundsätzlich möglich ist.

In der elektronischen Datenverarbeitung besteht jedoch auch der Anspruch des möglichst automatisierten Erkennens von unplausiblen und unvollständigen Daten. Entsprechende Prüfkriterien – (Nicht-)Einhaltung welcher Bedingungen welche Hinweise auf potentiell falsche oder fehlerhafte Daten liefern soll – müssen, so wie das Datenformat selbst, für alle am Datenaustausch teilnehmenden Partner transparent und einheitlich sein. Eine Liste solcher Kriterien wird separat vom Datenformat in einem sogenannten **Datenanforderungs- und Prüfgeldokument** veröffentlicht (siehe 2.1.5).

2.1.2 XML

XML-Dateien (*Extended Markup Language* Dateien) sind Text-Dateien, in welchen die Inhalte mit Namen gekennzeichnet sind und eine hierarchische Struktur aufweisen.

XML-Dateien zeichnen sich insbesondere dadurch aus, dass sie sowohl menschenlesbar, als auch für die maschinelle Verarbeitung geeignet sind.

XML [1] ist ein vom *World Wide Web Consortium* (<http://www.w3.org>) veröffentlichter Standard.

2.1.3 Zeichencodierung: UTF-8

XML Dateien können – so wie alle Text-Dateien – in verschiedenen Zeichencodierungen gespeichert sein, z.B. ISO 8859-1 oder UTF-8.

Unicode und *UTF-8* [2] sind als ISO-Standard veröffentlicht. UTF-8 zählt zu den gebräuchlichsten Zeichencodierungen. Auf bereits bestehende Funktionen zur Speicherung von Text in UTF-8 Zeichencodierung kann in nahezu allen Programmiersprachen zurückgegriffen werden. Auch alle gängigen textverarbeitenden Programme unterstützen diese Codierung.

Das in diesem Dokument beschriebene Webservice setzt eine Codierung von Request- und Response-Daten in UTF-8 voraus – siehe die Vorgabe mit der ID 628 auf Seite 18.

2.1.4 XML Schema

Die hochzuladenden Dateien müssen gewisse Strukturvorgaben einhalten, um verarbeitet werden zu können. Diese Strukturvorgaben betreffen insbesondere Anzahl, Anordnung und Kennzeichnung der zu übermittelnden Inhalte, und sind daher mit Formularvorlagen im papierbasierten Meldewesen vergleichbar.

Für die Festlegung von Strukturvorgaben für XML Dateien existieren mehrere Standards. Der verbreitetste davon ist *XML Schema* [5],[6], ein ebenfalls vom *World Wide Web Consortium* (<http://www.w3.org>) veröffentlichter Standard.

Die Strukturvorgaben für XML-Dateien sind als XML Schema definiert. Diese XML Schema Dateien besitzen die Dateierweiterung „.xsd“ und stehen am EDM Anwendungsportal zum Download zur Verfügung.

Für Dokumentationszwecke steht weiters jeweils ein sogenanntes „*annotated XML Schema*“ (mit Kommentaren versehenes XML Schema) zur Verfügung. Die Kommentare entsprechen genau den Beschreibungstexten aus dieser Schnittstellenbeschreibung.

Eine XML Datei heißt *gültig* bezüglich eines XML Schemas, wenn sie die im XML Schema definierten Strukturvorgaben einhält. Es gibt Anwendungen und Funktionsbibliotheken, sogenannte *XML Schema Validatoren*, mit deren Hilfe es möglich ist, bei vorliegendem XML Schema und vorliegender XML Datei die XML Datei zu validieren, d.h. deren Gültigkeit bezüglich des XML Schemas zu überprüfen. Mit solchen Validatoren lässt sich also schon vor einem Upload überprüfen, ob eine XML Datei den Strukturvorgaben des XML Schemas entspricht.

XML-Dateien, die bezüglich der veröffentlichten XML Schema Dateien nicht gültig sind, werden beim Upload abgelehnt.

2.1.5 Datenanforderungen und Datenprüfungen

Diese Schnittstellenbeschreibung und die zugehörigen XML Schema Definitions-Datei (xsd-Datei) beschreibt die Grundvoraussetzungen für die Interaktion zwischen einer Software-Anwendung und dem EDM über das eBegleitschein Webservice.

Über diese Grundvoraussetzungen hinaus gibt es weitergehende Anforderungen an Form und Inhalt übermittelter Daten. Damit sind Anforderungen wie die folgende gemeint: „Beginn und Ende des angegebenen Zeitraums haben innerhalb desselben Kalenderjahres zu liegen“.

Solche sogenannten **Datenanforderungen** werden aus mehrerlei Gründen nicht innerhalb der vorliegenden Schnittstellenbeschreibung dokumentiert, sondern in einem separaten Dokument: Zum Einen sind Datenmodell- und Schnittstellenbeschreibungs-Veröffentlichungen im Allgemeinen sehr schlecht dafür geeignet, darin fachliche Anforderungen an Daten allgemeinverständlich und übersichtlich wiederzugeben. Zum Anderen müssen Schnittstellen möglichst stabil sein, d.h. möglichst lange möglichst unverändert bleiben, um hohen technischen Anpassungsaufwand zu vermeiden. Insbesondere muss vermieden werden, dass die Notwendigkeit entsteht, Software neu zu kompilieren, auszuliefern bzw. zu installieren. Anpassungen bei Datenanforderungen sind hingegen wesentlich unproblematischer. Solche Anpassungen behält sich das EDM vor. Wird beispielsweise von einer zuständigen Behörde festgestellt, dass ein bestimmter (formal erkennbarer) inhaltlicher Fehler in den Meldungen sehr häufig auftritt, so kann als Service für Meldende und deren IT-Dienstleister eine neue Datenanforderung spezifiziert und veröffentlicht werden, die dabei unterstützt, diesen Fehler zu vermeiden.

Datenanforderungen sind von **Datenprüfungen**, die in IT-Anwendungen implementiert sind, zu unterscheiden. Datenanforderungen gelten unabhängig davon, ob in IT-Anwendungen dazugehörige Datenprüfungen implementiert sind oder nicht.

Die Abarbeitung von Operationsaufrufen des EDM Webservice kann auf die folgenden Arten verlaufen:

1. Der Operationsaufruf kann regulär abgearbeitet werden, es wird ein gewöhnlicher Response geliefert (kein SOAP-Fault);
2. Der Operationsaufruf kann nicht regulär abgearbeitet werden („exception“). Das wird dadurch signalisiert, dass anstelle des Response, wie ihn die reguläre Abarbeitung eines Aufrufs liefert, ein SOAP-Fault zurückgemeldet wird.

In Zusammenhang mit Datenprüfungen ist weiter zu unterscheiden:

- a. Die reguläre Abarbeitung ist nicht möglich, weil Daten an das Webservice übergeben wurden, von welchen die Webservice-Operation feststellt, dass verpflichtend einzuhaltende Datenanforderungen nicht eingehalten sind.

Erkennbar ist dieser Fall daran, dass im SOAP-Fault als Fehlerkategorie „Verletzung von Datenanforderungen“ (Code 203 aus Codeliste 5156) angegeben ist.

- b. Die reguläre Abarbeitung ist aus anderen Gründen nicht möglich, etwa weil die Authentifizierung fehlschlug, oder der authentifizierte EDM-Benutzer nicht über ausreichende Berechtigungen verfügt, oder wegen Wartungsarbeiten am EDM.

Bei der **Übermittlung von Daten** erfolgt – sofern nicht aufgrund von Fehlern wie etwa Verletzung der XML Schema Vorgaben oder falsche Zeichencodierung die Abarbeitung schon zuvor abgebrochen werden muss – automatisch eine **Überprüfung der Einhaltung jener Datenanforderungen, für die es Datenprüfungen gibt**. Es steht dann ein **Validierungsergebnis** (auch „**Prüfprotokoll**“ genannt) zur Verfügung:

- Im Fall 1 „reguläre Abarbeitung“:
 - Zugriff auf das Validierungsergebnis besteht für all jene, die auch Zugriff auf die übermittelten Dokumente besitzen, jedenfalls aber für Sender und Empfänger (zuständige Behörde);
 - Das Validierungsergebnis enthält lediglich **Hinweise auf potentiell fehlerhafte Daten**. Eine Verletzung von verpflichtend einzuhaltenden Datenanforderungen wurde nicht festgestellt, andernfalls wäre die reguläre Abarbeitung der Webservice-Operation abgebrochen worden;
- Im Fall 2:
 - Die Operation konnte nicht ordnungsgemäß abgearbeitet werden. Für die Benutzer des EDM ist der Zustand des EDM unverändert: Bei Datenübermittlungs-Operationen konnten die übermittelten Daten konnten nicht entgegengenommen werden. EDM-Benutzer wie etwa die Adressaten der Datenübermittlung (z.B. zuständige Behörde) „wissen nichts“ über den Datenübermittlungsversuch: Weder sind die Daten, deren Übermittlung gescheitert ist, für diese Benutzer in irgendeiner Form im EDM sichtbar oder abrufbar, noch sind irgendwelche Informationen zum fehlgeschlagenen Datenübermittlungsversuch für die Benutzer sichtbar oder abrufbar (Ausnahme: Zugriff auf das Prüfprotokoll im Fall 2.a für den Webservice-Benutzer, dessen Operationsaufruf fehlschlug). Ein „technisches“ Protokollieren findet sehr wohl statt, dieses ist aber nur für IT-Administratoren zugänglich.
- Im Fall 2.a „Keine reguläre Abarbeitung aufgrund der Verletzung verpflichtend einzuhaltender Datenanforderungen“:
 - Ein Validierungsergebnis steht zur Verfügung, und zwar ausschließlich für jenen EDM-Benutzer, der bei der Datenübermittlung authentifiziert wurde;
 - Das Validierungsergebnis – die Liste von Nicht-Einhaltungen von Datenanforderungen – enthält mindestens einen Eintrag, der auf die Nicht-Einhaltung einer verpflichtend einzuhaltenden Datenanforderung aufmerksam macht;

- Im Validierungsergebnis können darüber hinaus auch Hinweise auf potentiell fehlerhafte Daten enthalten sein, die für sich allein nicht zu einer Ausnahmesituation, d.h. dem Abbruch der Abarbeitung der Webservice-Operation geführt hätten;
- Im Fall 2.b „Keine reguläre Abarbeitung aus anderen Gründen“:
 - Es gibt kein Ergebnis der Validierung von Datenanforderungen, da die Abarbeitung der Webservice-Operation aus nicht mit Datenanforderungen zusammenhängenden Gründen abgebrochen wurde.

Es wird empfohlen, die Einhaltung von Datenanforderungen bereits Client-seitig zu überprüfen. Das ist vor allem eine Usability-Frage: Im vom EDM gelieferten Validierungsergebnis kann lediglich darauf Bezug genommen werden, welche XML-Dateninhalte eine Prüffregelverletzung bewirken. Der Konnex zu Benutzeroberfläche-Elementen der Client-Software fehlt darin zwangsläufig. Durch die Client-seitige Überprüfung kann ein solcher Konnex hergestellt werden.

2.1.6 Codelisten

Das Datenformat sieht unter anderem die Identifikation von Objekten vor, und zwar nach den folgenden beiden Prinzipien:

1. Identifikation von Personen, Standorten, oder Anlagen, die im elektronischen Register für Anlagen- und Personen-Stammdaten registriert sind. Zur Identifikation solcher Personen, Standorte, oder Anlagen sind die *GLNs* (*Global Location Numbers*) zu verwenden, die im EDM diesen Einträgen zugeordnet sind. Eine Abfrage von registrierten Personen, Standorten und Anlagen ist am EDM Anwendungsportal möglich;
2. Identifikation von Objekten aus vorgegebenen Listen. Ein Beispiel ist die Auswahl einer Größeneinheit für einen Massenangabe, z.B. Kilogramm, aus einer vorgegebenen Liste von Größeneinheiten. Solche Listen, die die in einem bestimmten Kontext vorgegebene Auswahl von Einträgen festlegen, werden **Codelisten** genannt. Für jeden Eintrag existiert ein Code, z.B. eine *GTIN* (*Global Trade Item Number*), der diesen Eintrag identifiziert.

Die in einem bestimmten Kontext zulässigen Codes, z.B. die Codes, die zur Auswahl einer Größeneinheit zulässig sind, sind bewusst **nicht** im XML Schema hinterlegt. Der wichtigste Grund dafür: Codelisten können sich häufiger ändern, ohne dass sich an der Schnittstelle etwas ändert. Entsteht beispielsweise aufgrund einer Unabhängigkeitserklärung ein neuer Staat, so muss die Liste der zur Auswahl stehenden Nationalstaaten angepasst werden. An dem Meldungsformat selbst hat sich nichts geändert. Wären die zulässigen Codes im XML Schema hinterlegt, so müsste bei jeder Aktualisierung von Codelisten auch das XML Schema aktualisiert werden, wodurch es für gewöhnlich notwendig wäre, Software anzupassen.

Anstelle der Hinterlegung im XML Schema sind die **Codelisten am EDM Anwendungsportal** (<http://edm.gv.at>) unter dem Menüpunkt „Zuordnungstabellen“ **veröffentlicht**. Zudem steht ein Webservice für den Bezug von Codelisten zur Verfügung. Die Beschreibung dieses Webservices ist am EDM Portal „Technische und organisatorische Spezifikationen“, Unterpunkt „Schnittstellenbeschreibungen“, Eintrag „Referenzdaten Webservice“ zu finden.

Die **Verweise auf Codelisten** sind direkt in den **Datenelementbeschreibungen** angegeben, typischerweise durch den Zusatz „(Codeliste xxxx)“ zum Beschreibungstext, z.B. „Abfallart gemäß Anlage 5 der Abfallverzeichnisverordnung (Codeliste 5174)“. Am EDM Anwendungsportal <http://edm.gv.at> ist es möglich, die Auswahl genau jener Codelisten anzuzeigen, die im vorliegenden Datenformat verwendet werden. Dazu wird unter „Zuordnungstabellen“ unter dem Punkt „Gruppierung nach Schnittstellen für den elektronischen Datenaustausch“ dem passenden Link gefolgt.

2.1.7 Identifikationszeichenketten und natürlichsprachige Angaben

Identifikationszeichenketten sind für die eindeutige Interpretierbarkeit, die Interoperabilität, sowie die Möglichkeit der Automatisierung von Abfragen und Auswertungen von Daten von großer Bedeutung.

Beispiele für Identifikationszeichenketten:

- Identifikationszeichenketten, z.B. GTINs (Global Trade Item Numbers), die genutzt werden, um einen Bezug auf einen Codelisten-Eintrag herzustellen, z.B. um eine Abfallart zu identifizieren;
- Identifikationszeichenketten, z.B. Firmenbuchnummern oder GLNs (Global Location Numbers), die genutzt werden, um Personen, Orte, Anlagen oder andere „Objekte“ zu identifizieren.

Die Bedeutung von Identifikationszeichenketten am Beispiel der Interoperabilität: Durch die Verwendung einheitlicher Identifikationszeichenketten können dieselben Daten ohne „Übersetzungen“ in verschiedenen Sprachräumen (deutsch, französisch, englisch, usw.) interpretiert und verarbeitet werden. Würden nur natürlichsprachige Bezeichnungen verwendet, so wären Datenübersetzungen erforderlich.

Zum Teil können im Datenformat Identifikationszeichenketten mit natürlichsprachigen Angaben kombiniert werden, z.B. bei der Angabe von Transporteuren. Es kann somit der Fall eintreten, dass Identifikationszeichenketten und natürlichsprachige Angaben nicht zusammenpassen. Dabei wichtig:

- Es handelt sich um einen schweren inhaltlichen Mangel, der eine Zurückweisung des Dokuments zur Folge haben kann;
- Maßgeblich für die Interpretation der Inhalte ist jedenfalls die Identifikationszeichenkette;

2.1.8 XML Schema Design Pattern: Venetian Blind

Es gibt verschiedene sogenannte *Design Patterns* für ein XML Schema. Die gängigsten davon sind unter den Namen *Russian Doll*, *Salami Slice*, *Venetian Blind* und *Garden of Eden* bekannt.

Wie in Abschnitt 2.1.1 dargestellt, werden Schnittstellen-Spezifikationen für EDM aus einem syntaxunabhängigen Datenmodell abgeleitet. Das syntaxunabhängige Datenmodell enthält eine Sammlung von semantischen Bausteinen (die *Core Components* und *Business Information Entities*). Um den modulartigen, kompakten und weitestgehend redundanzfreien Aufbau aus dem syntaxunabhängigen Datenmodell in XML Schema Definitionen zu übernehmen, werden die Bausteine durchwegs als sogenannte *global types* abgebildet. Das sind benannte und damit wiederverwendbare XML Schema Typdeklarationen. Dieser Ansatz ist genau der *Venetian Blind* XML Schema Design Pattern.

Ein Beispiel zur Illustration, was das in der Praxis bedeutet: Eine Adressstruktur braucht im XML Schema nur 1 Mal (als *complex type*) deklariert zu werden, auch dann, wenn die Adressstruktur an mehreren Stellen in der hierarchischen Struktur verwendet wird (z.B. für eine Absender- und eine Empfänger-Adresse).

Auch für die vorliegende Schnittstellenbeschreibung ergibt sich aus diesem Design Pattern ein sehr konkreter Nutzen: Die Beschreibung kann modulartig erfolgen, d.h. es erfolgt eine Beschreibung der Komponenten (complex types) zusammen mit der Information, an welchen Stellen die Komponenten verwendet werden. Auf diese Weise kann auch die Beschreibung von sehr umfassenden Schnittstellen kompakt und weitgehend redundanzfrei erfolgen.

2.2 Zuordnung von Fachbegriffen zu Datenelementen

Abfallart

- Im Datenformat: *ClassificationCode* in *Material*

Abfallmasse

- Im Datenformat: *MassQualifiedMeasurement* in *Material*

Begleitschein

- Im Datenformat: *ConsignmentNote*

Behandlungsverfahren

- Im Datenformat: *DesignatedPhysicalProcess* in *MaterialMovement*

Datum

- Im Datenformat: *MovementPeriod* in *MaterialMovement*

Kontamination

- Im Datenformat: *ContaminationMaterial* in *Material*

Streckengeschäftspartner

- Im Datenformat: *IntermediateParty* in *MaterialMovement*

Transporteur

- Im Datenformat: *CarrierParty* in *TransportMaterialMovement*

Übergeber

- Im Datenformat: *HandOverParty* in *Transfer*

Übernehmer

- Im Datenformat: *TakeOverParty* in *Transfer*

3 XML BEISPIELDATEN

3.1 Einleitung

Die nachfolgenden Abschnitte enthalten XML Beispieldaten und erläutern diese.

Darüber hinaus enthält das Schnittstellen-Spezifikationspaket eine Reihe von XML-Beispieldateien.

3.2 Beispieldaten

```
<?xml version="1.0" encoding="UTF-8"?>
<EBSSignmentNoteNotification xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
  <NotifierPartyID>9008390271261</NotifierPartyID>
  <SpecifiedConsignmentNote>
    <WasteTransportMaterialMovement>
      <TakeOverPartyID>113</TakeOverPartyID>
      <LoadingLocation>
        <!--OperatingSiteID--></OperatingSiteID-->
        <PostalAddress>
          <PostcodeCode>4840</PostcodeCode>
          <CountryID>AT</CountryID>
        </PostalAddress>
      </LoadingLocation>
      <UnloadingLocation>
        <!--OperatingSiteID--></OperatingSiteID-->
        <PostalAddress>
          <PostcodeCode>4860</PostcodeCode>
          <CountryID>AT</CountryID>
        </PostalAddress>
      </UnloadingLocation>
      <MovementPeriod>
        <StartDateTime>2013-10-20</StartDateTime>
        <EndDateTime>2013-10-21</EndDateTime>
      </MovementPeriod>
      <SubordinateMaterialMovement>
        <TransportModeCode>9008390100059</TransportModeCode>
        <CarrierParty>
          <ID>9008390233214</ID>
        </CarrierParty>
      </SubordinateMaterialMovement>
      <DesignatedPhysicalProcess>
        <TypeCode>9008390008058</TypeCode>
      </DesignatedPhysicalProcess>
      <EffectiveTransfer>
        <HandOverParty>
          <ID>9008390167465</ID>
        </HandOverParty>
        <TakeOverParty>
          <ID>9008390271261</ID>
        </TakeOverParty>
      </EffectiveTransfer>
      <PreliminaryCargoMaterial>
        <ClassificationCode>9008390010037</ClassificationCode>
        <MassQualifiedMeasurement>
          <MeasurementMeasure>50</MeasurementMeasure>
          <MeasurementMethodCode>9008390100004</MeasurementMethodCode>
        </MassQualifiedMeasurement>
      </PreliminaryCargoMaterial>
    </WasteTransportMaterialMovement>
  </SpecifiedConsignmentNote>
</EBSSignmentNoteNotification>
```

3.3 Erläuterungen

- NotifierPartyID beinhaltet die GLN, mit welcher der Meldende im EDM registriert ist.
- TakeOverPartyID beinhaltet die vom Übernehmer vergebene fortlaufende Nummerierung einschließlich einer 2-stelligen Jahreszahl
- LoadingLocation beinhaltet die Informationen zum Absendeort
- UnloadingLocation beinhaltet die Informationen zum Empfangsort
- MovementPeriod beinhaltet die Informationen zum Datum des Transportbeginns und des Empfangs
- SubordinateMaterialMovement beinhaltet die Informationen zu Transporteuren
- DesignatedPhysicalProcess beinhaltet das vorgesehene Abfallbehandlungsverfahren
- EffectiveTransfer beinhaltet die Angaben zum Absender und Empfänger
- PreliminaryCargoMaterial beinhaltet die Angaben zum Abfall, die vor Transportbeginn feststanden (allfällige Korrekturen der Abfallmasse und der Abfallart, die nach Durchführung des Transports festgestellt wurden, werden hingegen in CorrectedCargoMaterial eingetragen)

4 WEBSERVICE BESCHREIBUNG

4.1 Unterstützte Begleitscheinverfahren

4.1.1 Elektronische Begleitscheinmeldung (EBSM)

Entsprechend § 14 Abs. 1 Abfallnachweisverordnung 2012 werden innerhalb von sechs Wochen nach der Übernahme Begleitscheine an den Landeshauptmann übermittelt.

In einer einzelnen Übermittlung können mehrere Begleitscheine enthalten sein.

Der Gesamtprozess des Abfalltransports bzw. der Abfallübergabe stellt sich wie folgt dar: Der Übergeber füllt einen Begleitschein für gefährliche Abfälle aus und erstellt mehrere Ausfertigungen. In der Praxis ist es durchaus üblich, dass dem Übergeber ein durch den Übernehmer oder Transporteur vorausgefüllter Begleitschein zur Unterfertigung vorgelegt wird. Vor dem Transport, auf Übergeberseite, sind mitunter nur näherungsweise Angaben zu Abfallart und Abfallmasse möglich. Die Präzisierung bzw. wenn notwendig Korrektur dieser Angaben durch den Übernehmer nach dem Transport ist auf dem Begleitscheinformular vorgesehen.

Der Transporteur führt während des Transports den vor dem Transport durch den Übergeber unterschriebenen Begleitschein mit und legt diesen bei Kontrollen (z.B. durch die Polizei) vor.

Nach dem Erhalt des Abfalls prüft und vervollständigt der Übernehmer den Begleitschein und übermittelt ihn anschließend an den Landeshauptmann sowie eine weitere Ausfertigung zurück an den Übergeber. Für die Übermittlung an den Landeshauptmann steht die EDM EBSM Schnittstelle zur Verfügung.

4.1.2 Vollelektronisches Begleitscheinverfahren (VEBSV 1.0)

Das BMK bietet das Vollelektronische Begleitscheinverfahren 1.0 nicht mehr an. Das Webservice enthält die VEBSV 1.0 bezogenen Operationen nur noch aus Gründen der Abwärtskompatibilität.

Es gibt ein Nachfolge-Pilotprojekt VEBSV 2.0, zu welchem die Abteilung V/2 Abfall- und Altlastenrecht des BMK gerne Auskünfte erteilt.

4.2 Begleitschein-Identifikation: Begleitscheinnummer

In EDM eBegleitschein im Allgemeinen, und im eBegleitschein-Webservice im Besonderen, erfolgt der eindeutige Bezug auf „Begleitscheine“ (auf Transporte bzw. Übergaben gefährlicher Abfälle) mittels sogenannter Begleitscheinnummern.

Einem Begleitschein kann vom Übergeber eine Nummer zugewiesen sein, oder vom Übernehmer, oder „unabhängig voneinander“ sowohl vom Übergeber, als auch vom Übernehmer.

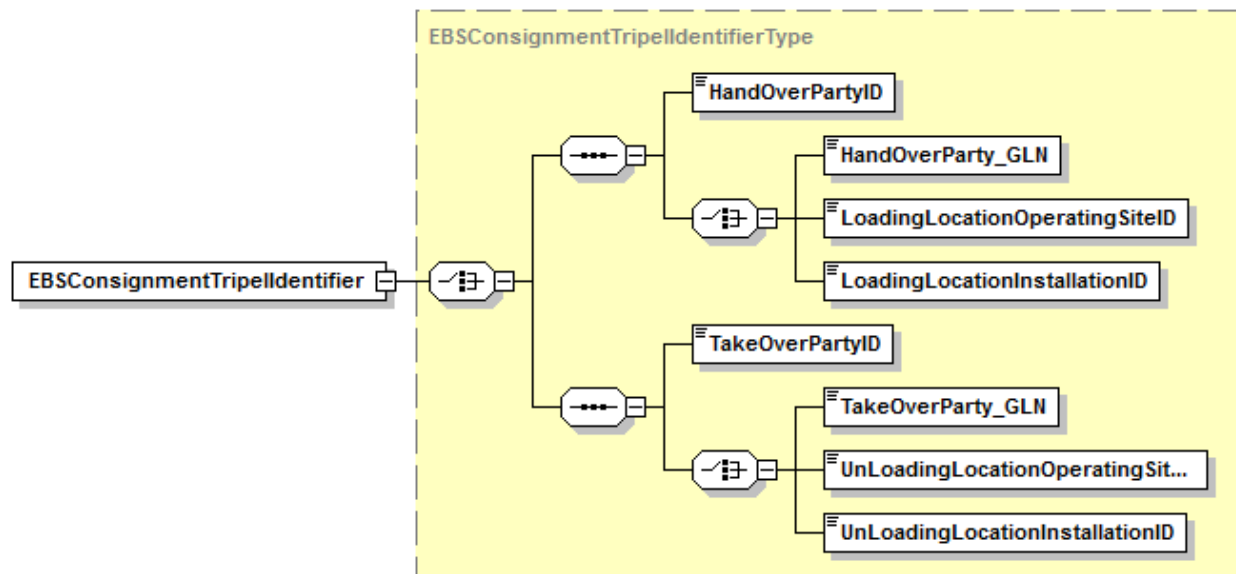
Begleitscheinnummern sind dreiteilig:

1. GLN (Global Location Number), die zu dem die Nummer vergebenden Übergeber oder Übernehmer gehört
2. Jahreszahl (zweistellig), z.B. 16
3. Fortlaufende Nummer: Fortlaufende Nummerierung der Begleitscheine, die mit Beginn eines neuen Kalenderjahres jeweils neu von vorne begonnen wird

In den zu einem Begleitschein übermittelten Angaben finden sich diese drei Bestandteile der Begleitscheinnummer an den folgenden Stellen:

- Fortlaufende Nummer und Jahreszahl: HandOverPartyID (Übergeber) bzw. TakeOverPartyID (Übernehmer) in *MaterialMovement*
- GLN:
 - Sofern die GLN einer ortsfesten Anlage angegeben ist, wird diese als Bestandteil der Begleitscheinnummer herangezogen: Falls vorhanden, MobileInstallationOperationLocationStationaryInstallationID, andernfalls InstallationID in *Location*, für LoadingLocation (Übergeber) oder UnloadingLocation (Übernehmer) in *MaterialMovement*
 - Andernfalls wird, sofern die GLN eines Standorts angegeben ist, diese als Bestandteil der Begleitscheinnummer herangezogen: OperatingSiteID in *Location*, für LoadingLocation (Übergeber) oder UnloadingLocation (Übernehmer) in *MaterialMovement*
 - Andernfalls wird die Personen-GLN des Übergebers bzw. des Übernehmers herangezogen: ID in HandOverParty (Übergeber) bzw. in TakeOverParty (Übernehmer) in *Transfer*

Außerhalb von Begleitschein-Angaben werden Begleitscheinnummern in Requests und Responses mit der EBSSignmentTripleIdentifier-Struktur abgebildet:



In dieser finden sich die drei Bestandteile der Begleitscheinnummer an den folgenden Stellen:

- Fortlaufende Nummer und Jahreszahl: HandOverPartyID (Übergeber) bzw. TakeOverPartyID (Übernehmer)
- GLN: LoadingLocationInstallationID (Anlage, Übergeber), UnLoadingLocationInstallationID (Anlage, Übernehmer); LoadingLocationOperatingSiteID (Standort, Übergeber), UnLoadingLocationOperatingSiteID (Standort, Übernehmer); HandOverParty_GLN (Person, Übergeber), TakeOverPartyGLN (Person, Übernehmer)

Zu beachten ist, dass der Betreiber der „Absendeort-Anlage“ bzw. des „Absendeort-Standorts“ nicht in allen Fällen der Übergeber sein muss, und dass der Betreiber der „Empfangsort-Anlage“ bzw. des „Empfangsort-Standorts“ nicht in allen Fällen der Übernehmer der Abfälle sein muss. Die in Begleitscheinnummern enthaltenen GLNs geben also nicht in allen Fällen Auskunft über den Übergeber bzw. Übernehmer, der die Begleitscheinnummer vergeben hat. Wenn der Betreiber des per GLN angegebenen „Absendeorts“ nicht der Übergeber ist, bzw. der Betreiber des „Empfangsorts“ nicht der Übernehmer, dann ist zudem eine Kollision mit einer bereits von jemand anderem vergebenen Begleitscheinnummern nicht ganz auszuschließen, was zu einer Zurückweisung bei der Übermittlung der Begleitscheindaten führt. Es muss dann eine neue fortlaufende Nummer zugewiesen werden.

4.3 Handhabung bestimmter Fälle von Abfallübergaben und Abfalltransporten

4.3.1 Streckengeschäft

Ein Streckengeschäft liegt vor, wenn ein Abfallsammler einen Abfall direkt zu einem weiteren Übernehmer transportiert oder transportieren lässt, ohne dass ein Standort des Abfallsammlers in tatsächlicher Hinsicht berührt wird. Ein zusammengesetztes Streckengeschäft liegt vor, wenn ein Streckengeschäft von mehreren Abfallsammlern, deren Standorte dabei nicht in tatsächlicher Hinsicht berührt werden, abgewickelt wird. (§13 Abs. 1 Abfallnachweisverordnung 2012).

Streckengeschäfte können „gewöhnlich“ dokumentiert werden (für jede rechtliche Abfallweitergabe ein separater „Begleitschein“), oder es kann die „Erleichterung Streckengeschäft“ (§13 Abs. 3 Abfallnachweisverordnung 2012) in Anspruch genommen werden. Bei letzterer ist ein einziger „Begleitschein“ ausreichend, auf dem Übergeber, (endgültiger) Übernehmer, und die Abfallsammler im Streckengeschäft, die rechtlich über den Abfall verfügen und deren Standorte von diesem Abfall nicht in tatsächlicher Hinsicht berührt werden, angeführt sind.

Bei „gewöhnlicher“ Dokumentation eines Streckengeschäfts ist in jedem der Begleitscheine ein Verweis auf den nachfolgenden Begleitschein anzugeben, und beim letzten zum Streckengeschäft gehörenden Begleitschein die besondere Kennung für das Ende des Streckengeschäfts. Im Detail sind die Erfordernisse für die Beschreibung eines Streckengeschäfts, sowohl in der „gewöhnlichen“ Variante, als auch in der Variante „Erleichterung Streckengeschäft“, im Datenanforderungsdokument beschrieben.

4.3.2 Sammeltour

Bei einer Sammeltour holt ein Abfallsammler Abfälle nacheinander von mehreren Übergebern ab und bringt sie gemeinsam zu einem Empfangsort. Sofern dieser Empfangsort ein Standort des Abfallsammlers ist, handelt es sich um eine Sammeltour. Wenn der Empfangsort von einem anderen Sammler oder Behandler betrieben wird, liegt eine Kombination aus einer Sammeltour mit einem Streckengeschäft vor. (Anhang 2 Abfallbilanzverordnung).

Bei Sammeltouren sind die „Begleitscheine“, analog zum Streckengeschäft, zu „verketteten“, d.h. Verweise auf Nachfolgebegleitscheine anzugeben, bzw. eine besondere Kennung für das Ende der Sammeltour, bzw. der Kombination aus Sammeltour und Streckengeschäft. Auch dazu sind die Details im Datenanforderungsdokument beschrieben.

4.3.3 Begleitscheinsplitting

Das sogenannte Begleitscheinsplitting ist für den Fall vorgesehen, dass nach dem Transport bzw. der Übergabe der Abfälle festgestellt wird, dass entgegen den davor gemachten Angaben Teile des transportierten bzw. übergebenen Abfalls unterschiedlichen Abfallarten zuzuordnen sind. Da sich ein „Begleitschein“ (Angaben zu einem Transport bzw. einer Übergabe) immer nur auf eine Abfallart bezieht, sind hier im Nachhinein zusätzliche Begleitscheine erforderlich.

In diesem Fall ist in den nachträglich erstellten „Korrekturbegleitscheinen“ der Bezug zum originalen Begleitschein, der damit korrigiert wird, einzutragen. Siehe Element *ReferredMaterialMovementPartyIdentificationID* und *ReferredMaterialMovementIdentificationID* in *ConsignementNote*. Details zu den Vorgaben beim Begleitscheinsplitting gehen aus dem Datenanforderungsdokument hervor.

4.4 Korrektur und Stornierung

Das Korrigieren von bereits an die zuständige Behörde bzw. die Kontrollorgane übermittelten Informationen zu einem Transport bzw. einer Übergabe gefährlicher Abfälle ist über das Begleitschein-Webservice möglich.

Das Stornieren ist über das EBSM-Webservice nicht möglich, aber beispielsweise über die EDM Begleitschein Web-Anwendung.

4.5 Zugriffsbeschränkungen

Mit den lesenden Operationen, insbesondere dem Fetch Service, ist immer nur der Zugriff auf solche im EDM eingetragenen Informationen zu Transporten bzw. Übergaben gefährlicher Abfälle („Begleitscheine“) möglich, in welchen der zum Webservice-Benutzer gehörende Registrierte als Übergeber, Übernehmer, Transporteur oder Streckengeschäftspartner auftritt.

Auf Prüfprotokolle hat neben der zuständigen Behörde sonst nur der zum Webservice-Benutzer gehörende Registrierte Zugriff, dessen Webservice-Aufruf Auslöser der Prüfprotokollerstellung war (d.h. nur Zugriff auf „eigene“ Prüfprotokolle).

4.6 Prüfprotokolle

Bei der Übermittlung von Daten zu Transporten bzw. Übergaben gefährlicher Abfälle (betrifft initiale Übermittlung, Korrekturen, usw.) werden durch EDM eBegleitschein automatisierte Prüfungen dieser Daten durchgeführt.

Ein wichtiger Aspekt dieser Prüfungen ist, dass damit die technische Verarbeitbarkeit überprüft bzw. sichergestellt wird. Ergeben die Prüfungen, dass die übermittelten Daten nicht technisch verarbeitbar sind, erfolgt eine sogenannte „Ablehnung“. Der gewünschte Vorgang, z.B. das Übermitteln von Informationen an die Behörde, konnte in diesem Fall nicht erfolgreich durchgeführt werden. Die Behörde erlangt in diesem Fall weder Kenntnis über die Informationen, deren Übermittlung versucht wurde, noch über den „Informationsvermittlungsversuch“ selbst.

Prüfungen können aber auch zum Ergebnis haben, dass die technische Verarbeitbarkeit vorliegt, jedoch anderweitig ein Hinweis auf potentiell fehlende oder unrichtige Daten erkannt wurde.

Welche Prüfungen an welchen übermittelten Inhalten „angeschlagen“ haben, und ob dies zur Ablehnung führt, oder nicht zur Ablehnung führt, aber als Hinweis auf zu ergänzende oder korrigierende Daten zu verstehen ist, diese Informationen werden über sogenannte Prüfprotokolle bereitgestellt.

In der „elektronischen Begleitscheinmeldung“ können mehrere „Begleitscheine“ auf einmal übermittelt werden. Hier erfolgt der Zugriff auf das Prüfprotokoll asynchron. D.h. im Response der jeweiligen Operationen ist kein Prüfprotokoll enthalten. Stattdessen wird das Prüfprotokoll per separatem Request (GetEBSConsignmentRequest) abgerufen (bis es EDM-seitig fertig berechnet wurde, und zum Abruf zur Verfügung steht, können mehrere Sekunden vergehen).

Beim „vollelektronischen Begleitscheinverfahren“ werden hingegen pro Request immer nur Daten zu einem Transport bzw. einer Übergabe gefährlicher Abfälle übermittelt. Die dazugehörigen Webservice-Operationen funktionieren synchron. Das zum Request gehörende Prüfprotokoll wird sofort im Response mitgeliefert.

Der HTML-Anhang zur Schnittstellenbeschreibung enthält Details zum Prüfprotokoll-Format.

4.7 Authentifizierung

4.7.1 Varianten

Sämtliche Operationen des eBegleitschein-Webservice erfordern eine Authentifizierung.

Das Webservice unterstützt die folgenden Varianten der Authentifizierung:

1. „Benutzername/Passwort“: Bei jedem Request werden die Zugangsdaten mit übermittelt und im EDM geprüft
2. „Token“ („Session-ID“): Zunächst wird ein Request durchgeführt, bei dem die Authentifizierung mit einer anderen Methode erfolgt, z.B. „Benutzername/Passwort“. In den „Response-Headers“ bzw. im Response liefert das Webservice ein „Token“ („Session-ID“). Dieses „Token“ ist für eine begrenzte Dauer zur Authentifizierung geeignet, und wird in nachfolgenden Requests an das Begleitschein-Webservice in den „Request-Headers“ mit an das Webservice übergeben, anstelle anderer Identifikations- und Authentifizierungsmittel
3. „PVP“: Die Authentifizierung ist auch über das sogenannte Portalverbundprotokoll (PVP) möglich. Der Portalverbund ist vorwiegend zur Kommunikation zwischen Körperschaften öffentlichen Rechts vorgesehen bzw. wird vorwiegend dafür genutzt. Folglich ist davon auszugehen, dass die PVP-Authentifizierung in Zusammenhang mit dem Begleitschein-Webservice keine oder nur eine geringe Rolle spielen wird. Auf die Authentifizierung mittels PVP wird daher in der vorliegenden Schnittstellenbeschreibung nicht näher eingegangen. Nähere Informationen zu dieser Authentifizierungsvariante bitte über den EDM-Helpdesk zu beziehen.

4.7.2 Wahl der passenden Authentifizierungsvarianten

Im EDM kommen aus Sicherheitsgründen sogenannte kryptologische Hashfunktionen zum Einsatz (Funktionen, die aus einem angegebenen Passwort einen „Hashwert“ berechnen, aus dem nicht auf das Passwort rückschließbar ist, mit dem aber überprüfbar ist, ob ein richtiges Passwort angegeben wurde – im EDM ist nur der Hashwert gespeichert, nicht das Passwort). Bei „State of the Art“ Hashfunktionen ist die Berechnung aufwändig, sie enthält viele Iterationen. Der Passwortvergleich auf Basis solcher Hashfunktionen kann bis zu einige Sekunden in Anspruch nehmen. In diesem Sinne sind Requests an das eBegleitschein-Webservice, die mit „Benutzername/Passwort“-Authentifizierung erfolgen, langsam. In Fällen, in welchen innerhalb einer kurzen Zeitspanne eine größere Zahl an Requests an das eBegleitschein-Webservice abgesetzt werden, ist daher empfehlenswert, die „Token“ („Session-ID“) Authentifizierungsvariante zu nutzen. Dadurch wird ein Akkumulieren der durch die Berechnung kryptologischer Hashwerte entstehenden „Verzögerungen“ vermieden.

4.7.3 „Username/Passwort“ Authentifizierung

Die „Username/Passwort“-Authentifizierung erfolgt in Form eines „Basic“ HTTP Authorization-Headers mit einer Base64 codierten `username:password` Kombination eines EDM-Benutzers (Haupt- oder Neben-Benutzer), der beim Request mit übermittelt wird.

Für einen User „max“ mit Passwort „test“ würde zum Beispiel der Base64 codierte String „max:test“ wie folgt lauten: „dXNlcjpwZXN0==“. Der HTTP Request Header für Basic Authentication müsste demnach folgenden Eintrag enthalten:

```
Authorization: Basic dXNlcjpwZXN0==
```

Schlägt die Authentifizierung fehl, dann wird ein SOAP-Fault retourniert.

HTTP Basic Authentication wird von zahlreichen Entwicklungsumgebungen unterstützt. Die Spezifikation kann unter <http://www.ietf.org/rfc/rfc2617.txt> abgerufen werden.

4.7.4 „Token“ („Session-ID“) Authentifizierung

Grundprinzip der Token-Authentifizierung ist, dass zunächst eine Authentifizierung mit den Zugangsdaten eines EDM-Benutzers (Haupt- oder Nebenbenutzer) erfolgt (siehe 4.7.3). Dabei wird vom Webservice ein „Token“ („Session-ID“) zurückgeliefert, das vom Client in Folge anstelle der „Username/Passwort“-Authentifizierung genutzt werden kann.

Bei den nachfolgenden Requests an das eBegleitschein-Webservice wird dieses Token dann Base64-codiert im HTTP-Request-Header für Token Authentication mitgeschickt:

Authorization: Token <Base64EncodedToken>

Der Bezug des Tokens ist sowohl mit beliebigen Operationen des eBegleitschein-Webservice möglich (in den Request-Headern werden „Username/Passwort“-Authentifizierungsdaten mitgeliefert, aus den Response-Headern kann das Token abgelesen werden), als auch über eine eigene „Login“-Operation des EDM Authentifizierungs-Webservice, welches zusätzlich auch eine „Logout“-Funktionalität (zum Beenden der Gültigkeit einer Session-ID) und eine „Ping“-Funktionalität (mit welcher die Gültigkeit einer Session-ID innerhalb eines maximalen Nutzungszeitfensters verlängert werden kann) zur Verfügung stellt.

Für das EDM-Authentifizierungs-Webservice ist am EDM Portal eigens eine Beschreibung veröffentlicht. Dort sind auch Details zur Gültigkeitsdauer von Tokens spezifiziert.

Für die Gültigkeit von Tokens gilt das folgende Grundprinzip:

- Es ist eine „Inaktivitätszeitspanne“ definiert (z.B. eine halbe Stunde; für aktuellen tatsächlichen Wert siehe Beschreibung des Authentifizierungs-Webservice): Wird das Token so lange nicht genutzt (d.h. gibt es mindestens so lange keinen Request an ein EDM-Webservice, in dem das Token in den HTTP-Request-Headern mit übermittelt wird), dann läuft die Gültigkeit des Token ab. Im Authentifizierungs-Webservice gibt es eine „Ping“-Operationen, die dafür genutzt werden kann, ein Token vor Ablauf der Gültigkeit durch Überschreiten der Inaktivitätszeitspanne zu bewahren.
- Es ist eine „maximale Nutzungsdauer“ für Token definiert (z.B. 24 Stunden; für aktuellen tatsächlichen Wert siehe Beschreibung des Authentifizierungs-Webservice). Nach Erstellung/Bereitstellung eines Tokens ist dieses jedenfalls nicht länger gültig, als es durch die „maximale Nutzungsdauer“ definiert ist. Das heißt, sofern ein Token nicht schon zuvor durch Überschreiten der Inaktivitätszeitspanne seine Gültigkeit verliert, so verliert es (trotz „laufender Nutzung“) dennoch nach Überschreiten der „maximalen Nutzungsdauer“ seine Gültigkeit.

Sollen nach Ablauf der Gültigkeit eines Tokens in nachfolgenden Requests weiterhin Tokens zur Authentifizierung verwendet werden, so ist das Anfordern eines neuen Tokens, z.B. durch neuerliche Benutzername/Passwort-Authentifizierung, erforderlich.

Für die Umsetzung der Anbindung an EDM-Webservices bedeutet das, dass Client-Software, welche Tokens zur Authentifizierung verwendet, mit dem Abauf der Gültigkeit von Tokens umgehen können muss (z.B. durch Wiederholung des Requests mit Benutzername/Passwort-Kombination, und Verwendung des daraus erhaltenen neuen Tokens in Folge-Requests).

4.8 Fehlerbehandlung

Bei Webservice-Aufrufen können Situationen eintreten, die eine gewöhnliche Abarbeitung des Aufrufs verhindern (Ausnahmesituation – „Exception“). Ein Beispiel für eine solche Ausnahmesituation ist das Fehlen von Berechtigungen für den lesenden oder schreibenden Datenzugriff. Für solche Ausnahmesituationen wird die sogenannte „SOAP Fault“-Systematik verwendet. Das heißt: Anstelle eines gewöhnlichen Response liefert das Webservice einen speziellen Fault-Response.

Dieser ist vom Typ „FailureType“ und besitzt die folgenden Inhalte:

Name	Type	Definition
Code	1 .. 1 xs:string	Eine ID (Identifikationszeichenkette), die auf einen Eintrag aus Codeliste 5156 „Fehlerkategorien“ verweist und solcherart den Fehler klassifiziert. Anmerkung: Die Fehlerkategorie kann bei der Fehlersuche durch IT-Personal hilfreich sein. Für den Endanwender ist die Fehlerkategorie im Allgemeinen unverständlich.
Reason	1 .. 1 xs:string	Eine Beschreibung des Fehlers. Anmerkung: Die Beschreibung des Fehlers kann bei der Fehlersuche durch IT-Personal hilfreich sein. Für den Endanwender ist die Fehlerbeschreibung im Allgemeinen unverständlich.
Detail	0 .. 1 xs:string	Eine Detailbeschreibung des Fehlers.

Für die Verarbeitung solcher SOAP-Faults gilt es zu berücksichtigen, dass das Auftreten eines solchen Fehlers in vielen Fällen weder vom Endanwender verursacht ist, noch von diesem behebbar ist. Die bei einem SOAP-Fault zurückgelieferten Inhalte sind somit auch nicht dafür gedacht, von der Client-Software dem Anwender „ungefiltert“ mitgeteilt zu werden, sondern dienen in erster Linie dazu, IT-Personal die Möglichkeit zu geben die Ursachen für den Fehler zu identifizieren und wenn notwendig zu beheben. Für den Anwender genügt bei den meisten Fehlerkategorien ein Hinweis, dass ein technischer Fehler vorliegt, und dass bei wiederholtem Auftreten des Fehlers Support durch IT-Personal eingeholt werden soll.

5 VORGABEN AN SOFTWARE MIT SCHNITTSTELLENANBINDUNG UND AN DEREN BENUTZER

5.1 Allgemeines

Zur Schnittstellenspezifikation zählen auch die im Folgenden aufgelisteten Vorgaben an Software, für die eine Schnittstellenanbindung umgesetzt wird, sowie Vorgaben an Benutzer dieser Software. Die Zielsetzungen hinter diesen Vorgaben sind unter anderem ein friktionsfreies, sicheres und für Anwender gut benutzbares Zusammenspiel von Software-Produkten mit dem EDM.

5.2 Vorgaben, die ausschließlich die Software betreffen

5.2.1 Erstellung und Verarbeitung von Dateninstanzen

Vorgabe 1 (ID 341): Generierte Dateninstanzen MÜSSEN bezüglich der am EDM Anwendungsportal veröffentlichten XML Schema Definition gültig sein.

Anmerkung: Es darf insbesondere nicht möglich sein, dass Nutzer der Software durch ihre Interaktion mit der Software (z.B. Eingabe unsinniger Daten oder Weglassen erforderlicher Daten) das Generieren ungültiger Dateninstanzen auslösen können.

Beispiel: Ein Software-Benutzer hat zu eine Abfallart ausgewählt, aber noch keine Masse angegeben, und wählt nun die Funktion „XML-Export/Übermittlung“. Gemäß XML-Datenformat ist die Angabe der Masse zwingend erforderlich. Würde die Software eine XML-Dateninstanz erstellen, in der die Angabe der Masse fehlt, so handelte es sich um eine ungültige Dateninstanz, und die Software wäre mangelhaft. Vielmehr ist es Aufgabe der Software, den Benutzer darauf aufmerksam zu machen, dass die vorliegenden Angaben unzureichend sind um eine gültige Dateninstanz zu erzeugen. ■

Vorgabe 2 (ID 628): Bei der Zeichencodierung generierter Dateninstanzen MUSS es sich um UTF-8 handeln. ■

Vorgabe 3 (ID 705): Generierte Dateninstanzen MÜSSEN allen der folgenden am EDM Anwendungsportal veröffentlichten Datenanforderungen entsprechen:

1. Datenanforderungen die als verpflichtend gekennzeichnet sind. Das sind insbesondere solche Datenanforderungen, zu der die Beschreibung enthalten ist, dass eine Verletzung zur Zurückweisung der Dateninstanz führt;
2. Datenanforderungen welche die Kennzeichnung enthalten, sich in erster Linie auf die korrekte XML-Repräsentation von Daten zu beziehen. ■

Vorgabe 4 (ID 394): Software SOLL so implementiert sein, dass generierte Dateninstanzen ALLEN am EDM Anwendungsportal zur Schnittstelle veröffentlichten Datenanforderungen entsprechen.

Anmerkung: Diese Vorgabe impliziert unter anderem das folgende Verhalten von Software: Sind von Benutzern stammende Angaben auf eine Weise unvollständig oder inkonsistent, die das Erstellen einer allen Datenanforderungen genügenden Dateninstanz verhindert, dann soll durch die Software keine Dateninstanz erstellt oder übermittelt werden, sondern stattdessen der Software-Benutzer auf das Fehlen oder die Inkonsistenz von Daten aufmerksam gemacht werden. ■

Vorgabe 5 (ID 816): Bei der Verarbeitung von Dateninstanzen MÜSSEN Dateninstanzen, welche sämtliche der als verpflichtend gekennzeichneten Datenvorgaben – insbesondere Gültigkeit bezüglich des XML Schemas und Einhaltung aller als verpflichtend gekennzeichneten Datenanforderungen – erfüllen, akzeptiert werden und dürfen nicht automatisch zurückgewiesen werden.

Anmerkung: Eine bei der Verarbeitung akzeptierte Dateninstanz kann in Folge von einem Menschen inhaltlich nicht akzeptiert bzw. zurückgewiesen werden. Diese Vorgabe bezieht sich lediglich auf ein

automatisches Zurückweisen, welches es ausschließlich unter den genannten Voraussetzungen geben darf. ■

5.2.2 Persistierung und (De-)serialisierung

Vorgabe 6 (ID 549): Funktionen zur Entgegennahme und Persistierung von Dateninstanzen MÜSSEN in Bezug auf die Inhalte (XML-Element- und Attributwerte) abwandlungsfrei und verlustfrei sein. Datenabwandlungen und Verluste MÜSSEN für die gesamte Dauer der Persistierung ausgeschlossen sein.

Anmerkungen:

- Dateninstanzen MÜSSEN so persistiert werden, dass die persistierten Daten für das Erstellen einer XML-Instanz geeignet sind, die sich von der entgegengenommenen XML-Instanz in den Inhalten (XML-Element- und Attribut-Inhalte) nicht unterscheidet.
- Dateninstanzen brauchen NICHT so persistiert zu werden, dass eine exakte Reproduktion der entgegengenommenen XML-Instanz grundsätzlich möglich ist. Unterschiede zwischen entgegengenommener XML-Instanz und aus persistierten Daten generierter bzw. generierbarer XML-Instanz sind zulässig, sofern sie nicht die Inhalte betreffen. Beispiele für solche nicht die Inhalte betreffenden Unterschiede zwischen XML-Instanzen sind in der W3C Empfehlung „Canonical XML“ beschrieben. Werden etwa in einer XML-Instanz Tabulatorzeichen zur Einrückung von XML-Tags verwendet, und in der anderen stattdessen Leerzeichen, so sind die beiden XML-Instanzen zwar als Byte- oder Zeichenfolge nicht exakt übereinstimmend, inhaltlich aber dennoch äquivalent.
- De facto bedeutet diese Vorgabe auch, dass entgegengenommene und verarbeitete XML-Element- und Attributwerte allesamt einzeln für sich persistiert werden müssen. Es sind insbesondere die folgenden Arten der Persistierung nicht geeignet:
 1. Entgegengenommene Element- oder Attributwerte stimmen mit Werten aus Stammdaten überein, auf welche die Daten entgegennehmende Software Zugriff hat. Anstelle die Element- und Attributwerte einzeln für sich zu persistieren wird lediglich ein Verweis auf den Stammdateneintrag gespeichert;
 2. Entgegengenommene Element- oder Attributwerte stimmen mit Werten aus Codelisten überein, auf welche die Daten entgegennehmende Software Zugriff hat. Anstelle die Element- und Attributwerte einzeln für sich zu persistieren wird lediglich ein Verweis auf den Codelisteneintrag gespeichert.

Diese Arten der Persistierung sind aus dem folgenden Grund nicht geeignet: Für Anpassungen von Stamm- und Referenzdaten soll unabhängig von deren Historisierung jedenfalls sichergestellt sein, dass deren Anpassungen keine automatischen (und im allgemeinen unbeabsichtigten) Änderungen von Meldungsinhalten nach sich ziehen. ■

5.2.3 Umgang mit Codelisten

Vorgabe 7 (ID 216): Software MUSS so implementiert werden, dass eine Aktualisierung von Codelisten bzw. ein Verwenden der Software mit aktualisierten Codelisten ohne neues Kompilieren, Ausrollen und Installieren der Software möglich ist. ■

Vorgabe 8 (ID 481): Im EDM werden über ein Webservice Codelisten zum Abruf angeboten. Software DARF NICHT so implementiert werden, dass jeder Zugriff auf Codelisten ad hoc und unmittelbar über das EDM Webservice erfolgt. Stattdessen MUSS Software mit „lokalen Kopien“ der Codelisten arbeiten. Das EDM Webservice zum Bezug von Codelisten DARF NICHT für andere Zwecke verwendet werden als das Initialisieren und Aktualisieren solcher „lokaler Codelisten-Kopien“. ■

Vorgabe 9 (ID 634): Es wird EMPFOHLEN, Software so zu implementieren, dass die Verfügbarkeit aktualisierter Codelisten in regelmäßigen Abständen automatisch geprüft wird.

Anmerkung: Eine solche Überprüfung der Verfügbarkeit aktualisierter Codelisten ist durch Implementierung einer Anbindung an das EDM Codelisten-Webservice möglich. ■

Vorgabe 10 (ID 788): Wird von Software in regelmäßigen Abständen automatisiert die Verfügbarkeit aktualisierter Codelisten geprüft, dann SOLL die Prüfung auf die Verfügbarkeit aktualisierter Codelisten zumindest alle 30 Tage erfolgen. ■

Vorgabe 11 (ID 580): Wird von Software in regelmäßigen Abständen automatisiert die Verfügbarkeit aktualisierter Codelisten unter Verwendung des EDM Webservice für Codelisten geprüft, dann DARF die

Prüfung auf die Verfügbarkeit einer aktualisierten Liste nicht öfter als ein Mal alle 12 Stunden erfolgen, und SOLL nicht öfter als ein Mal alle 24 Stunden erfolgen. ■

Vorgabe 12 (ID 909): Wenn bei der Entgegennahme bzw. Verarbeitung von Daten geprüft wird, ob in den entgegengenommenen Daten enthaltene Identifikationszeichenketten gültig in dem Sinn sind, dass sie mit der zu einem Codelisten-Eintrag gehörigen Identifikationszeichenkette übereinstimmen, dann MUSS folgende Bedingung eingehalten werden: Eine automatisierte Zurückweisung darf nur dann erfolgen, wenn sichergestellt ist, dass die von der empfangenden Software genutzten Codelisten-Kopien mindestens so aktuell sind wie die vom Dokumentersteller bzw. der dokumenterstellenden Software genutzten Codelistenkopien. ■

5.2.4 Fehlerbehandlung

Vorgabe 13 (ID 757): Tritt bei einem Webservice-Request eine Ausnahmesituation („Exception“) auf, d.h. ein SOAP-Fault, dann SOLL es dazu Client-seitig einen Log-Eintrag geben. ■

Vorgabe 14 (ID 530): Wird ein Webservice-Request (oder eine Folge von Webservice-Requests) durch eine Benutzerinteraktion ausgelöst, und tritt dabei eine Ausnahmesituation, d.h. ein SOAP-Fault, auf, dann SOLL der Benutzer darüber informiert werden, dass die Interaktion der Software mit dem EDM-Webservice fehlschlug. ■

Vorgabe 15 (ID 530): Wird ein Benutzer über das Fehlschlagen einer Interaktion mit dem EDM-Webservice informiert, dann SOLL mit den Informationen, die das EDM-Webservice als Beschreibung des Fehlers in der SOAP-Fault Nachricht liefert, in der Information an den Benutzer ausschließlich auf eine der beiden folgenden Arten umgegangen werden:

1. Die vom EDM Webservice gelieferte Beschreibung des Fehlers wird dem Benutzer NICHT bzw. nicht unmittelbar angezeigt.

Beispiel: Das EDM Webservice liefert als Fehlerbeschreibung die Fehlerkategorie-ID „101“ für „Authentifizierung fehlgeschlagen“. Diese Information (der Code 101) wird dem Benutzer nicht unmittelbar angezeigt. Der Benutzer sollte aber in diesem Fall sehr wohl darauf aufmerksam gemacht werden, dass die Authentifizierung fehlschlug. Aber eben NICHT durch unmittelbares Anzeigen der (nicht für Benutzer bestimmten) Informationen aus der SOAP-Fault-Nachricht;

2. Die vom EDM Webservice gelieferte Beschreibung des Fehlers wird dem Benutzer so angezeigt, dass offensichtlich ist, dass nicht der Benutzer selbst dazu angehalten ist, sich mit dieser Information auseinanderzusetzen, sondern dass dem Benutzer diese Information nur deswegen angezeigt wird, damit er sie im Bedarfsfall an Software-Servicepersonal weitergeben kann. ■

5.2.5 Authentifizierung

Vorgabe 16 (ID 284): Ein Vorhalten von EDM-Zugangsdaten durch die Client-Software für Webservice-Aufrufe ist grundsätzlich gestattet. Bevor EDM-Zugangsdaten vorgehalten werden MUSS zunächst jedoch eine explizite Einwilligung des Benutzers eingeholt werden. ■

Vorgabe 17 (ID 405): Es ist zulässig, dass die Einwilligung zum Vorhalten von EDM-Zugangsdaten durch Software, die als Client gegenüber EDM Webservices agiert, vom einem Benutzer der Software über einen Dialog in einer graphischen Benutzeroberfläche der Software eingeholt wird. Dazu MUSS Folgendes gewährleistet sein:

1. Der Benutzer MUSS gegenüber der Software authentifiziert sein, z.B. per Username und Passwort angemeldet;
2. Für die Einwilligung zum Vorhalten von EDM-Zugangsdaten MUSS der Benutzer zumindest die folgenden beiden Interaktionen durchführen:
 - a. Setzen einer „Checkbox“ oder eines vergleichbaren Interaktionselements zur Erklärung der Einwilligung;
 - b. Drücken einer Schaltfläche (eines „Buttons“) zur Bestätigung der Einwilligung. ■

Vorgabe 18 (ID 852): Vorgehaltene EDM-Zugangsdaten MÜSSEN in der Software so verwaltet werden, dass Unbefugte keinen Zugriff auf diese Zugangsdaten erhalten.

Anmerkung: Insbesondere DÜRFEN EDM-Zugangsdaten jedenfalls NICHT ohne Verschlüsselung gespeichert werden. ■

Vorgabe 19 (ID 939): Für Benutzer, deren EDM-Zugangsdaten eine Software für Webservice-Aufrufe vorhält, MUSS diese Software dem Benutzer die Möglichkeit bieten, die vorgehaltenen EDM-Zugangsdaten zu jedem beliebigen Zeitpunkt zu aktualisieren bzw. zu löschen.

Anmerkung: Daraus leitet sich auch ab, dass für durch User-Interaktionen unmittelbar ausgelöste EDM-Webservice-Aufrufe, für die das EDM Webservice ein Fehlschlagen der Authentifizierung rückmeldet, der Benutzer die Möglichkeit haben MUSS, die in der Software für Webservice-Aufrufe hinterlegten Zugangsdaten sofort und unmittelbar zu aktualisieren. ■

5.3 Vorgaben, die auch den Benutzer der Software betreffen können

5.3.1 Authentifizierung

Vorgabe 20 (ID 954): Die beim Aufruf jeder Webservice-Operation per HTTP Basic Authentication Header übermittelten Zugangsdaten MÜSSEN einen im EDM registrierten Benutzer authentifizieren. ■

5.3.2 Fristen

Vorgabe 21 (ID 681): Meldungen SOLLEN innerhalb der rechtlich definierten Fristen an zuständige Behörden übermittelt werden.

Anmerkung: Fristüberschreitungen, etwa Meldungen oder Korrekturen, die viele Monate oder gar Jahre zu spät erfolgen, können zu einer automatischen Zurückweisung führen (und beispielsweise das Eintragen über Web-Anwendung, oder das Freischalten durch die Behörde für eine Übermittlung via Webservice erfordern). ■