AM.exchange TrackEventInformationService Handbuch für SW-Entwickler

Autor:
Deutsche Post, Service Niederlassung IT Post & Paket Deutschland,
Abt. 1510 Kundenintegration Post

IT Customer Support Post (IT CSP)

Version 1.1.4 vom 01. April 2019

Änderungsnachweis

Für eine detaillierte Historie der Änderungen s. Anhang K – Änderungshistorie

Version	Bearbeiter	Datum	Bemerkung
1.0	R. Rondot	25.06.2015	Erstellung
1.1	R. Rondot	30.06.2015	Überarbeitung für Service-Version 1.1
1.1.1	D. Ludwig	01.11.2015	Einbau Ländernachweis
1.1.2	D. Ludwig	10.04.2016	Ergänzung Track&Match und Einbau Zustell-nachweis
1.1.3	D. Ludwig	01.11.2017	Ergänzung Zustellnachweis um Warenpost
1.1.4	D. Ludwig	01.04.2019	Einfügen Nutzungsbedingungen, Anhang I, Entfernen Track&Match, kleine textuelle An-passungen

Inhaltsverzeichnis

1 Nutzungsbedingungen für TrackeventinformationService

Mit der Nutzung des Trackeventinformation Services erklären Sie sich mit den nachfolgenden Nutzungsbedingungen einverstanden.

Nutzungsbedingungen

der

Deutsche Post AG

Charles-de-Gaulle-Str. 20

53113 Bonn

- im Folgenden „Deutsche Post“ -

über die Anbindung des TrackEventInformationService (TEIS) zur automatischen Abfrage des aktuellen Sendungsstatus der Produkte Einschreiben, Nachnahme, Prio, Warenpost national, Warenpost international, Ländernachweis und Telegramm

Präambel

Der Kunde versendet große Mengen verfolgbarer Sendungen (Einschreiben, Nachnahme, Prio, Warenpost national, Warenpost international, Ländernachweis und Telegramm) über die Deutsche Post. Der Kunde kann im Rahmen dieser Vereinbarung den aktuellen Sendungsstatus seiner Sendungen automatisiert über den **TrackEventInformationService (TEIS) der Deutschen Post** abfragen und in seine Kundensysteme übernehmen, um diesen z.B. direkt in seinem Onlineshop anzuzeigen.

1. **Gegenstand dieser Nutzungsbedingungen**

Gegenstand dieser Nutzungsbedingungen ist die Bereitstellung und der Betrieb des TEIS durch die Deutsche Post.

Die Nutzung des TEIS erfordert die Anbindung des Kunden an das TEIS und die Freischaltung durch die Deutsche Post AG

Durch die Anbindung an und die Nutzung des TEIS stimmt der Kunde diesen Nutzungsbedingungen zu. Darüber hinaus wird auf die Nutzungsbedingungen des IT-Systems AM (Auftragsmanagement) verwiesen https://auftragsmanagement.deutschepost.de.

2. Leistungen der Deutschen Post

Die Deutsche Post stellt TEIS gemäß dem Entwicklerhandbuch „Track Event Information Service- TEIS“ zur Verfügung, der für den Kunden über das IT-System AM (Auftragsmanagement) erreichbar ist.

Deutsche Post unterstützt den Kunden durch Support, Test- und Abnahmemöglichkeiten im Rahmen seiner Anbindung an TEIS.

Übergeben werden der Status zu jeder abgefragten Sendungsnummer mit den entsprechenden Bedeutungen (s. Entwicklerhandbuch TEIS). Die Deutsche Post stellt die Statusinformationen als XML Datensatz per Web Service oder auf einem SFTP Account der Deutschen Post zur Abholung bereit.

Der technische Support der Deutschen Post (IT CSP) steht unter der E-Mailadresse it-csp@deutschepost.de zu folgenden Servicezeiten zur Verfügung:
Montag bis Donnerstag 8.00 bis 17.00 Uhr
Freitag 8.00 bis 16.00 Uhr

Bei Erfüllung der Voraussetzungen durch den Kunden laut Punkt 3 führt die Deutsche Post die Aufschaltung auf den Web-Service innerhalb von 8 Tagen nach Zustimmung zu den Nutzungsbedingungen durch. Deutsche Post steht es frei die Aufschaltung des Kunden zu verweigern.

Bei einem Verstoß gegen gesetzliche Vorschriften oder diese Nutzungsbedingungen durch den Kunden oder einen ihm zurechenbaren Dritten oder bei einer technischen Störung von TEIS oder der für TEIS genutzten IT-Systeme ist die Deutsche Post berechtigt, TEIS vorübergehend ganz oder teilweise gegenüber dem Kunden zu sperren oder dessen Nutzungsmöglichkeiten einzuschränken.

Deutsche Post kann die abrufbaren Informationen (Sendungsnummern, das Entwicklerhandbuch TEIS etc.) als auch TEIS und die IT-Systeme auf denen TEIS beruht, während der Vertragslaufzeit jederzeit ändern (u.a. aktualisieren, erweitern oder einschränken). Es obliegt dem Kunden notwendige Anpassungen an seiner Anbindung an TEIS nach entsprechender Mitteilung durch Deutsche Post auf eigene Kosten vorzunehmen.

Es bleibt der Deutsche Post vorbehalten, sämtliche nach diesen Nutzungsbedingungen zu erbringenden Leistungen ganz oder teilweise durch Dritte zu erbringen.

3. Rechte und Obliegenheiten des Kunden

Der Kunde muss die Programmierung, die für die automatisierte Abholung und Verarbeitung der Daten erforderlich ist, eigenverantwortlich und auf eigene Kosten durchführen.

Die Kunden können online auf die Track Events zugreifen, wie im Entwicklerhandbuches „Track Event Information Service- TEIS“ beschrieben.

Der Kunde darf nur die Sendungsnummer der vom ihm selbst verschickten trackbaren Sendungen abfragen. Die Zugangsdaten, insbesondere EKP und Passwort, dürfen nicht an Dritte weitergegeben werden.

Bei der Sendungsabfrage dürfen folgende Höchstgrenzen von Anfragen nicht überschritten werden:

- pro Tag (zwischen 0.00 und 23:59 Uhr) max. 1.000 Anfragen mit insgesamt 10.000 Sendungen
- max. 3 Anfragen pro Sekunde

Für bereits zugestellte Sendungen darf keine erneute Abfrage des Sendungsstatus erfolgen. Außerdem darf der Kunde keine Abfragen des Sendungsstatus für Dritte durchführen.

4. Preise

Die Nutzung des TEIS ist für den Kunden kostenlos.

5. Gewerbliche Schutzrechte, Nutzungsrechte und Nutzungsumfang

Deutsche Post räumt dem Kunden an den zur Verfügung gestellten Informationen (Sendungsnummern, das Entwicklerhandbuch TEIS etc.) ein einfaches, widerrufliches, nicht übertragbares, nicht unterlizenzierbares, zeitlich unbeschränktes Nutzungsrecht ein, das den nachfolgenden Einschränkungen unterliegt:

a. das Nutzungsrecht beschränkt sich ausschließlich auf die jeweils aktuellen von Deutsche Post bereitgestellten Informationen;

b. das Nutzungsrecht wird ausschließlich für die in diesem Vertrag genannten Zwecke, insbesondere der Anbindung an TEIS und deren Anpassung eingeräumt;

Sämtliche Rechte an den zur Verfügung gestellten Informationen verbleiben bei Deutsche Post.

6. Geheimhaltung, Datenschutz

Die Parteien verpflichtet sich, sämtliche Informationen, die ihnen im Zusammenhang mit dieser Vereinbarung von der jeweils anderen Partei mitgeteilt werden oder auf andere Weise bekannt werden, geheim zu halten und nicht gegenüber Dritten offen zu legen oder an Dritte weiterzugeben, sei es direkt oder indirekt – ausgenommen hiervon sind in die Vertragsabwicklung einbezogene Dritte, vor allem technische Dienstleister des Kunden.

Die Vertraulichkeitsverpflichtung gemäß vorstehenden Ziffern 12 Abs. 1 und Abs. 2 gilt nicht für Informationen, wenn und soweit:

a. Diese Informationen im Rahmen einer Sendungsabfrage von Deutsche Post zur Verfügung gestellt wurden;

b. diese bereits vor Offenlegung und ohne Vertraulichkeitsverpflichtung in dem Besitz der jeweiligen Partei war,

c. diese ohne das Zutun einer Partei veröffentlicht worden oder anderweitig ohne das Verschulden einer Partei allgemein bekannt geworden sind,

d. diese der jeweiligen Partei nach Abschluss des Vertrages von einem oder mehreren Dritten ohne Vertraulichkeitsverpflichtung rechtmäßig, also ohne Bruch dieses Vertrages, übermittelt wurden,

e. diese nach gesetzlichen oder verwaltungsrechtlichen Vorschriften offen gelegt werden müssen.

Deutsche Post erbringt ihre Leistungen unter Beachtung der einschlägigen Datenschutzbestimmungen.

Personenbezogene Daten des Kunden werden nur erhoben, verarbeitet oder genutzt, sofern dies für die Bereitstellung der Leistungen erforderlich ist. Eine darüber hinausgehende Nutzung erfolgt nur, sofern der Kunde eingewilligt hat und die Datenschutzgrundverordnung (DSG VO) oder eine andere Rechtsvorschrift es anordnet oder erlaubt.

Beide Parteien verpflichten sich zur Einhaltung sämtlicher einschlägiger datenschutzrechtlicher Vorschriften. Die Parteien werden personenbezogene Daten, die ihnen im Rahmen der Zusammenarbeit unter dieser Vereinbarung zugänglich gemacht werden, allein für die Zwecke der Leistungserbringung nutzen und gegenüber Zugang und Kenntnisnahme durch Dritte schützen.

7. Aufbewahrungsfrist

Die Verfügbarkeit der Daten mit Informationen zu einem Sendungsstatus variiert je nach verwendetem Produkt. Für alle Sendungsstatus gilt jedoch, dass diese für mindestens 7 Tage nach Eintrittsdatum verfügbar sind und spätestens nach 60 Tagen gelöscht werden.

8. Haftung

Ansprüche des Kunden, gleich aus welchem Rechtsgrund, sowie seine Ansprüche auf Ersatz vergeblicher Aufwendungen sind ausgeschlossen, es sei denn, die Schadensursache beruht auf einer grob fahrlässigen oder vorsätzlichen Pflichtverletzung.

Die vorstehende Haftungsbegrenzung gilt nicht für Schäden, die auf der Verletzung des Lebens, des Körpers oder der Gesundheit beruhen oder bei einer Haftung nach dem Produkthaftungsgesetz.

Die Deutsche Post haftet keinesfalls für Schäden infolge von Leistungsausfällen und Leistungsverzögerungen aufgrund unvorhersehbarer von der Deutsche Post, ihren gesetzlichen Vertretern oder ihren Erfüllungsgehilfen nicht zu vertretender Ereignisse (höhere Gewalt). Als Ereignisse höherer Gewalt gelten insbesondere Krieg, Unruhen, Naturgewalten, Feuer,

Sabotageangriffe durch Dritte (wie z.B. durch Computerviren), Stromausfälle, behördliche Anordnungen, rechtmäßige unternehmensinterne Arbeitskampfmaßnahmen und der Ausfall oder eine Leistungsbeschränkung von Kommunikationsnetzen anderer Betreiber.

9. Schlussbestimmungen

Deutsche Post ist berechtigt, diese Nutzungsbedingungen aus betrieblichen, gesetzlichen oder sonstigen Gründen zu ändern. Änderungen der vorliegenden AGB werden dem Kunden durch Deutsche Post in geeigneter Weise, z.B. per E-Mail, mitgeteilt. Soweit nicht ein schriftlicher Widerspruch des Kunden innerhalb eines Monats nach Zugang bei Deutsche Post eingeht, gelten diese Änderungen als akzeptiert. Auf diese Folgen wird Deutsche Post den Nutzer bei der Mitteilung der Änderung hinweisen.

Für sämtliche Rechtsbeziehungen der Vertragspartien gilt deutsches Recht bei Ausschluss des UN-Kaufrechts.

Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder anlässlich dieses Vertrages ist Bonn.

2 Einleitung

2.1 Kurzübersicht AM.exchange-Protokoll

Das AM.exchange-Protokoll bietet eine Sammlung von Nachrichten, sog. Requests und Responses, zum Austausch von Informationen mit dem Auftragsmanagement-System der Deutschen Post AG. Es werden zwei Services angeboten:

- **OrderManagement**: Dient dem Austausch von auftragsbezogenen Informationen. Den Kern dieser Nachrichtensammlung bildet die Nachricht zur Auftragsanlage. Für diesen Service existiert ein eigenes Entwicklerhandbuch.
- **TrackEventInformationService**: Ermöglicht den Abruf von Track-Events zu postalischen Einheiten, z. B. Sendungen oder Paletten, die im Laufe der Bearbeitung bei der Deutschen Post AG entstehen. Dieses Entwicklerhandbuch bezieht sich ausschließlich auf diesen Service.

2.2 Ziel des Dokuments

Dieses Dokument gibt IT-Projektleitern und Softwareentwicklern alle wichtigen Informationen zum Service TrackEventInformation des AM.exchange-Protokolls der Deutschen Post an die Hand. Es beantwortet daher unter anderem die folgenden Fragen:

- Welche Möglichkeiten bietet das AM.exchange-Protokoll?
- Wie sehen die Prozesse im Detail aus?
- Welche Daten werden ausgetauscht?
- Welche technischen Übertragungskanäle können genutzt werden?
- Welche Möglichkeiten zum Testen stehen Ihnen zur Verfügung?
- Wer ist Ansprechpartner bei Fragen zu AM.exchange?

2.3 Aufbau des Dokuments

In Kapitel 3 werden als Einstieg in das Thema die technische Systemarchitektur und die sich daraus ergebenden Kommunikationsmöglichkeiten erläutert. Das Kapitel behandelt Themen wie Übermittlungskanäle, Datensicherheit etc.

In Kapitel 4 wird der inhaltliche Aufbau der AM.exchange-Nachrichten des Services TrackEventInformation im Detail erklärt. Alle möglichen Nachrichtensektionen und Datenfelder einer AM.exchange-Nachricht für den Service TrackEventInformation werden beschrieben.

Eine detaillierte Beschreibung aller Feldinhalte der AM.exchange-Nachrichten befindet sich in Anhang C bzw. Anhang D. Auf diese Anhäng sei daher hier – insbesondere für die Entwickler – gesondert verwiesen.

Das Kapitel 5 erläutert die zur Verfügung stehenden Systemumgebungen der Deutschen Post. Dies ist einerseits die sog. „Abnahmeumgebung“, die für den Test bzw. die Abnahme

von AM.exchange-Software verwendet wird und andererseits die „Produktionsumgebung“, auf der Produktivdaten eingeliefert werden.

Kapitel 6 erklärt Details der zur technischen Kommunikation bzw. Datenübermittlung zur Verfügung stehenden Nachrichtenübertragungskanäle.

Kapitel 7 gibt wichtige Hinweise zur Bedeutung der Service-Versionen.

Im umfangreichen Anhang des Dokuments befinden sich

- ein Glossar,
- die aktuellen XML-Schemas,
- eine umfassende Dokumentation der XML-Schemas im HTML und im PDF-Format,
- die zur Entwicklung des Webservices erforderlichen WSDL-Dateien,
- Beispiele für den Service TrackEventInformation im AM-XML Format,
- die derzeit gültigen Code-Tabellen,
- die Liste der möglichen Fehlercodes und Fehlermeldungen der Schnittstelle,
- Ihre Ansprechpartner bei der Deutschen Post,
- die Änderungshistorie dieses Handbuches.

3 Architekturüberblick

3.1 Übertragungskanäle

Die Deutsche Post bietet Ihren Kunden zwei Datenübertragungskanäle zur Nutzung des TrackEventInformationServices an. Jeder Kunde kann abhängig von den ihm zur Verfügung stehenden technischen Möglichkeiten und des Anwendungsfalls entscheiden, welche der folgenden Optionen er verwenden möchte:

SOAP-Webservice

Die Kommunikation mit dem Webservice TrackEventInformation läuft dabei ausschließlich auf Basis von SOAP über https. Damit ist eine sichere, verschlüsselte Übertragung der Daten zwischen Kunden und der Deutschen Post gewährleistet. Der Webservice ermöglicht eine synchrone Datenkommunikation zwischen Kunden und der Deutschen Post, das heißt, die Verbindung bleibt bestehen, bis die Anfrage beantwortet wurde und der Aufrufer kann anschließend umgehend die Antwort verarbeiten.

Secure File Transfer Protocol (SFTP)

Die Nutzung von SFTP ist aus Sicht des Benutzers der von FTP sehr ähnlich. Ein wesentlicher Unterschied ist jedoch, dass beim SFTP Protokoll die Daten bei der Datenübertragung durch Nutzung des SSH-Protokolls verschlüsselt werden. Bei dieser Übertragungsart erfolgt die Kommunikation asynchron, d. h. der Kunde legt auf dem ihm zugewiesenen SFTP-Account eine Datei mit der Response ab und erhält, sobald die Verarbeitung des Requests abgeschlossen ist, im gleichen Account eine Datei mit der Response bereitgestellt.

Handlungsempfehlung

Der Webservice ermöglicht eine synchrone Kommunikation unter Verwendung moderner Technologien. Die Beschreibung des Webservices ist als WSDL-Datei verfügbar, die in vielen Systemen eine schnelle und unproblematische Anbindung ermöglicht. Daher sollte der Webservice als bevorzugte Möglichkeit angesehen werden.

3.2 Authentifizierung und Autorisierung

Der Aufruf des Services ist gegen den unbefugten Zugriff geschützt. Beim Aufruf des Service müssen ein gültiger AM-Benutzername sowie das dazu passende Passwort mitgeliefert werden. Ihre Zugangskennungen zum AM-System erhalten Sie auf Anfrage bei Ihren Ansprechpartnern des IT Customer Support Post (IT CSP, s. Anhang J).

Zusätzlich müssen beim Aufruf als Webservice im SOAP-Header ein Benutzername und ein Passwort angegeben werden sowie bei der SFTP-Übertragung eine authentifizierte Anmeldung am Server erfolgen. Diese Zugangsdaten erhalten Sie im Rahmen der initialen Anbindnung ebenfalls von Ihrem Ansprechpartner des IT CSP.

3.3 Unterstützte Datenformate

Mit AM-XML wird das Datenformat für den elektronischen Datenaustausch bereitgestellt.

Das AM-XML Format folgt dem Statement of Mailing Submission (SMS) des Comité Européen de Normalisation (CEN) – dem Europäischen Pendant zur DIN.

3.4 Datenprüfungen und Fehlerbehandlung

Prinzipiell werden zwei Arten von Prüfungen auf den elektronisch eingelieferten Daten durchgeführt:

- Syntaktische Prüfungen
- Fachliche Prüfungen

Für syntaktische und fachliche Fehler erfolgt eine unterschiedliche Fehlerbehandlung. Während die Fehlerbehandlung bei fachlichen Fehlern immer gleich ist, unterscheidet sich die Fehlerbehandlung bei syntaktischen Fehlern je nach Übertragungskanal.

3.4.1 Behandlung syntaktischer Fehler beim SOAP-Webservice

Tritt bei einem Aufruf des SOAP-Webservice ein syntaktischer Fehler auf, so wird eine entsprechende SOAP-Response mit einem „SOAP Fault“ Element erzeugt, die die Fehlermeldung in den Tags „faultcode“ und „faultstring“ enthält. Die Nachricht enthält keinen weiteren Nutzinhalt (SOAP Body), sondern nur die Fehlermeldung.

3.4.2 Behandlung syntaktischer Fehler beim Aufruf über SFTP

Tritt beim asynchronen Aufruf über den Übertragungskanal SFTP ein syntaktischer Fehler auf, so wird über einen separaten Nummernkreis eine entsprechende Fehlermeldung erzeugt. Diese wird als „normale“ Response zurückgegeben, d. h. als Element ErrMsg in der Sektion Return der Response.

3.4.3 Behandlung fachlicher Fehler

Syntaktisch korrekte Nachrichten werden an das AM System weitergeleitet. Im AM System durchläuft eine Nachricht bzw. ein Operationsaufruf fachliche Prüfungen. Im Zuge dieser Prüfungen werden Warnungen und ggf. eine Fehlermeldung erzeugt und in die Response mit Nummer und entsprechendem Text eingefügt.

In jeder Response sind neben dem Gesamtrückgabewert der Operation (OK, Warnungen, Fehler) auch die bei der Verarbeitung aufgetretenen Warnungen und Fehlermeldungen inklusive Fehlernummer und Text enthalten.

4 Inhaltlicher Nachrichtenaufbau

Dieses Kapitel gibt einen Überblick über den logischen bzw. inhaltlichen Aufbau der AM.exchange Nachrichten des Services TrackEventInformation.

Es wird die allgemeine Funktionsweise der Operation erläutert. Die folgende Beschreibung der Service-Operation bezieht sich auf die logischen Dateninhalte, die beim Aufruf zu liefern sind.

Die genaue technische Beschreibung des AM-XML-Formates für TrackEventInformationService ist über die jeweiligen im Anhang B enthaltenen XML-Schema-Dateien bzw. die im Anhang E enthaltenen WSDL-Dateien gegeben. In der im Anhang C bzw. Anhang D referenzierten Übersicht befindet sich eine detaillierte Beschreibung aller Felder.

Die folgende Abbildung gibt einen Überblick über die Sektionen, aus denen ein Request TrackEventInformation.getTrackEvents besteht und wie oft diese in der Nachricht auftreten können. Es werden auch die jeweils englischen Begriffen für die Sektionen genannt, da die AM-XML Nachrichtenstruktur nur diese verwendet.

Sektion 1	Nachrichten Header	Message Header	(1,1)
Sektion 2	Trackevent-Filter	Trackevent Filter	(1, *)

Abbildung 1: Die Sektionen des Requests TrackEventInformation im Überblick

Neben dem oben aufgeführten Nachrichten-Header, der in den Request- und Response-Dateien der AM.exchange-Nachricht auftritt, gibt es zwei weitere Sektionen, die nur in den Response-Dateien der Deutschen Post verwendet werden:

Sektion 3	Operationsergebnis	Return	(1, 1)
Sektion 4	Trackevent-Liste	Trackevent List	(1, 1)

Abbildung 2: Spezielle Nachrichtensektionen

In den folgenden Unterkapiteln wird die grundsätzliche Bedeutung der Sektionen erläutert.

4.1 Sektion 1 – Nachrichten-Header (MsgHeader)

Der Nachrichten-Header (engl. Message Header) ist in jeder AM.exchange Nachricht genau einmal enthalten. Er enthält allgemeine Informationen zum Ursprung der Nachricht und zum Nachrichtenversand. Der Inhalt des Nachrichten Header hat keinerlei fachlichen Bezug zu dem mit der Nachricht versendeten Operationsaufruf.

Folgende Informationen sind beispielsweise im Nachrichten Header enthalten:

- Eine eindeutige Nachrichten-ID, die diese Nachricht (zusammen mit der Kundennummer des Nachrichtenübermittlers) identifiziert (siehe Absatz 4.5).
- Der Zeitpunkt der Erzeugung der Nachricht.
- Die Kundennummer sowie ggf. die Adresse und fachliche und technische Ansprechpartner des Nachrichtenübermittlers.
- Informationen zur Herkunft der Nachricht
  (Kundensystem und ID der Nachricht in diesem System)

4.2 Sektion 2 - Trackevent-Filter (TrackeventFilter)

Über die Sektion 2 Trackevent-Filter werden die Eigenschaften der gesuchten TrackEvents übermittelt. Über das Element Process.type wird dabei gesteuert, zu welchem postalischen Prozess die TrackEvents gesucht werden. Dadurch ergeben sich auch die möglichen Belegungen der weiteren Felder. Derzeit gibt es drei Prozesse, die darüber angesteuert werden können:

1. Track&Trace Brief:
   Für diesen Prozess können drei Konstanten für den Prozess-Typ verwendet werden:
   - TNT_LETTER_SEARCH-BY-BZL-SHIPMENT-ID
   - TNT_LETTER_SEARCH-BY-SHIPMENT-ID
   - TNT_LETTER_SEARCH-BY-CUSTOMER-DATA

   Diese ermöglichen jeweils die Angabe einer Sendungs-ID und eines (optionalen) Einlieferungsdatums als Suchmuster. Die weiteren Felder bleiben für diese Prozess-Typen ungenutzt.

   Bitte beachten Sie, dass für diese Prozess-Typen derzeit maximal 10 TrackEventFilter im Request enthalten sein dürfen, obwohl das XML-Schema mehr zulässt. Sind mehr als 10 TrackEventFilter enthalten, erhalten Sie eine entsprechende Fehlermeldung.

2. Letter International

   Für diesen Prozess wird die Konstante LETTER_INTERNATIONAL für den Prozess-Typ verwendet.

   Sie ermöglich die Suche nach Trackevents für Ländernachweis anhand einer internationalen Sendungsnummer, einer Auftragsnummer oder einer Absender - Kundenummer in Verbindung mit einem Zeitraum. Eine Kombination von Auftragsnummer, Sendungsnummer und/oder Absender-Kundennummer mit Zeitraum ist dabei nicht ausgeschlossen, allerdings wird bei unpassenden Parametern ein leeres Ergebnis zurück geliefert. Die Nutzung dieses Prozesstyps setzt eine Auftragsnummer im Auf-

tragsmanagement System der Deutschen Post voraus.

3. Warenpost national

   Für diesen Prozess gibt es zwei Prozesstypen: PROOF_OF_DELIVERY und PROOF_OF_DELIVERY_CREATION_DATE

   Der Prozesstyp PROOF_OF_DELIVERY ermöglicht die Suche von Trackevents anhand einer Auftragsnummer und/oder eines Zeitraumes (in Verbindung mit einer Absender-Kundennummer). Zusätzlich kann über das neu eingeführte Element MailEntityInterval ein Sendungsnummernintervall angegeben werden, um ggf. das Suchergebnis weiter einzuschränken. Das kann beispielsweise erforderlich sein, wenn ansonsten mehr als 200.000 Sendungs-IDs gefunden würden, für die Trackevents vorliegen, da aufgrund von technischen Einschränkungen eine größere Zahl an Sendungs-IDs nicht zurückgeliefert werden kann.

   Der Prozesstyp PROOF_OF_DELIVERY_CREATION_DATE ermöglicht die Suche von Trackevents anhand einer Auftragsnummer und eines Zeitraumes (in Verbindung mit einer Absender-Kundennummer) wobei sich hier der Zeitraum auf den Anlagezeitraum des Trackevent im AM System bezieht.

   Hinweis: zur Zeit können mittels dieser Prozesstypen nur Trackevents für DV – freigemachte Warenpost national geladen werden.

4.3 Sektion 3 – Operationsergebnis (Return)

In der Sektion 3, engl. Return-Sektion, wird das Gesamtergebnis eines Operationsaufrufes zusammen mit den ggf. aufgetretenen Warnungen und Fehlermeldung zurückgeliefert. Die Return-Sektion ist in der Response jedes Operationsaufrufes enthalten.

Das Gesamtergebnis einer Operation hat eine der folgenden drei Ausprägungen:

- **OK** - die Operation wurde fehlerfrei und ohne Warnmeldungen abgeschlossen.
- **WARNING** – die Operation wurde fehlerfrei, aber mit Hinweisen bzw. Warnmeldungen abgeschlossen.
- **ERROR** – bei der Operationsdurchführung traten Fehler auf.

Folgende Informationen werden zu jeder Warnung und Fehlermeldung zurückgeliefert:

- **Level** – WARNING oder ERROR
- **Nummer** – die eindeutige zur Warnung bzw. dem Fehler gehörende Nummer.
- **Text** – der ausführliche Klartext der Warnung bzw. Fehlermeldung.

4.4 Sektion 4 – Trackevent-Liste (TrackEventList)

In der Sektion 5 Trackevent-Liste werden die Daten der gefundenen Trackevents bereitgestellt. Zu jedem gefundenen Trackevent wird ein Element TrackEvent erzeugt. Dieses enthält die verfügbaren Daten des Trackevents, d. h. Angaben zum Erzeuger des Trackevents, der betroffenen Sendung und weitere Beobachtungen (Observation) bzw. Erwartungen (Expectation) zur Eigenschaften der Sendung (z. B. Maße) bzw. zum Trackevent selbst (z. B. Ort). Auch hier ist es wieder abhängig vom Prozess (Process.type), aus dem die Trackevents stammen, welche Felder gefüllt werden.

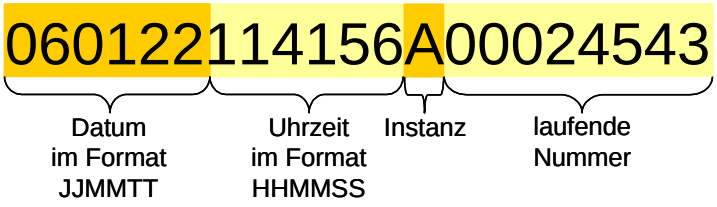
4.5 Besonderheiten Nachrichten-ID (MsgID)

Jede AM.exchange Nachricht verfügt über einen Nachrichtenkopf. Dieser beinhaltet (je Nachrichtenübermittler) eine **eindeutige ID** für jede Nachricht. Die Nachrichten-ID ist vom Nachrichtenübermittler nach den folgenden Konventionen zu vergeben:

Jede Nachrichten ID hat immer genau 21 Stellen und ist wie folgt zusammengesetzt:

<Datum und Uhrzeit> + <ID der SW-Instanz> + <fortlaufende Nummer>

Ein Beispiel:



<Datum und Uhrzeit>
Aktuelles Datum und Uhrzeit der Erstellung der Nachricht (z.B. "060122114156"). Das Tagesdatum wird 6-stellig im Format YYMMDD angegeben. Danach folgt die Angabe der Uhrzeit mit im Format hhmmss.

<ID der SW-Instanz>
Dies ist die einstellige ID der Software-Instanz, mit der die Nachricht erzeugt wurde (z.B. „A“ für die erste Instanz, „B“ für die zweite Instanz etc.). In diesem Zusammenhang ist mit „SW-Instanz“ das IT-System gemeint, das die Daten für die AM.exchange Schnittstelle aufbereitet. Durch die Verwendung einer eindeutigen ID je IT-System können Kunden, bei denen mehrere IT-Systeme laufen, die AM.exchange Nachrichten mit der Deutschen Post austauschen, dennoch eindeutige Nachrichten-IDs erzeugen. Denn durch die ID der SW-Instanz entsteht je Instanz ein eigener „Nummernkreis“ für die Nachrichten-IDs. Dazu muss jede beim Kunden laufende SW-Instanz eine andere Software-Instanz-ID innerhalb der Nachrichten-ID verwenden.

<fortlaufende Nummer>
Dies ist die 8-stellige, fortlaufende Nummer der Nachricht. Die Nummer soll nicht täglich wieder bei 1 beginnen, sondern immer weiter hochgezählt werden. Um auf acht Stellen zu kommen, sind führende Nullen zu ergänzen.

Zulässig sind alphanumerische Zeichen (Ziffern und Buchstaben).

In jeder Response wird die Nachrichten-ID des zugehörenden Requests von der Schnittstelle zurückgeliefert. Bei der asynchronen Verarbeitung der Responses bzw. Antworten über Dateiaustausch ermöglicht dies eine eindeutige Zuordnung einer Response zum Request. (Neben der Möglichkeit der Zuordnung über die Dateinamen von Request/Response).

5 Produktions- und Abnahmeumgebung

Die Deutsche Post stellt Ihnen zwei Umgebungen bzw. Systeme zur Verfügung, die über die in Kapitel 3.1 beschriebenen technischen Übertragungskanäle erreichbar sind, die „Produktionsumgebung“ und die „Abnahmeumgebung“.

5.1 Produktionsumgebung

Die Produktionsumgebung ist das produktive System der Deutschen Post. Daher dürfen in dieser Umgebung auf keinen Fall Testdaten, sondern nur Echtdaten eingespielt werden.

Bitte beachten Sie:

Die XML-Schemas der Produktionsumgebung unterscheiden sich von denen der Abnahmeumgebung. (Der Unterschied liegt lediglich im Service-Namen, der in den Name-Spaces der XML-Dateien angegeben wird.)

Damit Dateien korrekt in das Produktionssystem laufen, muss das Attribut „testcase“ in den Requests explizit auf den Wert „false“ gesetzt werden.

Informationen zu den verschiedenen Datenübertragungsmöglichkeiten finden Sie in den Kapiteln 3.1 und 6.

5.2 Abnahmeumgebung

Die Abnahmeumgebung wird verwendet, um neue Software-Systeme bzw. Kundensysteme, die erstmals Daten im AM.exchange-Format einliefern, durch einen definierten Abnahmeprozesses zu „verifizieren“ und damit für die Datenkommunikation mit dem Produktionssystem freizugeben.

Auskunft darüber, ob in Ihrem Fall eine Abnahme erforderlich ist, kann Ihnen das IT CSP (s. Anhang J) geben. Beispiele für besondere Fälle, in denen eine Abnahme durch das IT CSP stattfinden muss, sind:

- Softwaresysteme, die von Drittanbietern am Markt angeboten werden, werden in Zusammenarbeit zwischen dem Anbieter und dem IT CSP abgenommen.
- Eigenentwickelte Kundensysteme werden in Zusammenarbeit zwischen dem Kunden und dem IT CSP abgenommen.

Die Service-Operationen in der Abnahmeumgebung und der Produktionsumgebung sind fachlich absolut identisch.

Sie werden jedoch von zwei unterschiedlichen Services („CertificationTrackEventInformation“ bzw. „TrackEventInformation“) angeboten, zu denen auch jeweils unterschiedliche XML-Schemas gehören.

Der kleine Unterschied der XML-Schemas liegt zwar lediglich in den verwendeten Name-Spaces. Daraus folgt aber dennoch, dass eine XML-Datei, die valide gegen das Schema der Abnahmeumgebung ist, nicht gegen das Schema der Produktionsumgebung validiert! Da auf Seiten der Deutschen Post eine Schemaprüfung stattfindet, kann eine Datei, die für die Abnahmeumgebung bestimmt war, daher nie unbeabsichtigt in das Produktionssystem laufen. Achten Sie bei der Entwicklung daher bitte darauf, die jeweils richtigen XML-Schemas für die Produktionsumgebung und die Abnahmeumgebung zu verwenden.

Zur Unterscheidung von „Testdaten“, die nur für das Abnahmesystem bestimmt sind, und „Echtdaten“, die in das Produktionssystem laufen müssen, dient das sog. Testcase-Flag. Ein Datensatz läuft nur fehlerfrei in die Produktionsumgebung, wenn testcase=“false“ explizit gesetzt ist. Umgekehrt läuft ein Datensatz nur dann fehlerfrei in die Abnahmeumgebung, wenn testcase=“true“ im Request gesetzt ist.

5.3 Beantragung des Zugangs zum AM-System

Um den Zugang zur Abnahme- sowie zur Produktionsumgebung der AM.exchange-Schnittstelle zu erhalten, kontaktieren Sie bitte das IT CSP (s. Anhang J).

6 Detailinformationen zu Übertragungskanälen

6.1 Webservice

Wichtiger Hinweis zur Beachtung bei jedem Operationsaufruf via Webservice:

Zum erfolgreichen Aufrufen jeder der hier genannten Service-Operationen muss immer eine gültige AM-Kennung im Datenstrom des Requests übermittelt werden. Dies bedeutet, dass die Felder MsgHeader.User und MsgHeader-Passwort bei jedem Webservice Request mit einer Ihrer gültigen AM Benutzer/Passwort-Kennung belegt sein müssen. Übermitteln Sie im Webservice-Request keine oder eine nicht korrekte AM-Kennung, erhalten Sie die folgende Fehlermeldung:

```
<ErrMsg>
   <ErrDateTime>2007-06-28T08:46:04</ErrDateTime>
   <ErrCat>ERROR</ErrCat>
   <ErrCode>518089</ErrCode>
   <ErrDesc>Die von Ihnen übermittelte Userkennung ist unbekannt
      oder ungültig.
   </ErrDesc>
</ErrMsg>
```

Wichtiger Hinweis zur maximal via Webservice verarbeitbaren Nachrichtengröße:

Bitte beachten Sie, dass der über den Webservice nur Nachrichten bis zu einer maximalen Größe von etwa 3 Megabyte verarbeitet werden können!

Hinweis zur Datenübertragungszeit bei Verwendung des Webservice:

Bei kleiner Nachrichtengröße (gemeint ist eine Größenordnung bis zu 100 KB) und schnellen Internet-Verbindungen werden die Webservice-Request normalerweise innerhalb weniger Sekunden verarbeitet. Für Webservice-Requests mit großer Nachrichtengröße (z.B. 3 MB) können je nach Geschwindigkeit der Datenübertragung jedoch auch durchaus Übertragungszeiten im zweistelligen Minutenbereich auftreten. Bitte ziehen Sie dies bei der Einstellung der Timeout-Zeiten für die Datenübermittlung in Ihrer Software in Betracht.

Datensicherheit

Die Kommunikation via Webservice ist grundsätzlich durch SSL verschlüsselt. Damit können die SOAP-Nachrichten bei der Übertragung über das Internet nicht mitgelesen werden.

Wichtiger Hinweis zur Datensicherheit:

Prüfung des Server-Zertifikates. Bei der Kommunikation Ihres Software-Systems mit dem Webservice der Deutschen Post muss Ihre Software das Server-Zertifikat des Servers der Deutschen Post prüfen. Nur so können Sie sicher sein, mit dem richtigen Deutschen Post-Server zu kommunizieren, und eine sog. „Man-in-the-Middle-Attacke“ verhindern.

Durch eine solche Attacke ist es dem Angreifer im Erfolgsfall möglich, sich in die Datenkommunikation zwischen Ihrem System und dem Server der Deutschen Post einzuklinken und dadurch die übertragenen Daten bei der Nachrichtenübertragung zu lesen und sogar zu ändern. Durch die Prüfung des Server-Zertifikates durch ihre Software wird dies verhindert.

Zur Zertifikatsprüfung durch Ihre Software bieten sich mehrere Alternativen, aus den Sie die für Sie am besten geeignete auswählen können.

Zunächst besteht die Möglichkeit, eine Trust Chain zu einer vertrauten Root Certification Authority (in diesem Fall GlobalSign) aufzubauen. Es können, als eine Variante hierzu, auch die mit der neuesten Version des Internet-Explorer ausgelieferten Root-Zertifikate verwendet werden.

Daneben können vereinfachte Verfahren (wie z.B. Fingerprint) verwendet werden, dann müssen aber alle Clients angepasst werden, wenn das Zertifikat des Servers der Deutschen Post (einmal jährlich) ausgetauscht wird.

Ein Hinweis für Java-Anwendungsentwickler:

Ab Java 1.4.2 ist die "Java Secure Socket Extension" (JSSE) enthalten. Diese kann z.B. für die Handhabung von SSL-Verbindungen verwendet werden. In JSSE wird auch die Verwaltung von TRUST-Chains behandelt. Offenbar gibt es sowohl eine einfache Standardimplementierung von SUN als auch die Möglichkeit diese Schnittstelle selbst zu implementieren.

Links zu JSSE:

- https://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/JSSERefGuide.html

Weiterhin hilfreich ist das Verständnis zum Java Keytool. Mit dem Keytool können Sie Zertifikate auf eine sichere Art und Weise verwalten.

- https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html

Dateinamen

Da beim Webservice keine Dateien, sondern Requests über das SOAP-Protokoll versendet werden, spielen Dateinamen hierbei keine Rolle.

Aufruf

Der Aufruf einer Webservice-Operation wird eingeleitet mit der SOAP-URL sowie der SOAP-Action, die sich nach der gewünschten Serviceoperation richtet.

Die **SOAP-URL** ist eine https-basierende URL, die Sie bei Aufnahme Ihres Entwicklungsprojekts vom IT CSP-Team erhalten.

Die **SOAP-Action** hat folgendes, syntaktisches Muster:

„TrackEventInformation/TrackEventInformation/[VERSION]#[OPERATION]“

VERSION: entspricht der betriebenen TrackEventInformation-Version, aktuell „1.1“

OPERATION: Basisname der Serviceoperation, z.B. „getTrackEvents“

Beispiel: *„TrackEventInformation/TrackEventInformation/1.1#getTrackEvents“*

WSDL-Dateien

Die WSDL-Dateien für den Service TrackEventInformation 1.1 finden Sie in den Anhängen zu diesem Handbuch. Diese enthalten die wesentlichen Informationen, die Sie zur Kommunikation via Webservice benötigen. Bitte beachten Sie, dass diese kein „Binding“ an die tatsächliche Zieladresse des Services (sondern nur ein Localhost-Binding) und keine Angaben zum benötigten WS-Security-SOAP-Header (siehe nachfolgender Hinweis) enthalten. Sollten Sie die WSDL-Datei zur automatischen Generierung einer Anbindung an den Service verwenden wollen, müssen diese Angaben ergänzt werden.

Bitte beachten Sie:

Mit jedem Request muss ein Benutzer/Passwort-Token im SOAP-Envelope mitgeschickt werden. Ihr Benutzer/Passwort-Token erhalten Sie vom IT CSP. Das mit dem Handbuch ausgelieferte Beispiel zeigt, wie Sie das Token im SOAP-Envelope einbinden müssen:

WebService\SOAP-Envelope-Beispiel\SOAP_Envelope_Beispiel.txt

Java-Beispielcode

Das mit diesem Handbuch ausgelieferte Java-Beispiel zeigt, wie ein SOAP-Request an die Webservice-Schnittstelle versendet werden kann.

Webservice\Java-Beispiel\WSGUploaderTrackEventInformation.java

6.1.1 Zugang zum AM-Produktivsystem via Webservice

- Basis-URL des Webservice und ggf die TCP/IP-Adresse
- Benutzer/Passwort-Token im SOAP-Envelope (WS-Security)
- Benutzer/Passwort im MsgHeader

erfragen Sie bitte beim IT CSP (s. Anhang J)

6.1.2 Zugang zum AM-Abnahmesystem via Webservice

- Basis-URL des Webservice und ggf die TCP/IP-Adresse
- Benutzer/Passwort-Token im SOAP-Envelope (WS-Security)
- Benutzer/Passwort im MsgHeader

erfragen Sie bitte beim IT CSP (s. Anhang J)

Bitte beachten Sie:

Bei der Webservice Kommunikation wird der Port 443 verwendet. Als Protokoll wird SOAP über https verwendet. Bei der Konfiguration Ihrer Netzwerkinfrastruktur sind daher insbesondere folgende Punkte zum erfolgreichen Aufrufen des Webservice zu konfigurieren:

- ein evtl. vorhandener Proxy
- ein Port für diesen Proxy

- Firewall-Einstellungen zur Kommunikation mittels SOAP via https über Port 443

Bitte stellen Sie bei der Implementierung Ihrer Software zudem sicher, dass der Datenstrom, der über die Webservice Schnittstelle läuft (Request und Response), bei Bedarf über die Einstellung eines entsprechenden Konfigurationsschalters in einer Datei protokolliert werden kann. Dies erleichtert die Abnahme und ggf. die Fehleranalyse im Produktivbetrieb.

6.2 Secure File Transfer Protocol (SFTP)

Datensicherheit

Im wesentlichen Unterschied zur FTP-Kommunikation werden bei SFTP sowohl die Anmelde- als auch die Nutzdaten bei der Datenübertragung verschlüsselt.

Client-Software

Zur Kommunikation über SFTP benötigen Sie einen entsprechenden SFTP-Client wie z.B. FileZilla oder WinSCP bzw. eine Software-Bibliothek, die Sie in Ihre Anwendung einbinden wie z. B. Apache Commons VFS™ für Java.

Dateinamen

Die Einlieferung von Dateien via SFTP unterliegt Namenskonventionen, die für die korrekte Verarbeitung der Dateien unbedingt einzuhalten sind. Zudem ist zusätzlich zur eigentlichen zu verarbeitenden Datei bzw. Request eine so genannte Triggerdatei erforderlich, um die Verarbeitung der Requestdatei anzustoßen. Diese ist leer, d.h. 0-Byte groß.

Gehen Sie daher bitte wie folgt vor:

- Request vollständig hochladen
- Danach die Trigger-Datei für diesen Request hochladen

Namenskonvention für Requests:

- Präfix „TEI_“ +
- 10-stellige EKP des Dateneinlieferers +
- ein Unterstrich („_“) als Trennzeichen +
- Tagesdatum der Datei im Format „YYYYMMDD“ +
- ein Unterstrich („_“) als Trennzeichen +
- Uhrzeit der Datei im Format „HHMMSS“ +
- ein Unterstrich („_“) als Trennzeichen +
- eine maximal 15-stellige, eindeutige Job-Nr. (ggf. auch alphanumerisch) +
- die Dateierweiterung „.xml“

Der Name der Trigger-Datei entspricht exakt dem Namen der Requestdatei inkl. Extension, erweitert um den Suffix „.ok“.

Hier ein Beispiel für korrekte Dateinamen von Request- und Triggerdatei:

- TEI_6000000121_20060425_235856_123456789012abc.xml
  TEI_6000000121_20060425_235856_123456789012abc.xml.ok

Bereitstellung von Responses

Die Responses werden im entsprechenden Verzeichnis (prod/out) unter dem Dateinamen des Requests abgelegt.

Verzeichnisse

Damit die Requestdateien verarbeitet werden, müssen Requestdatei und danach die Triggerdatei im Verzeichnis „prod/in“ abgelegt werden.

Nach Weiterleitung des Requests an das AM-System wird die Requestdatei gelöscht.

Nach Verarbeitung Ihres Requests wird die entsprechende Response im Verzeichnis „prod/out“ abgelegt. Bitte löschen Sie unbedingt die Responses, wenn Sie diese aus Ihrem SFTP-Account abgeholt haben.

Speicherplatz

Der Ihnen per Default zur Verfügung stehende Speicherplatz ihres SFTP-Accounts beträgt 20 Megabyte (für Requests und Responses). Wenn Sie mehr Speicherplatz benötigen, teilen Sie dies bitte dem IT CSP im Rahmen der Beantragung Ihres Accounts mit.

Per Default werden Dateien, die älter als 10 Tage sind, aus dem prod/out Verzeichnis Ihres Accounts gelöscht. Wenn Ihr Account seine maximale Größe erreicht hat, werden zunächst die ältesten Dateien aus dem prod/out Verzeichnis entfernt.

Durchlaufzeit von Requests

Die Durchlaufzeit zur Request-Verarbeitung sollte **maximal eine Stunde** betragen. Bitte kontaktieren Sie das IT CSP, wenn diese Zeit nicht eingehalten wird.

Bitte beachten Sie:
Bitte überprüfen Sie nach jeder Datenübertragung zeitnah Ihre LOG-Protokolle auf Übermittlungsfehler und Abbrüche, um die in diesem Fall erforderliche Datennachlieferung unmittelbar anstoßen zu können.

Sonstiges

Bei der Dateneinlieferung via SFTP dürfen die Kommentare in den XML-Dateien maximal 250 Zeichen enthalten.

7 Verschiedenes

7.1 Die Bedeutung der Service-Versionen

Der TrackEventInformationService der Deutschen Post stellt Ihnen die im Abschnitt 3 im Detail erläuterten Service-Operationen bereit.

Um neue Funktionalitäten bereit zu stellen, werden von Zeit zu Zeit neue Service-Versionen und neue XML-Schemata definiert. Dabei wird darauf geachtet, dass die Schemata nur erweitert werden. D.h. in einer neuen Schema-Version kommen nur neue Datenfelder hinzu und es werden keine Datenfelder aus dem Schema entfernt.

Bei der Definition einer neuen Serviceversion wird entschieden, ob ggf. Vorgängerversionen zeitgleich abgeschaltet werden. In diesem Fall werden Sie von Ihrem Ansprechpartner beim IT CSP informiert und bezüglich der Migration auf die neue Serviceversion beraten.

Ein Aufruf einer Service-Operation mit einer bestimmten Service-Version X wird immer mit einer Response in derselben Service-Version X von der AM.exchange-Schnittstelle beantwortet. Eine volle Abwärtskompatibilität ist somit gegeben.

Anhang A- Glossar

Begriff	Erklärung
Absender	Der als Absender einer Sendung auftretende Geschäftspartner und damit der Auftraggeber der Deutschen Post.
AM.exchange	B2B-Protokoll der Deutschen Post zum elektronischen Datenaustausch der Kunden mit der Deutschen Post.
AM-System (AM)	Auftragsmanagement System: IT-System der Deutschen Post in der alle auftragsbezogenen verwaltet und verarbeitet werden
AM-XML	AM.exchange Datenformat, das auf dem XML Standard basiert.
Asynchrone Kommunikation	Unter asynchroner Kommunikation versteht man einen Modus der Kommunikation, bei dem das Senden und Empfangen von Daten zeitlich versetzt und ohne Blockieren des Prozesses durch bspw. Warten auf die Antwort des Empfängers (wie bei synchroner Kommunikation der Fall) stattfindet. Im AM.exchange-Kontext erfolgt die asynchrone Kommunikation durch die Übermittlung von Dateien. Auf Grund der damit verbundenen Übermittlungs- und Verarbeitungszeiten ist keine echte „Unterhaltung“ der beteiligten Systeme möglich. Es kann vielmehr erst nach einer gewissen Zeitdauer das Ergebnis einer Aktion (z.B. das Ergebnis der Prüfung eines übermittelten Auftrags) ausgewertet werden.
B2B	Business-to-Business: Nachrichtenaustausch zwischen zwei Geschäftpartner mit dem Ziel durch verbesserten Informationsfluss Geschäftsprozesse bei beiden Partnern zu optimieren.
Codetable	Die Codetable ist das Verzeichnis gültiger Werte für die verschiedenen im AM.exchange-Protokoll verwendeten Listen (z.B. Produkte, Produktionsstätten etc.) und somit Bestandteil des AM.exchange-Protokolls.
Data Matrix Code	Zweidimensionaler „Barcode“, in dem Informationen zu den Sendungen codiert und auf der Sendung bzw. deren Umhüllung aufgebracht werden können.
IT CSP	IT Customer Support Post: Organisationseinheit der Deutschen Post mit Sitz in Darmstadt, die für die fachliche Betreuung der AM.exchange-Schnittstelle im Unternehmensbereich P&P zuständig ist.
EKP	Eindeutige Kundennummer
Request	Anfrage-Nachricht: Nachricht des Kunden an die Deutsche Post.
Response	Antwort-Nachricht: Nachricht der Deutschen Post an den Kunden.
Sektion	Gliederung der AM.exchange-Nachricht.
Service	Im Rahmen einer Service Orientierten Architektur (SOA) stellt ein Service Geber im Rahmen eines Services eine Menge wohl definierter Funktionen (Service Operationen) zur Verfügung. Service Nehmer können diese Funktionen nutzen.
Serviceoperation	Eine einzelne Funktion, die durch einen Service zur Verfügung gestellt wird.
SFTP	Secure File Transfer Protocol. Auf SSH basierendes Dateiübertragungsprotokoll, das eine Verschlüsselung der kompletten Übertragung ermöglicht.
SOAP	Ein XML-basiertes Netzwerkprotokoll, mit dessen Hilfe Daten zwischen Systemen ausgetauscht werden können. SOAP ist ein industrieller Standard des World Wide Web Consortiums (W3C).
Synchrone Kommunikation	Unter synchroner Kommunikation versteht man einen Modus der Kommunikation, bei dem sich die Kommunikationspartner (Prozesse) beim Senden oder beim Empfangen von Daten immer synchronisieren, also warten (blockiert), bis die Kommunikation abgeschlossen ist. Im AM.exchange-Kontext erfolgt die synchrone Kommunikation über Webservices. I.d.F. erhält der Übermittler einer Nachricht sehr zeitnah die Rückmeldung des Auftragsmanagements und kann diese direkt in seinen Verarbeitungsprozess integrieren.
Übertragungskanal	Technischer Weg um eine AM.exchange-Nachricht vom Kunden zur Deutschen Post zu transferieren.

Begriff	Erklärung
Verschlüsselung	Technische Methode zur Sicherung von Daten gegen unbefugten Zugriff
Webservice	Eine Softwareanwendung, die über ein Netzwerk für die direkte Maschine-zu-Maschine-Interaktion bereitgestellt wird.
WSDL	Web Services Description Language. Eine Beschreibungssprache für Webservices zum Austausch von Nachrichten auf Basis von XML. WSDL ist ein industrieller Standard des World Wide Web Consortiums (W3C).

Anhang B – XML-Schemas

Schemas für das Produktivsystem

XML-Schemas\V1.1\Produktion\getTrackEventsRequest.xsd

XML-Schemas\V1.1\Produktion\getTrackEventsResponse.xsd

XML-Schemas\V1.1\Produktion\tecommon.xsd

XML-Schemas\V1.1\Produktion\errorHandling.xsd

Schemas für das Abnahmesystem

XML-Schemas\V1.1\Abnahme\getTrackEventsRequest.xsd

XML-Schemas\V1.1\Abnahme\getTrackEventsResponse.xsd

XML-Schemas\V1.1\Produktion\tecommon.xsd

XML-Schemas\V1.1\Produktion\errorHandling.xsd

Anhang C - XML-Schema Dokumentation (PDF)

In diesem Anhang finden Sie Hyperlinks zu der mit diesem Handbuch ausgelieferten Dokumentation für die XML Schema-Dateien im PDF-Format.

Die Strukturdiagramme geben eine Übersicht über die Struktur der XML-Schemas, die Guidelines enthalten detaillierte Informationen zu allen Elementen und Attributen.

Strukturdiagramme

PDF\AM.exchange-TrackEventInformation-getTrackEventsRequest Struktur.pdf

PDF\AM.exchange-TrackEventInformation-getTrackEventsResponse Struktur.pdf

Guidelines

PDF\AM.exchange-TrackEventInformation-getTrackEventsRequest Guide.pdf

PDF\AM.exchange-TrackEventInformation-getTrackEventsResponse Guide.pdf

Anhang D- XML-Schema Doku (HTML)

In diesem Anhang finden Sie Hyperlinks zu der mit diesem Handbuch ausgelieferten Dokumentation für die XML Schema-Dateien im HTML-Format.

Die Strukturdiagramme geben eine Übersicht über die Struktur der XML-Schemas, die Guidelines enthalten detaillierte Informationen zu allen Elementen und Attributen.

Strukturdiagramme

HTML\AM.exchange-TrackEventInformation-getTrackEventsRequest Struktur.html

HTML\AM.exchange-TrackEventInformation-getTrackEventsResponse Struktur.html

Guidelines

HTML\AM.exchange-TrackEventInformation-getTrackEventsRequest Guide.html

HTML\AM.exchange-TrackEventInformation-getTrackEventsResponse Guide.html

Anhang E - WSDL-Dateien

WSDL-Dateien für das Produktivsystem

XML-Schemas\V1.1\Produktion\TrackEventInformation_11.wsdl

WSDL-Dateien für das Abnahmesystem

XML-Schemas\V1.1\Abnahme\CertificationTrackEventInformation_11.wsdl

Anhang F- Beispieldateien

In dem Dokument AM.exchange-TrackEventInformation-Beispielübersicht.pdf finden Sie einige typische Anwendungsfälle mit Links zu den zum Beispiel gehörenden Dateien.

Anhang G - Codetables

Hier finden Sie folgende Schlüsseltabellen:

- **Allgemeine Code-Tabelle TrackEventInformationService**
  Die allgemeine Schlüsseltabelle enthält alle im AM.exchange Protokoll für den TrackEventInformationService verwendeten Codes. Zur einfachen elektronischen Verarbeitung der enthaltenen Werte wird Ihnen diese Tabelle in den Formaten PDF und XML bereitgestellt.

  Codetables\AM.exchange-TrackEventInformation-Codetable.pdf

  Codetables\AM.exchange-TrackEventInformation-Codetable.xml
- **Spezielle Code-Tabelle für Process.type = TNT_LETTER_***

  Codetables\AM.exchange-TrackEventInformation-Codetable - TNT_LETTER.pdf

  Codetables\AM.exchange-TrackEventInformation-Codetable - TNT_LETTER.xml
-
- **Spezielle Code-Tabelle für Process.type = LETTER_INTERNATIONAL**

  Codetables\AM.exchange-TrackEventInformation-Codetable - LETTER_INTERNATIONAL.pdf

  Codetables\AM.exchange-TrackEventInformation-Codetable - LETTER_INTERNATIONAL.xml
- **Spezielle Code-Tabell für Process.type = PROOF_OF_DELIVERY***

  Codetables\AM.exchange-TrackEventInformation-Codetable - PROOF_OF_DELIVERY -.pdf

  Codetables\AM.exchange-TrackEventInformation-Codetable - PROOF_OF_DELIVERY - .xml

Anhang H- Fehlercodes und Fehlermeldungen

Diese Tabelle enthält die für den TrackEventInformationService relevanten AM.exchange Fehlercodes und Fehlermeldungen.

Meldungstexte\AM.exchange-TrackEventInformation-Meldungstexte.pdf

Anhang I- Leistungsmatrix TrackeventInformationService

In diesem Angang wird zusammengestellt, welche Prozesstypen für den Abruf der Trackevents welcher Produkte in Abhängigkeit der Freimachungsart verwendet werden können.

Leistungsmatrix_TEI_Service.pdf

Anhang J – Ansprechpartner bei der Deutschen Post

Ihr Ansprechpartner zu allen Themen rund um AM.exchange und AM.portal ist der **IT Customer Support Post (IT CSP)**.

Die Geschäftszeiten sind:

Montag bis Donnerstag von 08:00 bis 17:00 Uhr und Freitag von 08:00 bis 16:00 Uhr

Telefon: 06151 908 8000

Fax: 06151 908 8001

Email: IT-CSP@deutschepost.de

Anschrift:

Deutsche Post AG
SNL IT Post & Paket Deutschland
Abt. 1510 Kundenintegration Post
IT Customer Support Post (IT CSP)
64276 Darmstadt
Deutschland

Anhang K – Änderungshistorie

Dieser Anhang listet kurz die wesentlichen Änderungen für die verschiedenen Handbuchversionen auf. Die letzten Änderungen finden Sie am Anfang dieses Anhangs, die Änderungen in den älteren Handbüchern stehen weiter hinten.

Änderungen in der Handbuchversion 1.1.4

Neue Version des Entwicklerhandbuches für die Service-Version 1.1. Im Entwicklerhandbuch wurden dazu die folgenden Kapitel angepasst

- Einfügen von Bedingungen für die Nutzung des TrackeventInformationServices
- Entfernen von Track&Match (Beschreibung, Codetables und Beispiele)
- Diverse kleine textuelle Anpassungen in allen Kapiteln
- Anhang I Leistungsmatrix TrackeventInformationService

Änderungen in der Handbuchversion 1.1.3

Neue Version des Entwicklerhandbuches für die Service-Version 1.1. Im Entwicklerhandbuch wurden dazu die folgenden Kapitel angepasst:

- Ergänzung Kap. 3.2 PROOF_OF_DELIVERY um Warenpost (die Ausführungen zum PROOF_OF_DELIVERY gelten auch für Warenpost ab 01.01.2018)
- Anhang G – Codetables

Ergänzung Codetable für PROOF_OF_DELIVERY um 2 neue Status

Änderungen in der Handbuchversion 1.1.2

Neue Version des Entwicklerhandbuches für die Service-Version 1.1. Im Entwicklerhandbuch wurden dazu die folgenden Kapitel angepasst:

- Kap. 3.2 TrackEventFilter: Zusätzlicher Process.typen TRACK_AND_MATCH_IP_CREATION_DATE, PROOF_OF_DELIVERY und PROOF_OF_DELIVERY_CREATION_DATE
- Anhang C und D

Erweiterung der Dokumentation um TRACK_AND_MATCH_IP_CREATION_DATE, PROOF_OF_DELIVERY und PROOF_OF_DELIVERY_CREATION_DATE

- Anhang F – Beispieldateien

neue Beispiele 12 bis 14 für TRACK_AND_MATCH_IP_CREATION_DATE sowie 15 bis 19 für PROOF_OF_DELIVERY

- Anhang G – Codetables

Ergänzung Codetable für Track&Match und PROOF_OF_DELIVERY

Änderungen in der Handbuchversion 1.1.1

Neue Version des Entwicklerhandbuches für die Service-Version 1.1. Im Entwicklerhandbuch wurden dazu die folgenden Kapitel angepasst:

- Kap. 3.2 TrackEventFilter: Zusätzlicher Process.type LETTER_INTERNATIONAL
- Anhang C und D
  Erweiterung der Dokumentation um LETTER_INTERNATIONAL
- Anhang F – Beispieldateien

  neue Beispiele 8 bis 11 für LETTER_INTERNATIONAL
- Anhang G – Codetables

  neue spezielle Codetabellen
- Anhang H
  neue Meldungstexte

Änderungen in der Handbuchversion 1.1

Neue Version des Entwicklerhandbuches für die Service-Version 1.1. Im Entwicklerhandbuch wurden dazu die folgenden Kapitel angepasst:

- Kap. 4.2 TrackEventFilter: Zusätzlicher Process.type TRACK_AND_MATCH_IP
- Kap. 7.1 Die Bedeutung der Service-Versionen: Abschaltung von Version 1.0 beschrieben
- Anhang B – XML-Schemas
- Anhang E – WSDL-Dateien
- Anhang F – Beispieldateien
  neue Beispiele 5 bis 7 für TRACK_AND_MATCH_IP
- Anhang G – Codetables
  neue spezielle Codetabellen

Änderungen in der Handbuchversion 1.0

Initiale Erstellung.