e-GOVERNMENT BUND-LÄNDER-GEMEINDEN
http://reference.e-government.gv.at

Elektronische Zustellung – Nachweisliche Zusendung im Auftrag von Privaten	Konvention zusepriv-1.3.1 Entwurf Intern

Kurzbeschreibung	Dieses Dokument spezifiziert die Änderungen der einzelnen Komponenten der behördlichen Zustellinfrastruktur, welche sich durch die Einführung der nachweislichen Zusendung von Dokumenten im Auftrag von Privaten ergeben.	
Autor(en):	Arne Tauber Thomas Rössler Peter Reichstädter	Projektteam / Arbeitsgruppe AG-II / PG ZUSE
Beiträge von:		

Version	1.3.0	:	**23.02.2009**	Fristablauf:	**23.02.2009**
Detail-Version	1.3.1	:	**09.09.2009**	Freigabe:	**09.09.2009**

Inhaltsverzeichnis:

Abbildungen 3
Revision History 4
1 Einleitung 5
1.1 Schlüsselwörter 5
1.2 Geschlechtsspezifische Bezeichnungen 5
2 Rechtliche Rahmenbedingungen 6
3 Voraussetzungen 7
3.1 Zustimmung zur Annahme von private Zusendungen 7
3.2 Explizit gekennzeichnete private Ermittlungsleistung 7
4 Prozess 8
4.1 Zustellkopf 8
4.1.1 Registrierung als authorisierter Versender 8
4.1.2 Authentifizierung 8
4.1.3 LDAP Verzeichnisstruktur 8
4.1.4 Gekennzeichnete Ermittlungsleistung 9
4.1.5 Abfragesyntax 10
4.1.6 Antwortsyntax 12
4.1.7 Vorschrift zur Bildung der edID in der Zustellkopfantwort 14
4.2 Zustellserver 15
4.2.1 Annahme von Zustellstücken 15
4.2.2 Benutzerschnittstelle 18
4.2.3 Verrechnung 19
5 Referenzen 20

Abbildungen

Abb. 4.1 XML Schema der Bulk Anfrage an den Zustellkopf (privat) 11
Abb. 4.2 XML Schema der Antwort auf Einzelanfrage des Zustellkopfs (privat) 12
Abb. 4.3 XML-Schema der Bulk Antwort (privat) 13
Abb. 4.4 XML-Schema der DeliveryRequest Nachricht für eine private Zusendung 16

Revision History

Version	Datum	Autor(en)	
0.0.1	25.11.2008	Arne Tauber (EGIZ)	Initialversion
0.0.2	02.12.2008	Arne Tauber (EGIZ)	Änderungen B.Karning
0.0.3	16.12.2008	Arne Tauber (EGIZ)	Zustellqualitäten Zeitpunkt edID Token Dokumentenklasse global
1.3.0	13.01.2009	Arne Tauber (EGIZ) Thomas Rössler (EGIZ)	gvZbPK für Behörden Token-Frist auf 48h editorielle Korrekturen
1.3.1	04.09.2009	Arne Tauber (EGIZ)	4.2.1.3 Zustellqualität mit behördlichen Zustellqualitäten harmonisiert Editorelle Korrekturen (Anmerkung 4.1.5)

1 Einleitung

In privatwirtschaftlichen Geschäftsprozessen ist die nachweisliche Zusendung von Dokumenten seit je her ein kosten- und ressourcenintensiver Vorgang. Besonders in ihrer konventionellen Ausprägung, nämlich in Form eines eingeschriebenen Briefes, ist eine nachweisliche Zusendung sowohl aus der Perspektive der manuellen Vorbereitung und Bearbeitung, als auch aus Sicht des Entgelts für das Produkt "Einschreiben" selbst, mit erheblichen Kosten für den Versender und in vielen Fällen mit einem einhergehenden Medienbruch verbunden.

Sucht man nach zeitgemäßen Alternativen unter Einbeziehung der IK-Technologien, so sind heute etablierte Standards wie die E-Mail zwar als solches kostengünstiger im Vergleich zur konventionellen Alternative (Brief), jedoch in ihrer Qualität mit den Anforderungen einer nachweislichen Zusendung keinesfalls vergleichbar. Im Bereich des E-Government wurde daher schon die adäquate technische Lösung einer rechtsverbindlichen und qualitätsvollen Zustellung geschaffen - die elektronische Zustellung - die vor allem aus Sicht des Senders eine Erleichterung, medienbruchfreie Geschäftsprozesse und erhebliche Aufwands- und Kostenreduktionen mit sich bringt.

Das Zustellgesetz ermöglicht zugelassenen Zustelldiensten auch nachweisliche Zusendungen von Dokumenten im Auftrag von Privaten vorzunehmen und schafft die Voraussetzungen, dass für diesen Zweck auch das System der elektronischen Zustellung einschließlich der "Zustellkopfabfrage" verwendet werden kann.

Dieses Dokument spezifiziert die Änderungen der einzelnen Komponenten der behördlichen Zustellinfrastruktur, welche sich durch die Einführung der nachweislichen Zusendung von Dokumenten im Auftrag von Privaten ergeben.

1.1 Schlüsselwörter

Dieses Dokument verwendet die Schlüsselwörter MUSS, DARF NICHT, erforderlich, sollte, sollte nicht, empfohlen, darf, und optional zur Kategorisierung der Anforderungen. Diese Schlüsselwörter sind analog zu ihren englischsprachigen Entsprechungen must, must not, required, should, should not, recommended, may, und optional zu handhaben, deren Interpretation in [KEYWORDS] festgelegt ist.

1.2 Geschlechtsspezifische Bezeichnungen

Alle Personenbezeichnungen, die in diesem Dokument in der männlichen Form verwendet werden, gelten sinngemäß auch für die weibliche Form.

2 Rechtliche Rahmenbedingungen

Das österreichische Zustellgesetz (ZustG) - zuletzt geändert mit dem Verwaltungsverfahrens- und Zustellrechtsänderungsgesetz 2007 - siehe [ZUSTG] - definiert, dass ein behördlich zugelassener Zustelldienst auch weitere Leistungen, wie die nachweisliche Zusendung von Dokumenten im Auftrag von Privaten erbringen kann.

§ 29. *(3) Zustelldienste können weitere Leistungen, wie insbesondere die nachweisliche Zusendung von Dokumenten im Auftrag von Privaten, entgeltlich anbieten. Für die nachweisliche Zusendung von Dokumenten im Auftrag von Privaten hat der Ermittlungs- und Zustelldienst die Ermittlungsleistung (Abs. 2 Z 2) zu denselben Bedingungen wie bei der Zustellung behördlicher Dokumente zu erbringen.*

§ 34. *(2) Eine Abfrage zur Ermittlung der in Abs. 1 angeführten Daten darf nur auf Grund eines Auftrags einer Behörde nach Abs. 1 oder zum Zweck der nachweislichen Zusendung von Dokumenten im Auftrag von Privaten (§ 29 Abs. 3) vorgenommen werden. Als Suchkriterien dürfen nur die Daten gemäß § 33 Abs. 1 Z 1 bis 5 verwendet werden.*

§ 34 Abs. 2 ZustG definiert genau die Suchkriterien, welche bei einer Abfrage am Zustellkopf (Ermittlungs- und Zustelldienst / Ermittlungsleistung) verwendet werden dürfen. Diese sind wie folgt in § 33 Abs. 1 Z 1 bis 5 definiert:

§ 33. *(1) Die Anmeldung bei einem Zustelldienst kann nur unter Verwendung der Bürgerkarte (§ 2 Z 10 E-GovG) erfolgen. Jeder Zustelldienst hat im Internet ein elektronisches Verfahren für die Anmeldung bereitzustellen. Bei der Anmeldung sind folgende Daten zu speichern:*

1. *Name bzw. Bezeichnung des Kunden,*
2. *bei natürlichen Personen das Geburtsdatum,*
3. *die zur eindeutigen Identifikation des Kunden im Bereich „Zustellwesen“ erforderlichen Daten:*
    a. *bei natürlichen Personen das bereichsspezifische Personenkennzeichen (§ 9 E-GovG),*
    b. *sonst die Stammzahl (§ 6 E-GovG),*
4. *eine elektronische Adresse, an die die Verständigungen gemäß § 35 Abs. 1 und 2 erster Satz übermittelt werden können,*
5. *gegebenenfalls eine inländische Abgabestelle, an die die Verständigungen gemäß § 35 Abs. 2 übermittelt werden können,*

Wird eine Ermittlungsleistung für eine nachweisliche Zusendung im Auftrag von Privaten durchgeführt, so DARF das in § 33 Abs. 1 Z 3 lit. a angegebene bereichsspezifische Personenkennzeichen (§ 9 E-GovG) für natürliche Personen zur Abfrage verwendet werden. Dies setzt klarerweise voraus, dass es sich beim Absender um eine Behörde handelt, da ein privates Unternehmen nicht das Zustell-bPK des Empfängers besitzen darf.

Zur Abfrage können somit folgende Suchkriterien herangezogen werden:

1. Zustell-bPK, falls es sich beim Absender um eine Behörde handelt
2. Vorname, Familienname und Geburtsdatum bei natürlichen Personen
3. Bezeichnung des Kunden bzw. Stammzahl (Firmenbuchnummer, Vereinsnummer) bei juristischen Personen
4. Verständigungsadresse (z.B. E-mail oder Telefonnummer)
5. Abgabestelle

3 Voraussetzungen

3.1 Zustimmung zur Annahme von private Zusendungen

Das Zustellgesetz regelt behördliche Zustellungen. Im Fall der elektronischen Zustellung kann ein Zustellserver die zusätzliche Leistung der nachweislichen Zusendung im Auftrag von Privaten gemäß § 29 Abs. 3 ZustG als Option anbieten. Es macht somit Sinn, eine Trennung dieser beiden Leistungen auf organisatorischer und technischer Ebene zu bewerkstelligen.

Im zentralen Zustellkopf ist daher für jeden registrierten Empfänger ein verpflichtendes Kennzeichen für die Zustimmung zur Annahme von nachweislichen Zusendungen im Auftrag von Privaten vorgesehen. Dies impliziert die Existenz eines Pendants dieses Kennzeichens auf Seite eines jeden Zustellservers.

3.2 Explizit gekennzeichnete private Ermittlungsleistung

Wie in Abschnitt 3.1 beschrieben, führt der zentrale Zustellkopf ein verpflichtendes Kennzeichen für die Zustimmung des Empfängers zur Annahme von nachweislichen Zusendungen im Auftrag von Privaten.

Um nun eine Auskunft im Sinne einer nachweislichen Zusendung im Auftrag von Privaten am Zustellkopf zu erkennen und somit eine Suche gemäß der mitgeführten Kriterien und des Kennzeichens für die Zustimmung seitens des Empfängers durchführen zu können, MUSS diese Auskunft explizit gekennzeichnet sein.

Die Kennzeichnung einer solchen Auskunft basiert teilweise auf dem verwendeten Transportprotokoll mittels SSL-Client-Authentifizierung, als auch auf eine explizite Angabe innerhalb des Kommunikationsprotokolls. Dadurch kann sichergestellt werden, dass auch ein als Behörde oder Dienstleister authentifizierter Versender eine nachweisliche Zusendung im Auftrag von Privaten durchführen kann.

4 Prozess

Die nachweisliche Zusendung im Auftrag von Privaten bringt - basierend auf den rechlichten Grundlagen (siehe Abschnitt 2) und den Voraussetzungen (siehe Abschnitt 3) - einige grundlegende Modifikationen der Komponenten der behördlichen Zustellinfrastruktur mit sich. Dieser Abschnitt beschreibt ausführlich die notwendigen Änderungen gegliedert nach den einzelnen Komponenten der behördlichen Zustellinfrastruktur.

4.1 Zustellkopf

4.1.1 Registrierung als authorisierter Versender

Die Prozedur und Modalitäten der Registrierung als authorisierter Versender wird aktuell auf den Informationsseiten des Zustellkopfs publiziert.

4.1.2 Authentifizierung

Die Spezifikation der behördlichen elektronischen Zustellung sieht ausschließlich eine Authentifizierung am Zustellkopf mittels SSL-Client-Zertifikat vor, welches eine Verwaltungs- oder Dienstleistereigenschaft besitzen MUSS (siehe [ZUSEKOPF][CERTOID]).

Die nachweisliche Zusendung im Auftrag von Privaten erfordert nunmehr auch das Zulassen von SSL-Client-Zertifikaten, welche nicht eine Verwaltungs- oder Dienstleistereigenschaft besitzen. Eine Aufstellung der akzeptierten Zertifizierungsdiensteanbieter wird in regelmäßigen Abständen auf den Informationsseiten des zentralen Zustellkopfs publiziert. Ausgestellte Zertifikate genau jener Zertifizierungsdiensteanbieter müssen von behördlich zugelassenen Zustelldiensten[1] zur Übermittlung von Zustellstücken akzeptiert werden.

Darüber hinaus ist es dem Zustellkopf überlassen, eine eigene Certification Authority (CA) zu betreiben und Zertifikate im Rahmen einer Registrierung als Absender am Zustellkopf auszustellen. In diesem Fall müssen behördlich zugelassene Zustelldienste[1] ebenfalls genau jene Zertifikate zur Übermittlung von Zustellstücken seitens der Absender akzeptieren, falls sie die Zusendung von privaten Schriftstücken als Option vorsehen.

4.1.3 LDAP Verzeichnisstruktur

Die Struktur des Directory Information Trees (DIT) des Verzeichnisses des zentralen Zustellkopfs bleibt durch die Integration der nachweislichen Zusendung im Auftrag von Privaten unberührt.

Im Rahmen der Spezifikation 1.3.1 der behördlichen Zustellung (Elektronische Zustellung – LDAP Schemabeschreibung – siehe [ZUSELDAP]) wurde das LDAP Attribut *gvAcceptPrivate* eingeführt im Sinne eines Kennzeichens für die explizite Zustimmung zur Annahme von privaten Schriftstücken seitens des Empfängers.

Für natürliche Personen MUSS im Rahmen einer privaten Abfrage das LDAP Attribut *gvZbPK* ignoriert werden falls es sich nicht um eine Behörde handelt. Im Falle der Zustimmung zur Annahme von privaten Zusendungen ist zusätzlich zum LDAP Attribut *gvAcceptPrivate* das Attribut *edID* (electronic delivery ID) in das zentrale Verzeichnis einzutragen.

Die *edID*, welche seitens des Zustellservers erzeugt wird, MUSS eine Eindeutigkeit über die gesamte Zustellinfrastruktur garantieren. Daher MUSS folgende Berechnungsvorschrift für die Erzeugung der *edID* eingehalten werden:

[1] http://www.bka.gv.at/zustelldienste

1. Basis der Berechnungsvorschrift ist das bPK des Zustellservers für die Verwendung im privaten Bereich (im Weiteren als wbPK bezeichnet – siehe [SZ-bPK-Algo V1.1.1]). Das wbPK steht dem Zustellserver jedenfalls zur Verfügung, nachdem an jedem behördlich zugelassenen Zustelldienst ein Empfängerkonto ausschließlich mit einer Bürgerkarte[2] eröffnet werden kann.

   Zu welchem Zeitpunkt der Zustellserver die Ermittlung der wbPK über die Bürgerkarte des Empfängers durchführt (Registrierung, explizite Zustimmung zur Akzeptanz von privaten Schriftstücken, etc.) ist nicht Gegenstand dieser Spezifikation.

2. Das wbPK MUSS mit dem RIPEMD160 (siehe [RIPEMD160]) Algorithmus gehasht werden. Das Ergebnis der Hashfunktion MUSS anschließend mit dem Base64 (siehe [RFC4648]) Algorithmus kodiert werden und bildet die *edID*, welche über das Push Protokoll (siehe [ZUSEPUSH]) an den Zustellkopf unverzüglich übermittelt werden MUSS.

Beispiel:

wbPK, Base64	`j/NxdRQhp+tNyE9WhHdBSYuy3hA=` (28 Zeichen)
wbPK, hexadezimal	`8F F3 71 75 14 21 A7 EB 4D C8 4F 56 84 77 41 49 8B B2 DE 10` (20 Byte)
edID, RIPEMD160, hexadezimal	`23 C6 48 93 EC 1B 7D 00 8D 91 D6 3F 8D F7 BF 37 20 92 B4 2E` (20 Byte)
edID, Base64	`I8ZIk+wbfQCNkdY/jfe/NyCStC4=` (28 Zeichen)

Das LDAP Attribut *edID* ist vom gleichen Typ wie das LDAP Attribut *gvZbPK* (siehe [ZUSELDAP]).

Der LDAP Object Identifier für das *edID* Attribut ist mit `1.2.40.0.10.2.1.1.114` festgelegt.

Ein Speichern der wbPK am Zustellkopf neben der *edID* ist weder datenschutzrechtlich zulässig noch technisch notwendig, da zur eindeutigen Identifizierung im Rahmen der Zustellstückübergabe vom Zustellkopf ausschließlich die *edID* (in verschlüsselter Form zusammen mit einem Token – siehe Abschnitt 4.1.7) zurückgegeben wird.

4.1.4 Gekennzeichnete Ermittlungsleistung

Die Kennzeichnung einer Ermittlungsleistung zur nachweislichen Zusendung im Auftrag von Privaten basiert teilweise auf dem verwendeten Transportprotokoll mittels SSL-Client-Authentifizierung, als auch auf einer explizite Angabe innerhalb des Kommunikationsprotokolls. Dadurch kann sichergestellt werden, dass auch ein als Behörde oder Dienstleister authentifizierter Versender eine nachweisliche Zusendung im Auftrag von Privaten durchführen kann.

Für eine Einzelabfrage, welche auf der HTTP GET Methode basiert, existieren hierfür zwei Möglichkeiten:

1. Angabe eines speziellen zusätzlichen HTTP Parameters
2. Angabe eines speziellen zusätzlichen HTTP Headers

Für die Bulkabfrage MUSS im Root Element des XML Dokuments der Abfrage ein spezielles Attribut gesetzt werden. Details dazu finden sich in Abschnitt 4.1.5.

[2] http://www.bürgerkarte.at

4.1.5 Abfragesyntax

4.1.5.1 Einzelabfrage

Die Abfragesyntax bei der Einzelabfrage unterscheidet sich von der behördlichen Zustellung in folgenden Punkten:

1. Die Abfrage mit einem bereichsspezifischen Personenkennzeichen (bPK) des Bereichs „Zustellung“ bzw. einem solchen verschlüsselten ist ausschließlich für Behörden zulässig.
2. Es ist zusätzlich der HTTP Parameter *private* mit dem Wert *true* zu übermitteln.
3. Alternativ dazu kann auch der HTTP Header *Private* mit dem Wert true übermittelt werden.

Anmerkung: die Adressierbarkeitsabfrage einer natürlichen Person ohne Angabe des Geburtsdatums ist erlaubt.

Ein praktisches Beispiel: es wird der Zustellkopf mit der URL https://zkopf.zustellung.gv.at/ angefragt. Als Identifikation werden hier Vorname, Familienname und die E-mail Adresse des Empfängers verwendet.

```
https://zkopf.zustellung.gv.at?private=true&sn=Tauber&givenName=Arne&mail=arne.t
auber@egiz.gv.at
```

Wird der HTTP Header *Private* als Kennzeichnen einer Abfrage für eine private Zusendung verwendet, so sollte der Header die folgende Form besitzen:

```
GET /Query?sn=Tauber&givenName=Arne&mail=arne.tauber@egiz.gv.at HTTP/1.1
Private: true
Connection: close
```

Sind sowohl der HTTP Parameter *private*, als auch der HTTP Header *Private* in der Abfrage nicht vorhanden und wird für die Authentifizierung ein Zertifikat mit Verwaltungs- oder Dienstleistereigenschaft verwendet, so MUSS von einer Abfrage für eine behördliche Zustellung ausgegangen werden.

Sind sowohl der HTTP Parameter *private*, als auch der HTTP Header *Private* in der Abfrage nicht vorhanden und wird für die Authentifizierung ein Zertifikat ohne Verwaltungs- oder Dienstleistereigenschaft verwendet, so MUSS der Zustellkopf eine entsprechende Fehlermeldung mit dem Fehlercode 410 (siehe [ZUSEKOPF]) retournieren.

4.1.5.2 Bulkabfrage

Die Abfragesyntax bei der Bulkabfrage unterscheidet sich von der behördlichen Zustellung in folgenden Punkten:

1. Die Abfrage mit einem bereichsspezifischen Personenkennzeichen (bPK) des Bereichs „Zustellung“ bzw. einem solchen verschlüsselten ist ausschließlich für Behörden zulässig.
2. Es MUSS zusätzlich das Attribut *private* mit dem Wert *true* für das XML-Root-Element *BulkQuery* angegeben werden.

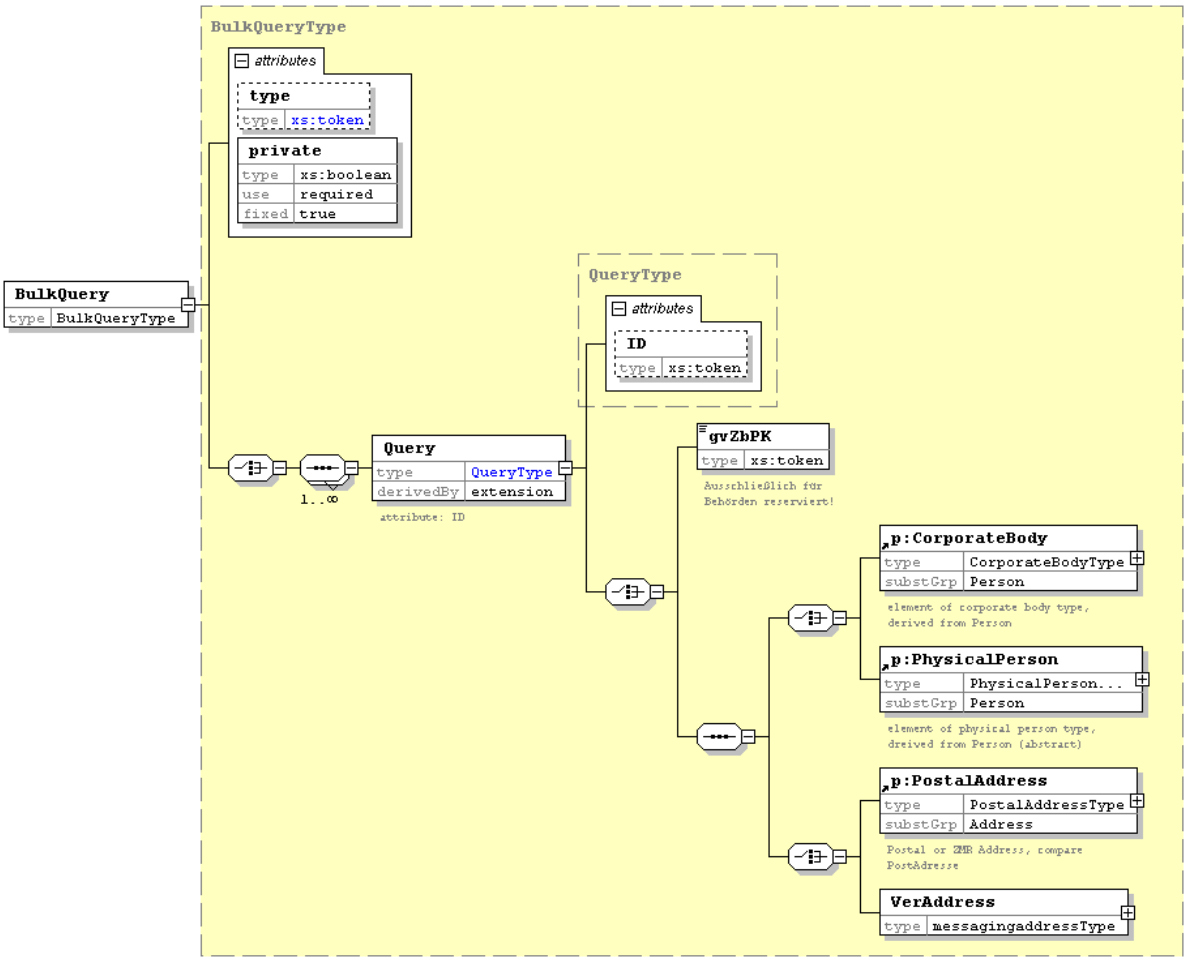

Abb. 4.1 XML Schema der Bulk Anfrage an den Zustellkopf (privat)

Beispiel:

```
<?xml version="1.0" encoding="UTF-8"?>
<BulkQuery xmlns="http://reference.e-government.gv.at/namespaces/zustellung/kopf"
          private="true">
       <Query ID="0">
              <p:PhysicalPerson>
                     <p:Name>
                            <p:GivenName>Arne</p:GivenName>
                            <p:FamilyName>Tauber</p:FamilyName>
                     </p:Name>
                     <p:DateOfBirth>1979-08-21</p:DateOfBirth>
              </p:PhysicalPerson>
              <VerAddress>
                     <p:TelephoneAddress>
                            <p:Number>

       <p:FormattedNumber>+435551234567</p:FormattedNumber>
                            </p:Number>
                     </p:TelephoneAddress>
                     <p:InternetAddress>
                            <p:Address>arne.tauber@egiz.gv.at</p:Address>
                     </p:InternetAddress>
              </VerAddress>
       </Query>
</BulkQuery>
```

4.1.6 Antwortsyntax

4.1.6.1 Einzelabfrage

Die Antwortsyntax bei der Einzelabfrage unterscheidet sich von der behördlichen Zustellung dadurch, dass im Erfolgsfall kein einzelnes *gvZbPK* Element für alle gefundenen Zustelldienste zurückgegeben wird, sondern für jeden einzelnen Zustelldienst ein *edID* Element retourniert wird.

Das XML Schema - basierend auf dem XML Schema für die behördliche Einzelabfrage – siehe [ZUSEKOPF] - im Falle der privaten Zusendung ist in folgender Abbildung ersichtlich.

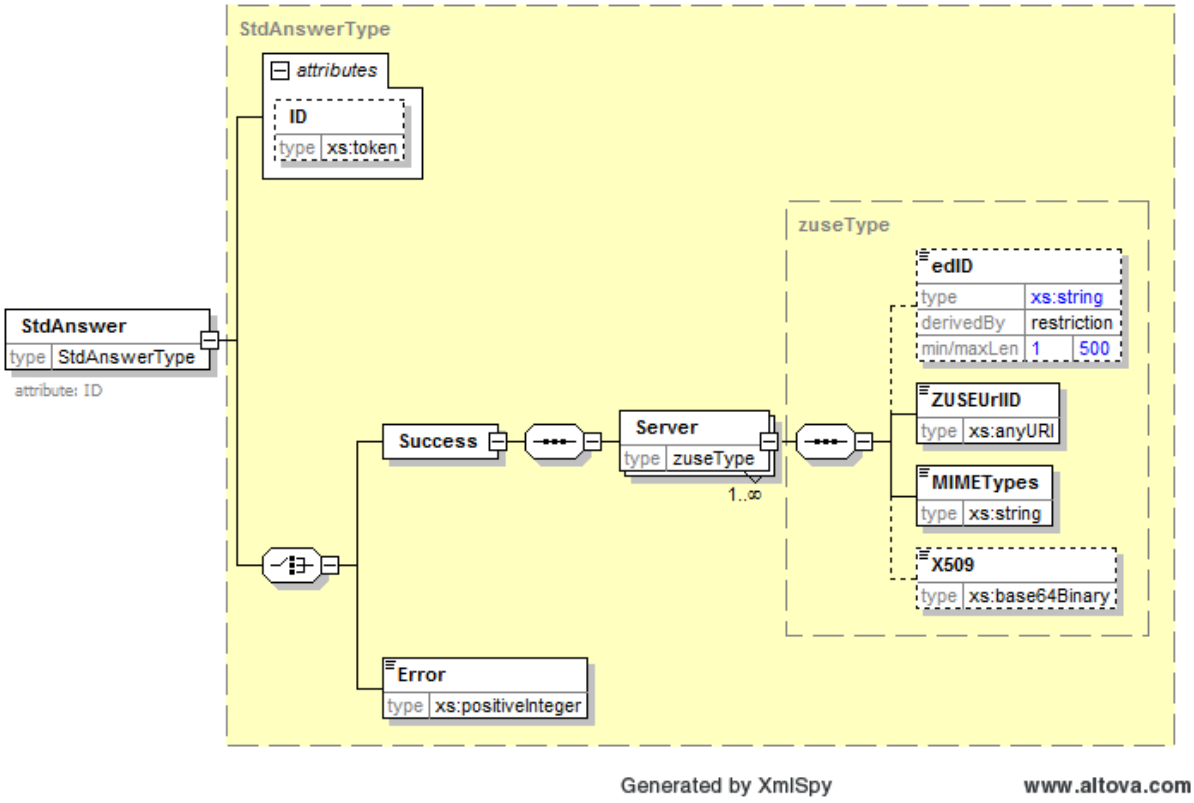

Abb. 4.2 XML Schema der Antwort auf Einzelanfrage des Zustellkopfs (privat)

Der Inhalt des *edID* Elements wird gemäß der Vorschrift zur Bildung der edID erzeugt (siehe Abschnitt 4.1.7).

Beispiel für den Erfolgsfall:

```
<?xml version="1.0" encoding="UTF-8"?>
<StdAnswer xmlns="http://reference.e-government.gv.at/namespaces/zustellung/kopf">
	<Success>
		<Server>
			<edID>MryWk8hlwvru6WoL...</edID>

	<ZUSEUrlID>http://www.privatzustellung.at/DeliveryRequest</ZUSEUrlID>
			<MIMETypes>application/pdf,text/xml</MIMETypes>
			<X509>MIIFJTCCBA2gAwIBAgI...</X509>
		</Server>
		<Server>
			<edID>3kGTIE6zpNIYaJU...</edID>
			<ZUSEUrlID>http://www.zd2.at/DeliveryRequest</ZUSEUrlID>
			<MIMETypes>*/*</MIMETypes>
		</Server>
	</Success>
</StdAnswer>
```

Der Fehlerfall unterscheidet sich nicht von der behördlichen Zustellung und wird somit in dieser Spezifikation nicht gesondert behandelt.

4.1.6.2 Bulkabfrage

Die Antwortsyntax bei der Bulkabfrage unterscheidet sich von der behördlichen Zustellung dadurch, dass im Erfolgsfall kein einzelnes *gvZbPK* Element für alle gefundenen Zustelldienste zurückgegeben wird, sondern für jeden einzelnen Zustelldienst ein *edID* Element retourniert wird.

Das XML Schema - basierend auf dem XML Schema für die behördliche Bulkabfrage – siehe [ZUSEKOPF] - im Falle der privaten Zusendung ist in folgender Abbildung ersichtlich.

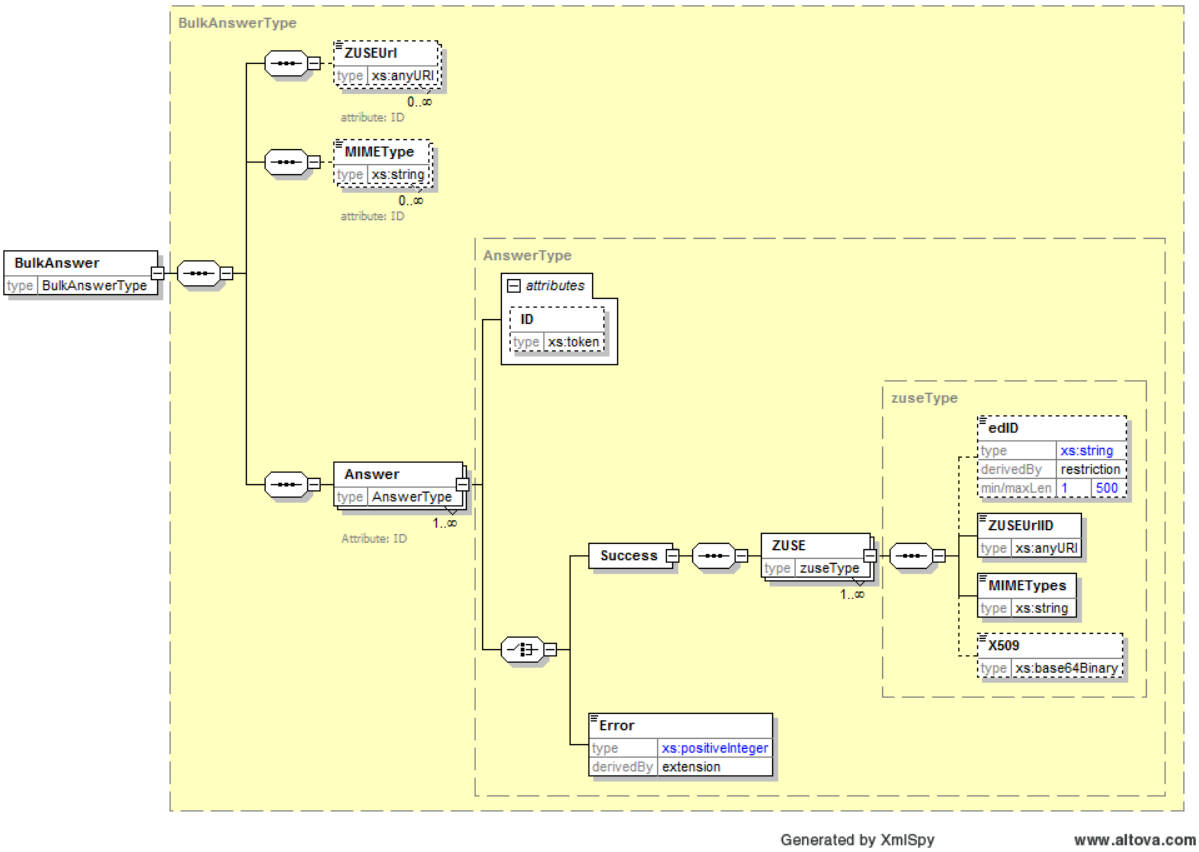

Abb. 4.3 XML-Schema der Bulk Antwort (privat)

Der Inhalt des *edID* Elements wird gemäß der Vorschrift zur Bildung der edID erzeugt (siehe Abschnitt 4.1.7).

Beispiel:

```
<?xml version="1.0" encoding="UTF-8"?>
<BulkAnswer xmlns="http://reference.e-government.gv.at/namespaces/zustellung/kopf">
        <ZUSEUrl>http://www.privatzustellung.at/DeliveryRequest</ZUSEUrl>
        <ZUSEUrl>www.zd2.at/DeliveryRequest</ZUSEUrl>
        <MIMEType>application/pdf</MIMEType>
        <MIMEType>text/xml</MIMEType>
        <MIMEType>image/gif</MIMEType>
        <MIMEType>application/msword</MIMEType>
        <Answer ID="1">
                <Success>
                        <ZUSE>
                                <edID>lHNu6nXb3K9Ouagsdq...</edID>
                                <ZUSEUrlID>2</ZUSEUrlID>
```

```
                        <MIMETypes>1,2,4</MIMETypes>
                    </ZUSE>
                </Success>
        </Answer>
        <Answer ID="2">
                <Error>404</Error>
        </Answer>
        <Answer ID="3">
                <Success>
                    <ZUSE>
                        <edID>229849k</edID>
                        <ZUSEUrlID>1</ZUSEUrlID>
                        <MIMETypes>3,4</MIMETypes>
                        <X509>...</X509>
                    </ZUSE>
                    <ZUSE>
                        <edID>3kGTIE6zpNIYaJU...</edID>
                        <ZUSEUrlID>1</ZUSEUrlID>
                        <MIMETypes>2,3,4</MIMETypes>
                    </ZUSE>
                </Success>
        </Answer>
</BulkAnswer>
```

Der Fehlerfall unterscheidet sich nicht von der behördlichen Zustellung und wird somit in dieser Spezifikation nicht gesondert behandelt.

4.1.7 Vorschrift zur Bildung der edID in der Zustellkopfantwort

Die *edID*, der eindeutige Identifier für die private Zusendung, welcher vom Zustellkopf in der Antwort zurückgeliefert wird, MUSS nach folgender Vorschrift gebildet werden:

$$(\text{Token} + :: + \text{Zeitstempel} + :: + \text{edID}_{(\text{LDAP})}) \; [\text{RSA}_{\text{priv}}]$$

Der Zeitstempel (Datum und Uhrzeit) MUSS gemäß ISO-8601 [ISO-8601] §5 im „extended format“: YYYY-MM-DDThh:mm:ss vorliegen.

Für jeden registrierten Zustelldienst wird vom Zustellkopf ein Schlüsselpaar zur Verfügung gestellt, wobei dem Zustelldienst der öffentliche Schlüssel in einem out-of-band Verfahren ausgehändigt wird. Details zum out-of-band Verfahren sind nicht Gegenstand dieser Spezifikation.

Der Zustellkopf erzeugt mittels eines Zufallsgenerators ein eindeutiges Token für die spätere Verrechnung, welches mit dem *edID* LDAP Attribut des gefundenen Empfängers konkateniert wird. Als Trennzeichen wird ein zweifaches Kolon („::“) verwendet. Das Ergebnis dieser Konkatenation wird mit dem privaten Schlüssel für den jeweiligen Zustelldienst verschlüsselt. Das Token wird als hexadezimaler String repräsentiert und besitzt keine vorgegebene Länge. Zur Verrechnung über den Zustellkopf MUSS genau jener String (case sensitive) als Verrechnungstoken verwendet werden.

Beispiel:

Token, hexadezimal	6A776ADF65FB65CE9DB (19 Zeichen)
edID, Base64	K1rURmb+CvBP01LbQn1tAeUiJms= (28 Zeichen)
Eingangsdaten für Verschlüsselung	6A776ADF65FB65CE9DB::2008-12-16T10:13:54::K1rURmb+CvBP01LbQn1tAeUiJms= (49 Zeichen)
RSA-Private Key	private exponent: 0D A0 47 2C C9 93 51 01 DB F7 C2 FE 16 6D 68 D1 C1 E1 E0 5F 26 BC 32 1A 6E E3 EF 15 83 7A A4 8D 5C 7B 53 6A 5A 27 DA DD A3 50 A2 C2 E0 A8 3D 94 3A 5C B9 DC 8C A3

	E0 04 1D E7 4A AC 4A 0D B3 24 46 B8 C2 DD 60 95 66 14 17 53 EE 47 4D 23 E9 50 3B E9 A7 DD A2 41 72 F6 76 71 5C 2C A4 0E D1 68 17 65 1F 83 91 A4 91 6D 4D 5D 71 1B 03 16 12 29 38 CD 1F 36 E5 4C 27 F5 8D 1E EB C4 05 01 93 71 (1016 bits = 127 Bytes) modulus: 00 A9 42 6A 9A EA D9 80 8A D1 B1 26 84 D2 F2 92 4C FD 43 D8 74 CB F4 01 DF D4 72 06 47 EF B4 4E CC 9E 05 0A 8F E4 EF 5B AE 65 3A B6 FF F8 C6 A8 AF 10 27 CC 6F 55 39 7B 3E 96 C6 C5 C0 F5 08 99 0A D6 B6 BD 37 96 97 66 CF 34 2C 4A 16 9F D1 D8 AD A3 6F 58 7F 9E C1 C3 8C 16 94 30 84 AD 66 B2 D6 52 C0 46 06 33 2F 5F 3D 4C 92 F2 DB 3C 6D 3A 7A 0C 1B 2A 80 64 13 D5 6F 53 37 76 CD A7 D7 84 C1 (1024 bits = 128 Bytes)
Resultat der Verschlüsselung (edID in Zustellkopfantwort) hexadezimal	9E 80 63 09 22 1C E4 95 F2 CC 0A 4C 23 98 2D B0 39 92 AE 29 81 06 DA E2 EA 1E DC 2F 56 E7 77 59 0C A3 62 AD F4 9E 19 92 53 04 FC D5 0F CF CE 53 43 25 93 1B B1 F0 70 2C 3D A5 59 63 96 C3 1A 35 F7 DC CB 02 70 A7 46 E1 9E F7 FD 91 33 43 53 DB E0 8D 36 32 6F DC 4A B0 08 EC 62 90 FE 38 22 BA 92 9B 5A 95 25 A6 FB 4A B9 02 DE 2D 7C 4F 77 7C 61 2E EF 04 BF FA 56 CE 42 47 98 F6 47 67 CF 7E (128 Bytes)
Resultat der Verschlüsselung (edID in Zustellkopfantwort) Base64	noBjCSIc5JXyzApMI5gtsDmSrimBBtri6h7cL1bnd1kMo2Kt9J4Zk lME/NUPz85TQyWTG7HwcCw9pVljlsMaNffcywJwp0bhnvf9kTNDU9 vgjTYyb9xKsAjsYpD+OCK6kptalSWm+0q5At4tfE93fGEu7wS/+lb OQkeY9kdnz34= (172 Zeichen)

4.2 Zustellserver

4.2.1 Annahme von Zustellstücken

Das XML-Schema für eine *DeliveryRequest* Nachricht zur Übergabe von privaten Zusendungen an den Zustellserver basiert auf dem behördlichen Schema (siehe [ZUSEMSG]) und wird in den in diesem Abschnitt beschriebenen Punkten erweitert.

Folgende Abbildung zeigt das erweiterte Schema:

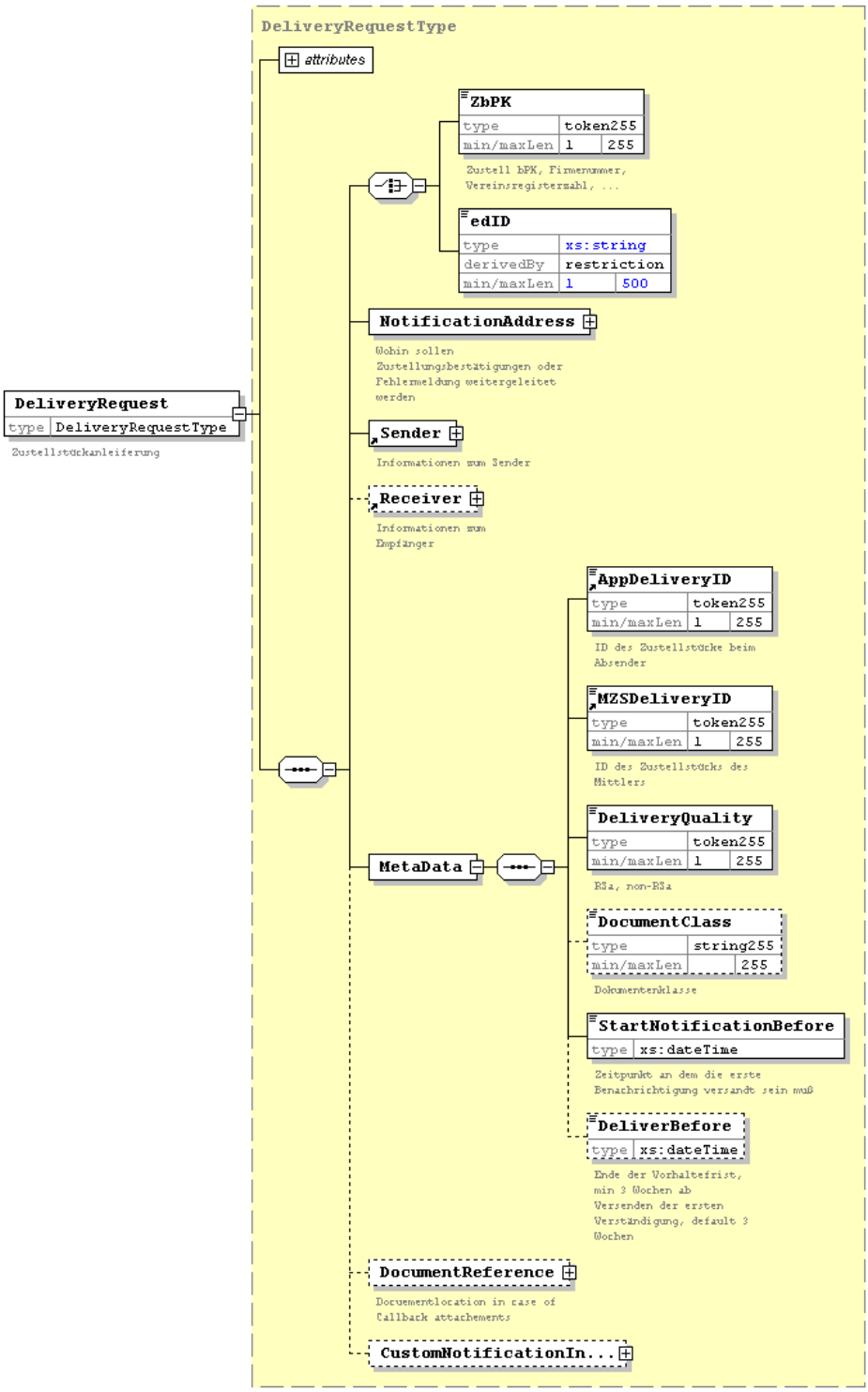

Abb. 4.4 XML-Schema der DeliveryRequest Nachricht für eine private Zusendung

4.2.1.1 Identifikation

Wie in Abb. 4.4 ersichtlich MUSS anstelle des *ZbPK* Elements der behördlichen Zustellung das *edID* Element verwendet werden. Dort MUSS jenes Element eingetragen werden, das der Zustellkopf für den jeweiligen Zustellserver retourniert. Der in der edID enthaltene Zeitstempel (siehe Abschnitt 4.1.7) MUSS vom Zustellserver überprüft werden und DARF NICHT älter als 48h sein.

4.2.1.2 Dokumentenklasse

Die private Zusendung sieht als Erweiterung zur behördlichen Zustellung die Definition einer sogenannten Dokumentenklasse für Schriftstücke vor. Zweck dieser ist die einfachere Verwaltung von empfangenen privaten Schriftstücken am Zustellserver. Private Schriftstücke können so bspw. visuell nach Dokumentenklassen (auch prioritär) geordnet werden.

Dokumentenklassen müssen gemäß den Vorgaben für MIME-Types (siehe [RFC2048]) angegeben. Als Präfix wird „*x-edclass*“ verwendet. Zulässige Dokumentenklassen werden in regelmässigen Abständen aktualisiert auf den Informationsseiten des behördlichen Zustellkopfs publiziert.

Die Dokumentenklasse gilt für die gesamte Zustellung (*DeliveryRequest*) und kann nicht für einzelne in der Zustellung enthaltene Dokumente differenziert werden. Sie kann daher optional in den Metainformationen im *DocumentClass* Element übergeben werden.

4.2.1.3 Zustellqualität

Die Zustellqualitäten RSa und nonRSa sind ausschließlich für die behördliche Zustellung definiert. Für die nachweisliche Zusendung privater Schriftstücke sind folgende Qualitäten zulässig:

1. Normalbrief (nonR)
2. Normalbrief eigenhändig (nonR+)
3. Einschreiben (R)
4. Einschreiben eigenhändig (R+)
5. Einschreiben mit Rückschein (RS)
6. Einschreiben mit Rückschein eigenhändig (RS+)

In den letzten beiden Fällen wird vom Zustellserver ein Zustellnachweis gemäß den Vorgaben und Spezifikationen der behördlichen Zustellung generiert (siehe [ZUSEMSG]). Die Qualität R+ definiert weiters, dass das Schriftstück ausschließlich vom Empfänger selbst und nicht durch einen Stellvertreter (bspw. mittels einer Postvollmacht, etc.) abgeholt werden kann. Bei juristischen Personen ist somit die Abholung nur durch die die juristische Person unmittelbar vertretende natürliche Person (z. Bsp. Prokuristen lt. Firmenbuch, etc.) zulässig.

4.2.1.4 Verschlüsselung

Eine Bevorzugung von Zustellservern, bei denen ein Verschlüsselungszertifikat hinterlegt ist(siehe [ZUSTG] § 34 Abs. 3), ist für eine private Zusendung nicht verpflichtend.

4.2.1.5 Empfängerverständigungen

Für private Zusendungen gelten nicht die Vorgaben des Zustellgesetzes (siehe [ZUSTG]) bzgl. der optischen Gestaltung der Empfängerverständigungen (sowohl für elektronische als auch für postalische Verständigungen).

Eine postalische Verständigung ist im Rahmen von privaten Zusendungen nicht vorgesehen, kann jedoch optional umgesetzt werden.

4.2.1.6 Letztmöglicher Zeitpunkt der ersten Empfängerverständigung

Über das `StartNotificationBefore` Element ist es beispielsweise möglich, mehrere Zusendungen für einen Empfänger innerhalb eines bestimmten Zeitraums (z.B. 24h) zu einer Sendung zusammenzufassen.

Das Element zur Vorgabe des Zeitpunkts für die erste Empfängerverständigung ist vor dem Hintergrund des aktuellen Zustellgesetzes für die behördliche Zustellung obsolet, da dieser Aspekt im Gesetz detailliert geregelt ist.

Details dazu siehe [ZUSEMSG].

Für private Zusendungen DARF dieses Element NICHT ignoriert werden.

4.2.1.7 Letztmöglicher Zeitpunkt der Abholung der Sendung durch den Empfänger

Das `DeliverBefore` Element zur Vorgabe von Abholfristen ist vor dem Hintergrund des aktuellen Zustellgesetzes für die behördliche Zustellung obsolet, da die Abholfristen im Gesetz detailliert geregelt sind. Bei behördlichen Zustellungen DARF dieses Element NICHT verwendet werden.

Details dazu siehe [ZUSEMSG].

Für private Zusendungen DARF dieses Element NICHT ignoriert werden.

4.2.1.8 Empfängerverständigungsintervalle

Das Element zur Vorgabe von Empfängerverständigungsintervallen ist vor dem Hintergrund des aktuellen Zustellgesetzes für die behördliche Zustellung obsolet, da die Verständigungsintervalle und –arten im Gesetz detailliert geregelt sind.

Details dazu siehe [ZUSEMSG].

Für private Zusendungen DARF dieses Element NICHT ignoriert werden.

4.2.2 Benutzerschnittstelle

Dieser Abschnitt definiert Modifikationen und Erweiterungen der Benutzerschnittstelle eines Zustellservers (siehe [ZUSESPEC]) im Rahmen der nachweislichen Zusendung im Auftrag von Privaten.

4.2.2.1 Zustimmung und Widerruf der Annahme von privaten Zusendungen

Bietet ein Zustellserver die optionale Möglichkeit der nachweislichen Zusendung im Auftrag von Privaten an, so MUSS über die Benutzerschnittstelle die Möglichkeit geboten werden, dieser explizit zuzustimmen bzw. zu widerrufen.

Die modifizierten LDAP Attribute *gvAcceptPrivate* (siehe [ZUSELDAP]) bzw. *edID* (siehe Abschnitt 4.1.3) müssen unverzüglich über das Push-Protokoll (siehe [ZUSEPUSH]) an den Zustellkopf übermittelt werden.

Ein Zustellserver kann im Rahmen der Zustimmung zur Annahme von privaten Zusendungen über ein entsprechendes Formular das wbPK zur Berechnung der *edID* über die Bürgerkarte des Empfängers berechnen lassen, sofern das wbPK nicht bereits zuvor (z.B. bei der Registrierung am Zustellserver) berechnet wurde.

4.2.2.2 Visuelle Differenzierung von behördlichen Schriftstücken

Private Zusendungen müssen visuell auf der Benutzeroberfläche von behördlichen Schriftstücken klar getrennt aufgelistet und angezeigt werden. Die individuelle Umsetzung dieser Differenzierung ist dem Zustellserver vorbehalten.

4.2.2.3 Visuelle Differenzierung nach Dokumentenklassen

Es wird empfohlen, private Zusendungen nach Dokumentenklassen (falls bei der Übergabe des Zustellstücks angegeben) geordnet dem Empfänger auf der Benutzeroberfläche aufzulisten und anzuzeigen. Eine optionale individuelle Umsetzung dieser Differenzierung ist dem Zustellserver vorbehalten.

4.2.3 Verrechnung

Die Verrechnung erfolgt analog zum und im Rahmen des behördlichen Verrechnungsprozesses (siehe [ZUSERECH]). Als Verrechnungstoken für die private Zusendung MUSS jenes vom Zustellkopf retournierte und an den Zustellserver übergebene Token (siehe Abschnitt 4.1.7) verwendet werden.

5 Referenzen

[ZUSELDAP]	Tauber A., Reichstädter P., Hörbe R., Zustellung LDAP Schemabeschreibung 1.3.1
[ZUSEKOPF]	Tauber A., Rössler T., Elektronische Zustellung - Zustellkopf Schnittstellenspezifikation 1.3.1
[ZUSEMSG]	Rössler T., Tauber A., Reichstädter P., Zustellung Message Spezifikation 1.3.1
[ZUSEPUSH]	Tauber A., ZUSE Push Protokoll 1.3.1
[ZUSESPEC]	Tauber A., Rössler T., Reichstädter P., Elektronische Zustellung – Technische Spezifikation 1.3.1
[ZUSERECH]	Reichstädter P., Rössler T., Tauber A., Modell und Prozesse der Zustellungs-Verrechnung 1.3.1
[ZUSTG]	Verwaltungsverfahrens- und Zustellrechtsänderungsgesetz 2007, BGBl. I Nr. 5/2008 abgerufen von http://ris.bka.gv.at/ am 24.11.2008
[RFC2048]	Multipurpose Internet Mail Extensions (MIME), Nov. 1996; Freed. et. al. http://www.ietf.org/rfc/rfc2048.txt
[RFC4648]	The Base16, Base32, and Base64 Data Encodings, Oct. 2006; S. Josefsson. http://www.ietf.org/rfc/rfc4648.txt
[RIPEMD160]	RIPEMD-160: A Strenghtened Version of RIPEMD, http://homes.esat.kuleuven.be/~bosselae/ripemd160.html
[SZ-bPK-Algo V1.1.1]	Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (bPK)
[CERTOID]	Hollosi, Arno: X.509-Zertifikatserweiterungen für die Verwaltung. Version 1.0.3 vom 21.02.2005.
[ISO-8601]	ISO 8601:2000 – Data elements and interchange formats -- Information interchange -- Representation of dates and times, Stage date: 2000-12-21
[KEYWORDS]	Bradner, S.: RFC 2119: *Key words for use in RFCs to Indicate Requirement Levels*. IETF Request For Comment, März 1997. Abgerufen aus dem World Wide Web am 20.09.2007 unter http://www.ietf.org/rfc/rfc2119.txt