

# ZUSE – Push Protokoll

## Spezifikation

Version 1.0.0, 24.01.2008

DI Arne Tauber – [arne.tauber@egiz.gv.at](mailto:arne.tauber@egiz.gv.at)

### Zusammenfassung:

Dieses Dokument spezifiziert das Protokoll, mit welchem elektronische Zustelldienste die unverzügliche Weiterleitung der Daten gemäß § 29 Abs. 1 Zustellgesetz an den Zustellkopf (elektronischer Zustelldienst gemäß § 29 Abs. 2) durchführen müssen.

### Inhaltsverzeichnis:

1	Motivation.....	5
1.1	Schlüsselwörter	5
1.2	Geschlechtsspezifische Bezeichnungen	5
1.3	Einleitung	5
2	Modell.....	6
3	Protokoll.....	7
3.1	Zeitpunkt der zu übermittelnden Daten	7
3.2	Kommunikation	7
3.3	Request	7
3.3.1	Content-Type	7
3.3.2	Content-Length	7
3.3.3	Encoding	7
3.3.4	HTTP Body	7
3.3.5	LDIF Content	7
3.3.5.1	LDIF Version	7
3.3.5.2	LDIF Format	7
3.4	Response	7
3.4.1	Erfolgsfall (Success)	8
3.4.2	Fehlerfall (Error)	8
4	LDAP Struktur.....	10
4.1	Verwendete Standards	10
4.2	Directory Information Tree	10
4.3	Klassen und Attributbeschreibung	10
4.4	Verwendung der Klassen im DIT	10
4.5	Objektklassen	12

5	Anhang.....	14
5.1	Beispiel LDIF HTTP POST (Request)	14
5.2	Antwort (PushResponse)	14
5.2.1	Allgemeiner Fehler	14
5.2.2	Fehler beim Ändern einzelner Einträge	14
6	Referenzen.....	15

## Abbildungen

Abbildung 1: Modell des Push Protokolls.....	6
Abbildung 2: PushResponse Element .....	8

## Revision History

Version	Datum	Autor(en)	
0.0.1	20.08.2007	Arne Tauber (EGIZ)	Erstellt.
0.0.2	21.08.2007	Arne Tauber (EGIZ)	Änderungen HL.
0.1.0	23.08.2007	Arne Tauber (EGIZ)	LDIF Version festgelegt.
0.2.0	17.09.2007	Arne Tauber (EGIZ)	LDIF Format festgelegt. XML-Schema für Response.
0.3.0	24.09.2007	Arne Tauber (EGIZ)	Mehrere LDIF Änderungen explizit festgelegt.
0.9.0	09.01.2008	Arne Tauber (EGIZ)	Obligatorisches Encoding auf ISO-8859-1 gesetzt.
1.0.0	23.01.2008	Arne Tauber (EGIZ)	LDAP Struktur festgesetzt.

# 1 Motivation

## 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.

## 1.3 Einleitung

Das Zustellgesetz [EGovG] definiert in § 29 Abs. 1 die Leistungen von elektronischen Zustelldiensten, welche auch die Weiterleitung der in § 33 Abs. 1 definierten Daten sowie die Kommunikation der Änderungen derer bzw. der Abwesenheiten an den Zustellkopf inkludiert. Nachfolgend ist ein Ausschnitt aus dem Begutachtungsentwurf der Novellierung des Zustellgesetzes angeführt:

### Leistungen von elektronischen Zustelldiensten

§ 29. (1) Jeder elektronische Zustelldienst hat nach den näheren Bestimmungen dieses Bundesgesetzes die Zustellung behördlicher Dokumente an seine Kunden vorzunehmen (Zustelleistung). Die Zustelleistung umfasst folgende, nach dem jeweiligen Stand der Technik zu erbringende Leistungen:

1. die unverzügliche Weiterleitung
  - a) der Daten gemäß § 33 Abs. 1,
  - b) einer vom Kunden bekanntgegebenen Änderung dieser Daten (§ 33 Abs. 2 erster Satz) sowie
  - c) von Mitteilungen gemäß § 33 Abs. 2 zweiter Satzan den elektronischen Zustelldienst gemäß Abs. 2;

### An- und Abmeldung

§ 33. (1) Die Anmeldung bei einem elektronischen Zustelldienst kann nur unter Verwendung der Bürgerkarte erfolgen. Jeder Zustelldienst hat im Internet ein elektronisches Verfahren für die Anmeldung bereitzustellen. Bei der Anmeldung sind jedenfalls die folgenden 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 des E-Government-Gesetzes – E-GovG, BGBl. I Nr. 10/2004),
  - b) sonst die Stammzahl (§ 6 E-GovG),
4. eine Abgabestelle im Inland und eine elektronische Adresse, an die die Verständigungen gemäß § 35 übermittelt werden können,
5. gegebenenfalls Angaben des Kunden über die Formate, die die zuzustellenden Dokumente haben müssen, damit er zur Annahme bereit ist, und deren inhaltliche Verschlüsselung.

Dieses Dokument spezifiziert das Protokoll, mit welchem elektronische Zustelldienste die unverzügliche Weiterleitung der Daten gemäß § 29 Abs. 1 an den Zustellkopf (elektronischer Zustelldienst gemäß § 29 Abs. 2) durchführen müssen.

## 2 Modell

Der Ablauf des Push Prozesses ist wie folgt dargestellt:

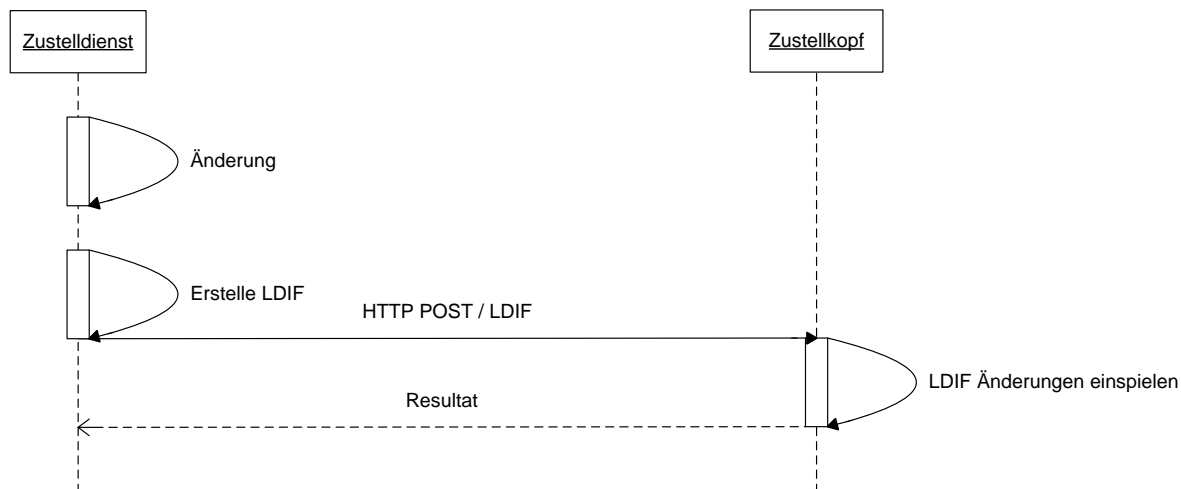


Abbildung 1: Modell des Push Protokolls

Nachdem der elektronische Zustelldienst eine Änderung der Stammdaten gemäß § 33 Abs. 1 bzw. § 33 Abs. 2 Zustellgesetz erfährt, erstellt dieser eine Datei im LDIF (LDAP Data Interchange Format) [LDIF] Format mit den Änderungen aller Objekte im DIT (Directory Information Tree) im Vergleich zum Zeitpunkt der letzten Synchronisation mit dem Zustellkopf. Der Inhalt des LDAP Servers muss der ZUSE-LDAP Spezifikation entsprechen [ZUSE-LDAP].

Der Zustelldienst authentifiziert sich mittels Client-Zertifikat am Zustellkopf und übermittelt via HTTP POST die LDIF Datei. Der Zustellkopf versucht anschließend anhand der LDIF Datei den aktuellen Datenbestand zu aktualisieren und gibt einen entsprechenden Rückgabewert (für Erfolg, Fehler, etc.) an den Zustelldienst zurück.

## 3 Protokoll

### 3.1 Zeitpunkt der zu übermittelnden Daten

Laut Zustellgesetz § 29 Abs. 1 müssen jegliche Änderungen unverzüglich übermittelt werden.

### 3.2 Kommunikation

Die Kommunikation zwischen Zustelldienst und Zustellkopf basiert auf einem HTTPS (TLS) POST mit Client-Authentifizierung seitens des Zustelldienst.

### 3.3 Request

#### 3.3.1 Content-Type

Der Content-Type HTTP Header muss vorhanden sein und auf `application/directory` gesetzt sein.

#### 3.3.2 Content-Length

Der Content-Length HTTP Header muss gesetzt sein.

#### 3.3.3 Encoding

Das Encoding des Request muss in ISO-8859-1 erfolgen. Die entsprechende „charset“ Anweisung in den HTTP Headern muss gesetzt sein.

#### 3.3.4 HTTP Body

Der HTTP Body des POST Requests muss den Inhalt der LDIF Datei enthalten.

#### 3.3.5 LDIF Content

##### 3.3.5.1 LDIF Version

Der LDIF Inhalt muss dem Format der Versionsnummer 1 entsprechen.

##### 3.3.5.2 LDIF Format

Die LDIF Spezifikation unterscheidet zwei Formate. Entweder beschreibt die Datei eine Reihe von Verzeichniseinträgen oder eine Reihe von Änderungen an Verzeichniseinträgen (LDIF Request). Die LDIF Datei kann jedoch nur ein Format beinhalten.

Der HTTP POST Request muss eine LDIF Änderungsdatei beinhalten (LDIF Request), andernfalls muss eine entsprechende Fehlermeldung zurückgegeben werden. Die LDIF Datei kann Änderungsanweisungen für mehrere Einträge beinhalten.

Beispiele für einen Request des Push Protokolls finden sich in Anhang A.

### 3.4 Response

Die Antwort auf den Push Request ist ein XML Dokument das die Push-Antwort (`PushResponse`) enthält. Das XML Dokument ist direkt in den HTTP Body eingebettet.

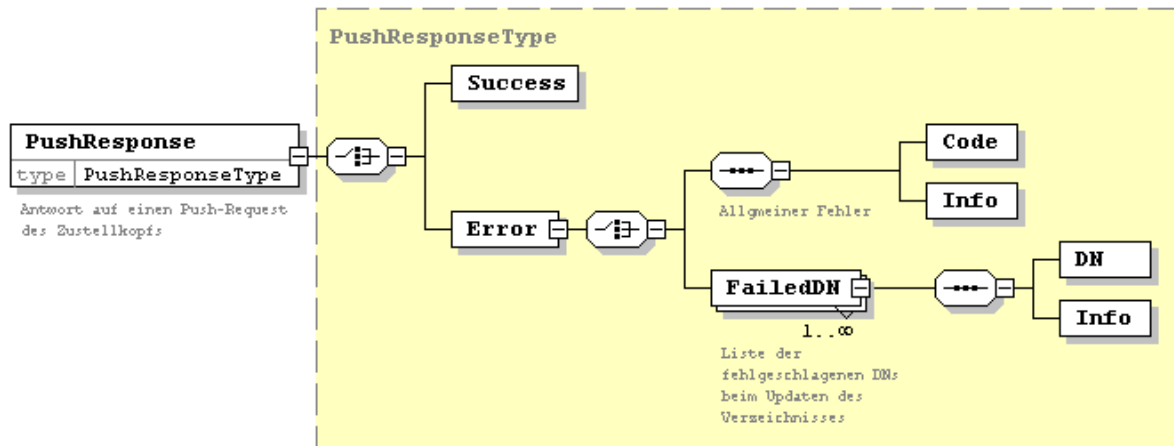


Abbildung 2: PushResponse Element

### 3.4.1 Erfolgsfall (Success)

Konnte die LDIF Datei erfolgreich verarbeitet werden, enthält das `PushResponse` Element als einziges Kindelement das `Success` Element.

### 3.4.2 Fehlerfall (Error)

Im Fehlerfall wird unterschieden, ob ein genereller Fehler aufgetreten ist, der für den gesamten Request gilt, oder ob nur das Aktualisieren einzelner Änderungsanweisungen der LDIF Datei ungültig ist.

Im Falle eines generellen Fehlers enthält das `Error` Element ein `Code` und ein `Info` Element. Das `Code` Element gibt die Fehlernummer an, das `Info` Element enthält eine menschenlesbare Beschreibung des Fehlers.

Im Falle des Fehlschlagens einzelner Änderungsanweisungen werden die betroffenen LDIF Einträge (`FailedDN` Element) anhand ihres Distinguished Names (`DN` Element) aufgelistet. Das `Info` Element enthält eine menschenlesbare Beschreibung des Fehlers.

Tabelle 1 zeigt eine Liste der Fehlermeldungen, die während der Verarbeitung des Requests auftreten können.

Fehlerklasse	Beschreibung
1xxx	Fehler in der Kommunikation
2xxx	Fehler im Transportprotokoll
3xxx	Fehler in der LDIF Datei
4xxx	Interner Server Fehler

Fehlercode	Beschreibung
1001	Client ist nicht authentifiziert.  Dieser Fehler tritt auf, falls eine Operation ausgeführt werden

	soll und der Client nicht dazu berechtigt ist.
2001	HTTP-Parameter Content-Type fehlt oder ist ungültig. Dieser Parameter muss vom Client gesetzt sein und auf den Wert „application/directory“ gesetzt sein.
2002	Die charset Anweisung ISO-8859-1 fehlt oder das Character Encoding ist nicht auf ISO-8859-1 gesetzt.
3000	Unklassifizierter Fehler beim Einlesen der LDIF Datei.
3001	Distinguished Name kann nicht geparkt werden.
3002	Unzulässiger Distinguished Name.
4001	Interner Server Fehler beim Einspielen der LDIF Datei.

## 4 LDAP Struktur

Der Zustellkopf verwendet einen Verzeichnisdienst zur Bereithaltung der Empfängerinformationen. Dieser Abschnitt beschreibt die LDAP Struktur dieses Verzeichnisdienstes. Das LDIF in der Push Anfrage muss dieser LDAP Spezifikation entsprechen.

### 4.1 Verwendete Standards

Für die Spezifikation des LDAP-Modells für den Verzeichnisdienst des Zustelldienstes wird der Standard Lightweight Directory Access Protocol (v3) (LDAP v3) gemäß [RFC 2251] zugrunde gelegt. Die Attributdefinition des vorliegenden Schemas bezieht sich auf den Standard Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions gemäß [RFC 2252].

### 4.2 Directory Information Tree

- Das DIT-Root Objekt (Klasse Organization) hat den DN `dc=at`.
- Auf der zweiten Hierarchie-Ebene sind Container-Objekte der Klasse Organization, die für jeden einzelnen Zustelldienst getrennte Namensräume schaffen. Dies ermöglicht eine einfache Verwaltung und Zugriffsmanagement für die einzelnen Zustelldienste. Die Vergabe der Organisationsbezeichnung an einen Zustelldienst erfolgt durch die den Zustellkopf betreibende Stelle im Zuge der Zulassung eines Zustelldienstes.
- Auf der zweiten Hierarchie-Ebene sind Container-Objekte der Klasse OrganizationalUnit, die für natürliche und nicht-natürliche Personen getrennte Namensräume schaffen

### 4.3 Klassen und Attributbeschreibung

Die Werte in der Spalte Eigenschaften eines Attributes bedeuten:

- **M** bedeutet mandatory (= required); Default ist optional (allowed).
- **L** bedeutet multi-valued, leer (Default) bedeutet single-valued

Vorkommende Typen:

- `bin`: binary
- `cis`: Directory String, Case Insensitive Match (Default)
- `ces`: Directory String, Case exact Match
- `date`: Datum Format: JJJJ-MM-TT
- `dn`: Distinguished Name
- `int`: Integer
- `tel`: Telephone Number: +LL VVVV AAAAAAA (es gilt L: Landescode; V: Vorwahl; A: Nummer [ITU-T E123])
- `uri`: URI [RFC 2396]
- `mail`: E-Mail-Adresse laut [RFC2822]

Alle Attribute, die nicht in einem RFC definiert sind, haben den Präfix 'gv'.

### 4.4 Verwendung der Klassen im DIT

Im folgenden Schema wird dargestellt, wie Objekte in Abhängigkeit von ihren Klassen im DIT (Directory Information Tree) positioniert werden:

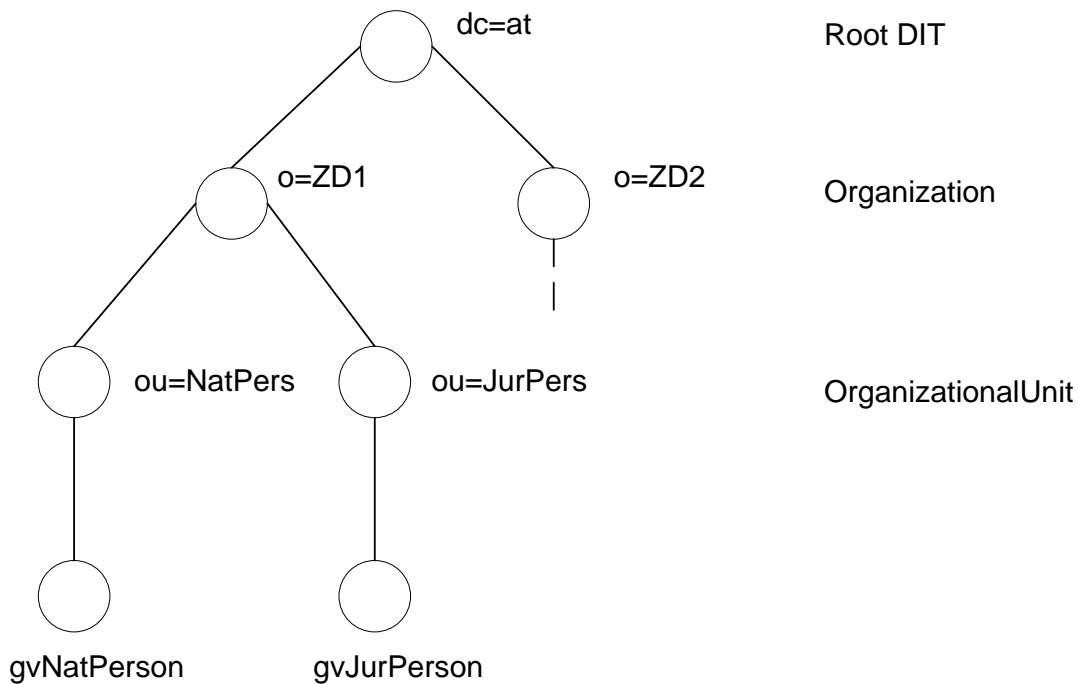


Abbildung 3: Klassen im DIT

- `gvNatPerson`: Natürliche Personen, identifiziert durch die Zustell-bPK. Namensschreibweise wie im ZMR, Zustelladressen.
- `gvJurPerson`: Nicht-natürliche („juristische“) Personen, zum Beispiel:
  - o registrierte Firmen (Firmenbuch)
  - o Vereine (Vereinsregister)
  - o Behörden (entsprechend der einschlägigen Gesetze)
  - o Selbstverwaltungskörperschaften
  - o Registrierte Genossenschaften
  - o Nicht registrierte Einzelunternehmer
  - o Andere nicht registrierte juristische Personen (z.B. GesmbR)
  - o Ausländische juristische Personen
- Unterhalb der Namensräume, die durch die Knoten der Klasse `organizationalUnit` definiert sind, gibt es keine weitere hierarchische Untergliederung.

## 4.5 Objektlassen

### Objektklasse gvNatPerson

<b>gvNatPerson</b> 1.2.40.0.10.2.1.0.100	Natürliche Person	
dn: gvZbPk (dn: gvZbPk=E8XfYRKHDiky/QL5q7k/L9kgMfU=, ou=natPers, c=at)		
Attribut	Beschreibung (Beispiel)	Eigenschaft
gvZbPK	Bereichsspezifisches Personenkennzeichen für den Bereich "Zustellung", base64-codiert (E8XfYRKHDiky/QL5q7k/L9kgMfU=)	ces, M
cn	Vorname Nachname (Arne Tauber)	cis, M
sn	Nachname laut ZMR-Anfrage (Tauber)	cis, M
givenName	Vorname laut ZMR-Anfrage (Arne)	cis, M
gvBirthdate	Geburtsdatum (laut Eintrag auf Bürgerkarte bzw. ZMR) (1979-08-21)	date, M
street	Strasse des Hauptwohnsitzes (Ballhausplatz 2)	cis, M
l	Ort des Hauptwohnsitzes (Wien)	cis, M
c	Land des Hauptwohnsitzes (2-stelliges Kürzel nach ISO 3166-1) (AT)	cis; M
postalCode	PLZ des Hauptwohnsitzes	M
mail	E-Mail-Adresse Format laut [RFC2882] ( <a href="mailto:arne.tauber@egiz.gv.at">arne.tauber@egiz.gv.at</a> )	mail, L
telephoneNumber	Festnetz-, Fax- oder Mobiltelefonnummer Format laut [ITU-T E123] (+43 1 5551234)	tel, L
gvAcceptedFormat	MIME-Typ eines akzeptierten Dokumentformats [RFC 2046] (application/pdf)	cis, M, L
gvAbsentFrom	keine Zustellung ab	date
gvAbsentUntil	keine Zustellung bis	date
userCertificate	Zertifikat des Empfängers im X.509 Format, DER kodiert, welches den öffentlichen Schlüssel enthält	bin

## Objektklasse gvJurPerson

<b>gvJurPerson</b> 1.2.40.0.10.2.1.0.101	juristischen Person	
dn: gvSourcePIN (dn: gvSourcePIN=FB:943509i,c=at)		
Attribut	Beschreibung ( <i>Beispiel</i> )	Eigenschaft
gvSourcePIN	Stammzahl der nicht-natürlichen Person mit Präfix für Register in dem diese Zahl geführt wird. (FB:212324q)	ces, M
cn	Bezeichnung der nicht-natürlichen Person	cis, M
sn	wie gvNatPerson, <b>aber nicht mandatory</b>	4 5 1
givenName	wie gvNatPerson, <b>aber nicht mandatory</b>	4 5 2
gvBirthdate	wie gvNatPerson, <b>aber nicht mandatory</b>	4 5 3
street	wie gvNatPerson	M
l	wie gvNatPerson	M
c	wie gvNatPerson	M
postalCode	wie gvNatPerson	M
mail	wie gvNatPerson	L
telephoneNumber	wie gvNatPerson	L
gvAcceptedFormat	wie gvNatPerson	M, L
gvAbsentFrom	wie gvNatPerson	4 5 4
gvAbsentUntil	wie gvNatPerson	4 5 5
userCertificate	wie gvNatPerson	4 5 6

### Anmerkungen:

- Attribute sn, givenName, gvBirthdate sind nicht mandatory:** Die Abfrage einer nicht natürlichen Person im Verzeichnis erfolgt vorzugsweise mit der Stammzahl der Person (= z.B. Firmenbuchnummer). Die nicht-natürliche Person kann allerdings in bestimmten Fällen (z.B.: bei einer Personengesellschaft) auch mit den Attributen einer natürlichen Person definiert werden und in diesen Fällen sind die dafür vorbereiteten Attribute zu verwenden. In allen anderen Fällen stellen sie aber kein Abfragekriterium dar und sind daher nicht als mandatory zu beschreiben.
- Zustellberechtigte Personen – Führung im Verzeichnisdienst:** Der Verzeichnisdienst eines Zustelldienstes dient ausschließlich dazu, festzustellen, ob ein Zustellbenutzer beim Zustelldienst angemeldet ist. Diese Auskunft kann mit den definierten Informationen in der Klasse gvJurPerson in allen festgelegten Fällen erteilt werden. Die Verständigung der zustellberechtigten Personen einer nicht-natürlichen Person erfolgt erst nach Abfrage des Zustelldienstes. Daher besteht keine Notwendigkeit, die Daten der zustellberechtigten Personen im Verzeichnisdienst zu führen.

## 5 Anhang

### 5.1 Beispiel LDIF HTTP POST (Request)

Das folgende Beispiel zeigt eine LDIF Änderungsdatei, welche für eine natürliche Person mit der Zustell-bPK uTvh8sZRiOVKOmtb8FLbparv43w= die Adresse auf „Musterstraße 1/a“ ändert.

```
POST /services/PushService HTTP/1.1
Content-Type: application/directory; charset=ISO-8859-1
Content-Length: 12345

version: 1
dn: gvZbPK=uTvh8sZRiOVKOmtb8FLbparv43w\=,ou=NatPers,o=bka,dc=at
changetype: modify
replace: street
street: Musterstraße 1/a
-
```

### 5.2 Antwort (PushResponse)

#### 5.2.1 Allgemeiner Fehler

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=UTF-8
Content-Length: 12345

<?xml version="1.0" encoding="UTF-8"?>
<PushResponse xmlns="http://reference.e-
government.gv.at/namespace/zustellung/kopf">
  <Error>
    <Code>2001</Code>
    <Info>HTTP Parameter Content-Type fehlt.</Info>
  </Error>
</PushResponse>
```

#### 5.2.2 Fehler beim Ändern einzelner Einträge

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=UTF-8
Content-Length: 12345

<?xml version="1.0" encoding="UTF-8"?>
<PushResponse xmlns="http://reference.e-
government.gv.at/namespace/zustellung/kopf">
  <Error>
    <FailedDN>
      <DN>gvZbPK=/iqNMjDj8dSBu/c0HBVdUKxJRZQ=,ou=gvNatPerson,o=bka,dc=at</DN>
      <Info>Eintrag nicht gefunden.</Info>
    </FailedDN>
    <FailedDN>
      <DN>gvZbPK=/iqNMjDj8dSBu/c0HBVdUKxJRZQ=,ou=gvNatPerson,o=egiz,dc=at</DN>
      <Info>LDAP Attribut gvBirthDate besitzt ungültiges Format.</Info>
    </FailedDN>
  </Error>
</PushResponse>
```

## 6 Referenzen

- [LDIF] G. Good, RFC2849, The LDAP Data Interchange Format (LDIF) – Technical Specification
- [ZUSE-LDAP] M. Liehmann, A. Hollosi, R. Hörbe, Elektronische Zustellung – LDAP Schemabeschreibung 1.1.0.
- [EGovG] Bundesgesetzblatt der Republik Österreich, ausgegeben am 27. Februar 2007, Bundesgesetz, mit dem ein E-Government-Gesetz erlassen wird sowie das Allgemeine Verwaltungsverfahrensgesetz 1991, das Zustellgesetz, das Gebührengesetz 1957, das Meldegesetz 1991 und das Vereinsgesetz 2002 geändert werden. Abgerufen am 23.07.2007 unter <http://www.cio.gv.at/egovernment/law/>
- [ 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 14. 05. 2004 unter <http://www.ietf.org/rfc/rfc2119.txt>.