

Elektronische Zustellung Push Protokoll		Konvention
		zusepush-1.4.1
		Empfehlung
Kurzbeschreibung	Diese Spezifikation beschreibt das PUSH Protokoll für Zustelldienste zur Übermittlung von neuen LDAP Empfänger Einträgen bzw. deren Änderung/Löschung am Zustellkopf.	
Autor(en):	Arne Tauber	Projektteam / Arbeitsgruppe:
		AG-ZUSE / AG-II
Beiträge von:	Thomas Rössler, Peter Reichstädter	

Version 1.4.0 : **02.02.2012**

Fristablauf: --.--.----

Abgelehnt von:

(Länderangabe bei ablehnender Stellungnahme)

Unter-Version 1.4.1 : **05.07.2016**

Fristablauf: --.--.----

Abgelehnt von:

(Länderangabe bei ablehnender Stellungnahme)

Detail-Version ... : **TT.MM.JJJJ**

Fristablauf: **TT.MM.JJJJ**

Anmerkungen:

(Detailangaben zur Freigabe)

Inhaltsverzeichnis

1. Einleitung	3
2. Prozessbeschreibung	4
3. Protokoll.....	5
3.1. Zeitpunkt der zu übermittelnden Daten	5
3.2. Kommunikation	5
3.3. Request	5
3.3.1. Content-Type	5
3.3.2. Content-Length	5
3.3.3. Encoding	5
3.3.4. HTTP Body.....	5
3.3.5. LDIF Content.....	5
3.4. Response.....	6
3.4.1. Erfolgsfall (Success)	6
3.4.2. Fehlerfall (Error)	6
4. Auszuführende Operationen des Zustellkopfes	8
4.1. TLS Clientauthentifizierung	8
4.2. Zugriffsrechte	8
4.3. Reservierte Attribute	8
4.4. Abgleich mit dem Zentralen Melderegister	8
4.4.1. Neuregistrierung bzw. Änderung des Namens	9
4.4.2. Neuregistrierung bzw. Änderung der Abgabestelle	9
5. Anhang A	10
5.1. Beispiel LDIF HTTP POST (Request)	10
5.2. Antwort (PushResponse)	10
5.2.1. Allgemeiner Fehler.....	10
5.2.2. Fehler beim Ändern einzelner Einträge	10
A. Abbildungsverzeichnis	11
B. Tabellenverzeichnis	12
C. Revision History	13
D. Referenzen	14

1. Einleitung

Das Zustellgesetz [ZUSTG] definiert in § 29 Abs. 1 die Leistungen von elektronischen Zustelldiensten, die auch die Weiterleitung der in § 33 Abs. 1 definierten Daten sowie die Kommunikation der Änderungen derer bzw. der Abwesenheiten an den Zustellkopf inkludieren. Das Zustellgesetz definiert diese Leistungen bzw. die zu übermittelnden Daten wie folgt:

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 Satz an den Ermittlungs- Zustelldienst;

[...]

An- und Abmeldung

§ 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,
6. Angaben des Kunden darüber, welche Formate die zuzustellenden Dokumente aufweisen müssen, damit er zu ihrer Annahme bereit ist, und
7. Angaben des Kunden, die für eine allfällige inhaltliche Verschlüsselung der zuzustellenden Dokumente erforderlich sind.

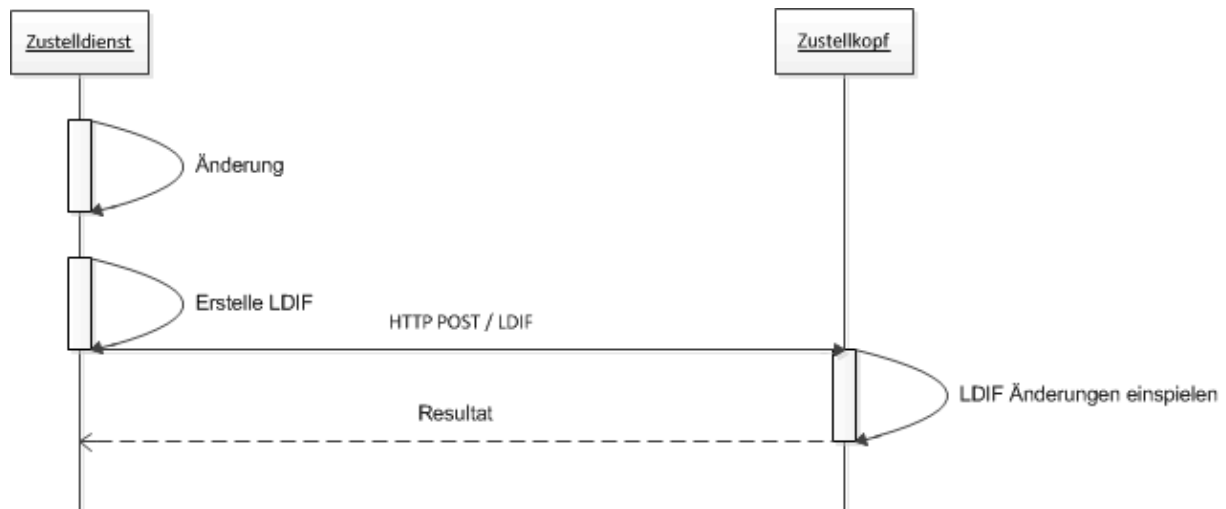
[...]

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. Prozessbeschreibung

Der Prozessablauf des PUSH Protokolls ist in nachfolgender Abbildung skizziert:

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 allen Änderungen betroffener Objekte im DIT (Directory Information Tree) im Vergleich zum Zeitpunkt der letzten Synchronisation mit dem Zustellkopf. Die Baumstruktur muss der LDAP Spezifikation entsprechen (siehe [ZUSELDAP]).

Der Zustelldienst authentifiziert sich mittels SSL Client-Zertifikat am Zustellkopf und übermittelt via HTTP POST die LDIF Datei. Anschließend aktualisiert der Zustellkopf anhand der LDIF Datei den aktuellen Datenbestand und gibt für Änderungsoperation einen entsprechenden Rückgabewert (Erfolg, Fehler, etc.) an den Zustelldienst zurück. Kann der Rückgabewert nicht an den Zustelldienst übermittelt werden, so wird die durchgeführte Aktualisierung wieder rückgängig gemacht. Zustelldienste müssen die Änderungsdatei solange erneut an den Zustellkopf übermitteln, bis eine entsprechende Statusmeldung retourniert wird.

3. Protokoll

Dieser Abschnitt beschreibt die wesentlichen Aspekte des PUSH Transport- sowie Datenprotokolls.

3.1. Zeitpunkt der zu übermittelnden Daten

Gemäß Zustellgesetz § 29 Abs. 1 Z 1 müssen jegliche Änderungen unverzüglich übermittelt werden. Im Sinne einer technischen Durchführbarkeit wird eine Frist von 5 Minuten definiert, innerhalb welcher Änderungen an den Stammdaten übermittelt werden müssen.

3.2. Kommunikation

Die Kommunikation zwischen Zustelldienst und Zustellkopf basiert auf HTTPs POST mit TLS-Client-Authentifizierung seitens des Zustelldienstes. Die Verwendung von TLS mit dem Stand der Technik entsprechenden Sicherheitsalgorithmen wird vorausgesetzt. Niedrigere SSL Versionen dürfen nicht verwendet werden.

3.3. Request

Dieser Abschnitt beschreibt die Eigenschaften des HTTPs POST Requests, sowie des LDIF Formats, das die Änderungen der Stammdaten beschreibt.

3.3.1. Content-Type

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

3.3.2. Content-Length

Der Content-Length HTTP Header muss gesetzt sein.

3.3.3. Encoding

Der Requests muss in ISO-8859-1 (Latin-1, siehe [ISO-8859-1]) oder ISO-8859-15 (Latin-9, siehe [ISO-8859-15]) kodiert erfolgen. Die entsprechende „charset“ Anweisung muss in den HTTP Headern gesetzt sein.

3.3.4. HTTP Body

Der HTTP Body des POST Requests muss ausschließlich 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 eine LDIF Datei eine Reihe von Verzeichniseinträgen oder eine Reihe von Änderungen an Verzeichniseinträgen (LDIF Request). Die LDIF Datei kann jedoch nur ein Format beinhalten (siehe [LDIF]).

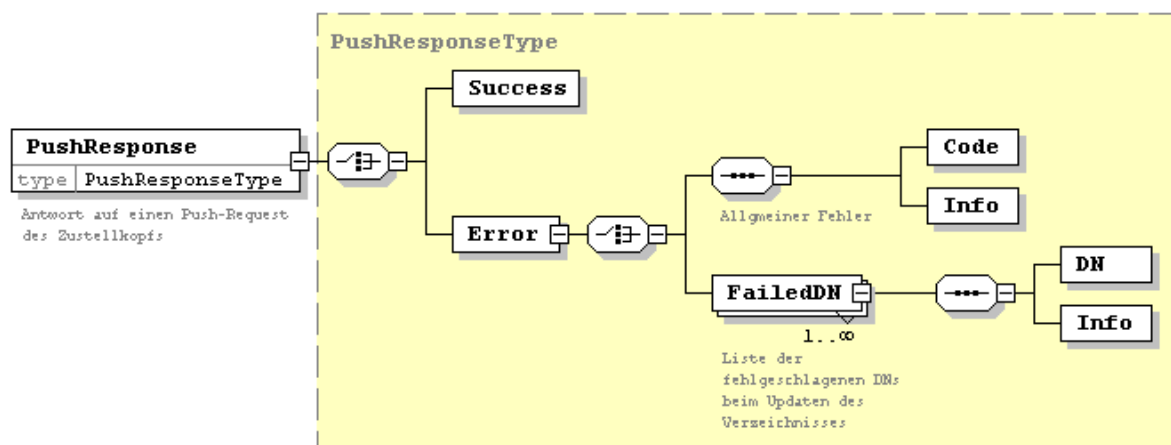
Der HTTP POST Request des PUSH Protokolls muss eine LDIF Änderungsdatei beinhalten (LDIF Request), andernfalls muss eine entsprechende Fehlermeldung zurückgegeben werden. Da für die Übermittlung von Stammdaten eine Zeitspanne von 5 Minuten erlaubt ist, kann die LDIF Datei Änderungsanweisungen für mehrere Einträge beinhalten.

Beispiele für Push Protokoll Requests 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 der Response eingebettet.

Abbildung 2 - PushResponse Element



Das Schema ist in der Datei `zkopf.xsd` definiert und ist normativer Bestandteil dieser Spezifikation.

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 nicht erfolgreich.

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.

Die nachfolgende Tabelle zeigt einen Überblick bzw. eine detaillierte Liste der Fehlermeldungen, die während der Verarbeitung des Requests auftreten können.

Tabelle 1 - Fehlerklassen

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

Tabelle 2 - Fehlercodes

Fehlercode	Beschreibung
1001	Client ist nicht berechtigt. 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(5) fehlt oder das Character Encoding ist nicht auf ISO-8859-1(5) 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. Auszuführende Operationen des Zustellkopfes

Der Zustellkopf muss grundsätzlich die Push-Anfragen von Zustelldiensten unverändert in den eigenen LDAP Verzeichnisdienst übernehmen. Dabei ist sowohl zu beachten, dass ein Zustelldienst nur Operationen in seinem jeweiligen Teilbaum ausführen darf und des Weiteren muss für jede Neuregistrierung bzw. Änderung von gewissen Stammdaten ein Abgleich mit dem ZMR durchgeführt werden. Diese durchzuführenden Operationen werden nachfolgend kurz erläutert.

4.1. TLS Clientauthentifizierung

Zustelldienste dürfen den PUSH Dienst des Zustellkopfs nur über eine gesicherte TLS Clientauthentifizierung nutzen. Die Verwaltung des Zertifikatsmanagements obliegt dem Zustellkopf. Bspw. könnten Zustelldienste das verwendete Zertifikat dem Zustellkopf übermitteln, welcher dieses dann explizit freischaltet. Alternativ kann der Zustellkopf in geeigneter Weise auch eigene Clientzertifikate den Zustelldiensten zur Verfügung stellen.

4.2. Zugriffsrechte

Der Zustellkopf muss für jeden einzelnen LDAP Verzeichniseintrag innerhalb des Push-Requests überprüfen, ob dieser Eintrag Teil des Unterbaums des jeweiligen Zustelldienstes ist. Ist dies nicht der Fall, so muss für den betreffenden Eintrag ein Fehler mit dem Code 1001 retourniert werden.

Beispiel: Zustelldienst Musterdienst mit Kürzel „md“ im DIT des Zustellkopfes

DN im Push-Request: `gvZbPK=3gT5FC..,ou=gvNatPerson,o=bka,dc=at`

Der Zustellkopf muss überprüfen, ob der Organisationseintrag (`o=..`) mit dem im Zustellkopf registrierten Kürzel des „pushenden“ Zustelldienstes übereinstimmt. In diesem Beispiel stimmt „md“ nicht mit „bka“ überein und somit muss der Änderungsversuch mit dem Fehlercode 1001 quittiert werden.

4.3. Reservierte Attribute

Die beiden LDAP Attribute `gvCRRCheckBirthdate` und `gvCRRCheckAddress` (siehe [ZUSELDAP]) sind reserviert und ausschließlich dem Zustellkopf vorbehalten und dürfen von Zustelldiensten weder erstellt, gelöscht noch modifiziert werden.

4.4. Abgleich mit dem Zentralen Melderegister

Ist der Typ eines Änderungseintrags (`changetype:`) `add` oder `modify` und betrifft dieser eine natürliche Person, so muss der Zustellkopf abhängig vom jeweiligen Typ und den betreffenden Stammdaten eine ZMR Abfrage [ZMR-Schnittstelle] für die betreffende Person machen.

4.4.1. Neuregistrierung bzw. Änderung des Namens

Ist der Typ des Änderungseintrags „add“ oder „modify“ und enthält der Änderungseintrag einen neuen bzw. geänderten Namen, so muss folgender ZMR (Zentrales Melderegister) Basischeck durchgeführt werden:

Erster (Doppel-)Vorname (*)+ Familienname/Nachname + Geburtsdatum

z.B. im Falle von Hans-Peter Michael Müller, geb. am 20.03.1965, müsste folgende Abfrage durchgeführt werden: Hans-Peter* + Müller + 1965-03-20.

Ist die ZMR Abfrage eindeutig, so muss der Wert des LDAP Attributs „gvCRRCheckBirthdate“ auf den Wert TRUE gesetzt werden, andernfalls auf FALSE.

4.4.2. Neuregistrierung bzw. Änderung der Abgabestelle

Ist der Typ des Änderungseintrags „add“ oder „modify“ und enthält der Änderungseintrag eine neue bzw. geänderte Abgabestelle, so muss folgender ZMR Basischeck durchgeführt werden:

Erster (Doppel-)Vorname (*) + Familienname/Nachname + Abgabestelle

z.B. im Falle von Hans-Peter Michael Müller, wohnhaft in Musterstrasse 1, 1010 Wien, müsste folgende Abfrage durchgeführt werden: Hans-Peter* + Müller + Musterstrasse 1 + 1010 + Wien.

Ist die ZMR Abfrage eindeutig, so muss der Wert des LDAP Attributs „gvCRRCheckAddress“ auf den Wert TRUE gesetzt werden, andernfalls auf FALSE.

Notation: die Wildcard (*) kennzeichnet beliebige weitere Vornamen. Besteht der Vorname des LDAP Eintrags aus mehreren Vornamen (z.B. Hans Peter; Hans-Peter ist als ein Vorname zu sehen), so ist die Abfrage am ZMR nur mit dem ersten Vornamen und einer zusätzlichen Wildcard zu stellen.

5. Anhang A

5.1. Beispiel LDIF HTTP POST (Request)

Das folgende Beispiel zeigt einen HTTP POST inklusive LDIF Änderungsdatei, welche für eine natürliche Person, die mit der Zustell-bPK aRta8sZRiOVK0mtb8FLbparv43w= am Zustelldienst „bka“ registriert ist, 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=aRta8sZRiOVK0mtb8FLbparv43w\=,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=
aRta8sZRiOVK0mtb8FLbparv43w\=,ou=NatPers,o=bka,dc=at</DN>
      <Info>Eintrag nicht gefunden.</Info>
    </FailedDN>
    <FailedDN>
      <DN>gvZbPK=
aRta8sZRiOVK0mtb8FLbparv43w\=,ou=NatPers,o=bmi,dc=at</DN>
      <Info>LDAP Attribut gvBirthDate besitzt ungültiges
Format.</Info>
    </FailedDN>
  </Error>
</PushResponse>
```

A. Abbildungsverzeichnis

Abbildung 1 - Modell des Push Protokolls.....	4
Abbildung 2 - PushResponse Element	6

B. Tabellenverzeichnis

Tabelle 1 - Fehlerklassen	7
Tabelle 2 - Fehlercodes.....	7

C. Revision History

Version	Datum	Autor(en)	
1.3.0	30.4.2008	Arne Tauber (EGIZ)	Initialversion
1.3.2	06.05.2010	Arne Tauber (EGIZ) Peter Reichstädter (BKA)	<p>editorielle Korrekturen sowie sprachliche Klarstellungen und Detaillierungen von Elementen:</p> <p>2 Prozess</p> <p>3 Protokoll</p> <p>5 Anhang</p> <p>3.1. detailliert</p> <p>4 neu hinzugefügt (bedingt durch praktische Erfahrung des Betriebes des Zustellkopfs bzw. der Notwendigkeit der Eindeutigkeit eines registrierten users (ZMR-Basischeck) bzw. Neuregistrierung und Änderung eines Namens bzw. Abgabestelle</p>
1.4.0	24.01.2012	Arne Tauber (EGIZ)	<p>ISO-8859-15 Kodierung hinzugefügt</p> <p>Textuelle sowie inhaltliche Korrekturen</p>
1.4.1	20.08.2012	Arne Tauber (EGIZ)	Anpassung Versionsnummer an ZUSE-Suite 1.4.1

D. Referenzen

[LDIF]	G. Good, RFC2849, The LDAP Data Interchange Format (LDIF) – Technical Specification
[ZUSELDAP]	A. Tauber, P. Reichstädter, Zustellverzeichnis – LDAP Schema-Beschreibung, 1.4.0
[ISO-8859-1]	ISO/IEC 8859-1:1998, Information technology -- 8-bit single-byte coded graphic character sets -- Part 1: Latin alphabet No. 1
[ISO-8859-15]	ISO/IEC 8859-15:1999, Information technology -- 8-bit single-byte coded graphic character sets -- Part 15: Latin alphabet No. 9
[ZUSTG]	Bundesgesetz, mit dem das Einführungsgesetz zu den Verwaltungsverfahrensgesetzen 1991, das Allgemeine Verwaltungsverfahrensgesetz 1991, das Verwaltungsstrafgesetz 1991 und das Zustellgesetz geändert werden (Verwaltungsverfahrens- und Zustellrechtsänderungsgesetz 2007), BGBl. Nr. 5/2008.
[ZMR-Schnittstelle]	http://zmr.bmi.gv.at/pages/home.htm