



Zustellkopf - Prototyp

Dokumentation

Version 0.1.0, 20.09.2007

DI Arne Tauber – arne.tauber@egiz.gv.at

Zusammenfassung:

Dieses Dokument beschreibt die Implementierung eines Zustellkopfes, der sowohl ein zentrales Verzeichnis mit allen Empfängerinformationen und dessen Aktualisierung gemäß Zustellgesetz nach dem Push Protokoll [ZKOPF-PUSH], sowie die standardmäßigen Dienste der Adressierbarkeitsabfragen gemäß [ZKOPF-SPEC] umsetzt.

Inhaltsverzeichnis:

1	Einleitung	5
1.1	Schlüsselwörter	5
1.2	Geschlechtsspezifische Bezeichnungen	5
2	Anwendungsbeschreibung	6
2.1	Query und Ping Dienst	6
2.2	BulkQuery	7
2.3	Push Dienst	7
2.4	LDAPv3 Server	7
3	Logging	9
3.1	Technisches Logging	9
3.2	Zugriffslogging	9
3.3	Performance Logging	9
3.4	Transaktions-ID	9
4	Installation / Konfiguration	10
4.1	Systemanforderungen	10
4.1.1	Server-Komponenten	10
4.2	Installation	10
4.2.1	Application Server	10
4.2.2	OpenLDAP Server	10
4.3	Konfiguration	11
4.3.1	Konfigurationsdatei einer Zustellkopf-Instanz	11
4.3.2	Log4j Konfiguration	13

4.3.3	OpenLDAP Konfiguration	14
5	Anhang A	15
5.1	Beispielkonfiguration	15
5.2	Deployment Descriptor für Push Service	16
5.2.1	Deployment Descriptor für Query Services.....	16
6	Referenzen.....	18

Abbildungen

Abbildung 1: Modell des Zustellkopfs	6
Abbildung 2: Baumstruktur des LDAP Verzeichnisses.....	8

Revision History

Version	Datum	Autor(en)	Anmerkung
0.0.1	18.09.2007	Arne Tauber (EGIZ)	Erstellt.
0.1.0	20.09.2007	Arne Tauber (EGIZ)	Logging Sektion hinzugefügt.

1 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;

Dieses Dokument beschreibt die Implementierung eines Zustellkopfes, der sowohl ein zentrales Verzeichnis mit allen Empfängerinformationen und dessen Aktualisierung gemäß Zustellgesetz nach dem Push Protokoll [ZKOPF-PUSH], sowie die standardmäßigen Dienste der Adressierbarkeitsabfragen gemäß [ZKOPF-SPEC] umsetzt.

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 Anwendungsbeschreibung

Das Modell des Prototyps des Zustellkopfs ist in folgender Abbildung dargestellt:

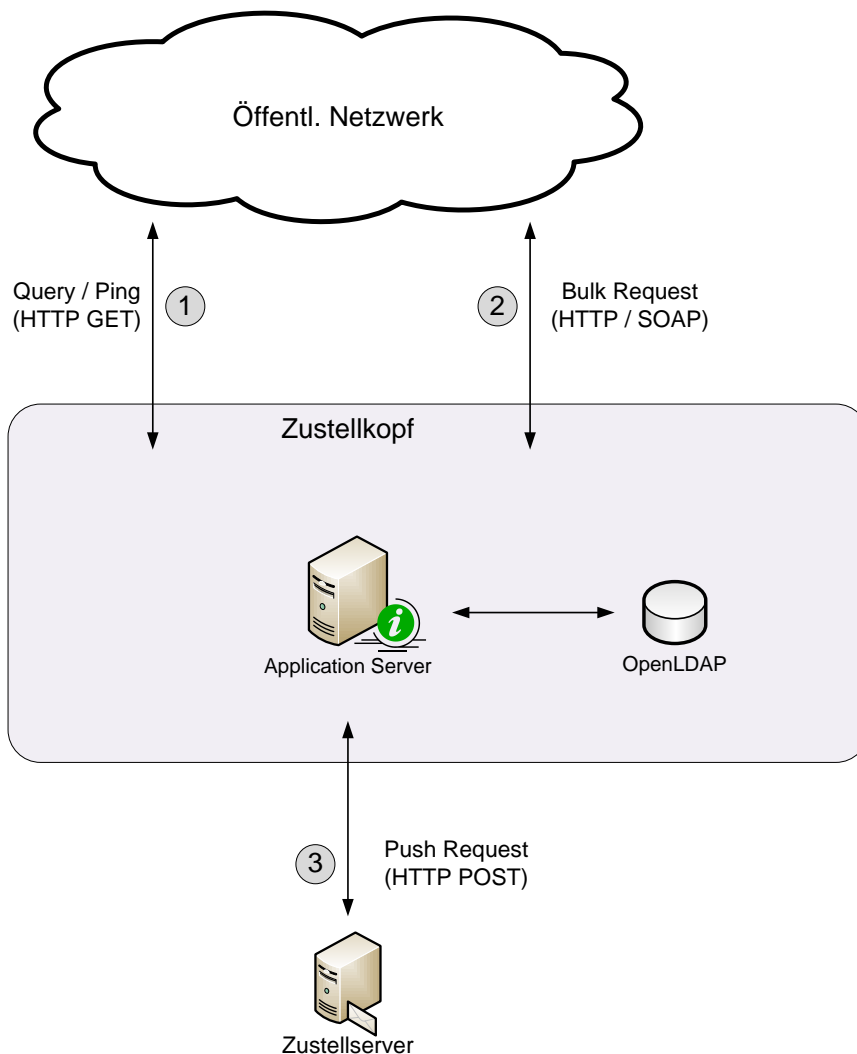


Abbildung 1: Modell des Zustellkopfs

Der Zustellkopf verfügt über insgesamt drei Schnittstellen nach aussen:

1. Query/Ping: diese sind die Dienste zur Standard Anfrage für eine einzelne Personenabfrage gemäß [ZKOPF-SPEC].
2. BulkQuery: dieser Dienst erlaubt Anfragen für mehreren Datensätzen (Bulk-Abfrage).
3. PushService: dieser Dienst ist nur registrierten Zustelldiensten zugänglich und ermöglicht das Aktualisieren der zentralen Verzeichnisinformationen des LDAP Servers.

Als zentrales Verzeichnis dient ein frei verfügbarer OpenLDAP Server.

2.1 Query und Ping Dienst

Der Query und Ping Dienst sind gemäß Spezifikation [ZKOPF-SPEC] via HTTP bzw. HTTPs GET Request zugänglich. Je nach Anforderung kann dieser Zugang auch nur auf HTTPs mit Überprüfung der Verwaltungs- bzw. Dienstleistereigenschaft beschränkt werden.

Beide Dienste sind als HTTP-Servlet gemäß der Spezifikation 2.5 [Servlet-SPEC] implementiert und überprüfen die angegebenen HTTP GET Parameter auf Konsistenz und Richtigkeit. Eine Verwendung von illegalen Zeichen innerhalb der HTTP Parameter ist nicht gültig und führt zu einem Fehler. Da die HTTP Parameter für die Suche innerhalb des LDAP Servers verwendet werden (bspw. `cn oä.`), können Zeichen wie `*`, `(`, `)`, `&` oder `|`, die Kommandoparameter eines LDAP Filter Strings sind, zu einer LDAP Injection Attacke führen.

2.2 BulkQuery

Der BulkQuery Dienst ist gemäß Spezifikation [ZKOPF-SPEC] via HTTP bzw. HTTPs POST Request zugänglich. Je nach Anforderung kann dieser Zugang auch nur auf HTTPs mit Überprüfung der Verwaltungs- bzw. Dienstleistungseigenschaft beschränkt werden.

Der Request wird mittels SOAP [SOAP] übermittelt. Als SOAP Software kommt Apache Axis [Apache-AXIS] zum Einsatz. Alle Parameter werden auf Konsistenz und Richtigkeit geprüft. Eine Verwendung von illegalen Zeichen innerhalb der Parameter ist nicht gültig und führt zu einem Fehler. Da die Parameter für die Suche innerhalb des LDAP Servers verwendet werden (bspw. `cn oä.`), können Zeichen wie `*`, `(`, `)`, `&` oder `|`, die Kommandoparameter eines LDAP Filter Strings sind, zu einer LDAP Injection Attacke führen.

Weiters ist es möglich, die Anzahl der in einer Bulk Anfrage auftretenden Query Element über die Konfigurationsdatei zu beschränken.

2.3 Push Dienst

Der Push Dienst ist gemäß Spezifikation [ZKOPF-PUSH] via HTTPs mit Client Authentifizierung zugänglich. Für die Beschränkung der zulässigen Zertifikate ist der Application Server verantwortlich.

Die zulässigen Zustelldienste werden anhand ihres Client Zertifikats identifiziert und müssen in der Konfigurationsdatei mit dem entsprechenden Organisationskürzel und den dazugehörigen Client-Zertifikatsdaten registriert werden. Dieses Organisationskürzel findet sich auch im DN der LDAP Einträge des entsprechenden Zustellervers wieder.

Beispiel:

```
dn: gvZbPK=uTvh8sZRiOVK0mtb8FLbparv43w\=,ou=gvNatPerson,o=egiz,dc=at
```

In diesem Beispiel ist ein LDAP Eintrag einer natürlichen dargestellt, der im LDAP Baumteil des E-Government Innovationszentrums (egiz) liegt. Ein Zustellserver, der sich mit einem bestimmten Clientzertifikat authentifiziert, kann somit a priori nur einen bestimmten Baumteil des LDAP Verzeichnisses durch LDIF Push Anweisungen verändern. Die Teilbäume anderer Zustellserver sind somit nicht zugänglich.

2.4 LDAPv3 Server

Als LDAP Server für das zentrale Verzeichnis aller Empfängerdaten wurde im Testbetrieb ein OpenLDAP Server verwendet. Es kann aber auch jeder beliebige andere LDAP Server verwendet werden, der die Version 3 des LDAP Protokolls unterstützt.

Die Baumstruktur des LDAP Verzeichnisses sieht wie folgt aus:

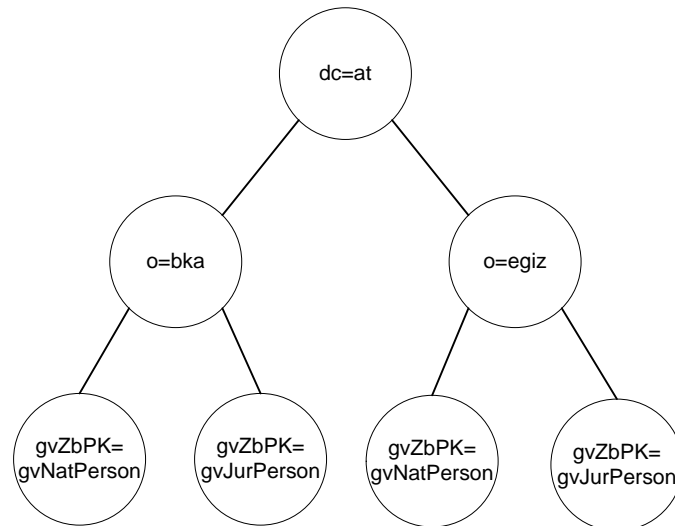


Abbildung 2: Baumstruktur des LDAP Verzeichnisses

Der LDAP Server muss lediglich mit dem Base Distinguished Name (BaseDN) `dc=at` vorkonfiguriert werden. Der Zugang zum LDAP Server mit Schreibrechten muss in der Konfiguration des Zustellkopfs eingetragen werden.

Die Basisverzeichnisstruktur der einzelnen Zustellservers (hier bspw. `bka` bzw. `egiz`) wird automatisch vom Zustellkopf bei einem Fehlen der Einträge erstellt. Somit müssen die einzelnen Teilbäume der Zustellservers nicht manuell erstellt werden.

Jeder Betreiber eines Zustellservers hat somit die Möglichkeit, via Push Protokoll seinen Teilbaum entsprechend zu aktualisieren. Dies geschieht mittels dem Push Dienst.

3 Logging

Der Zustellkopf unterstützt drei Logging Typen und basiert auf dem Logging Framework Log4J [Log4J].

Es wird empfohlen für alle Logging Typen eine eigene Ausgabedatei zu definieren.

3.1 Technisches Logging

Der technische Log dokumentiert die Prozessabläufe und gibt technische Meldungen aus. Der Präfix des entsprechenden Log4J Loggers ist „at.gv.egiz.zkopf.log.TechnicalLogger“. Dieser muss auch so in der Log4J Konfigurationsdatei definiert werden.

3.2 Zugriffslogging

Der Zugriffslog dokumentiert den Zugriff auf den Zustellkopf und dokumentiert folgende Operationen:

1. Zugriffsdaten wie IP-Adresse/Hostname und Port des Clients
2. Session-ID
3. SSL Clientzertifikatsdaten wie Issuename und Seriennummer des Zertifikats
4. Typ des Clientzertifikats (Verwaltungs- oder Dienstleistereigenschaft) im Falle einer zwinglich erforderlichen OID im Clientzertifikat (über Konfiguration einstellbar)

Der Präfix des entsprechenden Log4J Loggers ist „at.gv.egiz.zkopf.log.AccessLogger“. Dieser muss auch so in der Log4J Konfigurationsdatei definiert werden.

3.3 Performance Logging

Der Performance Log dient zur Performanceanalyse des Zustellkopfs und dokumentiert die Dauer von bestimmten Operation. Es wird empfohlen diesen Log nur im Falle der Performanceanalyse zu aktivieren.

Der Präfix des entsprechenden Log4J Loggers ist „at.gv.egiz.zkopf.log.PerformanceLogger“. Dieser muss auch so in der Log4J Konfigurationsdatei definiert werden.

3.4 Transaktions-ID

Für jede Zugriffssession auf den Zustellkopf wird eine eigene Transaktions-ID erstellt, die auch in den Protokolldateien aufscheint. Somit können alle Protokolleinträge genau dem jeweiligen Client zugeordnet werden.

4 Installation / Konfiguration

4.1 Systemanforderungen

Es gelten folgende Anforderungen an die Installationsplattform bzw. an die Client-komponenten (die angegebenen Versionen entsprechen der getesteten Umgebung):

4.1.1 Server-Komponenten

- JDK 1.6
- Application Server (getestet mit Tomcat 6.0)
- LDAPv3 Server (getestet mit OpenLDAP 2.2.29)

4.2 Installation

4.2.1 Application Server

Im Package ist die Datei zkopf.war enthalten. Dieses Webarchiv kann automatisch in allen gängigen Application Servern installiert werden, vorausgesetzt, der Application Server wird mit einer JDK 1.6 betrieben.

Der Zustellkopf selbst wurde mit Tomcat 6.0 [TOMCAT] mit dem JDK 1.6 getestet.

Es wird empfohlen, unterschiedliche Application Server Instanzen für die Abfragedienste (Query/Ping/Bulk) sowie für den Pushdienst aufzusetzen. Dies garantiert eine unabhängige Konfiguration der SSL Clientauthentifizierung für den Pushdienst. Für jede Instanz muss entsprechend die Webapplikations Deployment Descriptor Datei (web.xml) entsprechende angepasst werden. Nähere Informationen dazu sind im Abschnitt Konfiguration verfügbar.

4.2.2 OpenLDAP Server

Der Zustellkopf wurde mit OpenLDAP 2.2.29 getestet und kann problemlos mit dem frei verfügbaren OpenLDAP Server betrieben werden. Es eignet sich jedoch auch jeder andere LDAP Server, der die Protokollversion 3 unterstützt.

Der OpenLDAP Server kann via <http://www.openldap.org/software/download/> runtergeladen werden. Diese laufen jedoch nur unter einem Unix Betriebssystem oder Derivat (z.B. Linux). Verschiedene Linux Distributionen ermöglichen auch die automatische Installation via Packages (z.B. Debian, Redhat, Ubuntu usw.).

Einen Port für Windows Betriebssysteme stellt Lucas Bergmann auf seiner Website [OpenLDAP-Win32] zur Verfügung. Für diese Version ist jedoch kein einwandfreier Betrieb garantiert. Daher wird empfohlen, den OpenLDAP Server auf einem Unix Betriebssystem bzw. einem Derivat davon (z.B. Linux, Solaris etc.) zu installieren und zu betreiben.

Für die Inbetriebnahme des OpenLDAP Servers müssen die zwei Schemadateien `gvNatPerson.schema` und `gvJurPerson.schema` in das `schema` Verzeichnis des OpenLDAP Servers kopiert werden. Diese beiden Dateien werden für die Schemadefinitionen von Empfängerinformationen von natürlichen und juristischen Personen benötigt.

Falls ein anderer LDAP Server als OpenLDAP verwendet wird, so müssen die Schemadateien für den jeweiligen Server neu erstellt werden. Im Installationspackage sind nur die Schemadateien für den OpenLDAP Server inkludiert.

4.3 Konfiguration

Für die Inbetriebnahme einer Zustellkopf-Instanz muss eine Konfigurationsdatei angegeben werden. Es gibt 2 Möglichkeiten diese einzubinden:

1. Die Datei muss „zkopf_config.xml“ benannt werden und in den Classpath gegeben werden (z.B. WEB-INF/classes Verzeichnis).
2. Es wird die Systemvariable „zkopf.configuration“ gesetzt. Der Inhalt dieser Variable muss eine Pfadname sein, der auf die Konfigurationsdatei zeigt.

Anmerkung: Es wird Methode 2 empfohlen, da bei einem Update z.B. der gesamte Webcontainer gelöscht und durch das neue war-File ersetzt werden kann, ohne dabei die Konfigurationsdatei zu löschen.

4.3.1 Konfigurationsdatei einer Zustellkopf-Instanz

Die hier angeführten Parameter sind unbedingt vor Inbetriebnahme der Anwendung anzupassen und stellen somit eine Minimalkonfiguration dar.

General

Allgemeine Einstellungen

Property	Default-Wert	Beschreibung
pk.file	n/a	Absoluter Pfad zum Private Key des Zustellkopfs. Mit diesem Schlüssel kann der Zustellkopf Fremd-bPKs entschlüsseln.
check.oid	false	Überprüfen einer vorhandenen Verwaltungs- oder Dienstleistereigenschaft bei SSL Client-Authentifizierung. Ist dieser Wert auf true gesetzt, so wird bei vorhandener Client-Authentifizierung das verwendete Zertifikat auf eine vorhanden Verwaltungs- oder Dienstleistereigenschaft geprüft. [VerwEig].

bulk

Einstellungen des Auskunftsdienstes für Bulk Abfragen

Property	Default-Wert	Beschreibung
max.queries	100	Gibt die maximale Anzahl von Query Elementen innerhalb einer Bulkabfrage an.

ldap

Einstellungen für den LDAP Server, der als zentrales Verzeichnis aller Empfängerdaten dient.

Property	Default-Wert	Beschreibung
host	localhost	Hostname oder IP-Adresse des LDAP Servers
port	389	Portnummer des LDAP Servers.
base.dn	n/a	Base Distinguished Name.
login.dn	n/a	Login Name für den Zugriff auf den LDAP Server.
login.password	n/a	Login Passwort für den Zugriff auf den LDAP Server
version	3	Verwendete LDAP Version – sollte nicht geändert werden.

provider

Einstellungen zu Zustellserver Betreibern, die via Pushdienst Änderungsdaten in den LDAP Server einspielen können. Für jeden Betreiber muss eine eigene Kategorie (category) mit dem entsprechenden Providerkürzel angegeben werden. Dieses Providerkürzel muss eindeutig sein und entspricht dem Organisationsteil (o=providername) für jeden DN Eintrag im LDAP Server.

Property	Default-Wert	Beschreibung
auth.issuer.dn	n/a	Issuer-DN des Ausstellerzertifikats für Client-Authentifizierung am Push Dienst.
auth.serial	n/a	Seriennummer des Zertifikats für Client-Authentifizierung am Push Dienst.
service.url	n/a	URL zum Webservice des Zustelldienstbetreibers für die Anlieferung von Zustellstücken.

test

Einstellungen für die Tests der Zustellkopf Applikation. Für jeden Betreiber muss eine eigene Kategorie (category) mit den Einstellungen für die Authentifizierung am Pushdienst angegeben werden.

Property	Default-Wert	Beschreibung
push.service.url	n/a	URL zum Pushdienst für die Tests.
query.service.url	n/a	URL zum Standardauskunftsservice für einzelne Personenabfragen für die Tests.
bulk.service.url	n/a	URL zum Bulk Auskunftsservice für die Tests.

client.ks.file	n/a	Absoluter Pfad zum Keystore für die Clientauthentifizierung am Pushdienst.
client.ks.pw	n/a	Password des Keystores für die Clientauthentifizierung am Pushdienst.
client.ks.type	n/a	Typ des Keystores für die Clientauthentifizierung am Pushdienst. Kann JKS oder PKCS#12 sein.

4.3.2 Log4j Konfiguration

Die Log4j Konfigurationsdatei (`log4j.properties`) kann auf zwei Arten referenziert werden. Entweder befindet sich die Datei im Classpath der Webapplikation (`WEB-INF/classes` Verzeichnis) oder es wird die Systemvariable `log4j.configuration` der JVM auf den Pfad der Log4j Konfigurationsdatei gesetzt (`-Dlog4j.configuration=/container/...`).

Da es drei Arten von Loggern gibt (Performance-, Access- und technischer Log) sieht eine Beispielkonfigurationsdatei von Log4j wie folgt aus:

```
# commons-logging setup
org.apache.commons.logging.LogFactory=org.apache.commons.logging.impl.Log4j
Factory

# define log4j root loggers
log4j.rootLogger=warn, stdout
log4j.logger.at.gv.egiz.zkopf.log.PerformanceLogger=debug, PERFORMANCE
log4j.logger.at.gv.egiz.zkopf.log.AccessLogger=debug, ACCESS
log4j.logger.at.gv.egiz.zkopf.log.TechnicalLogger=debug, TECHNICAL

# configure the stdout appender
log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.appender.stdout.layout.ConversionPattern=%5p | %d{dd HH:mm:ss} | %20c
| %m%n

# performance logger
log4j.appender.PERFORMANCE=org.apache.log4j.RollingFileAppender
log4j.appender.PERFORMANCE.File=/container/tomcat-
zkopf/logs/performance.log
log4j.appender.PERFORMANCE.MaxFileSize=10000KB
log4j.appender.PERFORMANCE.MaxBackupIndex=9999
log4j.appender.PERFORMANCE.layout=org.apache.log4j.PatternLayout
log4j.appender.PERFORMANCE.layout.ConversionPattern=%5p | %d{dd
HH:mm:ss,SSS} | %t | %m%n

# access logger
log4j.appender.ACCESS=org.apache.log4j.RollingFileAppender
log4j.appender.ACCESS.File=/container/tomcat-zkopf/logs/access.log
log4j.appender.ACCESS.MaxFileSize=10000KB
log4j.appender.ACCESS.MaxBackupIndex=9999
log4j.appender.ACCESS.layout=org.apache.log4j.PatternLayout
log4j.appender.ACCESS.layout.ConversionPattern=%5p | %d{dd HH:mm:ss,SSS} |
%t | %m%n
```

```
# technical logger
log4j.appender.TECHNICAL=org.apache.log4j.RollingFileAppender
log4j.appender.TECHNICAL.File=/container/tomcat-zkopf/logs/technical.log
log4j.appender.TECHNICAL.MaxFileSize=10000KB
log4j.appender.TECHNICAL.MaxBackupIndex=9999
log4j.appender.TECHNICAL.layout=org.apache.log4j.PatternLayout
log4j.appender.TECHNICAL.layout.ConversionPattern=%5p | %d{dd HH:mm:ss,SSS}
| %t | %m%n
```

4.3.3 OpenLDAP Konfiguration

Die Konfiguration erfolgt gemäß dem OpenLDAP Administrator's Guide [OpenLDAP-Guide] durch Ändern der Einstellungen in der Datei `slapd.conf`.

Zuerst müssen die beiden installierten Schemadateien `gvNatPerson.schema` und `gvJurPerson.schema` in die Konfiguration inkludiert werden. Dies erfolgt über folgende Anweisungen:

```
include /etc/ldap/schema/gvNatPerson.schema
include /etc/ldap/schema/gvJurPerson.schema
```

Für den Test des Zustellkopfes wurde als Basis des LDAP Verzeichnisses eine Berkley Database (BDB) verwendet mit Indizierung. Die Indizierung bewirkt eine erhöhte Performance bei einer Suche mit bestimmten LDAP Attributen. Es wird empfohlen bei größeren Verzeichnissen (das auf den Zustellkopf zutrifft) die Indizierung von bestimmten LDAP Attributen zu aktivieren.

Die Beispielkonfiguration für den Test des Zustellkopfs ist wie folgt:

```
#####
# BDB database definitions
#####
database bdb
suffix "dc=at"
rootdn "cn=Manager,dc=at"
rootpw secret
directory /container/ldap-data
index
cn,gvSourcePIN,gvZbPK,gvBirthdate,sn,givenName,street,l,postalCode,c,mail,t
elephoneNumber pres,eq
index objectClass eq
```

Als Suffix muss auf jeden Fall `dc=at` gesetzt werden, da sonst der Betrieb des Zustellkopfs nicht gewährleistet ist.

Die Wahl der Authentifizierungscredentials für den Zugriff auf den OpenLDAP Server kann frei gewählt werden, muss jedoch in der Konfigurationsdatei des Zustellkopfs entsprechend angepasst werden.

In der obigen Beispielkonfiguration werden alle LDAP Attribute indiziert, nach denen der Zustellkopf potentiell sucht.

5 Anhang A

5.1 Beispielkonfiguration

```
<?xml version="1.0" encoding="UTF-8"?>
<properties>
  <!-- Allgemeine Einstellungen -->
  <category name="general">
    <!-- Absoluter Pfad zum Private Key des Zustellkopfs (Fremd-bPK Entschluesselung) -->
    <pk.file>/container/conf/certs/pk.der</pk.file>
    <!--
      Überprüfen einer vorhandenen Verwaltungs- oder Dienstleistereigenschaft bei
      SSL Client-Authentifizierung
    -->
    <check.oid>>false</check.oid>
  </category>
  <!-- Bulk Abfragen -->
  <category name="bulk">
    <!-- Gibt die maximale Anzahl von Query Elementen innerhalb einer Bulkabfrage an -->
    <max.queries>200</max.queries>
  </category>
  <!-- Zentrales LDAP Verzeichnis -->
  <category name="ldap">
    <host>localhost</host>
    <!-- Hostname oder IP-Adresse des LDAP Servers -->
    <port>389</port>
    <!-- Portnummer des LDAP Server -->
    <base.dn>dc=at</base.dn>
    <!-- Base Distinguished Name -->
    <login.dn>cn=Manager,dc=at</login.dn>
    <!-- Login Name für den Zugriff auf den LDAP Server -->
    <login.password>secret</login.password>
    <!-- Login Passwort für den Zugriff auf den LDAP Server -->
    <version>3</version>
    <!-- Verwendete LDAP Version - sollte nicht geändert werden -->
  </category>
  <!-- Zustellserver Betreiber -->
  <category name="provider">
    <!-- auth.issuer.dn - Issuer-DN des Ausstellerzertifikats für Client-
    Authentifizierung am Push Dienst -->
    <!-- auth.serial - Seriennummer des Zertifikats für Client-Authentifizierung am Push
    Dienst -->
    <!-- service.url - URL zum Webservice fuer die Anlieferung von Zustellstuecken -->
    <category name="bka">
      <auth.issuer.dn>CN=MOA Test CA Server,OU=EGIZ,O=TU Graz,C=AT</auth.issuer.dn>
      <auth.serial>0</auth.serial>
      <service.url>http://zustellung.gv.at/Zustellservice/</service.url>
    </category>
    <category name="plot">
      <auth.issuer.dn>CN=MOA Test CA Server,OU=EGIZ,O=TU Graz,C=AT</auth.issuer.dn>
      <auth.serial>1</auth.serial>
      <service.url>http://egov.plot.at/Zustellservice</service.url>
    </category>
    <category name="egiz">
      <auth.issuer.dn>CN=MOA Test CA Server,OU=EGIZ,O=TU Graz,C=AT</auth.issuer.dn>
      <auth.serial>3</auth.serial>
      <service.url>http://egiz.gv.at/Zustellservice/</service.url>
    </category>
  </category>
  <category name="test">
    <!-- URL zum Push Service -->
    <push.service.url>https://localhost:8443/zkopf/services/PushService</push.service.url>
    <!-- URL zum Query Service -->
    <query.service.url>http://localhost:8080/zkopf/Query</query.service.url>
    <!-- URL zum Bulk SOAP Service -->
    <bulk.service.url>http://localhost:8080/zkopf/services/BulkQuery</bulk.service.url>
    <!-- client.ks.file - Keystore fuer die Client Authentifizierung am Pushdienst -->
    <!-- client.ks.pw - Keystorepassword fuer die Client Authentifizierung am Pushdienst
    -->
    <!-- client.ks.type - Keystoretyp fuer die Client Authentifizierung am Pushdienst -->
    <category name="egiz">
      <client.ks.file>c:/eclipse/tomcats/ssl/localhost[pwd=server].keystore</client.ks.file>
      <client.ks.pw>server</client.ks.pw>
```

```
        <client.ks.type>JKS</client.ks.type>
    </category>
    <category name="bka">
        <client.ks.file>c:/eclipse/tomcats/ssl/customer1/moa-ssl-
kunde1[pwd=kunde1].p12</client.ks.file>
        <client.ks.pw>kunde1</client.ks.pw>
        <client.ks.type>PKCS12</client.ks.type>
    </category>
    <category name="plot">
        <client.ks.file>c:/eclipse/tomcats/ssl/customer1/moa-ssl-
kunde2[pwd=kunde2].p12</client.ks.file>
        <client.ks.pw>kunde2</client.ks.pw>
        <client.ks.type>PKCS12</client.ks.type>
    </category>
</category>
</properties>
```

5.2 Deployment Descriptor für Push Service

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app
xmlns="http://java.sun.com/xml/ns/javaee"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://java.sun.com/xml/ns/javaee/web-
app_2_5.xsd http://java.sun.com/xml/ns/javaee/web-app_2_5.xsd"
id="WebApp_ID" version="2.5">
    <display-name>zkopf</display-name>
    <!-- Main servlet listener -->
    <listener>
        <listener-class>at.gv.egiz.zkopf.server.listener.ZKopfListener</listener-class>
    </listener>
    <!-- UTF-8 filter -->
    <filter>
        <filter-name>UTF8Filter</filter-name>
        <filter-class>at.gv.egiz.zkopf.server.filter.UTF8Filter</filter-class>
    </filter>
    <!-- SSL Client Certificate filter for Push Service -->
    <filter>
        <filter-name>CertificateFilter</filter-name>
        <filter-class>at.gv.egiz.zkopf.server.filter.CertificateFilter</filter-class>
    </filter>
    <!-- SSL Client Certificate filter for Push Service -->
    <filter-mapping>
        <filter-name>CertificateFilter</filter-name>
        <url-pattern>/*</url-pattern>
    </filter-mapping>
    <!-- UTF-8 filter -->
    <filter-mapping>
        <filter-name>UTF8Filter</filter-name>
        <url-pattern>/*</url-pattern>
    </filter-mapping>
    <!-- Standard Query Service -->
    <servlet>
        <servlet-name>Query</servlet-name>
        <servlet-class>at.gv.egiz.zkopf.server.servlet.Query</servlet-class>
    </servlet>
    <!-- Push Service for delivery provider -->
    <servlet>
        <servlet-name>Push</servlet-name>
        <servlet-class>at.gv.egiz.zkopf.server.servlet.PushService</servlet-class>
    </servlet>
    <!-- Axis Service Provider -->
    <servlet>
        <servlet-name>AxisServlet</servlet-name>
        <servlet-class>
            org.apache.axis.transport.http.AxisServlet
        </servlet-class>
    </servlet>
    <!-- Push Service for delivery provider -->
    <servlet-mapping>
        <servlet-name>Push</servlet-name>
        <url-pattern>/services/PushService</url-pattern>
    </servlet-mapping>
</web-app>
```

5.2.1 Deployment Descriptor für Query Services

```
<?xml version="1.0" encoding="UTF-8"?>
```

Zustellkopf - Prototyp Elektronische Zustellung - ZUSE

```
<web-app xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://java.sun.com/xml/ns/javaee" xmlns:web="http://java.sun.com/xml/ns/javaee/web-
app 2_5.xsd" xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
http://java.sun.com/xml/ns/javaee/web-app_2_5.xsd" id="WebApp_ID" version="2.5">
  <display-name>zkopf</display-name>
  <!-- Main servlet listener -->
  <listener>
    <listener-class>at.gv.egiz.zkopf.server.listener.ZKopfListener</listener-class>
  </listener>
  <!-- UTF-8 filter -->
  <filter>
    <filter-name>UTF8Filter</filter-name>
    <filter-class>at.gv.egiz.zkopf.server.filter.UTF8Filter</filter-class>
  </filter>
  <!-- SSL Client Certificate filter for Push Service -->
  <filter>
    <filter-name>CertificateFilter</filter-name>
    <filter-class>at.gv.egiz.zkopf.server.filter.CertificateFilter</filter-class>
  </filter>
  <!-- SSL Client Certificate filter for Push Service -->
  <filter-mapping>
    <filter-name>CertificateFilter</filter-name>
    <url-pattern>/*</url-pattern>
  </filter-mapping>
  <!-- UTF-8 filter -->
  <filter-mapping>
    <filter-name>UTF8Filter</filter-name>
    <url-pattern>/*</url-pattern>
  </filter-mapping>
  <!-- Standard Query Service -->
  <servlet>
    <servlet-name>Query</servlet-name>
    <servlet-class>at.gv.egiz.zkopf.server.servlet.Query</servlet-class>
  </servlet>
  <!-- Push Service for delivery provider -->
  <servlet>
    <servlet-name>Push</servlet-name>
    <servlet-class>at.gv.egiz.zkopf.server.servlet.PushService</servlet-class>
  </servlet>
  <!-- Axis Service Provider -->
  <servlet>
    <servlet-name>AxisServlet</servlet-name>
    <servlet-class>
      org.apache.axis.transport.http.AxisServlet
    </servlet-class>
  </servlet>
  <!-- Standard Query Service -->
  <servlet-mapping>
    <servlet-name>Query</servlet-name>
    <url-pattern>/Query</url-pattern>
  </servlet-mapping>
  <!-- Axis Service Provider -->
  <servlet-mapping>
    <servlet-name>AxisServlet</servlet-name>
    <url-pattern>/services/*</url-pattern>
  </servlet-mapping>
</web-app>
```

6 Referenzen

- [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>.
- [ZKOPF-SPEC] Liehmann M., Hollosi A., Elektronische Zustellung – Zustellkopf-Schnittstellen-spezifikation 1.1.0.
- [ZKOPF-LDAP] Liehmann M., Hollosi A., Hörbe R., Elektronische Zustellung – LDAP-Schemabeschreibung 1.1.0
- [VerwEig] Hollosi, A.: X.509 Zertifikatserweiterungen für die Verwaltung. Abgerufen am 23.07.2007 unter <http://www.cio.gv.at/it-infrastructure/pki/X509ext-1.0.3-20050221.pdf>
- [OpenLDAP-Guide] OpenLDAP Software 2.3 Administrator's Guide. Abgerufen am 19.09.2007 unter <http://www.openldap.org/doc/admin23/>
- [OpenLDAP-Win32] OpenLDAP for Win32. Abgerufen am 19.09.2007 unter <http://lucas.bergmans.us/hacks/openldap/>
- [TOMCAT] Apache Tomcat. Abgerufen am 19.09.2007 unter <http://tomcat.apache.org/>
- [Servlet-SPEC] JSR-000154 Java Servlet 2.5. Abgerufen am 19.09.2007 unter <http://jcp.org/aboutJava/communityprocess/maintenance/jsr154/index3.html>
- [SOAP] SOAP Version 1.2. Abgerufen am 19.09.2007 unter <http://www.w3.org/TR/soap/>
- [Apache-AXIS] Apache Axis2/Java. Abgerufen am 19.09.2007 unter <http://ws.apache.org/axis2/>
- [ZKOPF-PUSH] Tauber A., ZUSE – Push Protokoll, Spezifikation.