LDAP-Verzeichnisse: ein unterschätztes Sicherheitsrisiko?

Karl Flieder

Lektor für EAI an der FH JOANNEUM
8010 Graz
karl.flieder@gmx.at

Schlagworte: E-Government, LDAP, Datenschutz, PKI, Workflow-Management-System

Abstract: Informationen sind in unserer elektronischen Welt in vielfältiger Weise zu einem begehrten Gut geworden. Damit steigen aber auch die Bedrohungsszenarien. Die Suche und das Eliminieren von Sicherheitsmängeln und Schlupflöchern ist ein wichtiger Beitrag im Sicherheitskontext geworden, um das Vertrauen in technische Lösungen zu stärken. In diesem Beitrag zeigen wir Anwendungsmöglichkeiten von LDAP-Verzeichnissen im Rahmen des E-Governments auf und berichten von einer Evaluierung österreichischer LDAP-Betreiber mit Bezug zur österreichischen Bürgerkarte. Unter dem Blickwinkel des Datenschutzes diskutieren wir plakativ zu Tage getretene Sicherheitsmängel und plädieren dafür, öffentliche LDAP-Verzeichnisse künftig besser zu schützen.

1. LDAP-Verzeichnisse im E-Government

Die Bezeichnung eines LDAP-Verzeichnisses (Lightweight Directory Access Protocol) als „Telefonbuch für E-Mails“ ist eine treffende Beschreibung für seine Nutzung als Verzeichnisdienst – auch im Rahmen von Public-Key-Infrastrukturen (PKI). Viele Anwendungen, insbesondere Web- und E-Mail-Clients, nutzen LDAP-Verzeichnisse als Quelle für personen- oder organisationsbezogene Daten. LDAP-Einträge können über einen anonymen Login, der grundsätzlich nur über Leserechte verfügt, abgefragt werden. Für das Ändern und Löschen der Daten sind spezielle Berechtigungen notwendig. Seit etwa 20 Jahren werden in der Informationstechnologie elektronische Genehmigungs- und Siegelverfahren eingesetzt. Auch wenn sich die ursprünglich euphorischen Erwartungen in dieses technische Verfahren bisher nicht erfüllt haben (ARGE Daten, 2007), werden LDAP-Verzeichnisse

im Rahmen des Einsatzes von elektronischen Signaturen häufig dazu benutzt, um gültige Zertifikate und Listen mit gesperrten, widerrufenen und zurückgezogenen Zertifikaten (Certificate Revocation List, CRL) zu veröffentlichen, wie dies im Signaturgesetz vorgesehen ist. Bei genauerer Hinsicht ist ein Zielkonflikt zwischen der optimalen Umsetzung der Veröffentlichungspflicht und der bestmöglichen Geheimhaltung von sensiblen Daten auszumachen.

1.1 Schnittstellen: Mensch und Maschine

Für die Abfrage von Daten aus LDAP-Verzeichnissen finden einerseits Graphische User Interfaces (GUI) in der Ausprägung von Suchformularen Verwendung, andererseits verfügen auch zahlreiche E-Mail-Clients über Schnittstellen zu LDAP-Servern. In einem E-Mail-Client kann nach einer Konfiguration der Verbindungsdaten über das Adressbuch im ausgewählten Verzeichnis, typischerweise über den Namen oder die E-Mail-Adresse, gesucht werden. Neben diesen beiden bekannten Möglichkeiten gewinnt zunehmend auch die Anbindung von LDAP-Verzeichnissen im Rahmen der Anwendungsintegration an Bedeutung. Mit der Directory Service Markup Language (DSML) und mit Web-Service-Schnittstellen zur Anbindung von heterogenen Systemwelten wird auch die automatisierte Integration von LDAP-Verzeichnissen auf eine breite und interoperable Basis gestellt. Typischerweise werden die Schnittstellen für LDAP-Verzeichnisse über Application Programming Interfaces (APIs) in das Toolset der Integrationswerkzeuge eingebunden. Im Rahmen einer SOA kann ein LDAP-Verzeichnis auch als Service-Verzeichnis eingesetzt werden (Heutschi, 2007).

1.2 Zustellung im Rahmen der öffentlichen Verwaltung

Auch im Rahmen der elektronischen Zustellung in der öffentlichen Verwaltung kommen LDAP-Verzeichnisse zur Auswahl des Zustellservices zum Einsatz. Die Anbindung erfolgt dabei über eine Web-Service-Schnittstelle (Reichstädter & Hollosi, 2003). Hinsichtlich des Subjekts wird dabei zwischen natürlichen und nicht natürlichen Personen unterschieden. Die über das Zustellservice umgesetzten Funktionen sind:

– Abfragen eines Zustellservices inklusive symmetrischem Schlüssel und eventueller Abwesenheitsinformationen zu einer bestimmten Person
– Übermitteln (Hinterlegen) eines Schriftstückes für eine Person

– Übermitteln eines Zustellnachweises
– Durchführen einer Rückzustellung bzw. Übermittlung einer entsprechenden negativen Nachricht, einer so genannten Unzustellbarkeitsanzeige.

2. LDAP in der Anwendungsintegration

Neben den zuvor geschilderten Anwendungen kommt zunehmend auch der automatisierten Integration von LDAP-Verzeichnissen über Web Services eine Schlüsselrolle zu. Diese und ähnliche Techniken werden vielfach unter dem Begriff Enterprise Application Integration (EAI) subsumiert und mit Workflow-Management-Systemen umgesetzt (Beer et al., 2007). Abbildung 1 zeigt jenen Workflow, der für unsere Evaluierung öffentlicher LDAP-Verzeichnisse verwendet wurde. Der Funktionsaufruf erfolgt durch eine SOAP-Nachricht, die über eine WSDL-Datei (Web Service Description Language) im Web-Service-Konnektor beschrieben wird. Über ein Mapping-Modul, das den Funktionsaufruf in die Auszeichnungssprache DSML umsetzt, gelangt die Abfrage an den LDAP-Konnektor. Dieser leitet die Anfrage (batchRequest) an das Verzeichnis weiter und gibt schließlich auch das Ergebnis in Form einer Liste zurück. Schließlich wird die Anzahl der retournierten Einträge gezählt; parallel dazu werden die Daten in eine SOAP-konforme Response-Nachricht verpackt.

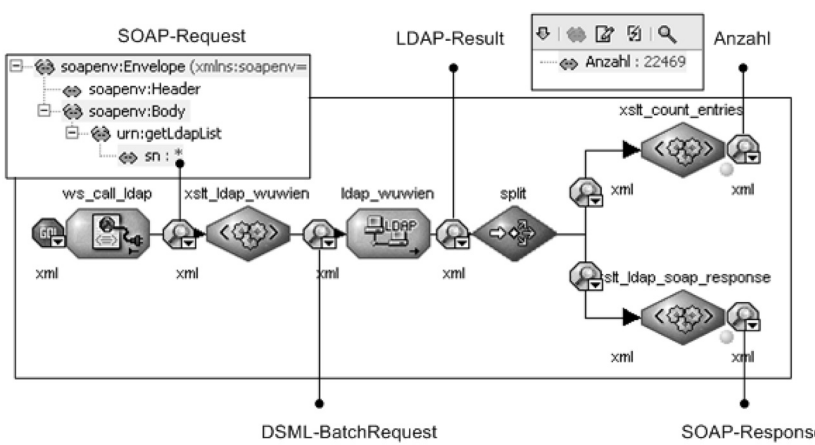

Abbildung 1: Workflow für die Evaluierung von LDAP-Verzeichnissen

Der Inhalt der Response-Nachricht kann an die unterschiedlichsten Applikationen weitergeleitet und mit XML-Technologien wie XSLT (eXtensible Stylesheet Language) und XPath (XML Path Language) universell weiterverarbeitet werden. Durch die Publizierung des Web Services in einem öffentlichen UDDI-Verzeichnis (Universal Description, Discovery and Integration) kann dieses dem globalen Marktplatz zur Verfügung gestellt werden. Damit wird eine Serviceadressierung nach dem Prinzip „find-bind-invoke" möglich. Dies ist ein Erfolg versprechender Weg in einer Welt von frei kombinierbaren Softwarekomponenten, den Services (Flieder, 2007). Mit BPEL-Elementen (Business Process Execution Language), wie Assign, Switch und While kann dem Workflow eine Programmlogik hinzugefügt und dieser für mehrere LDAP-Verzeichnisse wieder verwendbar gestaltet werden (Flieder, 2006).

Obwohl LDAP in der Literatur meist nicht in direktem Bezug zu einer SOA genannt wird, kann der in Abbildung 1 dargestellte Workflow als ein Service im Sinne einer SOA verstanden werden. Der standardisierte Zugriff erfolgt über eine Web-Service-Schnittstelle; seine Funktionalität wird in Form von Operationen und Parameter sowie den diesen zugrunde liegenden Datentypen beschrieben (Heutschi, 2007). Das funktionale Schema wird mit der technologieneutralen DSML, einer einheitlichen XML-Notation für automatisierte Interaktionen mit LDAP-Verzeichnissen, beschrieben.

3. Evaluierung österreichischer PKIs

In diesem Abschnitt werden ausgewählte Ergebnisse einer sicherheitstechnischen Evaluierung von öffentlich zugänglichen LDAP-Verzeichnissen aus Anwendersicht diskutiert. Wir wählten dafür Universitäten und führende Anbieter von Sicherheitsdienstleistungen aus Österreich aus. Der Grund liegt darin, dass der Endanwender von technischen Lösungen üblicherweise davon ausgehen wird, dass diese Einrichtungen nicht nur über aktuellstes Wissen verfügen, sondern dieses auch vorbildlich und zum Nutzen und Vorteil der Gesellschaft einsetzen. Unsere Ergebnisse lassen diesbezüglich allerdings Zweifel aufkommen. Die Abfragen erfolgten mit dem in Abschnitt 2 vorgestellten Workflow, parallel dazu wurde das jeweilige Testobjekt mit einem LDAP-Browser abgefragt.

3.1 RTR – Rundfunk & Telekom Regulierungs-GmbH

Als Einstiegspunkt für unsere Evaluierung diente das Verzeichnis der österreichischen Regulierungsbehörde RTR (Rundfunk & Telekom Regulierungs-GmbH). Diese Organisation stellt u. a. Zertifikate für vertrauenswürdige Zertifizierungsdienstanbieter, so genannte Certification Authorities (CA) aus und ist als Aufsichtsstelle gemäß österreichischem Signaturgesetz (SigG) zur Führung eines Verzeichnisses verpflichtet. Die technische Umsetzung erfolgte mittels LDAP[1]. Hier konnten wir uns nicht nur einen ersten Überblick über einzelne Zertifizierungsdienstanbieter in Österreich verschaffen; wir konnten auch deren Kontaktdaten abfragen. Neben den erwähnten Zertifikaten und Widerrufslisten veröffentlicht die RTR auf ihrer Webseite auch Rechtsvorschriften sowie technische Informationen zum Thema elektronische Signaturen.

3.2 A-Trust

Die Firma A-Trust ist einer der größten PKI-Anbieter in Österreich. A-Trust ist neben dem Hauptverband der Sozialversicherungsträger auch einer der Betreiber der österreichischen Bürgerkarte und bietet für sein LDAP-Verzeichnis[2] eine Web-Oberfläche zur Zertifikatssuche an. Daneben kann es auch automatisiert über die Abfragesprache DSML bedient werden. Die Öffentlichkeit erlangt damit Zugang zu den von A-Trust ausgestellten Zertifikaten, allen Stammzertifikaten sowie den dazugehörigen Sperrlisten. Darüber hinaus werden Vor- und Nachname, die Cardholder Identification Number (CIN), Karten- und Zertifikatseriennummer sowie weitere Angaben der Öffentlichkeit bereitgestellt. Bei Minderjährigen ist auch das Geburtsdatum unbedingt zu veröffentlichen und daher Bestandteil des Zertifikats. Im Gegensatz zum Webinterface können mit der DSML-Schnittstelle LDAP-Daten nicht nur abgefragt, sondern auch heruntergeladen und in der Folge lokal verarbeitet bzw. ausgewertet werden. Zum Zeitpunkt unserer Tests am 30. 05. 2008 war offenbar keine Beschränkung der maximalen Anzahl der zurückgegebenen Datensätze aktiv. Unter der Adresse, dem so genannten Distinguished Name (DN), ou=a-sign-Premium-Sig-02, o=a-trust, c=AT, konnten daher 82.738 Einträge abgerufen werden. Dieses Ergebnis deckt sich auch annähernd mit Stingl et al. (2007). Sie dokumentierten per 12. 04.

1 ldap://ldap.signatur.rtr.at.
2 ldap://ldap.a-trust.at:389.

2007 52.150 (gültige) Premium2-Zertifikate, die bei der österreichischen Bürgerkarte Verwendung finden und fanden je nach Zählweise 3,55 bis 12,29 Prozent doppelte Einträge in den LDAP-Verzeichnissen von A-Trust und dem Hauptverband der Sozialversicherungsträger.

3.3 Wirtschaftsuniversität Wien

Die Wirtschaftsuniversität (WU) Wien bezeichnet sich selbst mit über 20.000 Studierenden und mehr als 1.700 Mitarbeitern als die größte wirtschaftswissenschaftliche Ausbildungsstätte der Europäischen Union. Das LDAP-Verzeichnis der WU Wien[3] fällt zunächst dadurch auf, dass keinerlei Beschränkung der maximalen Rückgabewerte (Hits) implementiert wurde. Am 16. 02. 2008 konnten über den DN ou=users, dc=wu-wien, dc=ac, dc=at die Daten von 22.744 Personen abgefragt werden. Unter dem Knoten „Studierende“ konnte teilweise auch die Mobiltelefonnummer der im Verzeichnis geführten Personen abgerufen werden.

3.4 A-Cert

Beim LDAP-Verzeichnis des Vereins ARGE Daten[4], der Österreichischen Gesellschaft für Datenschutz, scheint zwar eine Beschränkung der maximal zurückgegebenen Datensätze aktiv zu sein, dennoch konnten Zertifikate und darauf Bezug nehmende Zusatzinformationen in größeren Mengen abgerufen werden. Diese Beschränkung ist allerdings zu hoch ausgefallen, wodurch eine automatisierte Abfrage lediglich erschwert wird. Um zum (vollen) Erfolg zu kommen, sind entweder mehrere Versuche notwendig oder man programmiert eine verschachtelte Schleife. Ein Abfrage unter dem DN ou=A-CERT GOVERNMENT, o=A-CERT, c=at mit givenName=* am 10. 01. 2008 ergab 289 Treffer. Andere Knoten lieferten – je nach Suchkriterium – bis zu 324 Treffer, ehe das Attribut sizeLimit wirksam wurde.

3.5 Hauptverband der Sozialversicherungsträger

Die österreichische Gesundheitskarte (eCard), der elektronische „Krankenscheinersatz“, war indirekt der Auslöser für unsere Untersuchung. Stingl et

3 http://www.wu-wien.ac.at/zid/anleitungen/ldap.
4 ldap://ldap.a-cert.at:389.

al. (2007) analysierten österreichische PKIs hinsichtlich der zuverlässigen Identifikation des Signators und des Zertifizierungspfades. Dabei berichteten sie unter anderem auch von Zertifikatsduplikaten in diesem Verzeichnis, das im Rahmen des österreichischen Bürgerkartenkonzepts eingesetzt wird. Sie kamen zum Schluss, dass in den beiden überprüften Fällen (A-Trust und Hauptverband) entgegen dem Identifikationsmodell der Bürgerkarte (Rössler & Leitold, 2005) *keine* eindeutige Identifikation des Signators möglich ist.

3.6 LDAP-Verzeichnis der Republik Österreich

Einen ganz besonderen „Service" bietet das LDAP-Verzeichnis der öffentlichen Verwaltung der Republik Österreich[5]. Dieses LDAP-Verzeichnis definiert Objekte zur Darstellung von Personen, Dienstverhältnissen und Funktionen sowie der Aufbauorganisation für das Telefonverzeichnis und den Amtskalender. Hier werden umfangreiche arbeitsplatzbezogene Daten von MitarbeiterInnen der folgenden Behörden bzw. Organisationseinheiten veröffentlicht, die von jedermann mit einem LDAP-Browser eingesehen werden können:

- Bundesministerium für Justiz (BMJ)
- Bundesministerium für Land- und Forstwirtschaft, Umwelt und Wasserwirtschaft
- Bundeskanzleramt (BKA)
- Bundesministerium für Inneres (BMI)
- Bundesministerium für Verkehr, Innovation und Technologie (BMVIT)
- Bundesministerium für Wirtschaft und Arbeit (BMWA)
- Land-, Forst- und Wasserwirtschaftliches Rechenzentrum (LFRZ).

Neben den öffentlich bereitgestellten Daten (gvScope = public) werden im LDAP-Verzeichnis des Bundes auch personenbezogene Daten wie Geburtsdatum, die bereichsspezifische Personenkennung (bPK) sowie Anmeldedaten (UserId) im lokalen Bereich gespeichert (Grandits, 2006). Bei einem Test am 15. 01. 2008 erhielten wir als Ergebnis 4.477 Personeneinträge, die unter dem DN ou=people, gvOuId=AT:b:200, dc=gv, dc=at (BMVIT) abgefragt wurden. Unter dem DN ou=people, gvOuId=AT:B:104, dc=gv, dc=at (BM für Land- und Forstwirtschaft, Umwelt und Wasserwirtschaft) konnten am 16. 02. 2008 12.356 Einträge selektiert werden. Die interessierte Öffentlichkeit kann über diesen zentralen Basisdienst umfangreiche Daten und

5 ldap://ldap.gv.at:389.

Informationen zur organisatorischen Zugehörigkeit der Staatsbeamten abrufen. Dabei werden auch sicherheitsrelevante Einstellungen wie Password-Policy und Security-Einstellungen dieses mit einem Gütesiegel[6] ausgezeichneten LDAP-Verzeichnisses über den Wurzelknoten an die Öffentlichkeit exponiert. Diese sicherheitskritischen Informationen können die Arbeit eines potenziellen Angreifers erleichtern, da sie Sicherheitsparameter offenlegt.

4. Diskussion und Fazit

Aus Anwendersicht und aus dem Blickwinkel des Datenschutzes betrachtet, konnte im Zuge der Recherchen der Eindruck gewonnen werden, dass zu viele Daten über öffentliche LDAP-Verzeichnisse exponiert werden. Die Hypothese des Autors ist, dass durch die weit verbreitete Nutzung von LDAP-Verzeichnissen über ein Suchformular und den damit verbundenen beschränkten Abfragemöglichkeiten die Gefahr von Massen-Downloads mit anschließender Nutzung dieser Daten – zum Beispiel für Spamming, für die private Nutzung der Daten oder für Social-Engineering-Attacken – bisher weitgehend vernachlässigt wurde. Vielfach ist keine Beschränkung der maximal zurückgegebenen Datensätze (sizeLimit) implementiert.

Über einen offenen Knoten „Root DSE“ können zudem bei manchen Verzeichnissen Metadaten wie die unterstützten LDAP-Versionen, Vendor-Informationen, Erweiterungen zum Protokoll, SASL-Mechanismen, Suffixe und Namenskontexte mit frei verfügbaren LDAP-Browsern eingesehen und im LDIF-Format lokal gespeichert werden. Weiters können über einen speziellen DN (cn=Schema) alle dem Server bekannten Objektklassen und Schema-Attribute aufgelistet werden. Ein nicht abgeändertes und verschlüsseltes Standardpasswort unter „rootpw“ stellt ein weiteres potenzielles Sicherheitsrisiko für öffentlich zugängliche LDAP-Verzeichnisse dar. Wie das Beispiel ldap.gv.at zeigt, sind hier neben den Administratoren auch die Verteiler der Gütesiegel gefordert. Dieses Verzeichnis legt sogar seine Sicherheitsparameter, beispielsweise die zulässige Passwortlänge von 1–64, offen.

Wie der Webseite der Fa. A-Trust zu entnehmen ist, vertrauen österreichische Banken, wie Bawag-PSK, Schoellerbank, einzelne Hypos, Raiffeisen, der Sparkassensektor, BKS, BTV, Oberbank u. a. auf das Produkt

6 http://reference.e-government.gv.at/Guetesiegel.340.0.html.

a-sign premium dieser Firma. Umso mehr verwundert es, dass unter dem DN cn=Schema auf über 3.200 Zeilen die „technische DNA" dieses LDAP-Verzeichnisses offengelegt wird. Unter demselben DN werden auch die LDAP-Schemata der Republik Österreich, der RTR – Rundfunk & Telekom Regulierungs-GmbH und des Hauptverbandes der Sozialversicherungsträger exponiert. Dieses teilweise verblüffende Ergebnis stärkt nach Meinung des Autors nicht gerade das Vertrauen in die österreichische PKI-Landschaft.

Literatur

ARGE Daten: Stellungnahme zur Änderung des Signaturgesetzes. Abruf am 20. 3. 2008 unter: ftp://ftp.freenet.at/privacy/gesetze/sigg-stellungnahme-2007.pdf

Beer D., Dümmler J., Rünger G.: Transformationen von Prozessmodellen in Workflowbeschreibungen. In: Schweighofer, E., Geist, A., Heindl, G., (Hrsg.): Tagungsband des 10. Internationalen Rechtsinformatik Symposions IRIS 2007. Boorberg, 180–187.

Flieder K.: Sicherheit in der Prozessintegration mit Web Services und SOA. In: Horster P. (Hrsg.): D•A•CH Security 2007, 83–97.

Flieder K.: Geschäftsprozessmanagement – Geschäftsprozesse mit dem virtuellen Reißbrett steuern? WINGbusiness 39 (3) 2006, 35–38.

Grandits, F.: E-Government, AG Verzeichnisdienst – LDAP-gv.at 2.3.0, Stellungnahme vom 20. 03. 2006. GZ: FA1B – B1.20–21440/2004–8. Abruf am 20. 3. 2008 unter: http://reference.e-government.gv.at/VD___LDAP-gv_at_2_3_0___Teil_1.777.0.html.

Heutschi, R.: Serviceorientierte Architektur – Architekturprinzipien und Umsetzung in der Praxis. Springer (2007).

Reichstädter, P., Hollosi, A.: Modell der elektronischen Zustellung (2003). Abruf am 20. 3. 2008 unter: http://www.cio.gv.at/it-infrastructure/delivery/spec/V10/ Zustellung_Modell_20030506.pdf.

Rössler, T., Leitold, H.: Identifikationsmodell der österreichischen Bürgerkarte. In: Horster P. (Hrsg.): D•A•CH Security (2005), 121–129.

Stingl, C., Slamanig, D., Reiner, M., Thierry, J.: Chipkarten in österreichischen PKIs – Analyse des Status Quo. In: Horster P. (Hrsg.): D•A•CH Security 2007, 479–477.