



Arbeitsgruppe Verzeichnisdienste

Konzept für den behördenübergreifenden Verzeichnisdienst

Version:	2.0
Datum:	28. Jänner 2002
Autor:	Rainer Hörbe/BMI-EDVZ

Wozu ein Verzeichnisdienst für die öffentliche Verwaltung?

E-Government bedeutet, dass die Tätigkeiten der Ministerien auf Basis der e-Technologie reorganisiert werden. Die e-Technologien müssen dabei Ressort-übergreifend betrachtet werden, wofür geeignete Schnittstellen und Standards zu definieren sind..

E-Government fordert und fördert einheitliche Verwaltungsstrukturen. Gemeinsame Datenstrukturen haben dabei einen standardisierender Effekt und erleichtern die Entwicklung Ressort-übergreifender Anwendungen.

Verzeichnisse sind Basis verschiedener Anwendungen, unter anderem die von Adressbüchern im weiteren Sinne, die Personen, Kontaktinformation und Aufbauorganisation enthalten.

Ein gemeinsames Adressbuch wird in Zukunft auf folgenden Gründen wichtig werden:

- E-Mail Kommunikation mit gesicherter Zustellung, Signatur und Verschlüsselung
- Verwaltungsbedienstete im One-Stop Government: in Zukunft wird vermehrt Zugriff auf verschiedene Verwaltungsbereiche benötigen, eine wichtige Datenquelle ist das Verzeichnis
- On-Line Transaktionen erfordern erhöhte Datenaktualität und -konsistenz
- Reduktion der Datenpflege in redundanten Beständen

Darüber hinaus sind weitere Organisations- und personenbezogene Information in ein Verzeichnis einzubringen, welche die Rollen und Rechte abbilden:

- Rollenmodell, das für vor allem den Elektronischen Akt verwendet wird
- Berechtigungen für Applikationen, zur Nutzung von Applikationsportalen

Umfang

Das Verzeichnis soll die Organisationen der öffentlichen Verwaltung umfassen, aber auch offen für Selbstverwaltungskörper und an Behördenverfahren beteiligten Personen sein, wie SV, Notare, Sachverständige, ..

Bürger und privatwirtschaftliche Nutzer werden in diesem Verzeichnis nicht enthalten sein, weil für Verwaltungsverfahren eine End-to-End Beziehung zwischen Anwendung und Anwender angestrebt wird, und dazu notwendige Verzeichniseinträge ohnehin vom Trust Center geführt werden müssen. Eine Identifikation am Portal soll nicht notwendig sein.

Nicht-Ziele

- Der Verzeichnisdienst ist keine Ersatz für eine Personalverwaltung, sondern stellt eine Untermenge der Personaldaten anderen Applikationen in geeigneter Weise zur Verfügung
- Der behördenübergreifende Verzeichnisdienst enthält keine EDV-spezifischen Ressourcen wie z.B. Drucker. Das wäre eine Aufgabe eines internen Dienstes
- Eine Kalender-Funktionalität ist derzeit nicht geplant

Vorgangsweise für den Verzeichnisdienst

Da von der Integration der Daten aus vielen inhomogenen Beständen unterschiedlicher Qualität viele bestehende Applikationen betroffen sind, wird eine iterative Vorgangsweise notwendig sein. Deswegen sollten zuerst die Datenbestände lokalisiert werden, die aktuelle und qualitativ hochwertige Daten über Bedienstete der Verwaltung (einschließlich externer Mitarbeiter wie Leihpersonal) sowie der Aufbauorganisation beinhalten.

Für die Organisationen, welche die Daten bereitstellen und nutzen, wird es mittelfristig sinnvoll sein, interne Verzeichnisse aufzubauen, die mit dem externen integriert sind, um den ökonomischen Nutzen zu maximieren.

Die ersten Anwendungen für den Verzeichnisdienst sollten keine Daten automatisiert weiterverarbeiten, sondern durch einen Medienbruch¹ Datenfehler abfangen.

Für den Zweck der Grobanalyse werden die Daten daher vorläufig in die Zugriffsstufen öffentlich, Verwaltung und intern eingeteilt.

Ziel der Arbeitsgruppe ist es, ein Rahmenwerk zur Zusammenführung von Daten aus unterschiedlichen Beständen zu schaffen. Das Rahmenwerk wird aus folgenden Teilen bestehen:

- Schemadefinition basierend auf LDAP/X.500 Normen
- Schnittstellen für Operationen am Verzeichnis (LDAP, HTTP/DSML)
- Testdirectory
- Referenzen zu existierenden Projekten, Beispiele

Vorschlag für die Projektphase 2: Siehe Dokument „Management Summary“

¹ Im Sinne des „Klassifikationsschema für E-Government-Verfahren“, Seite 6, www.bsi.de

Anwendungen

Öffentliche und Organisationen übergreifende Anwendungen

Die hier definierten Anwendungen zeigen die Nutzersicht auf die Daten. Für den Nutzer sind die Daten Read-Only, und über definierte Protokolle (LDAP, HTTP, ebXML) zugänglich. Die Wartung der Daten erfolgt durch Upload oder eine Wartungsapplikation, die durch einen LDAP-Provider zur Verfügung gestellt wird. Kandidaten für Anwendungen von Verzeichnisdiensten sind solche, wo eine wesentliche Nutzung gemeinsamer Daten erfolgt. Folgende Anwendungen wurden vorläufig definiert:

- White Pages listen Personen und Organisationen mit Kontaktinformationen wie Postadresse, Telefon und E-Mail. Jede Person einer Organisation kann (und sollte) verzeichnet sein.
Nutzung: Personenverzeichnis für die informelle Kommunikation.
- Amtskalender – Abbildung der (im Außenverhältnis relevanten) Organisationsstrukturen der Verwaltungseinheiten bis auf die Ebene von Dienststellen. Als Minimalerfordernis braucht eine Organisation nur die Aufgaben und die Einlaufstellen (Post, Fax, E-Mail) definieren.
Nutzung: Organisations- und Personenverzeichnis für die formale (rechtsverbindliche) Kommunikation.
- Portal (Rollen und Applikations-Berechtigungen)
Nutzen: Verifikation von Zugriffsrechten externer Benutzer; verfügbare Anwendungen eines Benutzers bei einem Portal.
- E-Mail-Integration: Die verschiedenen Konzepte der Directory-Integration (gemeinsames Directory, Replikation) sollten geklärt werden und wenn möglich Prototypen mindestens für Exchange und Lotus Notes beurteilt werden. Eine Koordination mit der E-Mail Strategie des BMF soll rechtzeitig erfolgen, um die Ergebnisse rechtzeitig vor Fertigstellung der Ausschreibung im BMF in die Verzeichnisspezifikation einfließen zu lassen.
- ELAK: Die Workflow-Informationen sind Teil der Anwendung und werden nicht im Verzeichnis gespeichert. Die Verwendung der Verzeichnisdaten im ELAK wird später im ELAK-Projekt definiert werden. In der ersten Phase wurde jedoch das LDAP-Schema dahin gehend angepasst, dass ein Benutzer mehreren Organisationseinheiten zugeordnet werden kann.
- Benutzerverwaltung: Derzeit wird die gesicherte Registrierung von Benutzern (Benutzer-Administratoren) zum Teil außerhalb des Netzwerks durchgeführt (Fax, Post, ..). Ein zukünftiges System, das auf digitalen Signaturen basiert, kann eingesetzt werden, wenn eine PKI etabliert ist.

Interne Anwendungen

- Personal-Informationssystem: Datenquelle für Basis-Attribute des Personen-Objekts (siehe [1])
- Intern ist in erster Linie die Integration in die Benutzerverwaltung es Netzwerkbetriebssystems interessant. Dafür kommen meistens Novell NDS und MS NT Domain Service/AD in Frage
- Die Integration mit Telefon-Nebenstellenanlagen kann die Zuordnung von Name, Nebenstelle und Ort verbessern. Außerdem ist dann die Möglichkeit gegeben, Callcenter mehrerer Organisationen zusammen zu legen.

- Die Personensuche kann eine Variante der Whitepage-Anwendung sein, mit geänderten Zugriffsrechten.
- Andere Anwendungen je nach Organisation

Geschäftsfälle

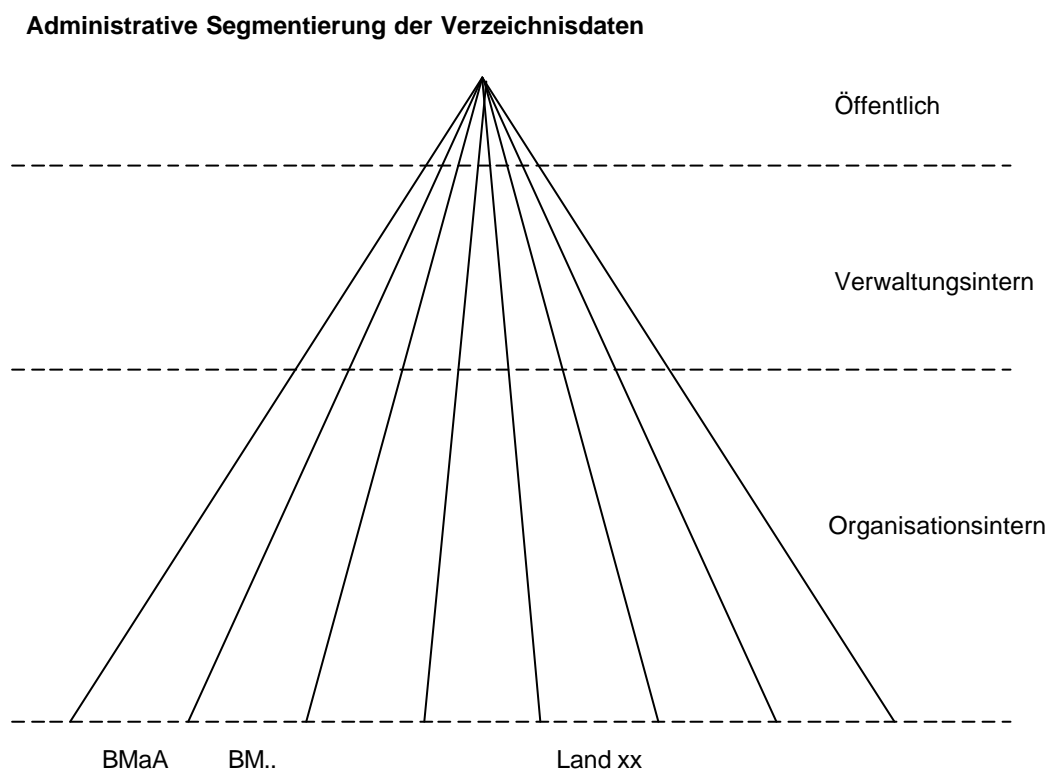
Für den Aufbau eines internen Verzeichnisdienstes, der eine Basis für den externen sein kann, sollten die dafür relevanten Geschäftsfälle untersucht werden, wie z.B.:

- Mitarbeiter neu
- Mitarbeiter Änderung
 - Versetzung
 - Namensänderung
 - Sonstige Datenänderungen
- Mitarbeiter beenden
 - Permanent
 - Temporär
- Organisationseinheit neu
- Organisationseinheit ändern
- Organisationseinheiten zusammenlegen
- Organisationseinheit trennen
- Organisationseinheit auflösen
- Organisationseinheit ausgliedern
- Anwendung freigeben
- Anwendung sperren
- Anwendungsrechte vergeben

Organisation und Betrieb des Verzeichnisses

Das Directory wird LDAP-konform realisiert. Die organisatorische Verteilung passiert analog zum DNS im Internet, wo der Besitzer einer Domäne für den Inhalt der Daten verantwortlich ist. Der Betrieb sollte zentralisiert oder auf eine kleine Anzahl von Servern verteilt werden. Jedenfalls sollte ein LDAP-Server eingerichtet werden, der die Datenbestände der Bundesverwaltung hält, und optional für andere Organisationen, die auf den Betrieb eines eigenen Servers verzichten.

Die logische Gesamtsicht der Verzeichnisdaten nach Zugriffsbereichen getrennt wäre wie folgt:



Technisch können die Verzeichnisdaten wie folgt in das Verzeichnis eingebracht werden:

- Über LDAP in den zentralen LDAP-Server
- Über ein Metadirectory-Produkt in den zentralen LDAP-Server
- Über einen eigenen Server (insgesamt sollte die Anzahl der Server eine Größenordnung von 10 Stück nicht überschreiten) für Organisationen außerhalb der Bundesverwaltung, die den zentral angebotenen Dienst nicht nutzen wollen
- Über ein Web-Interface am zentralen Server

Anmerkungen zur E-Mail-Integration

Um eine sichere E-Mail Kommunikation zu gewährleisten werden E-Mail Benutzer zertifizierte Schlüssel zur Signatur/Verschlüsselung ihrer Datei-Anhänge verwenden. Die Aufgabe des Verzeichnisdienstes ist es, die Zertifikate (oder Verweise dazu) an einer zentralen Adresse zugänglich zu machen. Es wird davon ausgegangen, dass diese Zertifikate von einem externen (auch privatem) Trust-Center verwaltet werden. Um eine sichere Kommunikation mit einer Person zu führen sind folgende Schritte notwendig:

- Person in Verzeichnis finden
- E-Mail Adresse aus Verzeichnis holen
- E-Mail Zertifikat von Trustcenter holen

Die kryptografischen Funktionen werden nicht in den herkömmlichen E-Mail Clients umgesetzt, sondern über Trusted Viewer, die über JavaScript die Datei-Anhänge öffnen.

Anmerkungen zu Zertifikaten

Die Zuordnung des Eintrages gvOrgPerson zu einem Zertifikat des Schlüssels einer Smartcard (z.B. Bürgerkarte, Dienstkarte) der Person findet über die sogenannte Personenbindung statt. Die Personenbindung ist ein von der zuständigen Behörde signiertes Tupel, das folgende Daten enthält:

- die öffentlichen Schlüssel der Karte (A und B)
- den Basisbegriff (ZMR-Nr, Verfahrenskennung, ...)
- Gültigkeitsdauer der Bindung (von – bis)

Diese Personenbindung wird auf der Smartcard gespeichert und ist auch über den Security-Layer abrufbar.

Beispielhaft soll hier die Identifikation an einem Portal angesprochen werden: zur Identifikation schickt die Person einen Authentifikationsblock zum Portal. Dieser Auth-Block kann je nach Anwendung und Portal unterschiedlich ausgeprägt sein (z.B. ist auch ein temporäres Session-Zertifikat denkbar). Die Sicherheit (und der Identifikationsaspekt) beruht jedoch in jedem Fall auf der digitalen Signatur dieses Auth-Blocks (z.B. ist im Falle des Sessionzertifikats dieses vom B-Schlüssel der Karte unterzeichnet/ausgestellt). In diesem Auth-Block ist auch die Personenbindung enthalten. Damit ist ausgehend von der Signatur (B-Schlüssel), über die Personenbindung (Zusammenhang B-Schlüssel -> Basisbegriff), ein Zusammenhang zum Record gvOrgPerson (enthält Basisbegriff) gegeben, und damit die Identifikation der Person gewährleistet, sowie eine Kontrolle der Rechte im Kontext der Applikation/des Portals möglich.

Die Einführung der Personenbindung entkoppelt die beiden Bereiche, Verzeichnisdienst einerseits und PKI des Zertifizierungsdienstes andererseits, vollständig. Damit ist eine größtmögliche Flexibilität auf beiden Seiten gegeben, ohne dass die Sicherheit des Systems beeinträchtigt wird.

Schema

Das Schema baut auf dem Entwurf des LDAP-Schemas der Arbeitsgruppe Autorisierungssysteme auf und ist im Dokument " Verzeichnisdienste gv.at LDAP" spezifiziert.

Projektbericht

Bisher wurden 5 Arbeitsgruppensitzungen und einige Sitzungen in kleinerem Rahmen abgehalten. Ein Teil der Diskussion erfolgte über Emails und Meiling-Listen. Der Ist-Stand der Ressorts in Bezug auf Daten von Bediensteten und der Aufbauorganisation wurde über Fragebogen abgefragt. Außerdem wurde mit Prof. Chadwick von der Universität Salford ein Workshop abgehalten.

Die Resultate dieser Aktivitäten wurden zusammen mit dem LDAP-Konzept der E-Gov-Länder Arbeitsgruppe „behördenübergreifende Autorisierungssysteme“ in das beiliegende Konzept eingearbeitet.

Der aktuelle Stand der Dokumente kann unter der Adresse <http://ln-inter1.bmi.gv.at/agvd/> abgeholt werden.

Die Mailinglisten sind wie folgt:

agvd@listen.bmi.gv.at: interne Diskussion

agvd-sum@listen.bmi.gv.at: Zusammenfassungen, Ergebnisse, Ankündigungen

Das Ergebnis ist die erste Version des Konzepts für den Verzeichnisdienst, das dem IKT-Board Anfang Februar 2002 vorgelegt wird.

Aufgaben und weitere Vorgangsweise

- Schaffung der rechtlichen Grundlagen für die Verwendung der aus der ZMR-Zahl abgeleiteten Verfahrenskennung als Schlüsselbegriff der Personen
- Pilotprojekt
 - Einrichtung eines Testservers mit dem definierten Schema (Produkt kann unabhängig von Ergebnis der Evaluierung gewählt werden)
 - Einrichtung eines Meta-Directories und Integration ausgewählter Anwendungen in ausgewählten Ressorts
 - Evaluierung von Directory-Produkten nach den Kriterien der Leistungsfähigkeit, Unterstützung offener Normen und Kosten
 - Ausschreibung/Auswahl des Directory-Betriebs
- Phase 1
 - Einrichtung des zentralen Directory-Servers für die Bundesverwaltung
 - Integration von PIS und E-Mail-Directories über alle Ressorts
 - Implementierung einer White-Page Web-Anwendung
- Phase 2

- Integration bestehender Landes-Directories

Referenzen

[1] Protokoll AGVD 20010918.doc