

Einführung eines bayernweiten zentralen Verzeichnisdienstes (zVD)

Dipl.-Inf. Rudolf Zenkert

1. Ausgangssituation

In der bayerischen Verwaltung werden an den unterschiedlichsten Stellen der Behörden Verzeichnisse gepflegt, in denen Informationen über Dienststellen und Mitarbeiter (z.B. Telefonnummer, E-Mail-Adresse, Postanschrift) gespeichert werden. Beispiele hierfür sind das Dienststellenverzeichnis des LfStAD, in dem sowohl staatliche als auch kommunale Behörden aufgeführt sind, und das E-Mail- und Telefonverzeichnis des Bayerischen Behördennetzes.

Die Anzahl solcher Verzeichnisse hat sich in den letzten Jahren durch den verstärkten Einsatz von EDV-Anwendungen stetig erhöht, da solche Anwendungen und Dienste jeweils eigene Verzeichnisse verwenden, um etwa benötigte Informationen über Benutzer und Kommunikationspartner abzuspeichern oder auch um Zugriffsrechte zu verwalten. Die Mitarbeiter in den Behörden besitzen dadurch oft

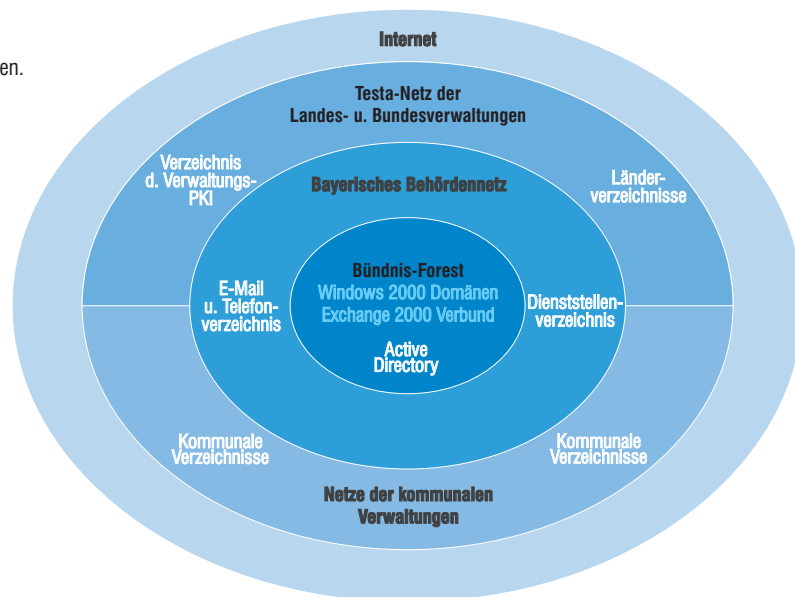
eine Vielzahl unterschiedlicher Kennungen und Kennwörter für die genutzten Anwendungen.

Diese große Anzahl an Verzeichnissen führt zu einem entsprechend hohen Verwaltungsaufwand, da die Daten mehrfach und an verschiedenen Stellen gespeichert und gepflegt werden. Inkonsistenzen und veraltete Daten sind die Folge. Ein manueller Abgleich von Daten erfordert jeweils einen immensen Bearbeitungsaufwand.

Ein weiteres Problem stellt die oftmals unzureichende Erreichbarkeit und Verfügbarkeit vorhandener Verzeichnisse dar. So werden redundante Verzeichnisse in vielen Fällen auch deswegen ins Leben gerufen, weil ein Zugriff über Netzgrenzen nicht möglich ist, oder zeitliche Rahmenbedingungen unbedingt eingehalten werden müssen. Die nachfolgende Graphik verdeutlicht dies am Beispiel einiger Verzeichnisse und Behörden:

Abb. 1 Netztopologie der Verzeichnisse

Netztopologie aus Sicht der staatlichen Behörden. Aus Sicht kommunaler Behörden ergeben sich jeweils analoge Strukturen.



Erreichbarkeit staatlicher Verzeichnisse

Die Mitglieder des Bündnis-Forest¹ (darunter nahezu alle Ministerien mit ihren nachgeordneten Behörden) können das zentrale Verzeichnis des Bündnis-Forest (u.a. ein gemeinsames E-Mail-Adressbuch) und die Verzeichnisse des Behördennetzes (z.B. das Dienststellenverzeichnis) abrufen. Für Behörden, die sich nur im Behördennetz befinden (u.a. unabhängige Behörden wie etwa der Landtag oder der Oberste Rechnungshof, aber auch manche Kommunen

und Landkreise), ist ein Zugriff auf die Informationsquellen des Bündnis-Forest nicht möglich.

¹ Mit dem Begriff Bündnis-Forest wird der Zusammenschluss von mehreren Domänen (d.h. Namensbereichen) bezeichnet, die Windows 2000 als zentrales Betriebssystem einsetzen, sich gegenseitig auf besondere Weise vertrauen und gemeinsame Dienste (z.B. Verzeichnisse) nutzen.

Zwar ist eine große Anzahl von Behörden und Geschäftsbereichen in den Bündnis-Forest integriert, jedoch ist dieser auf die staatlichen Dienststellen ausgerichtet. Die Aufnahme von kommunalen Dienststellen ist bislang nicht vorgesehen. Auch Behörden, die ausschließlich Open-Source-Produkte einsetzen, können derzeit nicht eingebunden werden.

Noch unangenehmer stellt sich die Situation für Nutzer in Behörden dar, die nicht im Behördennetz sind (z.B. die Landeshauptstadt München), oder die sich außerhalb Bayerns befinden (z.B. andere Landesverwaltungen). Hier ist ein gegenseitiger Zugriff auf die jeweiligen zentralen Verzeichnisse nicht möglich.

2. Ziele

Das grundlegende Ziel bei der Einrichtung des zVD besteht in der zentralen und koordinierten Bereitstellung der wichtigsten Informationen, die für die Kommunikations- und Geschäftsprozesse der bayerischen Behörden benötigt werden. Wichtig dabei ist die umfassende Einbindung aller staatlichen und kommunalen Behörden. Der künftige zVD wird die wichtigsten bereits vorhandenen (zum Teil sehr heterogen strukturierten) Verzeichnisse integrieren, aber bei Bedarf auch die Aufnahme zusätzlicher Informationen ermöglichen:

- **Behörden- und Dienststellenverzeichnis**
Es stellt das Rückgrat des zVD dar, das die wichtigsten Kontaktinformationen der staatlichen und kommunalen Dienststellen, wie zum Beispiel zentrale Postadressen und Telefonnummern oder auch Internetadressen bereitstellt.
- **Verzeichnis der Funktionsadressen**
Den einzelnen Dienststellen werden funktionsbezogene E-Mail-adressen zugeordnet, die es ermöglichen, Informationen an bestimmte Ressorts und Beauftragte (wie etwa Pressesprecher, EDV-Beauftragte oder verschiedene Referenten) weiterzuleiten, ohne die aktuellen konkreten Zuständigkeiten im einzelnen kennen zu müssen. Überdies besteht so die Möglichkeit, alle mit einer bestimmten Funktion beauftragten Mitarbeiter der im zVD aufgenommenen Dienststellen in einem Zug zu kontaktieren.
- **Mitarbeiterverzeichnis**
Als weiterer Baustein des zVD dient ein Verzeichnis, in dem die grundlegenden Kontaktinformationen der bei den Behörden tätigen Mitarbeiter (zum Beispiel Telefonnummern und E-Mail-Adressen) zur Verfügung gestellt werden. Das Mitarbeiterverzeichnis gibt darüber hinaus über die Eingliederung der Mitarbeiter in die Organisationsstrukturen der Dienststellen Auskunft. In einer späteren Ausbaustufe ist auch vorgesehen, die fachli-

chen Aufgaben der Mitarbeiter und deren Beschreibung in das Verzeichnis zu integrieren.

Im Fall der am Bündnis-Forest beteiligten staatlichen Dienststellen wird das dabei zugrunde liegende Active Directory² als Datenquelle verwendet. Auch im kommunalen Bereich sind zum Teil Active Directories und weitere Sammelverzeichnisse von Mitarbeiterdaten vorhanden.

- **Verzeichnis für den Betrieb der Public Key Infrastruktur (PKI)**
Hinsichtlich der künftigen Verwendung sicherer E-Mail-Verfahren wird die bereits vorhandene PKI in den zVD integriert. Da diese Verfahren auch im Rahmen der Kommunikation zwischen Behörden und Bürgern eine immer größere Rolle spielen werden, sollen insbesondere die für Funktionsadressen ausgestellten Zertifikate öffentlich (d.h. für Zugriffe aus dem Internet) zur Verfügung gestellt werden.
- **Benutzerverzeichnis**
Als langfristiges Ziel (im Rahmen eines gesonderten Projektes) wird die Bereitstellung eines Benutzerverzeichnisses angestrebt, in dem Kennungen und Passwörter von Behördenmitarbeitern verwaltet werden können, um hinsichtlich der Vielzahl von Identifikations- und Authentifizierungsverfahren bei der Verwendung unterschiedlicher Applikationen (etwa im eGovernment-Bereich) eine Straffung und Vereinheitlichung zu ermöglichen.

Alle im zVD enthaltenen Daten müssen für die Nutzer einheitlich und zentral verfügbar sein. Hierfür ist es erforderlich:

- übersichtlich und einheitlich gestaltete Web-Oberflächen zu entwerfen, die den Nutzern ein komfortables, aber einfaches und überschaubares Suchen ermöglichen.
- für eine nahtlose Integration der Verzeichnisdaten in die Standardprogramme der Bürokommunikation (z.B. Office, Mailprogramme) zu sorgen, um etwa die Erzeugung von Verteilern oder Serienbriefen zu ermöglichen.

Die Pflege der Daten wird dezentral an jeweils nur einer Stelle erfolgen, wobei die jeweiligen Zuständigkeiten zu regeln und abzugrenzen sind. Für die wichtigsten Arten vorhandener Informationsquellen sind geeignete Importschnittstellen vorgesehen, die eine Übernahme von Daten in den zVD mittels automatischer Prozesse ermöglichen.

² Produkt der Fa. Microsoft für die Bereitstellung eines Verzeichnisses und zentrale Komponente einer Windows-2000-Domäne

Wichtige Verzeichnisse für die Verwaltung

Komfortable Nutzung

3. Strukturelle Anforderungen

Gesamtverantwortung

Die organisatorische Gesamtverantwortung für den zVD wird zentral in die Hand einer entscheidungstragenden Stelle gelegt. Künftige Erweiterungen wie etwa die Aufnahme zusätzlicher Verzeichnisse in den zVD sind hier zu entscheiden und mit allen teilnehmenden Bereichen abzustimmen und zu koordinieren.

Lesezugriff

Die im zVD enthaltenen Informationen müssen für alle Nutzer mit entsprechender Leseberechtigung einheitlich und zentral verfügbar sein. Angesichts der Vielzahl unterschiedlicher Nutzer im Behördenumfeld und deren technischer Ausstattung dürfen dabei keine speziellen Anforderungen hinsichtlich Soft- und Hardware entstehen. Für Fachanwendungen, die beispielsweise im Rahmen von eGovernment-Verfahren Verzeichnisdaten automatisiert abgreifen, wird eine standardisierte Zugriffsschnittstelle eingerichtet, die auf dem Lightweight Directory Access Protocol (LDAP) basiert.

Datenimport und Datenpflege

Als grundlegendes Entwurfskriterium zur Datenpflege im zVD dient der Leitgedanke, die Daten so dezentral wie möglich zu pflegen. Aktualisierungen des Datenbestandes sollen generell nur an jeweils einer Stelle (i.d.R. beim Eigentümer der Information) erfolgen („single point of administration“).

Rechteverwaltung

Angesichts der sehr heterogen organisierten Struktur des Nutzerkreises des zVD ist eine feine Granulierung der Zugriffsrechte vor-

gesehen. Diese können nicht nur Verzeichnissen insgesamt, sondern bei Bedarf auch einzelnen Datenfeldern zugewiesen werden.

Datenschutz, Vertraulichkeit und Datensichtbarkeit

Während die zentrale Bereitstellung eines Dienststellenverzeichnisses sowie eines Verzeichnisses der Funktionsadressen zur Unterstützung der Kommunikation im Behördenbereich aus datenschutzrechtlicher Hinsicht unbedenklich ist, sind Mitarbeiter- und Benutzerverzeichnisse diesbezüglich sowohl hinsichtlich der in ihnen enthaltenen Angaben als auch hinsichtlich des zugelassenen Nutzerkreises zu überprüfen.

Soweit lokale Datenquellen von Behörden im Rahmen des zVD abgelöst werden, kann es sein, dass auch Informationen gepflegt werden können, die nur der internen Verwendung der jeweiligen Behörde dienen. Es muss deshalb unterschieden werden, ob

- nur innerhalb der Behörde, bzw. innerhalb des Geschäftsbereiches
- innerhalb der staatlichen Verwaltung bzw. unabhängiger Behörden
- in der gesamten bayerischen Verwaltung
- auch von außerhalb (durch andere Landesverwaltungen, Bürger und Firmen) zugegriffen werden darf.

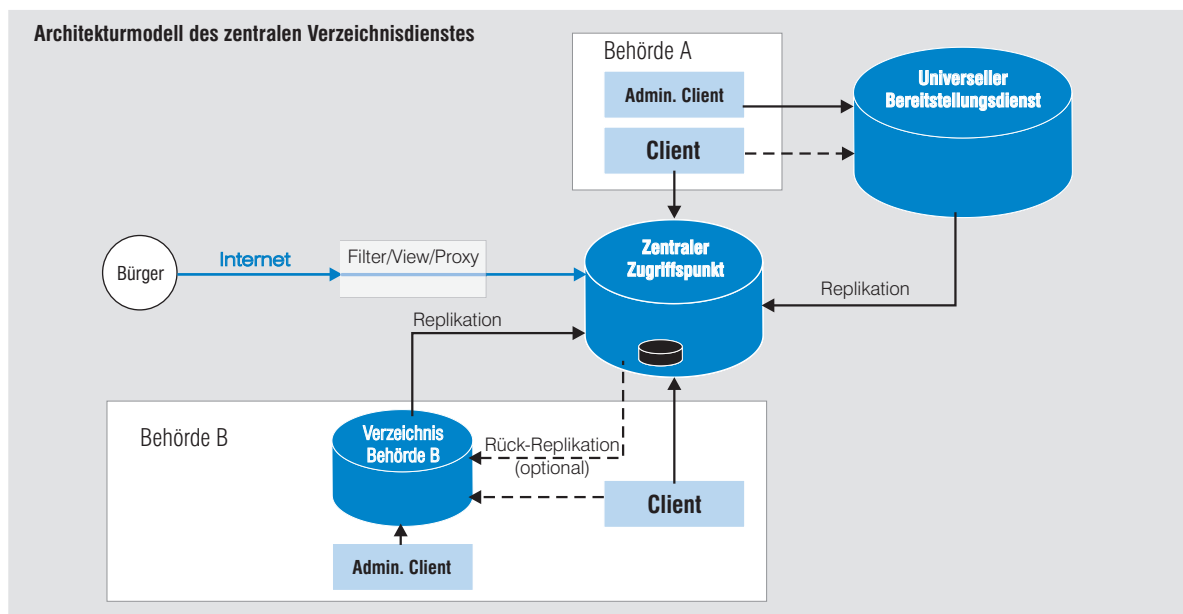
4. Architekturansatz des zVD

Das Architekturmodell des zVD besteht aus zwei miteinander kombinierten integrierten Bausteinen:

Den ersten Baustein stellt ein universeller Bereitstellungsdienst dar, der auf Wunsch existierende lokale Datenquellen ersetzt.

Bereitstellung der Informationen

Abb. 2



Zugriff auf
Informationen

Stellen, die ihre lokale Datenhaltung auflösen wollen, liefern ihre Daten einmalig an den Bereitstellungsserver und pflegen sie dort weiter. Der Bereitstellungsdienst wird initiale Migrationsprozesse und anschließend dezentrale Pflegeprozesse unterstützen und ein ausreichend feingranulares Management der Zugriffsrechte ermöglichen. Welcher Teil des Gesamtdatenbestandes des Bereitstellungsservers für welche Nutzer (auch externe) sichtbar ist, definiert jeweils die Stelle, der die Daten gehören.

Als zweiter Baustein dient ein zentraler Zugriffspunkt. Dieser erhält die Daten, die im zVD sichtbar sein sollen, über Replikationen aus den dezentralen Verzeichnissen oder vom universellen Bereitstellungsdienst. Die lokalen Verzeichnisse replizieren die notwendigen Daten regelmäßig in den zentralen Zugriffspunkt. Bei Bedarf ist auch eine Rückreplikation aus dem zentralen Zugriffspunkt in ein lokales Verzeichnis möglich.

Erläuterung zu dem in der Abbildung 2 wiedergegebenen Architekturmodell:

Die Behörde B steht beispielhaft für eine von vielen Stellen, die eigene Verzeichnisse betreiben und Daten aus diesen zuliefern, z. B. verschiedene Landkreise, Ministerien, die Stadt München oder die Landespolizei.

Hinsichtlich der Art der Datenbereitstellung ergeben sich die folgenden Leitregeln:

- Wenn die Dienststelle keinen eigenen Service betreibt oder den Betrieb einstellen will, überführt sie ihre Daten in den zentralen Service und pflegt sie dort weiter.
- Wenn die Dienststelle ein eigenes Verzeichnis betreibt, stellt sie den relevanten Datenbestand durch Replikation auf dem zentralen Zugriffspunkt zur Verfügung.

5. Weitere Schritte

Nach Abstimmung des Grobkonzeptes innerhalb der staatlichen und kommunalen Behörden werden die folgenden weiteren Schritte durchgeführt:

- Vorplanung des weiteren Projekts (Gegenüberstellung von geschätztem Aufwand und künftig bereitgestellten finanziellen und personellen Ressourcen)
- Anreicherung des Grobkonzeptes zu einem detaillierten Feinkonzept mit anschließender Ausschreibung und Produktauswahl
- stufenweise Implementierung der Verzeichnisse und Funktionalitäten des zVD (beginnend mit dem Dienststellenverzeichnis und der anschließenden Bereitstellung des Verzeichnisses von Funktionsadressen)
- initialer Datenaufbau und Migration bestehender Verzeichnisse sowie Einführung der automatischen Prozesse zur Datenpflege.

Im Feinkonzept werden unter anderem die folgenden Punkte berücksichtigt:

Feinkonzept

- Für jedes Verzeichnis wird geklärt, welche Informationen bereitgestellt werden und welcher Nutzerkreis in welchem Umfang zugriffsberechtigt ist.
- Des Weiteren werden die zu verwendenden hierarchischen Organisationsstrukturen sowie die Art und Zusammensetzung aller Einträge vereinbart.
- Alle zentral verwendeten Namen und Begriffe sind unter allen Beteiligten einvernehmlich abzustimmen.
- Für alle Prozesse, die zwischen bestehenden lokalen Verzeichnissen und dem zVD vermitteln, sind entsprechende Schnittstellen zu definieren.