



# Meta Directory als sicheres und zentrales Kommunikationsverzeichnis für das Land Baden-Württemberg

Rolf Häcker, Martin König

Zentrum für Kommunikationstechnik und Datenverarbeitung Baden-Württemberg

**Zusammenfassung** In der Landesverwaltung Baden-Württemberg werden Verwaltungsabläufe möglichst vollständig auf elektronischer Basis abgewickelt. Daran beteiligt sind neben Dienststellen der Landesverwaltung auch Kommunen sowie Stellen anderer Bundesländer. Künftig sollen auch Bürger über das geplante e-Bürgerdienste-Portal des Landes Baden-Württemberg an elektronischen Verwaltungsabläufen teilnehmen können. Da es sich bei den auszutauschenden Informationen häufig um sensible und rechtsverbindliche Verfahrens-Daten handelt, kommt zunehmend auch die Verschlüsselung und Signatur zum Einsatz.

Für eine bestmögliche Funktion ist eine zuverlässige und aktuelle Adress- und Zertifikatsverwaltung Grundvoraussetzung. Bisher werden aufgrund der Selbstständigkeit der Dienststellen auch unterschiedliche Verzeichnisse genutzt. Häufig tragen auch technische Gegebenheiten zu der Verzeichnisvielfalt bei. Die Folgen sind redundante Pflegeaufwände und oft nicht aktuelle Daten. Sowohl beim Anwender als auch bei den zuständigen Administratoren führt dies zu Ärgernissen und mangelnder Akzeptanz der elektronischen Kommunikation.

Um die Situation zu verbessern, setzt das Land Baden-Württemberg seit Sommer 2001 die Siemens Verzeichnissoftware DirX als zentrale Informationsplattform ein. Damit wird erreicht, dass Daten unterschiedlicher Systeme an einer Stelle zusammengeführt werden.

Das Metadirectory dient als zentraler Verzeichnisdienst, in den die Adressen der

- Landesdienststellen,
- Kommunen,
- Bundesbehörden (geplant)

sowie Zertifikate zur Verschlüsselung integriert werden, die in unterschiedlichen Systemen (z.B. MS-Exchange 5.5, Activ-Directory, LDAP-Servern, etc) geführt werden.

Den Anwendern des Landes, der Kommunen sowie des Bundes stehen verschiedenen Oberflächen zur Nutzung zur Verfügung. Geplant ist sogar die Bereitstellung von Informationen für die Bürger über das Internet.

## 1 Ausgangslage

Im Land Baden-Württemberg gibt es vielfältige elektronische Kommunikationsbeziehungen zu Partnern bei der EU, beim Bund, den Ländern, dem kommunalen Bereich bis hin

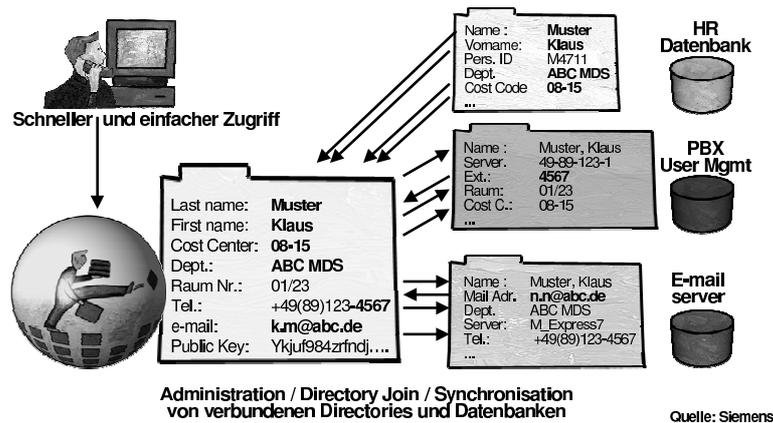


zum Bürger. Zum Schutz von sensiblen Informationen und zur Gewährleistung der Rechtssicherheit von Transaktionen werden Verschlüsselungstechnik und elektronische Signatur künftig eine zunehmende Bedeutung erlangen. Erste Pilotprojekte (BW-Card) hierzu laufen bereits.

Zu den wichtigsten Anforderungen an ein einheitliches Benutzerverzeichnis gehören ein leicht handhabbarer Zugriff auf die benötigten Informationen, hohe Aktualität und geringer Pflegeaufwand, außerdem Wirtschaftlichkeit und die Erweiterbarkeit für künftige Anforderungen. Zweckmäßig ist ferner, wenn neben den aktuellen E-Mail Adressen auch ggf. vorhandene Zertifikate der Partner bereitgestellt werden, die beim Absenden von verschlüsselten Nachrichten unmittelbar für den Versandprozess benötigt werden.

## 2 Meta-Directory

Ein Meta-Directory ermöglicht den Zugang zu sämtlichen Informationen einer Organisation, die in unterschiedlichen Verzeichnissen gespeichert sind sowie deren Administration von einer einzigen Stelle aus. Die Grundidee ist, dass Daten nur noch von den Stellen erfasst und gepflegt werden, die jeweils originär dafür zuständig sind.



**Abbildung 1:** Meta Directory Architektur / Funktionalität

So wird z.B.:

- der Datensatz für einen neuen Mitarbeiter von der Personalabteilung angelegt und entsprechend gepflegt (Name, Vorname, Abteilung, Kostenstelle...),
- die Telefonnummer vom entsprechenden Administrator nachgetragen,
- die E-Mail Adresse vom E-Mail Administrator auf der Basis der vorliegenden Informationen festgelegt und der Verzeichniseintrag entsprechend ergänzt. Damit erspart er sich das Eintragen des Namens und die Pflege der Telefonnummer für eventuelle Rückfragen.

Daraus ergeben sich Vorteile wie:

Hohe Datenverfügbarkeit und schneller Zugriff auf aktuelle Informationen, keine Medienbrüche, weniger Fehler, verbesserte Sicherheit sowie die effiziente Erfassung und Pflege von Daten.

Bei der Integration neuer Dienste kann das Verzeichnis einfach erweitert werden. Darüber hinaus bietet sich die Möglichkeit zu Automatisierung von Administrationsvorgängen (Bsp. Der Telefon- oder der E-Mail-Administrator könnten die benötigten Personaldaten, die ja in standardisierter Form im Meta-Directory vorliegen automatisiert von dort in ihr jeweiliges System übernehmen und anschließend ihren ggf. automatisch generierten Input einspeisen).

Kommunikationsabläufe werden optimiert, weitere Partner können eingebunden werden. Eine erweiterbare, skalierbare Lösung gewährleistet den Investitionsschutz.

### 3 Wichtigste Projektziele:

Im Land Baden-Württemberg gibt es zunehmenden Bedarf zur elektronischen Kommunikation zwischen staatlichen und kommunalen Stellen.

Die informationstechnische Infrastruktur ist historisch gewachsen und keineswegs homogen. Es gibt unterschiedliche Zuständigkeiten. Während die Landesdienststellen über das Landesverwaltungsnetz erreichbar sind, hat nur ein Teil der Kommunen eine entsprechende Anbindung an den Verbund der kommunalen Verwaltungsnetze (KVN), andere sind nur über das Internet erreichbar.

- Für die Kommunikationspartner ergeben sich eine ganze Reihe von Fragen:
- Wie lautet die E-Mail Adresse des Partners?
- Wird die Nachricht auf internem Weg über den KVN/LVN-Verbund zugestellt oder extern über das Internet?
- Welche Maßnahmen bzw. Verfahren zur Erhöhung der Sicherheit (Verschlüsselung, Signatur) unterstützt der Partner?
- Wo sind die entsprechenden Zertifikate verfügbar?

Die von den Produktherstellern vielfach gepriesenen Automatisierungsmöglichkeiten im Zusammenhang mit einem Meta-Directory wie z.B. die Erzeugung der E-Mail Adresse auf der Basis des Benutzernamens und der Dienststelle und die automatische Weitergabe an das Mail-System, spielen in Baden-Württemberg (zunächst) noch keine große Rolle.

Die Kompatibilität mit anderen Projekten muss jedoch beachtet werden. Hierzu gehören Optionen für den Einsatz von Active Directory und Exchange 2000 in der Landesverwaltung und die Möglichkeit der Anbindung von weiteren Verzeichnissen.

Wichtige Ziele sind: Eine hohe Aktualität der verfügbaren Daten mit einem geringen Administrationsaufwand zu erreichen und Redundanzen zu vermeiden. Gleichzeitig wird ein wichtiges Fundament für die Realisierung elektronischer Bürgerdienste gelegt. Dadurch vereinfacht sich die Kommunikation mit Partnern.

#### 4 Spezifische Informationen

Je nach Benutzergruppe sind unterschiedliche Sichten auf das Verzeichnis realisiert. Während den Kollegen und Kolleginnen innerhalb der Dienststelle alle Informationen über E-Mail-Adressen und Telefonnummern nebst Zimmernummer zur Verfügung stehen, werden außerhalb evtl. nur noch Adressen der Poststelle, d.h. des Sekretariats und die ausgewählter Mitarbeiter bekannt gegeben. Alle anderen Mitarbeiter werden im Regelfall über die Kopfstellen in die Arbeitsabläufe eingebunden und sollen von außen nicht direkt adressiert werden.

Die Beschränkung der Zugriffe auf die jeweils vorgesehenen Daten lässt sich auf verschiedene Art und Weise realisieren. Einerseits werden nur die benötigten Daten in das Meta-Directory übertragen, denn Informationen die dort nicht gespeichert sind, können auch nicht missbräuchlich abgerufen werden.

Andererseits können je nach Anwender – u.U. reicht auch eine Differenzierung nach Gruppenzugehörigkeit des Anwenders – unterschiedliche Berechtigungsprofile eingerichtet werden. Dadurch werden die Informationen aus dem Verzeichnis bedarfsgerecht und individuell gefiltert zur Verfügung gestellt.

#### 5 Praktische Umsetzung

Der Aufbau des Meta-Directories in Baden-Württemberg verlief in folgenden Abschnitten:

Zunächst wurde der Exchange 5.5-Verbund an das Meta-Directory angebunden. Die Daten werden vom Exchange Verbund (rund 100 MTAs) zum Meta-Directory übertragen. Zugriffsmöglichkeiten ergeben sich zunächst über einen Web-Client oder zwei verschiedene Plugins für Outlook, die im folgenden noch beschrieben werden.

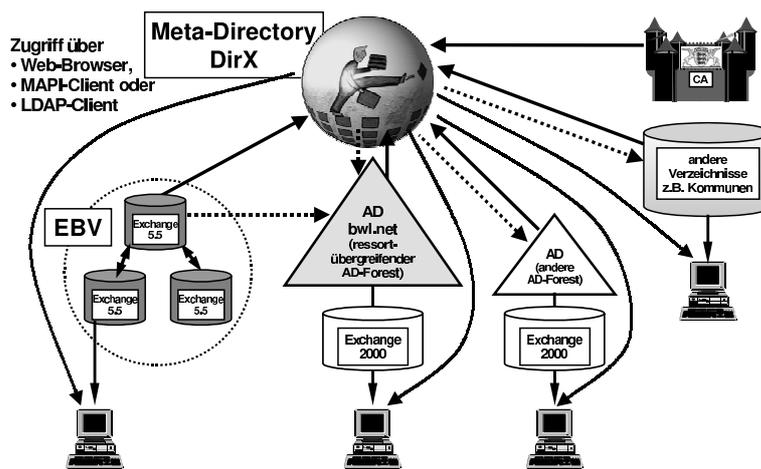


Abbildung 2: Kopplung von Verzeichnissen

Bei den staatlichen Stellen in Baden-Württemberg läuft die Umstellung auf das Active Directory, das ebenfalls direkt an das Meta-Directory angebunden wurde. Außerdem wird die Migration auf Exchange 2000 geprüft. Über Exchange 2000 wäre dann ebenfalls ein Zugriff auf die Daten im Meta-Directory möglich. Sofern es erforderlich ist mehrere getrennte Active Directories des Landes getrennt zu realisieren, könnten diese im erforderlichen Umfang über das Meta-Directory gekoppelt werden, um den notwendigen Datenaustausch zu realisieren.

Verzeichnisse des kommunalen Bereichs können ebenfalls direkt eingebunden werden. Interimsweise ist bereits eine File-Schnittstelle im Einsatz, über die die kommunalen Adressen importiert werden. Die kommunalen Rechenzentren sind jedoch dabei, ebenfalls Active Directories zu projektieren.

## 6 Zugriffsmöglichkeiten

Für den Zugriff auf die im Meta-Directory gespeicherten Daten gibt es heute bereits verschiedene Möglichkeiten:

Ein Web-Browser, der kostenlos zur Verfügung steht, bietet Suchmöglichkeiten und liefert bei gefundenen Adressen einen Hyperlink, der den Mail-Client öffnet und die Adresse als Adressat (im „AN“-Feld) einträgt. Das Hinzufügen weiterer Adressaten und die Nutzung der Felder „CC“ und „BCC“ ist über „copy and paste“ möglich.

Für den in der Landesverwaltung eingesetzten Mail-Client Outlook gibt es verschiedene Plugins:

Der MAPI-Client bietet bereits recht umfangreiche Suchmöglichkeiten und unterstützt auch die Versorgung der Felder „AN“, „CC“ und „BCC“. Es können nacheinander auch mehrere Adressaten übernommen werden.

Auch der LDAP-Client unterstützt die letztgenannten Möglichkeiten. Die Suchmöglichkeiten sind nicht so komfortabel, dafür ist der LDAP-Client unentgeltlich erhältlich.

Die Suche nach und die Bereitstellung von Zertifikaten wird bisher von keiner dieser Zugriffsmöglichkeiten unterstützt.

Für den Anwender steht und fällt die Nutzbarkeit eines Meta-Directories mit der Qualität des für den Zugriff bereitgestellten Werkzeugs.

Daher wird an einem Pflichtenheft zur Entwicklung eines optimalen Suchwerkzeugs gearbeitet, das dann als Outlook Plugin und ggf. auch als unabhängiges Tool (z.B. als Web-Client) bereitgestellt werden soll.

Für den Anwender ist wichtig, dass er nicht nur die E-Mail-Adresse eines Kommunikationspartners schnell und zuverlässig findet, sondern auch die Information darüber, ob das Mail-System dieses Partners elektronisch signierte und verschlüsselte Nachrichten verarbeiten kann und welche Verfahren es ggf. unterstützt. Im Bedarfsfall müssen auch die entsprechenden Schlüssel bzw. Zertifikate bereitgestellt werden.

Es können auch weitergehende Informationen wie Dienststelle, Dienstort, Raum, Telefonnummer etc. ausgegeben werden. Hierfür sind jedoch organisatorische Regelungen unter



Berücksichtigung des Datenschutzes erforderlich. Zur Bereitstellung der personenbezogenen Informationen müsste ggf. sogar die persönliche Zustimmung der Betroffenen eingeholt werden.

## 7 Erfahrungen

Neben der technischen Bereitstellung von Konnektoren zur Verbindung von Verzeichnissen, sind verbindliche organisatorische Festlegungen der zu pflegenden Informationen erforderlich. Dies betrifft auch einheitliche Namenskonventionen z.B. für Umlaute und für Dienststellenbezeichnungen.

Die Übernahme von Datensätzen aus dem bisherigen Exchange 5.5-Verbund von rund 100 Mail-Transfer-Agents (MTAs) in das Meta-Directory funktioniert problemlos. Wenn bisher das Feld „Dienstort“ jedoch aus Effizienzgründen nicht eingepflegt wurde, so kann im Meta-Directory auch nicht nach diesem Datum gesucht werden. Die beteiligten Organisationen müssen Aufwand und Nutzen für die möglicherweise bereitzustellenden Informationen prüfen und die einheitliche Vorgehensweise untereinander abstimmen.

Für die praktische Nutzbarkeit der im Meta-Directory bereitgestellten Informationen ist es hilfreich, wenn diese von den entsprechenden Anwendungen möglichst unmittelbar übernommen werden können. Beispielsweise wäre es zweckmäßig, wenn Plugins zur elektronischen Signatur und Verschlüsselung von E-Mails die entsprechenden X.509 Zertifikate direkt – z.B. über eine LDAP-Schnittstelle aus dem Verzeichnis übernehmen könnten. Dies ist derzeit noch nicht gegeben. Hier sind die Partner in den Pilotprojekten gefordert, ihre Software entsprechend weiter zu entwickeln. Entsprechende Absichtserklärungen liegen auch bereits vor.

