Corporate Information Research Center
IRC
TECHNOLOGY INFORMATION

SIEMENS

TECHNOLOGY INFORMATION TECHNOLOGY INFORMATION TECHNOLOGY INFORMATION

Directory Services

Vielseitig genutzte Werkzeuge für das Datenmanagement in integrierten Lösungen

Ein Technology Report von CT IRC TIS

Zusammenfassung

Dr. Dietmar Fauth, CT IRC TIS
Tel.: ++49-89-636-43343
dietmar.fauth@siemens.com

Dr. Waltraud Mayer-Amm, ICN EN SNS MDS
Dr. Hermann Wagner, ICN EN SNS MDS

Januar 2003

Inhaltsverzeichnis der Zusammenfassung

1 Management Summary

Bei Directory Services handelt es sich um eine Software-Technologie zum Abspeichern nicht-flüchtiger Informationen wie Adressdaten, Berechtigungen oder Profilen von Personen, Geräten oder Software-Applikationen, auf welche an vielen Orten durch die unterschiedlichsten Anwendungen hauptsächlich lesend zugegriffen wird.

Directory Services werden heute in den folgenden Anwendungsgebieten eingesetzt:

- Information
  z.B. als Mitarbeiter-, Partner-, oder Kundenverzeichnis in Unternehmen. Insbesondere bei Telekommunikationsunternehmen (Carriern) werden Millionen von Einträgen verwaltet.

- Kommunikation
  z.B. zur Benutzerverwaltung in Lösungen zu Unified Messaging , Voice over IP (VoIP) oder Billing und Accounting

- Benutzeradministration
  zur Verwaltung von Benutzern und deren Rechten an den in einem Unternehmen eingesetzten Anwendungen

- Security
  als wesentliche Komponenten in Firewall-, Single Sign-On oder Public Key Infrastrukturprojekten

- E-Business
  in Portal- oder Virtual Private Network-Lösungen, wobei die o.g. Felder ebenfalls eine bedeutende Rolle spielen.

Bei dem Directory-Geschäft handelt es sich vorwiegend um ein Dienstleistungsgeschäft. So bewegt sich der Markt für Directory-Produkte in den verschiedenen Einsatzfällen laut den Analysten in dem Bereich einiger Hundert Millionen US $; der Gesamtumsatz für die Realisierung kompletter Lösungen wird aber durchgehend auf ein 6-faches des o.g. Betrags geschätzt.

Die Trends zum Einsatz von Directory Services in den Unternehmen laufen auf die Unterstützung einer vollständig elektronischen Abwicklung der Beziehungen zwischen den Unternehmen und ihren Kunden und Partnern sowie zu deren Mitarbeitern hin. Weitere zukünftige Einsatzfelder bestehen in der Personalisierung mobiler Dienste oder im Umfeld von E-Government.

Es kann mit ziemlicher Gewissheit argumentiert werden, dass alle Software-Produkte und -Lösungen, welche eines der o.g. Gebiete abdecken, so konzipiert sein müssen, dass eine Integration mit einem zentralen Directory Service ohne Schwierigkeiten möglich ist.

2 An wen richtet sich dieser Technology Report?

Dieser Technology Report enthält aus Sicht der Autoren interessante Informationen für den folgenden Leserkreis:

- Verantwortliche und Experten für Produkte, die in den Gebieten Information, Kommunikation, Benutzeradministration, Security und E-Business eingesetzt werden und welche somit mit Directory Services integrierbar sein müssen
- Consultants für Lösungen auf den o.g. Gebieten
- Mitarbeiter von Infrastrukturabteilungen, die zur Optimierung ihres täglichen Betriebs einen Directory Service gewinnbringend einsetzen können
- Personen, welche über den Tellerrand ihrer eigenen Produkte und Lösungen schauen und neue Potentiale und Einsatzmöglichkeiten für dieselben erkennen wollen
- Interessierte Endanwender von Directory-basierten Produkten wie Siemens Corporate Directory, Telephonie-Anwendungen und dergleichen

Die Gliederung dieser Zusammenfassung widerspiegelt auch die Struktur der nachfolgenden Literatursammlung. Im anschließenden Kapitel 3 werden die vielfältigen Nutzungsmöglichkeiten von Directory Services aus Sicht eines Endanwenders aufgezeigt und es wird eine kurze Einführung in die Technologie von Directory Services gegeben.

Kapitel 4 erläutert jeweils an Hand einiger Beispielsszenarien, wie Directory Services in den bereits genannten Gebieten Information, Kommunikation, Benutzeradministration, Security und E-Business schon heute eingesetzt werden.

Es folgt in Kapitel 5 eine ausführliche Betrachtung von Markt und Herstellern, ehe in Kapitel 6 ein Ausblick auf zukünftige Nutzungsmöglichkeiten von Directory Services gegeben wird.

In der abschließenden Bibliographie 7 sind neben den Aufsätzen und Reports, welche in der Literatursammlung enthalten sind, noch weitere zitiert, welche über die Bibliothek oder CT IRC TIS zusätzlich bezogen werden können.

3 Basistechnologie

3.1 Was ist ein Directory Service?

Um es direkt auf den Punkt zu bringen: Ein Directory Service (deutsch: Verzeichnisdienst) ist eine spezielle Datenbanktechnologie, demzufolge also Software [1], [2], [3], [4]. Auch wenn Directory Services nicht annähernd den Bekanntheitsgrad relationaler Datenbanken haben, so nimmt deren Bedeutung doch fortwährend zu.

Obwohl es Directory Services schon sehr lange gibt — die ersten Standards für Directory Services wurden im Jahr 1988 verabschiedet — hat die Directory-Technologie bislang eher ein Schattendasein gefristet. Anbieter von Directory Services, die in kurzer Folge und mit großem Marketingaufwand neue Versionen ihrer Produkte ankündigen, sowie eine stetig wachsende Zahl von Herstellern directory-basierter Anwendungen lassen Directory Services mehr und mehr ins Rampenlicht der Öffentlichkeit gelangen. Hinzu kommt, dass Microsoft in sein allseits bekanntes Betriebssystem Windows einen eigenen Directory Service integriert hat (Microsoft Active Directory – ADS), was Directory Services zusätzlich in den Blickwinkel rückt (s. Kapitel 5.1 sowie die dort aufgeführte Literatur).

Wozu dienen Directory Services? Anhand eines Beispiels sei die Arbeitsweise eines Directory Services erläutert:

> *Herr Klein loggt sich jeden Morgen auf der Web Site seiner bevorzugten Tageszeitung ein. Dort studiert er zunächst lokale, nationale und internationale Nachrichten, liest die tägliche Kurzgeschichte und erkundigt sich nach den Wetteraussichten an seinem Wohnort. Der Web Server identifiziert (via Cookie) Herrn Klein und präsentiert ihm exakt die Informationen, die er präferiert. Herrn Kleins Präferenzen sind dabei in einem Directory Service hinterlegt (Nachrichten lokal, national und international, aber keine Sportnachrichten, Kurzgeschichte, Wetteraussichten am Wohnort). In dem Augenblick, in dem sich Herr Klein beim Web Server seiner Tageszeitung anmeldet, erfragt der Web Server beim Directory Service blitzschnell die Präferenzen von Herrn Klein und präsentiert diesem dann seine "persönliche" Tageszeitung mit Nachrichten ohne Sport, mit Kurzgeschichte und Wetteraussichten. Der Directory Service agiert also in diesem Fall völlig transparent. Er ist nur sehr mittelbar wahrzunehmen.*
>
> *Nach dem Studium seiner "persönlichen" Zeitung fährt Herr Klein ins Büro. Dort loggt er sich an seinem Arbeitsplatz-PC ins Netzwerk seines Arbeitgebers ein. Neue E-Mails und ein aktualisierter Kalender werden automatisch vom Netzwerk heruntergeladen. Außerdem erhält Herr Klein Ad-Hoc-Nachrichten, z. B., dass die Beantragung einer Video-Standleitung mit einer gewissen Bandbreite für eine Videokonferenz mit Kollegen in den USA genehmigt und eingerichtet wurde und die Teilnehmer der Konferenzschaltung benachrichtigt wurden. Während seiner Arbeit kann Herr Klein mit allen Ressourcen arbeiten, die er benötigt. Ein erneutes Einloggen an den Ressourcen ist nicht erforderlich. Insbesondere muss sich Herr Klein nicht unzählige Passwörter zum Einloggen in die Ressourcen merken.*
>
> *Am Abend wieder zu Hause fällt Herrn Klein ein, dass seine Tochter in wenigen Tagen Geburtstag hat. Er weiß, dass sie sich das neueste Buch ihres Lieblingsautors wünscht. Herr Klein loggt sich bei seinem bevorzugten Internet-Buchhändler ein und sucht nach dem entsprechenden Autor und seinem neuesten Werk. Innerhalb kürzester Zeit ist das Buch ermittelt und Herr Klein schickt eine Bestellung zur Lieferung an seine Tochter ab. Die Bestellapplikation des Internet-Buchhändlers weist die Bestellung jedoch zurück, da Herrn Kleins Kreditkarte abgelaufen ist. Herr Klein loggt sich bei seiner Bank ein und mit wenigen Mausklicks und einer Sicherheitsüberprüfung per Smartcard hat Herrn Klein seine Kreditkarte erneuert – und das Buch ist auf dem Weg zu seiner Tochter.*

In jedem dieser Szenarien spielen Directorys eine zentrale Rolle. Bei der Personalisierung von Web Sites, so wie im ersten Beispielszenario dargelegt, werden im Directory Service Informationen zu inhaltlicher Präferenz, Benutzerprofilen oder persönlichen Links verwaltet. Im zweiten Szenario verwaltet ein Directory Service alle betriebssystem-relevanten Informationen, beispielsweise Netzwerkeinstellungen inkl. E-Mail und Kalender, Zugriffsrechte für Applikationen, Desktop-Konfiguration. Im dritten Szenario verwaltet der Internet-Buchhändler mit einem Directory Service seine Kunden (Kundenprofil inkl. Kundenpräferenzen und Kreditkarteninformationen). Außerdem setzt Herrn Kleins Bank einen Directory Service zur Verwaltung ihrer Kunden und zur

Durchführung von Internet-Banking ein (Kundenprofil, Rechte der einzelnen Kunden im Internet-Banking).

Wie das zuvor behandelte Beispiel zeigt, sind Directory Services heute allgegenwärtig, allerdings in völlig transparenter Form. Diese Transparenz ist mit ein Grund dafür, dass Directory Services bislang weitgehend im verborgenen geblieben sind. Directory Services stellen eine leistungsfähige Technologie dar, welche die logisch zentrale Verwaltung von physikalisch verteilten Ressourcen ermöglicht. Als solches dienen Directory Services der sicheren Administration komplexer Systeme von zusammenhängenden Informationen und der verteilten und schnellen Bereitstellung dieser Informationen.

3.2 Directory Service vs. relationaler Datenbank

Wie zu Beginn erläutert, handelt es sich bei Directory Services rein technologisch um spezielle Datenbanken [5]. In einem Directory Service werden die Informationen hierarchisch gespeichert und nicht, wie in einer relationalen Datenbank, als Liste. Die hierarchische Speicherung von Informationen ist beispielsweise vom Telefonbuch her bekannt:

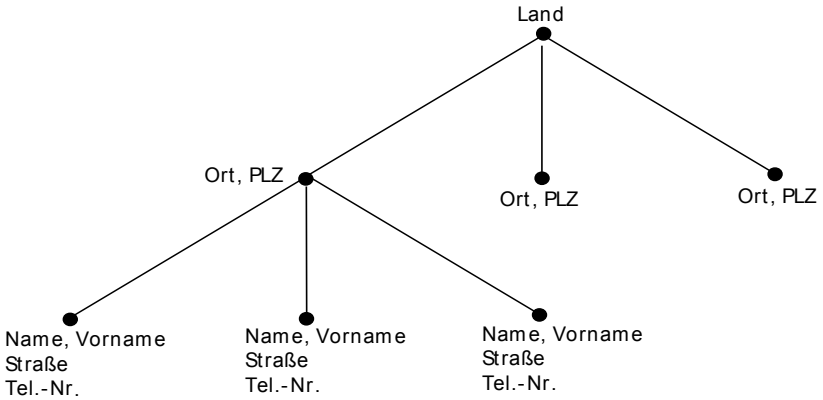

Abbildung 1: Hierarchische Datenstruktur eines Directory Service

Eine derartige hierarchische Struktur der Informationen ist immer dann von Vorteil, wenn es darauf ankommt, Informationen schnell zu finden und zu lesen [6]. Demgegenüber sind die listenartig organisierten relationalen Datenbanken von Vorteil, falls in erster Linie das Ziel verfolgt wird, Informationen oft und schnell in die Datenbank zu schreiben, mithin also in Szenarien, in denen sich die Informationen / Daten oft ändern. Des weiteren sind Directory Services, bedingt durch die baumartige Struktur, sehr leicht über ein Netzwerk verteilbar (Verteilen des ganzen Baumes oder von Teilen davon ab einer Verzweigung, s. z.B. [3]). Dies ermöglicht, dass die in einem Directory Service hinterlegten Informationen ohne weiteres vielen verschiedenen Ressourcen , die über viele verschiedene Orte verteilt sind, verfügbar gemacht werden können, ohne dass die Performance des gesamten Directory Service darunter leidet. Relationale Datenbanken eigenen sich eher in Szenarien, in denen viele Ressourcen gleichzeitig schreibend auf die Datenbank zugreifen und die Integrität der Transaktionen sowie die sofortige Verfügbarkeit aller Änderungen eine zentrale Rolle spielt.

Relationale Datenbanken sind also immer dann besonders gut geeignet, falls

- die in der relationalen Datenbank hinterlegten Informationen sich oft ändern,
- viele verschiedene Ressourcen gleichzeitig Informationen in der Datenbank ändern,
- Veränderungen an den in der Datenbank hinterlegten Informationen sofort allen Ressourcen zur Verfügung stehen müssen,
- die Integrität der Transaktionen absolute Priorität besitzt.

Beispiele für Szenarien, in denen eine relationale Datenbank erste Wahl ist, sind

- das Buchungssystem einer Fluglinie,
- das Buchungssystem einer Bank,
- das Ticket-Bestellsystem eines Veranstalters.

Relationale Datenbanken eigenen sich also in erster Linie als Basis für eher transaktionsorientierte Applikationen.

Directory Services sind hingegen immer dann erste Wahl, falls

- eine hierarchische Struktur der hinterlegten Informationen von Vorteil ist,
- das Verhältnis lesender Zugriff auf die hinterlegten Informationen zu schreibendem Zugriff hoch ist,
- schnelles Suchen und Finden von hinterlegten Informationen allerhöchste Priorität besitzt,
- die hinterlegten Informationen vielen verschiedenen Ressourcen an vielen verschiedenen Orten zugänglich gemacht werden müssen.

Beispiele für Szenarien, in denen ein Directory Service bevorzugt zum Einsatz kommen sollte, sind

- Elektronische Telefonbücher / Gelbe Seiten; (White und Yellow Pages),
- Verwaltung von Benutzerprofilen, Applikations- und Ressourcenprofilen, Sicherheitsprofilen,
- Verwaltung von Netzwerkparametern und -profilen (Netzwerk-Policies).

Directory Services bieten demzufolge einen zentralen Integrationspunkt für eine Vielzahl von Applikationen und Diensten. Organisationen, die einen Directory Service als zentralen Integrationspunkt für ihre Applikationen und Dienste benutzen, berichten über einen Return on Investment von weit über 100 % in den ersten beiden oder sogar im ersten Jahr nach Implementierung des Directory Service [7], [8].

3.3 Standards für Directory Services

Die Entwicklung von Directory Services hat sich in der Vergangenheit nicht unkontrolliert vollzogen. Vielmehr gibt es zwei fest definierte und kontinuierlich gepflegte Standards, welche die Entwicklung von Directory Services festlegen:

1. Der X.500 Standard [3], [4]: Dieser Standard wurde in den 80er Jahren von der ITU (International Telecommunication Union) entworfen. X.500 definiert den Aufbau eines Directory Service, das Datenmodell sowie Zugriffs- und Replikationsprotokolle.
2. Der LDAP Standard [9], [10]: Dieser Standard wurde Anfang der 90er Jahre von der IETF (Internet Engineering Task Force) entworfen. LDAP definiert ausschließlich den Zugriff auf einen Directory Service (nicht jedoch den Aufbau des Directory Service an sich) und stellt eine Vereinfachung des im X.500 Standard festgelegten Zugriffs dar. LDAP hat sich als Zugriffsprotokoll auf Directory Services heute allgemein durchgesetzt.

Ein Directory Service beruht damit auf zwei Standards: Dem X.500 Standard, der den Aufbau des Directory Service an sich definiert (d. h. wie Informationen zu hinterlegen sind), und dem LDAP Standard, der festlegt, wie auf die in einem Directory Service hinterlegten Informationen zugegriffen werden kann.

4 Anwendungsszenarien

Das eingangs geschilderte Beispiel lässt erahnen, dass die Einsatzmöglichkeiten für Directory Services vielfältiger Natur sind. Nachfolgend eine schematische Darstellung der unterschiedlichen Einsatzfelder für Directory Services:

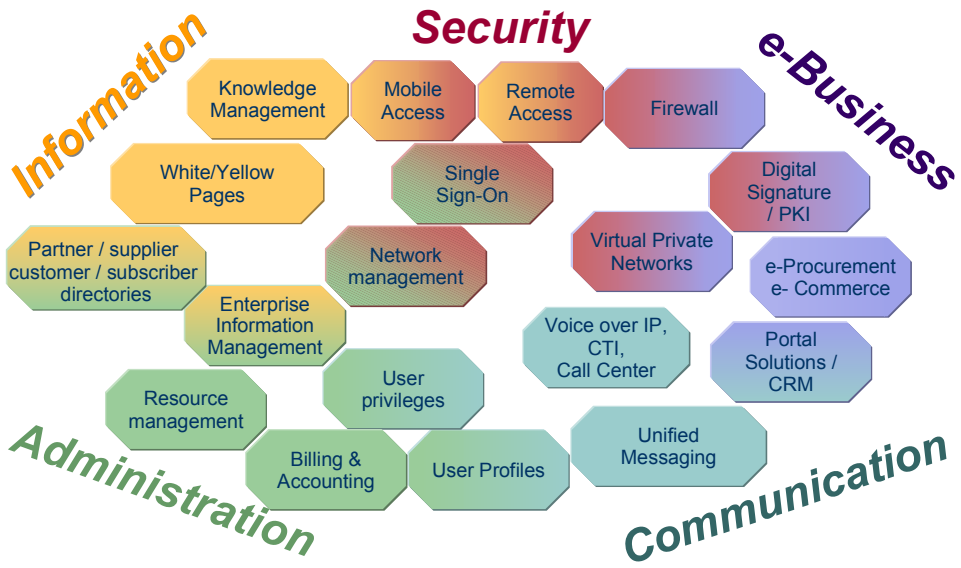

Abbildung 2: Einsatzszenarien von Directory Services

Auf eine Reihe dieser Einsatzfelder wird im Folgenden näher eingegangen. Mit zwei Sonderfällen wollen wir wegen derer allgemeinen Bedeutung bzw. ihrer Bedeutung für Siemens die Betrachtungen beginnen.

4.1 White / Yellow Pages: Siemens Corporate Directory (SCD)

Ein weit verbreitetes Anwendungsszenario für Directory Services ist die Bereitstellung eines Web-basierten elektronischen Telefonbuchs oder, allgemeiner, eines Web-basierten elektronischen Auskunftssystems für die Mitarbeiter eines Unternehmens. Auch Siemens macht hier keine Ausnahme. Das Siemens Corporate Directory (SCD) ist das unternehmensweite Information Center für Siemens Mitarbeiter. Es ist ein Directory Service, der viele unterschiedliche Informationen zu allen Mitarbeitern - aber auch institutionellen Kommunikationspartnern - zusammenführt, speichert, schnell verarbeitet und abgleicht. Es ermöglicht über eine bedienungsfreundliche Oberfläche einen leichten und schnellen Zugriff auf die inzwischen ca. 400.000 Einträge. Die mittlerweile unternehmensweit bekannte und genutzte Oberfläche für die Suche nach Mitarbeitern ist in der Abbildung 3 widergegeben.

Abbildung 3: Suchmaske des Siemens Corporate Directory

Zu einem im Directory hinterlegten Eintrag gehören beispielsweise Telefonnummern, e-Mail-Adressen oder auch Abteilung, Standort, Vertretung, Sekretariat oder Mobiltelefon. Auch lassen sich direkt im SCD per Mausklick weiterführende Quellen wie Standortpläne oder einzelne Homepages aufrufen. E-Mails lassen sich per Klick verschlüsseln und signieren. Hierzu werden im SCD Public Keys hinterlegt; die Private Keys erhalten die Mitarbeiter z.B. auf ihrem Firmenausweis. Weitere Zusatzdienste sind ScreenIt, Mailshopper, NetMeeting und vCard, welche die Übernahme einer Adresse in ein persönliches Adressbuch ermöglicht. Benutzer von PDAs können Datensätze aus dem SCD im Kontakte-Ordner von Outlook speichern und von dort auf den PDA synchronisieren. Weitere wesentliche Vorteile werden durch die Verwendung in anderen Applikationen gewonnen; so verwendet u.a. das Siemens Employee Portal seit Februar 2002 ein SCD-basiertes Login.

4.2 Meta Directory Services

Wie bereits mehrfach dargelegt, sind Directorys heute allgegenwärtig. Eine Untersuchung des renommierten Analystenhauses Forrester Research hat gezeigt, dass jedes Unternehmen heute durchschnittlich 180 Directory Services im Einsatz hat. In diesen vielen verschiedenen Directory Services verwaltet ein Unternehmen Informationen über Mitarbeiter und Kunden, über Netzwerke, Geräte, Anwendungen und vieles mehr. Sie sind einerseits Nachschlagewerke wie Telefon- oder e-Mail-Listen, andererseits aber auch Basis für immer zahlreicher werdende Anwendungen: e-Business, Mobile Business, Security-Anwendungen, Computer Telephony Integration (CTI) etc. Die meisten dieser Directory Services werden einzeln gepflegt, obwohl häufig ein und dieselben Daten in mehreren Directory Services parallel benötigt werden. Das Resultat: eine hohe Redundanz, eine hohe Fehleranfälligkeit und jede Menge verlorene Zeit.

Ein Meta Directory ordnet diesen Datendschungel. Aus vorhandenen Directory Services sucht es sich automatisch die Teile zusammen, die es für genau einen Eintrag mit allen Angaben zu einem Mitarbeiter, einem Rechner, Netz oder Kunden braucht:

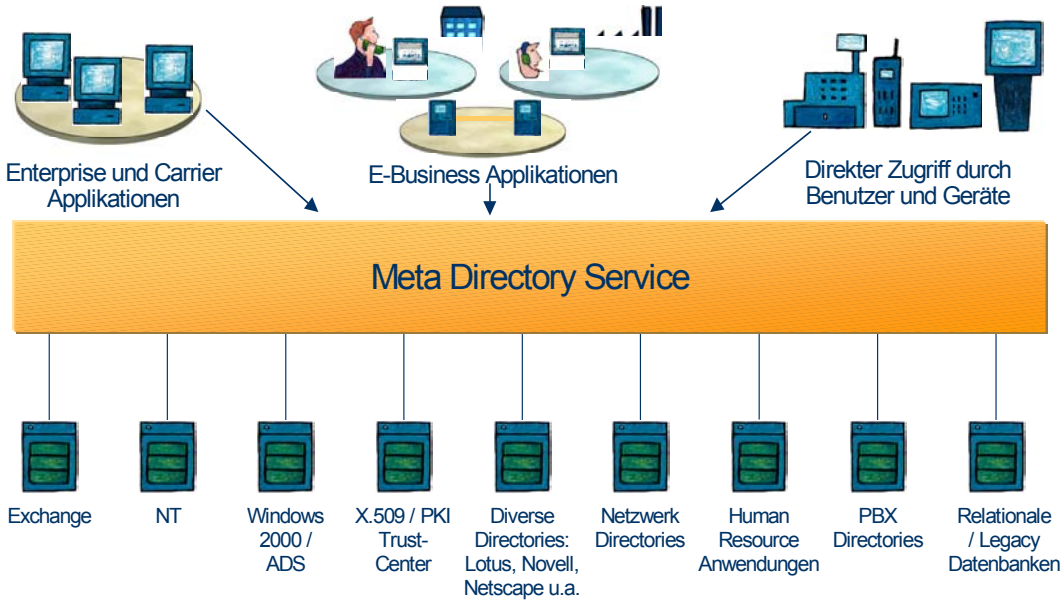

Abbildung 4: Grundgedanke des Meta Directory Service

Dabei werden neue Daten nur noch einmal eingegeben und automatisch in allen gewünschten Directory Services aktualisiert (synchronisiert). Und egal ob man gerade unter MS Exchange, Lotus Notes, im Web oder anderswo arbeitet – man findet die Informationen unternehmensweit schnell und zuverlässig. Weiterführende Literatur zu diesem wichtigen Anwendungsfall findet sich z.B. unter [11] und [12].

4.3 E-Business

E-Business, d. h. die Abwicklung geschäftlicher Prozesse über ein Netzwerk, ist auch weiterhin einer der ganz großen Treiber der gesamten IT-Welt. Es ist allerdings zu beobachten, dass die Euphorie im E-Business einem gewissen Realismus, zum Teil sogar Ernüchterung gewichen ist. In der Vergangenheit haben viele Anbieter von E-Business-Lösungen ihren Kunden Kostensenkungen von 70 % und mehr versprochen. Diese 70 % sind sicher in einzelnen Fällen auch nicht übertrieben; meistens sind diese Kostenvorteile aber ganz erheblich niedriger ausgefallen, was zu besagter Ernüchterung geführt hat.

Was sind die Gründe für das Scheitern der zum Teil hoch gesteckten Kostensenkungsziele infolge der Einführung von E-Business?

Viele Unternehmen haben vor allem im Bereich E-Business Front-Ends investiert, beispielsweise ein Portal für Kunden, Partner oder Zulieferer implementiert.

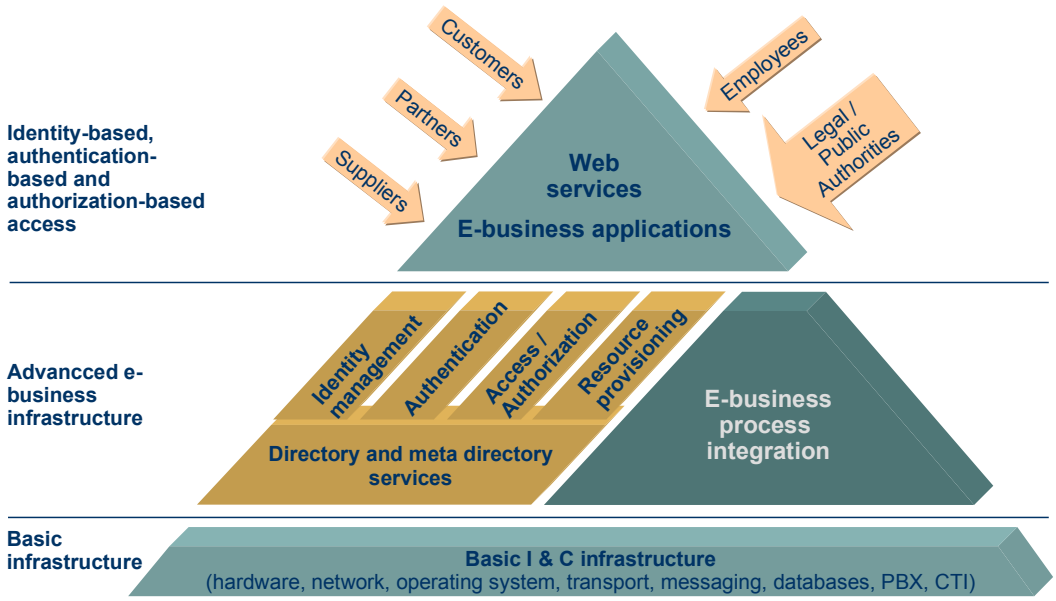

Abbildung 5: Directory Service in der E-Business Anwendungspyramide

Aber E-Business ist wesentlich mehr als nur die Einrichtung eines Portals. E-Business bedeutet die Transformation sämtlicher dazu geeigneter Geschäftsprozesse ins Netz und zwar so, dass die Geschäftsprozesse frei von Brüchen ablaufen können. Dies erfordert eine adäquate Infrastruktur, die die Transformation des Geschäfts hin zu netzbasierten Prozessen wirksam unterstützt. Zum einen handelt es sich dabei um Systeme, die den automatischen und bruchfreien Ablauf der netzbasierten Geschäftsprozesse ermöglichen. Zum anderen ist ein Infrastrukturkomponente vonnöten, welche die Frage “Wer darf was womit und zu welchem Zeitpunkt?” beantwortet. Eine derartige Infrastruktur besteht aus verschiedenen Teilen:

- einem Identity Management zur Registrierung aller Benutzer (Anmeldung am Portal),
- einer Authentifizierung zur Überprüfung der „Echtheit eines Benutzers“ (ist Herr Müller auch wirklich Herr Müller – Sicherheitsaspekt),
- einem Berechtigungsmanagement zur Festlegung von Rollen, Berechtigungen und damit verbundenen Zugriffsrechten (Single Sign-On, Role-Based Access Management),
- einem Resource Provisioning, um die Informationen über Benutzer und deren Rollen und Berechtigungen den verschiedenen Applikationen und Ressourcen zur Verfügung zu stellen (E-Provisioning).

Directory und Meta Directory Services stehen als zentrale Instanz für Benutzer und deren Profile, Rollen und Berechtigungen zur Verfügung und sorgen für die Verteilung und laufende Aktualisierung dieser Informationen; eine ausführliche Würdigung der Rolle von Directorys in E-Business-Lösungen findet sich in [13]. Im folgenden werden die Elemente betrachtet, welche für die Realisierung einer E-Business-Lösung unumgänglich sind.

4.4 Portale / Identity Management

Nahezu jede Organisation – private Unternehmen wie auch öffentliche Einrichtungen – sind heute im Internet mit einer eigenen Webseite vertreten. Das „Betreten“ einer Organisation auf dem Weg des Internet durch das World Wide Web (WWW) erfolgt dabei meist durch sog. Portale, die

netzseitig das Pendant zum realen Gebäudeeingang der Organisation darstellen. Neben einem völlig anonymen Zugang gestatten derartige Portale aber auch den mehr oder weniger personifizierten Zugang zu den Webinhalten einer Organisation. Dabei muss sich der Besucher dieser Webseiten am Portal anmelden, ganz so , als ob er sich am realen Gebäudeeingang einer Organisation beim Pförtner anmelden muss. Verschiedene Grade der Personifizierung sind möglich:

- Name und Adresse: Zur Akquisition zusätzlicher potentieller Kunden, zum Beispiel um Werbematerial / Produktkataloge zu verschicken.

- Name, Adresse und Präferenzen: Um dem Besucher sofort seine bevorzugten Webinhalte zu präsentieren, beispielsweise dem Besucher der Webseiten eines Reisebüros gleich Angebote für Reisen in eine bestimmte Region, für die er sich besonders interessiert.

- Name, Adresse und Zahlungsverbindung: Zum Beispiel beim On-Line-Einkauf im Internet.

- Name, Adresse und persönliches Merkmal zur Identifikation (z. B. Benutzername und Passwort, digitaler Schlüssel oder Fingerabdruck): Zur eindeutigen und sicheren Identifikation des Besuchers der Webseiten einer Organisationen, z. B. bei der Abwicklung von Bankgeschäften über das Internet.

Eine Mischung dieser verschiedenen Personifizierungsansätze ist möglich und üblich (s. [14] oder [15]). Im Rahmen einer derartigen Personifizierung übernehmen Directory Services die Rolle, die entsprechenden Benutzerinformationen aufzunehmen (zum Beispiel Name, Adresse, persönliche Vorlieben, Benutzername, Passwort, digitaler Schlüssel oder Fingerabdruck), sicher aufzubewahren und bei Bedarf bereitzustellen.

4.5 Authentifizierung

Wie bereits im vorigen Kapitel kurz dargelegt, reicht es i.A. nicht aus, wenn sich ein Benutzer an einem Portal oder einer Applikation nur mit seinem Namen anmeldet. In der Regel muss sich der Benutzer zusätzlich authentifizieren, d. h. nachweisen, dass er der er ist, der er vorgibt zu sein. Diese Echtheitsüberprüfung eines Benutzers erfolgt auf verschiedene Arten:

- Benutzername plus Passwort stellen die einfachste, aber auch am wenigsten sicherste Methode zur Echtheitsüberprüfung dar. Dieses Verfahren ist das derzeit mit Abstand am meisten genutzte Verfahren zur Authentifizierung.

- Eine sog. Public Key Infrastructure (PKI), ein Verfahren, bei dem die Echtheit eines Benutzers mit Hilfe zweier eindeutig zueinander passender Schlüssel überprüft wird (einem öffentlichen Schlüssel, der für jedermann zugänglich ist und einem privaten Schlüssel, den nur der Benutzer selbst besitzt, in der Regel auf einer Chipkarte). Eine derartige PKI gewährleistet ein hohes Maß an Sicherheit, erfordert aber auch einen gewissen Aufwand.

- Fingerabdruck und sonstige biometrische Merkmale zum Beispiel Iris (Auge) oder Gesichtsabdruck.

In allen Fällen kommt einem Directory Service die Aufgabe zu, die Identifikationsmerkmale eines Benutzers (Benutzername plus Passwort, digitale Schlüssel, biometrische Merkmale) aufzunehmen, sicher aufzubewahren und bei Bedarf für die Echtheitsüberprüfung bereitzustellen. Eine besondere Rolle spielen Directory Services im Rahmen der angesprochenen Public Key Infrastructure (PKI). Derartige PKIs beinhalten gemäß PKI-Standard einen Directory Service, der für die Bereitstellung der öffentlichen Schlüssel zuständig ist. Die folgende Abbildung 6 beschreibt das PKI-Prinzip.

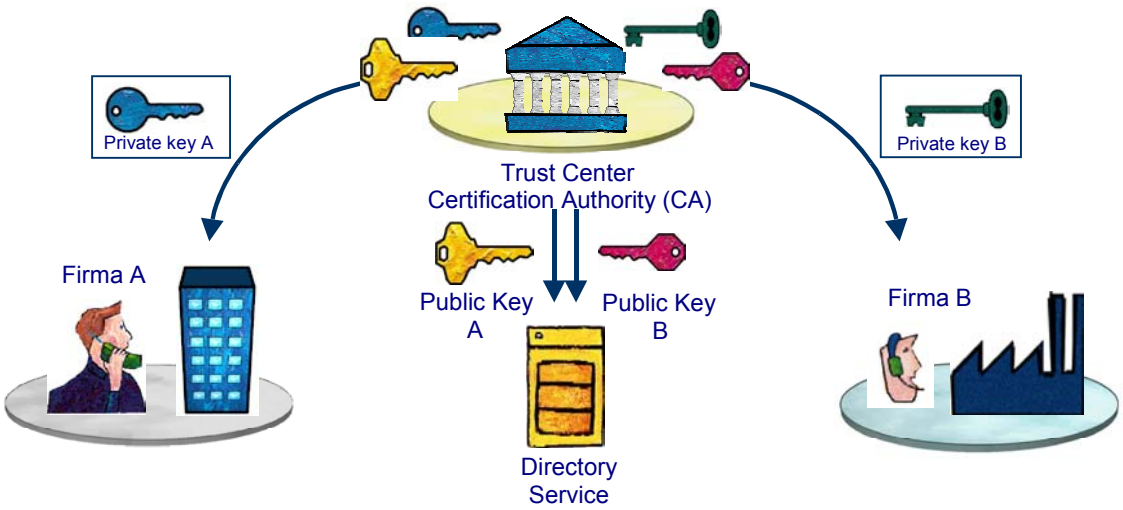

Abbildung 6: PKI Anwendungsszenario

Eine ausführliche Darstellung von PKI findet sich in [16].

4.6 Single Sign-On

Single Sign-On Systeme stellen eine oberhalb des System- und Applikationslayers liegende SW-Schicht dar. Ein Benutzer muss sich nur noch bei dieser gemeinsamen Schicht ein einziges Mal authentifizieren, um nach erfolgreicher Authentifizierung mit allen Systemen und Applikationen zu arbeiten, für die er eine Berechtigung besitzt.

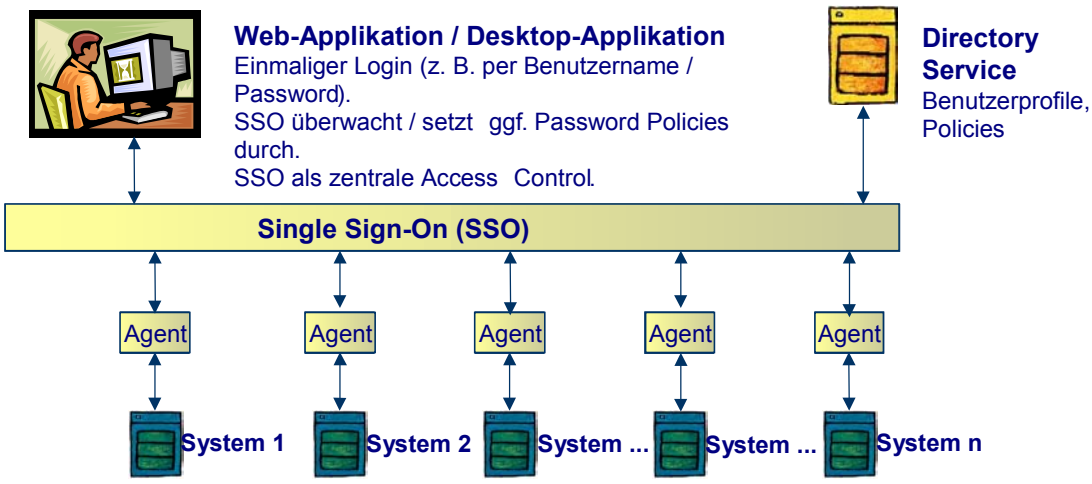

Abbildung 7Single-Sign-On Anwendungsszenario

In der Regel erfolgt die Authentifizierung an der gemeinsamen Schicht nicht nur via Benutzername und Password, sondern mindestens noch aufgrund eines weiteren Verfahrens (z. B. Smart Card, Biometrie, PKI, Token). Diese Vorgehensweise erhöht gegenüber reinen Password Synchronization Systemen die Sicherheit, da hier ein Password allein nicht reicht, um Zugang zu allen Zielsystemen zu erhalten (vgl. das nachfolgende Kapitel 4.7).

Bei Single Sign-On Systemen unterscheidet man heutzutage zwischen Web Single Sign-On Systemen, die ein Single Sign-On lediglich für Web-Applikationen ermöglichen (siehe [17] und [18]), und Legacy Single Sign-On Systemen, die ein Single Sign-On für nicht-Web-basierte Applikationen ermöglichen, wobei Mischformen im Markt erhältlich sind (zu Produkten s. [19] und [20]).

Single Sign-On Systeme benutzen einen Directory Service zur Hinterlegung von Informationen über Benutzer und deren Profile (Rollen, Rechte, Benutzername plus Passwort). Außerdem verwenden Single Sign-On Systeme zur Verwaltung gewisser Regelungen und Richtlinien (sog. Policies) einen Directory Service (z. B. Richtlinien zum Umgang mit Passworten oder Richtlinien im Umgang mit sich erstmalig anmeldenden Benutzern). Eine ausführliche Betrachtung von SSO kann in dem Report [17] der Burton Group nachgelesen werden.

4.7 Passwort Synchronisation / Passwort Reset

Wie im Abschnitt über Authentifizierung bereits erläutert, ist das Verfahren Benutzername plus Passwort das mit Abstand am meisten genutzte Verfahren zur Echtheitsüberprüfung von Benutzern. Jeder Benutzer arbeitet heute mit einer Vielzahl an Passwörtern, die nur allzu leicht vergessen werden und dann bei den zuständigen Anlaufstellen (Hotline, Helpdesk) bzw.

Administratoren für einen hohen Arbeitsaufwand sorgen. Aus diesem Grund sind zum einen Lösungen entstanden, welche die Passwörter eines Benutzers in allen Systemen gemäß vorher verabschiedeter Richtlinien (sog. Policies) auf einen einheitlichen Wert setzen:

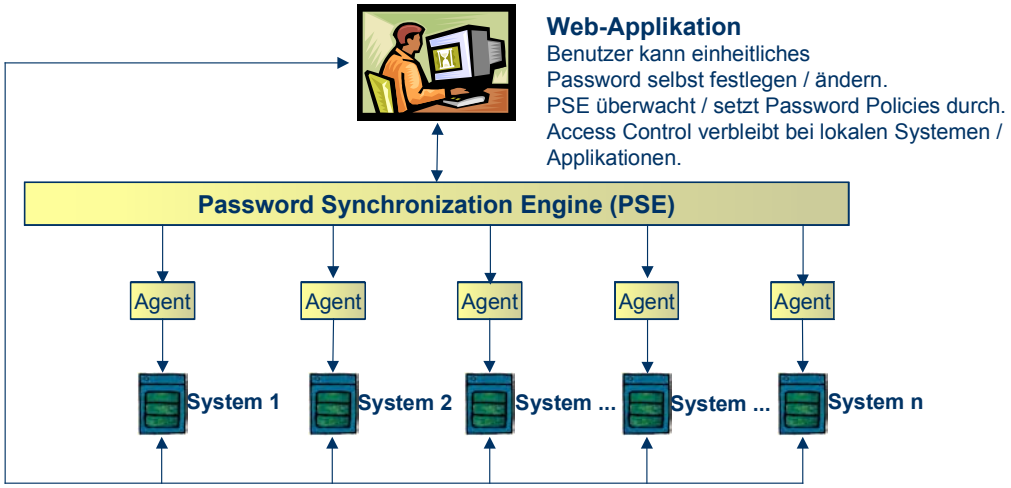

Abbildung 8: Passwort Synchronisation

Zum anderen existieren Lösungen, die das automatische, vom Benutzer selbst ausgelöste Zurücksetzen vergessener Passworte auf ein Standardpasswort gestatten:

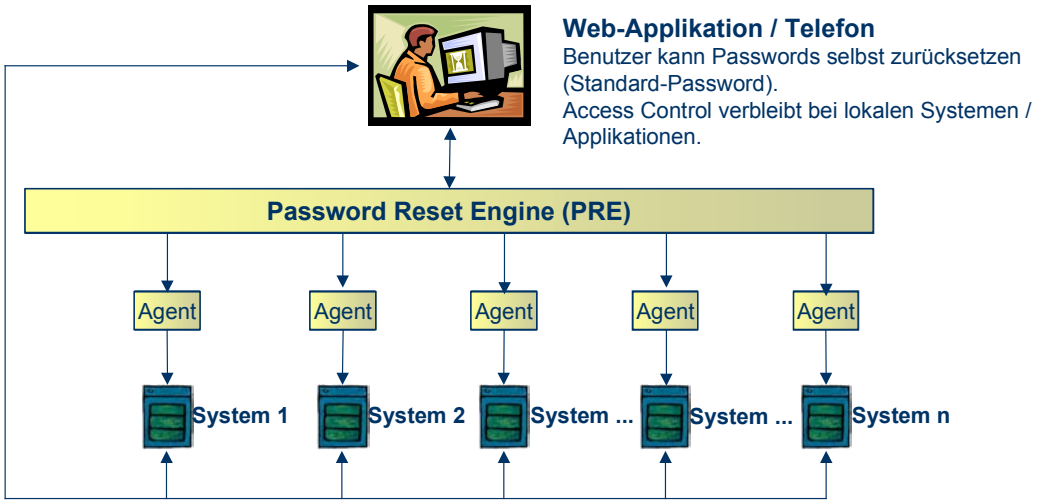

Abbildung 9: Vereinheitlichung von Passwörtern

Durch diese Lösungen lassen sich vergessene Passwörter weitgehend vermeiden, wenngleich, wie bei der Passwort Synchronisation üblich, ein einziges einheitliches Passwort pro Benutzer für alles Systeme und Applikationen ein gewisses Sicherheitsrisiko birgt.

Directory Services übernehmen im Zusammenhang mit Passwort Synchronisation bzw. Passwort Reset die Aufgabe, Benutzerinformationen inkl. synchronisierter Passwörter, Standardpasswörter sowie die Richtlinien zum Umgang mit Passwörtern zur Verfügung zu stellen. Derartige Lösungen werden i.A. als kundenspezifische Dienstleistungen z.B. von Anbietern wie Siemens ICN EN SNS MDS unter Einbeziehung der jeweils genutzten Anwendungen realisiert.

4.8 (Role-Based) Access Management / Provisioning

Bei der Verwaltung von Benutzern kommt es nicht nur darauf an, die Identität eines Benutzers festzustellen und die Echtheit dieser Identität zu überprüfen (Authentisierung). Vielmehr geht es

auch darum, den Benutzern Ihre Berechtigungen zuzuweisen, d. h. festzulegen (ggf. anhand vorgegebener Richtlinien), auf welche Systeme und Applikationen ein Benutzer zu welcher Zeit Zugriff haben soll. Dieser als Access Management bezeichnete Vorgang kann entweder individuell erfolgen, d. h. jedem einzelnen Benutzer werden nacheinander seine verschiedenen Rechte zugeordnet, oder in einem rollenbasierten Ansatz. Dabei werden, ausgehend von den Geschäftsprozessen einer Organisation, Rollen definiert, die innerhalb dieser Geschäftsprozesse vorhanden sind, beispielsweise Entwickler, Vertriebsmitarbeiter oder Kaufmann. Diese Rollen wiederum werden gewisse Zugriffsrechte auf Systeme und Applikationen zugeordnet, für eine Rolle „Vertriebsmitarbeiter“ zum Beispiel Zugriff auf ein Vertriebstool oder eine Customer Relationship Management Applikation (CRM). Sind einem Benutzer nun gewisse Zugriffsrechte einzuräumen, so hat man diesem Benutzer nur noch entsprechende Rollen zuzuweisen, die dann automatisch die richtigen Zugriffsberechtigungen implizieren. Durch ein derartige rollenbasierte Verwaltung von Zugriffsrechten verringert sich der administrative Aufwand bei der Zuordnung von Benutzern und deren Rechten enorm, da Zugriffsrechte hier nicht mehr individuell angesprochen werden, sondern über das Medium „Rolle“ ausgehend von der Platzierung des Benutzers in den Geschäftsprozessen vergeben werden.

Nachdem einem Benutzer die nötigen Zugriffsrechte für Systeme und Applikationen zugewiesen wurden (rollenbasiert oder individuell), müssen diese Informationen den lokalen Systemen und Applikationen mitgeteilt werden. Diesen Prozess der automatischen Bereitstellung bzw. Verteilung von Benutzer- und Zugriffsrechteinformationen bezeichnet man im allgemeinen als Provisioning (manchmal auch E-Provisioning, Resource Provisioning oder Service Provisioning). Die folgende Abbildung verdeutlicht das Prinzip des Access Managements und Provisionings:

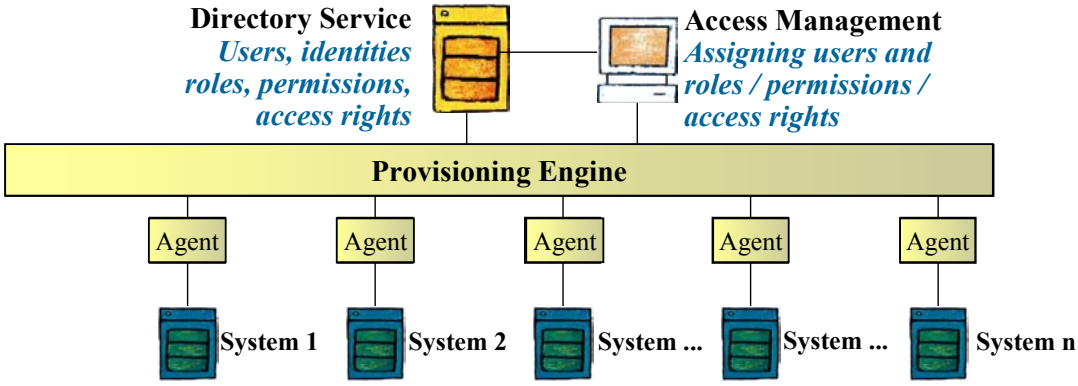

Abbildung 10: Rollenbasierte Vergabe von Zugriffsrechten

Eine Reihe von Analysten halten Access Management und Provisioning für die „Killer-Anwendungen“ für Directory Services [21], [22] und [23]. Die Aufgabe von Directory Services im Rahmen von Access Management und Provisioning besteht darin, die Benutzer und deren Rollen

und Zugriffsrechte zu verwalten und diese Informationen in einem Provisioning-Prozess den entsprechenden Systemen und Applikationen zur Verfügung zu stellen. Das bei Siemens ICN angewandte Verfahren ist in [24] beschrieben. Darstellungen zu Technik und Produkten finden sich in [25], zu Architekturen in [26], und zum Return of Investment in [27].

4.9 Carrier / Telekommunikation / Service Provider

Carrier, Unternehmen der Telekommunikation und Service Provider (Internet Service Provider – ISP, Application Service Provider – ASP) benutzen Directory Services zur Administration ihrer gesamten Betriebsmittel:

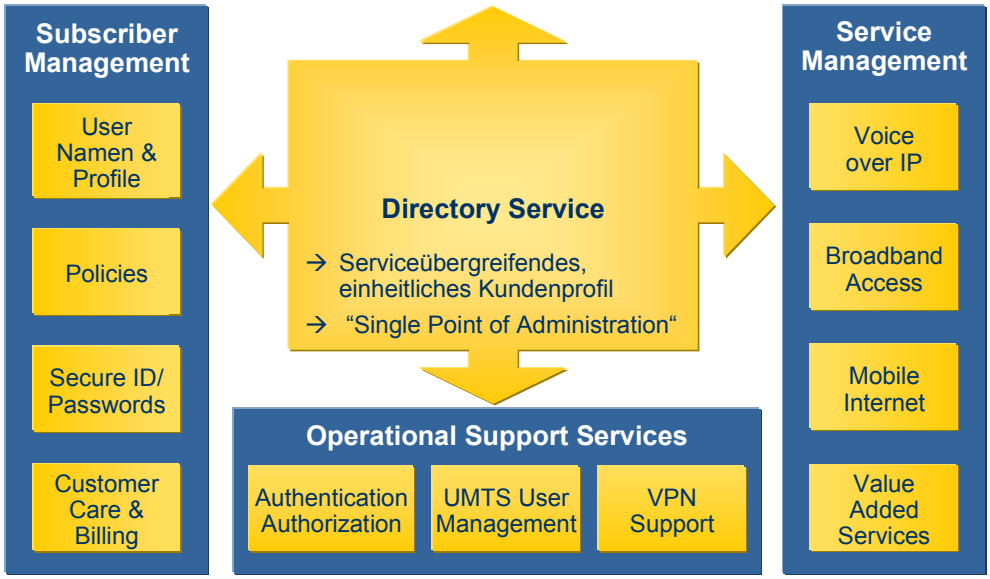

Abbildung 11: Directory Services in der Telekommunikation

Directory Services, die im Carrierumfeld eingesetzt werden, müssen ganz besondere Anforderungen erfüllen im Hinblick auf Skalierbarkeit (Speicherkapazität), Performance, Zuverlässigkeit und Verfügbarkeit. So hat ein Carrier in der Regel viele Millionen Kunden, wodurch sich die Anforderung nach hoher Speicherkapazität erklärt. Eine schlechte Performance des Directory Service, mangelhafte Zuverlässigkeit bzw. Verfügbarkeit (d. h. fortwährende Ausfälle des Directory Service) hätten für den Carrier den Stillstand seiner Betriebsmittel und damit seines gesamten Geschäfts zur Folge. Daher sind Performance sowie Zuverlässigkeit und Verfügbakeit eines Directory Service für einen Carrier wichtige Directory-Parameter. Siemens ist der derzeit einzige Anbieter eines Directory Service speziell für Carrier, Unternehmen der Telekommunikation und Service Provider.

4.10 Netzwerkmanagement / DEN

Vor einigen Jahren machte sich die Standardisierungsorganisation Distributed Management Task Force (DMTF) daran, eine Methode zu entwickeln, mit deren Hilfe es möglich sein sollte, ein komplettes Netzwerk inkl. seiner Parameter, Benutzer und deren Profile in einen Directory Service abzubilden und somit zentral zu verwalten. Diese Bemühungen der DMTF sind unter dem Namen Directory-Enabled Network (DEN) bekannt. Wenngleich die DMTF immer noch an DEN arbeitet, hat sich DEN als Standard mittlerweile ziemlich erledigt. Zu viele Netzbetreiber haben nicht auf die Verabschiedung eines offiziellen DEN-Standards gewartet und statt dessen ihre eigenen "directory-enabled" Netze aufgebaut. Auch die im vorherigen Unterpunkt genannten Einsatzszenarien von Directory Services bei Carriern, Unternehmen der Telekommunikation und Service Providern können DEN im weiteren Sinne zugeordnet werden (zu DEN allgemein siehe [28] und [29]).

5 Markt und Hersteller

Der Markt für Directory Services wird heute allgemein in vier Segmente unterteilt:

1. **Netzwerk-Betriebssystem-Directories:**
   Hierbei handelt es sich um Directory Services, die zur Administration eines Netzwerks genutzt werden. In der Regel sind die Netzwerk-Betriebssystem-Directories fest mit dem Netzwerk-Betriebssystem verbunden.

2. **Enterprise Directories:**
   Dies sind Directory Services, die in erster Linie unternehmensinterne Aufgaben übernehmen, z. B. Bereitstellung eines unternehmensweiten elektronischen (Web-basierten) Telefonbuchs (Beispiel: Siemens Corporate Directory – SCD) oder Integration der unternehmensinternen Applikationsinfrastruktur im Hinblick auf die von diesen Applikationen gemeinsam genutzten Informationen.

3. **Extranet Directories (bisweilen auch Carrier Directories genannt):**
   Directory Services, die hinsichtlich Skalierbarkeit (Speicherkapazität), Performance, Zuverlässigkeit und Verfügbarkeit optimiert sind für den Einsatz in unternehmenskritischen Umgebungen, z. B. bei Telekommunikationsunternehmen (Carriern) oder Service Providern oder im Bereich On-Line-Banking / On-Line-Brokerage. 7 x 24-Verfügbarkeit ist hier in aller Regel ein Muss.

4. **Meta Directory Services**:
   Hier handelt es sich um eine Technologie, die dazu dient, die in verschiedensten Directory Services hinterlegten Informationen miteinander abzugleichen (zu synchronisieren), d. h. für die Konsistenz der in unterschiedlichen Directory Services hinterlegten Informationen zu sorgen.

Ein Ausblick auf das Jahr 2003 sowohl die Technologien als auch die Hersteller betreffend ist in [54] zu finden.

5.1 Netzwerk-Betriebssystem-Directorys

Der Weltmarkt für Netzwerk-Betriebssystem-Directories stellt sich quantitativ wie folgt dar (in Mio. US-$):

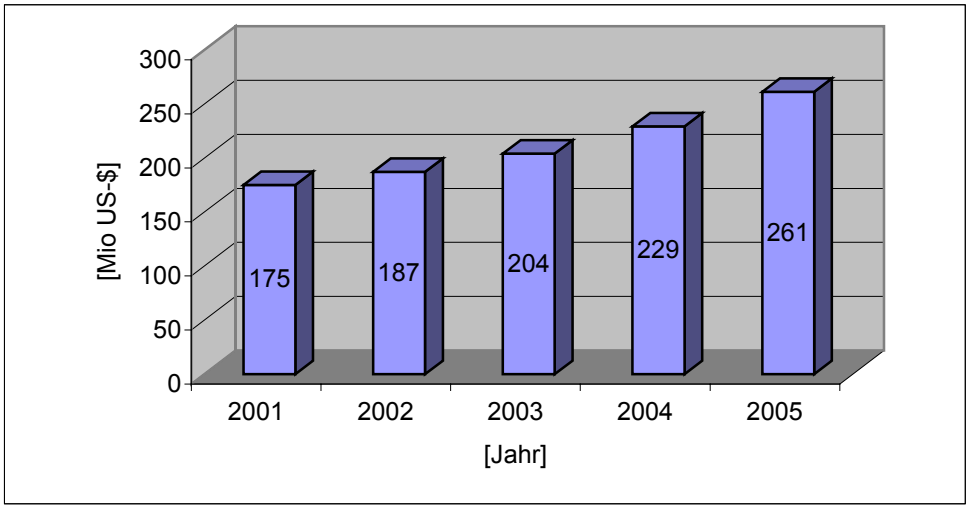

Abbildung 12: Markt für Netzwerk Directory SW-Lizenzen (Quelle: The Radicati Group 2002)

Bei diesen Zahlen handelt es sich um die reinen Software-Lizenzen. Die Radicati Group schätzt, dass sich der Gesamtmarkt für Netzwerk-Betriebssystem-Directories (Software-Lizenzen plus Dienstleistungen) auf den Faktor sechs beläuft.

Den Markt für Netzwerk-Betriebssystem-Directories teilen zwei Anbieter fast vollständig unter sich auf: Novell, mit einem Marktanteil von 49 % derzeit noch mit leichtem Vorsprung Marktführer, hat als erster Anbieter eines Netzwerk-Betriebssystems einen Directory Service in sein Netzwerk-Betriebssystem integriert (s. [30] und [31]). In der Folge ist es Novell gelungen, den Directory Service (Novell eDirectory) von seinem Netzwerk-Betriebssystem (Novell NetWare) zu entkoppeln. Beim zweiten Anbieter handelt es sich um Microsoft mit seinem Netzwerk-Betriebssystem Windows 2000 (Marktanteil 46 %) [32]. Microsoft hat Anfang 2000 zum ersten Mal einen Directory Service (Active Directory Service – ADS) in sein Betriebssystem Windows 2000 integriert. ADS übernimmt in Windows 2000 die von Windows NT her bekannte Rolle eines DNS Servers. Aufgrund der zunehmenden Verbreitung von Windows 2000 ist davon auszugehen, dass ADS in Zukunft aus keinem Directory Szenario mehr wegzudenken ist. Eine beispielhafte Auswahl von Büchern zum Einsatz von ADS findet sich in der Bibliographie unter [33], [34], [35] und [36]. In [37] und [38] werden Novell NDS und Microsoft ADS einander und weiteren Directorys gegenübergestellt. Zu Netzwerk-Directorys im Unix-Umfeld gibt es z.B. die Bücher [39], [40] [41]und [42].

5.2 Enterprise Directories

Der Weltmarkt für Enterprise Directories stellt sich quantitativ wie folgt dar (in Mio. US-$):

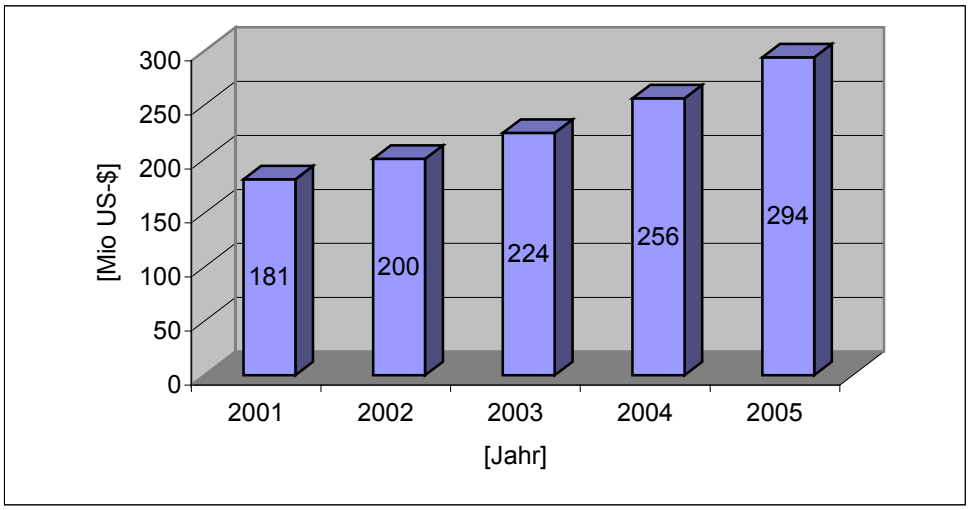

Abbildung 13: Markt für Enterprise Directory SW-Lizenzen (Quelle: The Radicati Group 2002)

Wiederum handelt es sich bei diesen Zahlen nur um die reinen Software-Lizenzen. Laut Radicati Group ist davon auszugehen, dass der Gesamtmarkt für Enterprise Directories (Software-Lizenzen plus Dienstleistungen) sich auf den Faktor sechs beläuft. Führend im Markt für Enterprise Directories ist derzeit Sun / iPlanet mit einem Marktanteil von 43 %. iPlanet ist eine ehemalige Allianz von Sun und Netscape. Im März 2002 wurde iPlanet vollständig in Sun integriert. Dies beinhaltet auch die völlige Integration von iPlanet's Software-Produkten in die Sun ONE Platform (Sun ONE = Sun Open Net Environment). Aus diesem Grund heißt der iPlanet Directory Server nun Sun ONE Directory Server. iPlanet hat sich in der Vergangenheit hauptsächlich auf das reine Produktgeschäft konzentriert und weniger auf directory-basierte Lösungen. Mit einem Marktanteil von 16 % folgt Siemens auf dem zweiten Rang (Produkt: DirX). Siemens betreibt seit über 10 Jahren Geschäfte mit Directory Services und ist einer der erfahrensten Anbieter auf dem Markt. Siemens fokussiert sich vor allem auf directory-basierte High-End-Lösungen. Auf dem dritten Rang folgt schließlich Critical Path mit einem Marktanteil von 10 %. Critical Path betreibt hauptsächlich Messaging-Geschäft und bietet in diesem Zusammenhang auch einen Directory Service an (CP Directory Server). Einen Überblick über die Hersteller von Enterprise und Extranet Directorys vermittelt die Gartner Studie [43]; [44] gibt eine Übersicht über die Einsatzmöglichkeiten des Siemens-Produkts DirX.

5.3 Extranet Directorys:

Der Weltmarkt für Extranet Directorys sieht quantitativ wie folgt aus (in Mio. US-$):

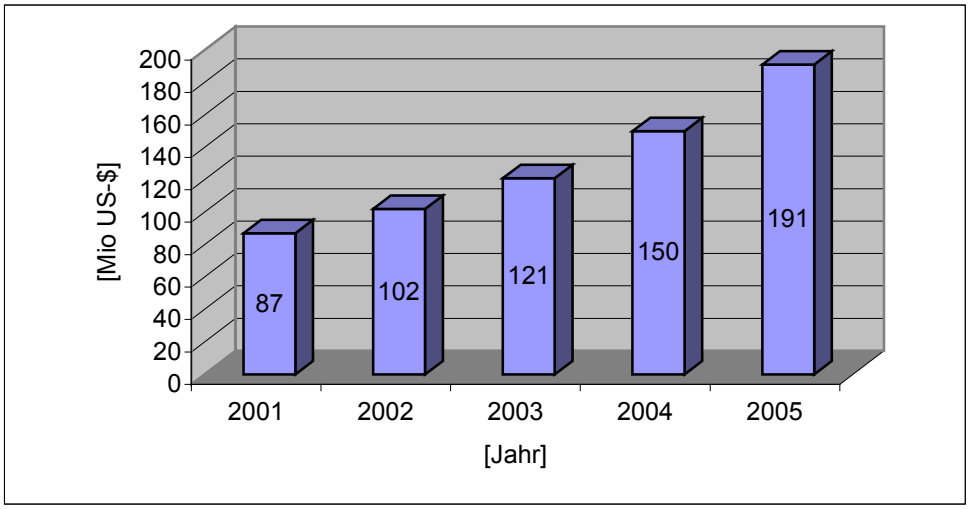

Abbildung 14: Markt für Extranet Directorys SW-Lizenzen (Quelle: The Radicati Group 2002)

Auch hier handelt es sich nur um den Markt für Software-Lizenzen. Die Radicati Group schätzt, dass der Gesamtmarkt (Software-Lizenzen plus Dienstleistungen) ebenfalls um den Faktor sechs höher liegt. Marktführer bei Extranet Directories ist wiederum Sun / iPlanet mit seinem Sun ONE Directory Server und einem Marktanteil von 39 %. Auf Rang zwei folgt Siemens mit einem Anteil von 26 % (Produkt: DirX Extranet Edition). Den dritten Rang schließlich hat, wie schon bei Enterprise Directories, Critical Path mit seinem Produkt CP Directory Server und einem Marktanteil von 20 % inne. Zu den drei genannten Anbietern gilt sinngemäß das schon im Abschnitt „Enterprise Directories“ Gesagte (siehe auch hierzu [43]).

5.4 Meta Directory Services

Der Weltmarkt für Meta Directory Services sieht quantitativ wie folgt aus (in Mio. US-$):

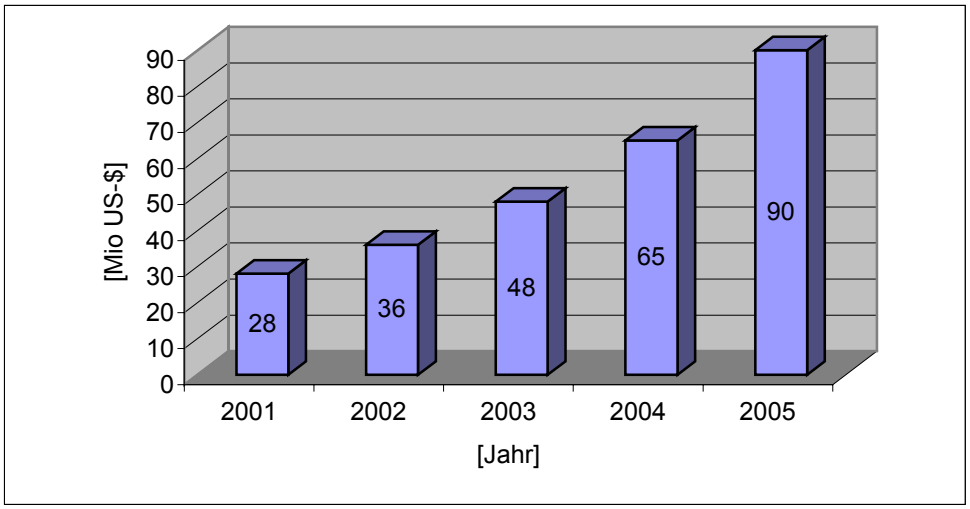

Abbildung 15: Markt für Meta Directory SW-Lizenzen nach Radicati (Quelle: The Radicati Group 2002)

Hierbei handelt es sich wiederum nur um die reinen Software-Lizenzen, wobei der Gesamtmarkt (Lizenzen plus Dienstleistungen) diesen Wert um den Fakto 6 übertreffen soll. Demgegenüber gibt die Giga Information Group für den Weltmarkt für Meta Directory Services folgende Werte an (in Mio. US-$):

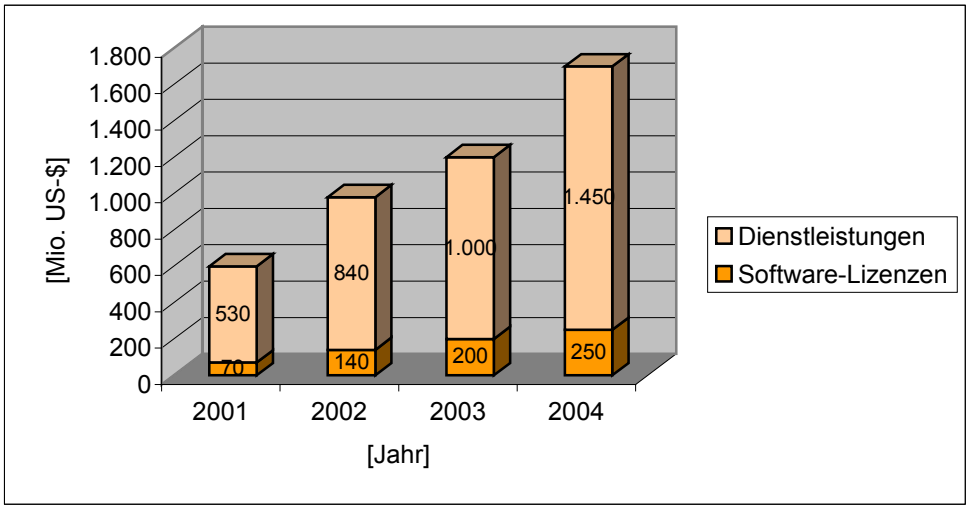

Abbildung 16: Markt für Meta Directorys nach Giga (Quelle: Giga Information Group 2001 [45])

Die eklatanten Abweichungen in den Marktzahlen der Radicati Group und der Giga Information Group sind offensichtlich. Dies betrifft sowohl den Markt für die Meta Directory Software-Lizenzen als auch die zum Meta-Directory-Geschäft gehörenden Dienstleistungen. Ausgehend von den aktuellen Umsätzen der wichtigsten Meta-Directory-Anbieter (Critical Path, Microsoft, Sun / iPlanet, Siemens) erscheinen die Schätzungen der Giga Information Group um mehr als den Faktor zwei zu groß. Die Marktzahlen der Radicati Group geben ein realistischeres Bild wieder. Aus diesem Grund wird bei der Betrachtung der Marktanteile im folgen auch mit den Zahlen der Radicati Group gearbeitet und auf eine weitere Verwendung der Einschätzung der Giga Information Group verzichtet.

Markführer im Bereich Meta Directory Services ist Critical Path mit einem Marktanteil von 24 % (Produkt: CP Meta Directory Server). Zu Critical Path gilt sinngemäß das bereits im Abschnitt „Enterprise Directories“ Dargelegte. Den zweiten Platz teilen sich mit je 19 % Sun / iPlanet und Microsoft. Auch zu Sun / iPlanet gilt dem Sinne nach das bereits im Abschnitt „Enterprise Directories“ Gesagte. Insbesondere fokussiert sich Sun / iPlanet auch im Bereich der Meta Directory Services auf das reine Produktgeschäft und kaum auf die Bereitstellung von Lösungen. Das Meta-Directory-Produkt von Sun / iPlanet trägt den Namen Sun ONE Meta-Directory. Microsoft hat im Jahr 1999 den Meta-Directory-Anbieter ZOOMIT übernommen und ist hierdurch zu einem eigenen Meta Directory Service gekommen. Der von ZOOMIT ursprünglich VIA genannte Meta Directory Service wurde von Microsoft in Microsoft Metadirectory Service (MMS) umbenannt. Ansonsten hat Microsoft am ursprünglichen ZOOMIT-Produkt nichts geändert. MMS ist damit auf dem Stand von 1999 und folglich relativ veraltet. Mit 17 % Marktanteil folgt Siemens auf Rang vier (Produktname: DirXmetahub). Siemens ist seit 1997 im Meta-Directory-Geschäft tätig und damit gemeinsam mit Critical Path einer der erfahrensten Anbieter. Auch im Bereich Meta Directory Services fokussiert sich Siemens auf die Bereitstellung von High-End-Lösungen im Gegensatz zu zum Beispiel Sun / iPlanet oder Microsoft, die hauptsächlich das Produktgeschäft forcieren.

6 Directory Services – Die Zukunft

In der Vergangenheit wurden Directory Services überwiegend unternehmensintern eingesetzt – zur Bereitstellung von elektronischen (Web-basierten) Telefonbüchern, zur Verwaltung von Netzwerken oder zur Schaffung einer gemeinsamen Informationsbasis für Applikationen. Diese unternehmensinternen Einsatzszenarien werden sich in Zukunft weiten zu unternehmensübergreifenden, ja, globalen Einsatzszenarien.

Als Folge davon werden Unternehmen, öffentliche Einrichtungen, Telekommunikationsunternehmen (Carrier) und Service Provider Directory Services als bedeutsamen Teil ihrer strategischen Infrastruktur ansehen, gerade so, wie Telefone oder IP-Technologie heute als Teil der strategischen Infrastruktur betrachtet werden.

Unternehmen werden Directory Services dazu verwenden, ihr komplettes Beziehungsgeflecht zu verwalten, beispielsweise ihre Beziehungen zu Kunden, Partnern, Lieferanten und Mitarbeitern (vor Ort und unterwegs). Mit Hilfe von Meta Directory Services werden Unternehmen in der Lage sein, eine einheitliche Sicht auf ihre Kunden zu erhalten. Dies erlaubt insbesondere die Implementierung von Quality-of-Service-Konzepten (d. h., dem Kunden wird ein vorher definierter Service Level garantiert) oder, als nächste Stufe, Quality-of-Experience-Konzepten (d. h., bei Interaktion mit dem Kunden wird den Erfahrungen, Gewohnheiten, Ansprüchen, „soft facts“ des Kunden mit Rechnung getragen). Ein darunterliegender Directory Service erkennt den Kunden, gleich mit welcher Abteilung des Unternehmens er in Kontakt tritt. Der Kunde erhält hierdurch eine „Single Point of Access“, d. h. Authentisierung (Überprüfung der „Echtheit“ des Kunden) und Authorisierung (Rechtevergabe) werden zentral erledigt – der Kunde kann sofort mit der entsprechenden Unternehmensabteilung und deren Ressourcen interagieren. „One face to the customer“ oder „Der Kunde steht im Mittelpunkt unseres Handelns“ – Directory Services werden das ermöglichen. Über die zukünftige Verwendung von Directory Services in Unternehmen siehe z.B. [46] oder [47].

Öffentliche Einrichtungen werden Directory Services dazu nutzen, den Bürgerinnen und Bürgern (die letztlich die Kunden der öffentlichen Einrichtungen sind) völlig neue Dienstleistungen anzubieten. Directory Services werden die zentrale Infrastruktur zum Aufbau eines „E-Rathauses“ bzw. eines virtuellen Rathauses. Die Einwohnerinnen und Einwohner werden nicht länger gezwungen sein, im Rathaus oder einer anderen öffentlichen Einrichtung von Abteilung zu Abteilung zu gehen, um Verwaltungsangelegenheiten zu erledigen (siehe dazu die Studien von Gartner [48] oder Giga [49] oder den Bericht über die Einführung einer „Service Card“ in Italien [50]).

Gesundheits-Directories („Healthcare Directories“) oder Patienten-Directories werden Informationen über Patientinnen und Patienten (die prinzipiell auch Kunden sind) zentral und sicher zur Verfügung stellen. Dies wird dazu führen, dass kranke oder verletzte Personen die bestmögliche Behandlung zu geringstmöglichen Kosten erhalten.

Directory Services werden Telekommunikationsunternehmen (Carrier) und Service Provider in die Lage versetzen, ihren Kunden völlig neue Dienste zur Verfügung zu stellen (value-added Services). Dazu zählen zum Beispiel Unified Messaging, gemischte Sprach- und Datendienste (IP-basiert; sog. Konvergenz) oder neue Möglichkeiten des Bezahlens (z. B. via Mobiltelefon oder Micro-Payment). Eine Beispielanwendung zum Auffinden des nächstliegenden Parkplatzes von einer gegebenen Position aus ist in [51] beschrieben. Die darunterliegenden Directory Services erlauben analog der Situation in Unternehmen eine Personalisierung dieser Services. E-Provisioning Systeme werden diese Services innerhalb weniger Minuten wenn nicht Sekunden den Kunden zur Verfügung stellen. Tage- oder wochenlanges Warten bis zur Bereitstellung eines beantragten Dienstes gehören damit der Vergangenheit an.

Die Vorteile der zuvor beschriebenen allgegenwärtigen Directory Services wären aber nur von geringem Wert, falls diese vielen unterschiedlichen und im Hintergrund (völlig transparent) agierenden Directory Services isoliert nebeneinander stehen würden. Neue Informationsinseln würden entstehen, und große Anstrengungen wären nötig, um die enormen Mengen an Informationen, die diese vielen Directory Services bereitstellen, zu verwalten, insbesondere auch konsistent zu halten. Universelle und globale Meta Directory Services werden daher die Verwaltung und Pflege dieser vielen Directory Services übernehmen. Ein leistungsfähiges globales Netzwerk von Directory Services entsteht.

Die zuvor geschilderte künftige Bedeutung impliziert eine Reihe von Anforderungen an die Directory Services von morgen und die darauf aufbauenden Applikationen (eine Einschätzung der Analysten der Giga und Burton Group die Entwicklungen des Directory Service Markts findet sich unter [53] und [54]):

- Directory Services müssen „well-connected“ sein, d. h. sie müssen sich nahtlos und ohne großen Programmieraufwand in jegliche Form von IT einfügen. Hierzu werden Directory Services neben der klassischen Zugriffsmöglichkeit über LDAP zusätzliche, weiter vereinfachte Zugriffsmöglichkeiten anbieten, beispielsweise über ein XML-Format (DSML = Directory Services Markup Language), das über ein spezielles Protokoll – SOAP – übertragen bzw. ausgetauscht wird [52]. SOAP, das sog. Simple Object Access Protocol, basiert auf dem vom World Wide Web (WWW) her bekannten HTTP (HyperText Transfer Protocol) und ist daraufhin optimiert, XML-Formate und darin enthaltene Anweisungen zu übertragen bzw. zwischen Systemen (Applikationen) auszutauschen.

- Web Services bzw. das Web Services Framework, das vom W3C vorangetrieben wird (W3C = World Wide Web (WWW) Consortium) sollen die reibungslose, automatische Interaktion von Applikationen innerhalb eines Unternehmens und über Unternehmensgrenzen hinweg ermöglichen. Um einen umfassenden Einsatz des Web Services Frameworks zu gewährleisten, legt das W3C daher bei der Definition dieses Rahmenwerkes besonderes Gewicht auf Einfachheit. Aus diesem Grund geht das Web Services Framework nicht auf Sicherheitsaspekte bei der Interaktion von Applikationen ein. Nichts desto trotz ist das Thema Sicherheit bei einer derartigen Integration von Applikationen von größter Bedeutung. Directory Services und die im Abschnitt über Directory-Anwendungen genannten Sicherheitsapplikationen wie beispielsweise Single Sign-On (SSO), Public Key Infrastructure oder auch Provisioning / Identity Management werden die im Web Services Framework nicht adressierten Sicherheitsaspekte aufgreifen und bestehende Sicherheitslücken schließen. Dabei werden innovative Technologien zum Zugriff auf Directories eingesetzt, insbesondere die zuvor geschilderte Methode über XML (DSML) und SOAP. Mit der Liberty Alliance, ursprünglich von Sun initiiert und mittlerweile aus über 60 Organisationen bestehend, u. a. auch Siemens und dem damit konkurrierenden Passport von Microsoft sind bereits zwei sehr konkrete Ansätze erkennbar, die sich die im Web Services Framework nicht adressierten Sicherheitsaspekte zu eigen machen und Lösungen anbieten.

- Die Mechanismen zur Absicherung der im Directory Service hinterlegten Informationen werden weiter verfeinert.

- Meta Directory Services, welche die Verwaltung erdumspannender Netzwerke von Directory Services erlauben, werden entstehen. Die Sicherheit der in den Directory Services hinterlegten Informationen und deren sichere Übertragung hat dabei aller erste Priorität.

- Hersteller von Applikationen werden nicht umhin kommen, ihre Applikationen directory-fähig zu machen, d. h., die Applikationen in die Lage zu versetzen, Informationen von Directory Services zu beziehen oder dort zu hinterlegen.

- Single Sign-On als einfache und sichere Technologie zur Anmeldung in kompletten Applikationslandschaften wird in seiner Bedeutung als directory-basiertes System zunehmen.

- Role-based Access Management / E-Provisioning wird die Killer-Applikation für Directory Services. Derartige Systeme übernehmen – directory-basiert – die Verwaltung der Bereitstellung von Applikationen und Diensten.

7 Literatur

Die unten aufgeführte Literatur (Reports, Bücher und Artikel) kann über die jeweils vermerkten Online-Bestellscheine bezogen werden. Aus urheberrechtlichen Gründen können Analystenreports nur an Siemens-Mitarbeiter verschickt werden.

Basistechnologie

[1] The Burton Group: Network Strategy Report, Directory-Enabled Computing: Enterprise Directory Concepts and Functions, Neuenschwander, Mike , v2 12 February 2001, 43 p.

[2] The Burton Group: Network Strategy Overview, Directory-Enabled Computing: The Directory´s Expanding Role; Gauthier, Larry; v2, 28 Dec 1999, 48 p.

[3] X.500 directory services. Technology and deployment (Buch); Radicati, S.; Van Nostrad Reinhold; 1994; ISBN 0-442-01816-9; NU240:Z401
http://fiz-ext.mchp.siemens.de/goto/ausleihe.html

[4] Understanding Directory Services (Buch); Sheresh, Dough; Sheresh, Beth; New Riders; 2000; ISBN 0-7357-0910-6; NA130:Z1138
http://fiz-ext.mchp.siemens.de/goto/ausleihe.html

[5] The Burton Group: Network Strategy Overview, Comparing Directories and Relational Databases: Not A Zero-Sum Game; Lewis, Jamie; Gauthier, Larry; v1, 25 Jan 2000, 25p.

[6] The Burton Group: Network Strategy Methodologies & Best Practices: Developing a Directory Namespace and Schema, Blum, Dan , Clark, Ian, Hudgins, Christy , v1 29 january 2001, 33 p.

[7] Siemens: DirX Meta Directory: Calculating Return on Investment (ROI); White Paper, August 2001, 22 p.
http://fiz-ext.mchp.siemens.de/goto/analystenreports.html

[8] Controlling infrastructure decisions in enterprise – a profitability analysis of X.500 directory services; Weitzel, T.; Son, S.; König, W.; Wirtschaftsinformatik (2001) vol. 43, no. 4, p. 371-81
http://fiz-ext.mchp.siemens.de/goto/kopie

[9] Big Book of Lightweight Directory Access Protocol (LDAP) RFCs (Buch); Loshin, P.; Morgan Kaufmann; 2000; ISBN 0-12-455843-7; NU240:Z570
http://fiz-ext.mchp.siemens.de/goto/ausleihe.html

[10] Understanding and deploying LDAP directory services (Buch); Howes, T.; Smith, M.; Good, G.; Macmillian; 1999; ISBN 1-57870-070-1; NU240:Z511
http://fiz-ext.mchp.siemens.de/goto/ausleihe.html

Anwendungsszenarien

[11] Gartner Research: So Many Directories, So Little Consistency; Enck J.; Reseach Note; 1 March 2002, 5 p.

[12] Unifying diverse directories; Chacon, M.; Network Magazine (2001) vol. 16, no. 2; p. 70-2, 74
http://fiz-ext.mchp.siemens.de/goto/kopie

[13] The Burton Group: Network Strategy Overview; The Directory-Enabled E-Business Value Chain; Kobielus, James; v1, 10 May 2001, 50 p.

[14] Giga Collaboration: Employee Directory Applications: A Must for Business-to-Employee Initiatives; Brosnahan, Michelle; 13 March, 2002, 9 p.

[15] Giga Information Group: Planning Assumption: Enterprise Portals: Evaluation Criteria; Hall, Kathleen; Heffner, Randy; 17 May 2001, 9 p.

[16] Gartner Research: Public Key Infrastructure (PKI): Overview; Noakes-Fry; Kirsten; Technology Overview; 11 Oktober 2001, 20 p.

[17] The Burton Group: Network Strategy Overview, Web Access Management: Maturing Market At A Crossroads; Neuenschwander, Mike; Schacter, Phil; Gebel, Gerry; v1, 19 Apr 2002, 53p.

[18] Giga Information Group: Planning Assumption: Federated Identity and Internet Single Sign-On (I-SSO): Standards Progressing, but the End Game is Unclear, Heffner, Randy, 9 October 2002, 9 p.

[19] Gartner Group: Password Management, Single Sign-On and Authentication Management Infrastructure Products: Perspective; Allan, Ant; 6 December 2002, 20p.

[20] Giga Infromation Group: Market Overview: Web Single Sign-On, Penn, Jonathan, 26 March 2002, 7p.

[21] Giga Information Group: Planning Assumption: Market Overview: User Account Provisioning; Penn, Jonathan; 22 October 2001, 12p.

[22] Gartner Research: Enterprise User Administration (EUA) Products: Perspective; Allan, Ant; Technology Overview; 29 October 2001, 18p.

[23] Giga Infromation Group: Planning Assumption: IT Trends 2003: Identity Management; Penn, Jonathan; September 26, 2002

[24] Siemens: Two NT servers for 50,000 users around the world
http://fiz-ext.mchp.siemens.de/goto/analystenreports.html

[25] The Burton Group: Directory and Security Strategies Research Report: Provisioning: Maturing Technologies, Converging Markets, Kampman, Kevin; Shacter, Phil; 25 November 2002, 64p.

[26] Giga Infromation Group: Planning Assumption: Identity Management Architecture; Penn, Jonathan; September 18, 2002, 8p.

[27] Giga Infromation Group: Idea Byte: Justifying the 2003 IT Budget: Identity Management Brings Quantifiable ROI to Security; Penn, Jonathan; October 22, 2002, 2p.

[28] Directory enabled networks (Buch); Goncalves, M.; McGraw-Hill; 1999; ISBN 0-07-134951-0; NA210:Z167
http://fiz-ext.mchp.siemens.de/goto/ausleihe.html

[29] DSML and DEN: signs of things to come; Allen, D.; Network Magazine (200) vol. 15, no. 6, p. 42,44,46,48;
http://fiz-ext.mchp.siemens.de/goto/kopie

Markt und Hersteller

[30] Administering NDS (Buch); Cadjan, N.; Harris, J.; McGraw-Hill; 2000; ISBN 0-07-212208-0; NA120:Z638
http://fiz-ext.mchp.siemens.de/goto/ausleihe.html

[31] Gartner Product Report: Novell eDirectory, Hubley, Mary; Osmundsen, Sheila; 23 May 2002, 8p.

[32] Gartner Technology Overwiew: Windows 2000 Active Directory: Perspective; Hubley, Mary; Lubrano Cynthia; Technology Overview; 11 June 2002, 15p.

[33] Windows 2000 Active Directory (Buch); Lowe-Norris, A. G.; O´Reilly; 2000; ISBN 1-56592-638-2; DV331:W582
http://fiz-ext.mchp.siemens.de/goto/ausleihe.html

[34] Windows 2000 Active Directory Services (Buch mit CD-ROM(s)); King, Robert; Sybex; 2000; ISBN 3-8155-5521-3; DV331:W606
http://fiz-ext.mchp.siemens.de/goto/ausleihe.html

[35] Active Directory Programming. The Authoritative Solution (Buch mit CD-ROM(s)); Kirkpatrick, G.; SANS; 2000; ISBN 0-672-31587-4; NA210:Z182
http://fiz-ext.mchp.siemens.de/goto/ausleihe.html

[36] Microsoft Windows 2000 – Design der Directory Services Infrastruktur – Original Microsoft Training. MCSE 70-219 (Buch mit CD-ROM(s)); Microsoft Press; 2001; ISBN 3-86063-913-7; DV331:W690
http://fiz-ext.mchp.siemens.de/goto/ausleihe.html

[37] Verzeichnisse aller Abteilungen, vereinigt euch (Directory services: ADS of Microsoft against NDA of Novell); Toeroek, E.; Information Week (2001), Nr. 13, S. 36,38,40,42
http://fiz-ext.mchp.siemens.de/goto/kopie

[38] Verzeichnisdienste im Netzwerk. NDS, Active Directory und andere (Buch); Larisch, D.; Hanser; 2000; ISBN 3-446-21290-6; NA120:Z663
http://fiz-ext.mchp.siemens.de/goto/ausleihe.html

[39] The Concise Guide to DNS and BIND (Buch); Langfeldt, N.; Que; 2001; ISBN 0-7897-2273-9; NA210:Z183
http://fiz-ext.mchp.siemens.de/goto/ausleihe.html

[40] Solaris and LDAP naming services : Deploying LDAP in the enterprose (Buch); Bialaski, Tom; Haines, Michael; Sun Microsystems Pr.; 2001 ISBN 0-13-030678-9; NU240:Z959
http://fiz-ext.mchp.siemens.de/goto/ausleihe.html

[41] LDAP unter Linux. Netzwerkinformationen in Verzeichnisdiensten verwalten (Buch); Banning, J.; Addison-Wesley; 2001; ISBN 3-8273-1813-0; DV331:L246
http://fiz-ext.mchp.siemens.de/goto/ausleihe.html

[42] Managing NFS & NIS (Buch); Stern, Hal; Eisler, Mike; O´Reilly; 2001; ISBN 1-56592-510-6; Na120:Z724
http://fiz.mchp.siemens.de/goto/ausleihe.html

[43] Gartner Research: 2H02 Directory Services Market and Magic Quadrant; Enck, J; Research Note; 19 August 2002, 6p.

[44] Siemens: DirX Solutions: Meta Directory & Provisioning, 12p.
http://fiz-ext.mchp.siemens.de/goto/analystenreports.html

[45] Giga Information Group: Planning Assumption: Market Overview: Metadirectories 2001; Penn Jonathan; March 29; 2001, 8p.

Directory Services – Die Zukunft

[46] The Burton Group: Network Strategy Overview, Vision 2003: The Path To Virtual Enterprise Networks; Blum, Daniel; v1, 24 May 2002, 41p.

[47] The Burton Group: Network Strategy Overview, Meta-Directory Services and the Emerging Enterprise Data Network; Neuenschwander, Mike; v1, 01 Feb 2002, 45p.

[48] Gartner Reseach: Directory Service Architecture for E-Government; Kreizmann; g.; Research Note; 7 August 2001, 6p.

[49] Giga Information Group: Planning Assumption: E-Government in 2002: Initiatives For Transforming Public Services Using Internet Technologies, Bartels, Andrew, June 14, 2002, 13p.

[50] Italiener haben Service Card, Government Computing, Nr. 09/02, 19. August 2002
http://fiz-ext.mchp.siemens.de/goto/kopie

[51] NAPA: Nearest Availible Parking lot Application; Hae Don Chon; Agrawal, D.; El Abbadi, A.; ed. Agrawal, RE.; Dittrich; K.; Proceedings of the 18th International Conference on Data Engineering (ICDE ´02); IEEE Computer Society p. 496-7; Conference: San Jose, CA, USA, 26 Feb.-1 March 2002
http://fiz-ext.mchp.siemens.de/goto/kopie

[52] The Burton Group: Network Strategy Report: Directory Services Markup Language Version 2 and Beyond, Kobelius, James, v2 28 March 2002, 21p.

[53] Giga Information Group: Ideabyte: Outlook for 2002: Directory Services; Penn, Jonathan; January 9, 2003; 2p

[54] The Burton Group: Directory and Security Strategies Research Report: Directory Landscape 2003: Crowded Market Challenges Sun's Leadership; Neuenschwander, Mike; January 14, 2003; 40p.

[55] Giga Information Group: Planning Assumption: Market Trends: Directory Management; Penn, Jonathan; December 21, 2000