

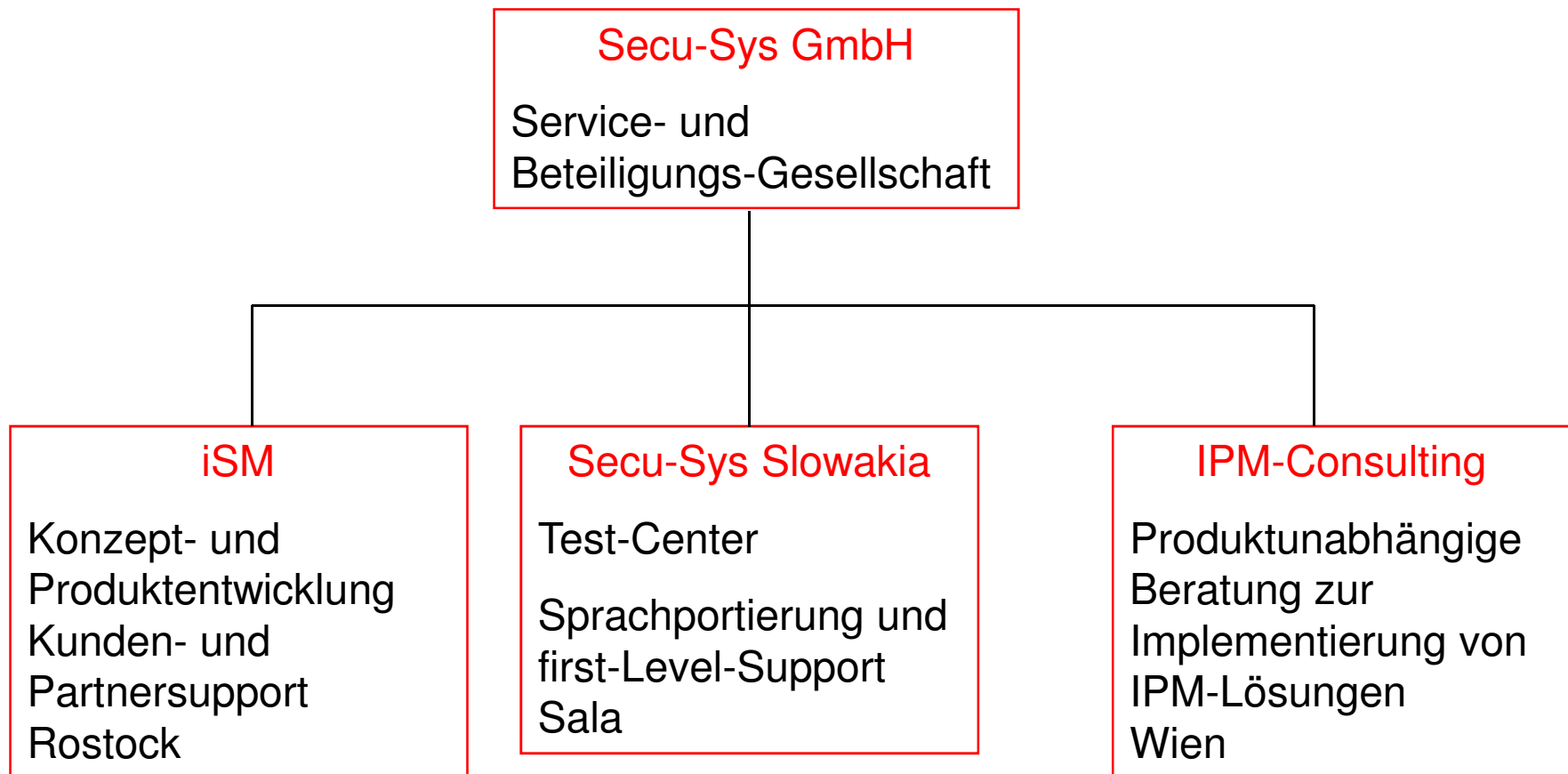


be Flexible † **be** Safe † **bi-Cube**

Identity- und Provisioning-Management Architektur und Erfahrungen mit Systemen der zentralen Nutzer- und Berechtigungsverwaltung

Prof. Dr. Dr. Gerd Rossa
CEO

iSM und die Secu-Sys Group



iSM und die Secu-Sys Group

Produkte:

Bi-Cube IPM (komplexes, modulares
Identity & Provisioning System)

Spezielle Ausprägungen

Auth-Server (Biometrie, Secu-Token,..)

SSO Professionell

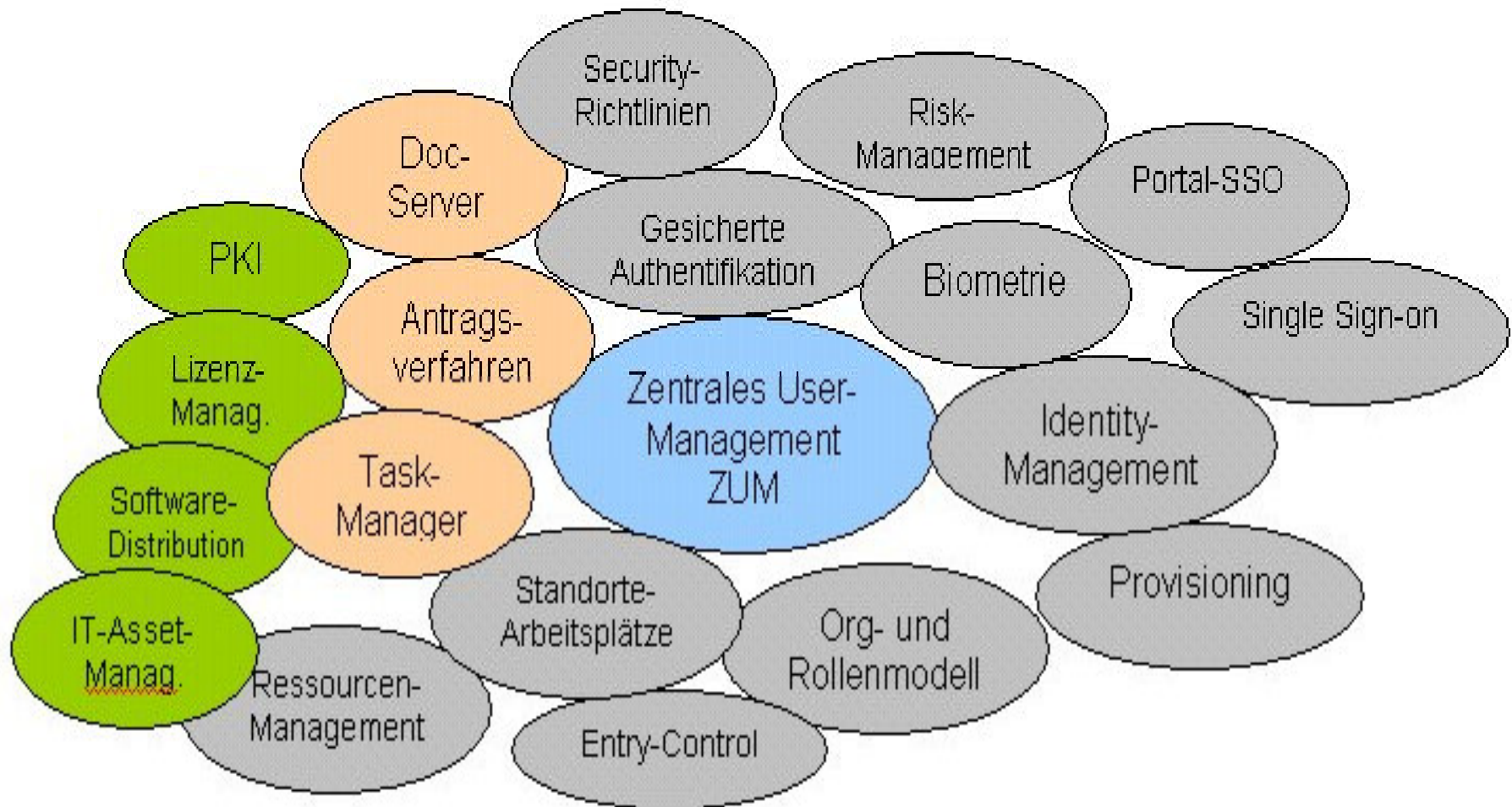
Entry Control

Ressourcen-Manager

USB-Blocker



Gesamtfunktionen von *bi-Cube*® Professional



Die *bi-Cube*® Produktfamilie des Instituts für System-Management.

iSM und die Secu-Sys Group

Das Institut für System-Management arbeitet seit mehr als 10 Jahren auf dem Gebiet des

Identity- und Provisioning-Management (IPM)

Es setzt diese Erfahrungen in konkrete Organisations- und SW-Lösungen um.

Durch die langjährige Wechselwirkung von Technologie-Entwicklung und realer Implementierung in großen Unternehmensstrukturen hat sich das iSM eine **Technologie-Führungsposition** im Bereich komplexer und integrierter IPM-Lösungen erarbeitet.

Es gibt derzeit keinen anderen Lösungsanbieter am Markt der den Stand der IPM-Architektur und -Funktionalität erreicht.



Alleinstellungen - Merkmale

- Konsequente Umsetzung einer modularen IPM-Architektur
- Technologie, asynchrones Messaging mit Logik-Prozessor
- Offene Architektur mit diversen Interfaces u.a. SOA-konforme Webservices
- Funktionsbreite (Identity-Management, Provisioning, SSO, Lizenz- und Ressourcen-Manager, Interne Kosten-Verrechnung, Biometrie)
- Intelligente SoP-Services (Selbstorganisierendes Provisioning)
- Einmaliges Rollen- und Prozeß- Management
- Compliance-Agenten und Internes Kontrollsystem
- Praktischer Nachweis einer kurzen und effektiven Einführungsphase



Stärken des *bi-Cube*® Professional

- Leistungsfähige Unterstützung der Organisations-Modellierung mit Berücksichtigung referentieller Integrität (Abhängigkeiten und Änderungsprozesse)
- Vollständige Unterstützung von Konzernstrukturen mit dezentralen Subsystemen
- Realitätskonformes und vielseitiges Rollenmodell / **Die Funktionalität des Rollenmanagements ist entscheidend für den Erfolg einer IPM-Lösung**
- Hoher Anteil an Prozeßautomatisierung in der User-Administration (bis zu 80%)
- Bereitstellung vordefinierter Generischer Prozeßmodelle
- **Funktionelle Breite** bei modularer System-Architektur
- Spezielle Funktionen für die Finanzwirtschaft
- Integration der User-Richtlinien in den Provisioning-Prozeß (IR)
- Integriertes Datenschutzkonzept / Compliance und IKS



bi-Cube® Professional: Anforderungen für Business Organisation

- **Allgemeine Organisations-Modellierung**
Aufbauorganisation, Standorte, Kostenstellen
Rollen, IT-Geschäftsprozesse, Teams
Modellierungen unter Berücksichtigung von Konzernstrukturen
- **IT- Organisation**
massive Entlastung der Administration und des UHD
Durchgängige Nachweisfähigkeit gegenüber WP und Revision
nur noch ein Bestand an Userdaten für alle Systeme
Keine zusätzlichen Pflegeprozesse für andere Systeme mit
Userdaten
Lose Kopplung dezentraler IT-Organisationen



Architektur - Anforderungen

Nur ein strategischer Ansatz für Identity- und Provisioning-Management kann erfolgreich sein.

Prozess-Security bei gleichzeitiger Rationalisierung der IT-Administration

- zentrale User- und Berechtigungsverwaltung als Kernfunktion des IPM
- logisches Organisations- und Rollenmodell mit effektivem Regelwerk
- integriertes Single Sign-On ohne Zusatzaufwand aber erhöhtem Security-Niveau
- Prozeß- und Task-Manager mit generischen Prozeßmodellen
- Automatisches AD-Ressourcenmanagement (z.B. dynamische Gruppen-LW)
- Identity-Management (Biometrie, Secu-Token, Zertifikat)
- PKI Integration

Direkte kostenwirksame Ergebnisse durch IPM-Einsatz in komplexen Unternehmensstrukturen:

- 70%-80% Rationalisierung durch Automatisierung
- ROI innerhalb von 2 Jahren



Architektur - Anforderungen

- Offene Architektur
- Die wesentlichsten Funktionen der User- und Kompetenzverwaltung stehen als API zur Verfügung.
- IPM-Funktionen stehen als SOA-Webservices zur Verfügung
- Das objekt-relationale Datenmodell soll diese Flexibilität und Offenheit weitgehend unterstützen. Es muss effektive Strukturen für Metadaten zur Unterstützung des Customizing anbieten.
- Die Datenverwaltung soll durch ein etabliertes DBMS realisiert werden
- Interfaces zu anderen Directory-Systemen (LDAP, AD, DirX..)
- Integration des SSO und gesicherte Authentifizierung



Architektur - Anforderungen

Einheitlicher und modularer Ansatz für Userverwaltung mit Identity-Management, Provisioning, Organisations- und Rollenmodell, Prozessautomatisierung und SSO

Offene System-Architektur mit Standard-Connectoren

Integrationsfähigkeit vorhandener Verwaltungssysteme

AD – Management und Automatisierung (z.B. dynamische LW)

Generierung synthetischer Rollen mittels des SoP (Selbstorganisierendes Provisioning)

Ex- und Importfunktionen für ein gesichertes Betriebskonzept

Bereitstellung eines SDK zur Integration der Provisioning-Prozesse in interne Abläufe und Systeme (nach SOA)

Transaktionskonzept und Auflösung von Rollenkonflikten

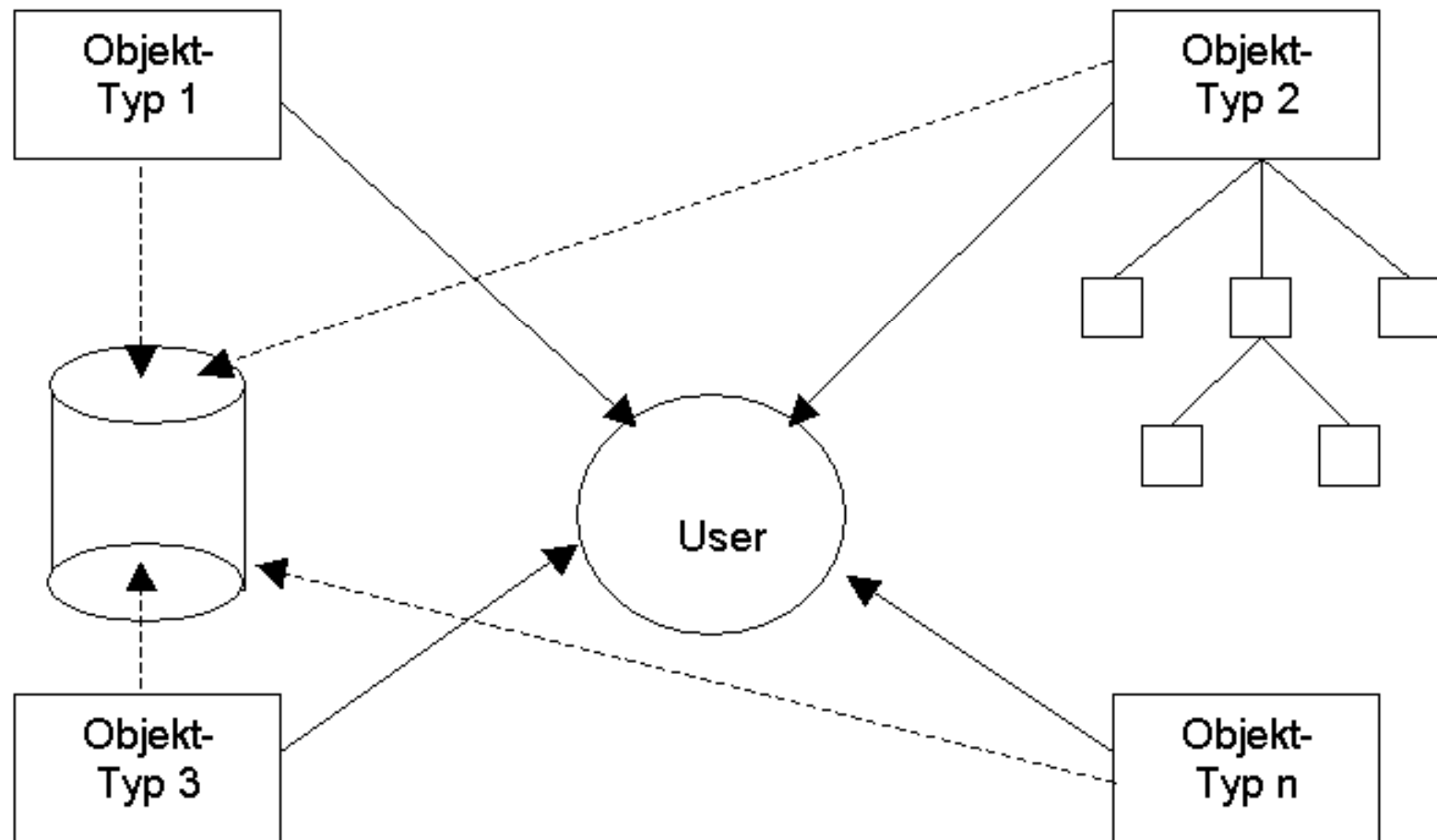
Revisionierbarkeit (SOX, KONTRAG, Basel II)

IKS (Internes Kontroll-System)

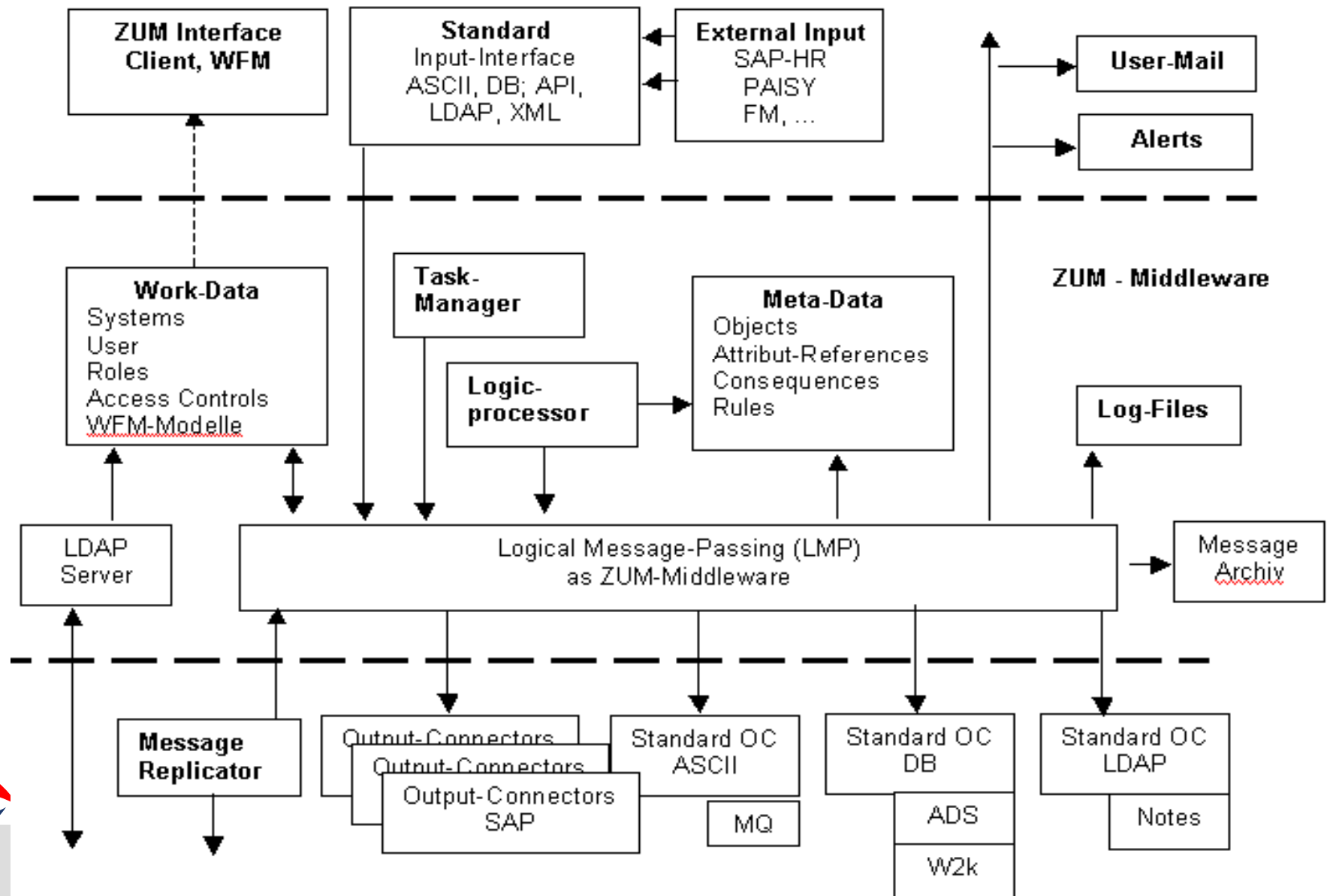


Architektur (USP)

- Objektorientierte Client-Server Architektur



bi-Cube[®] Professional - System-Architektur

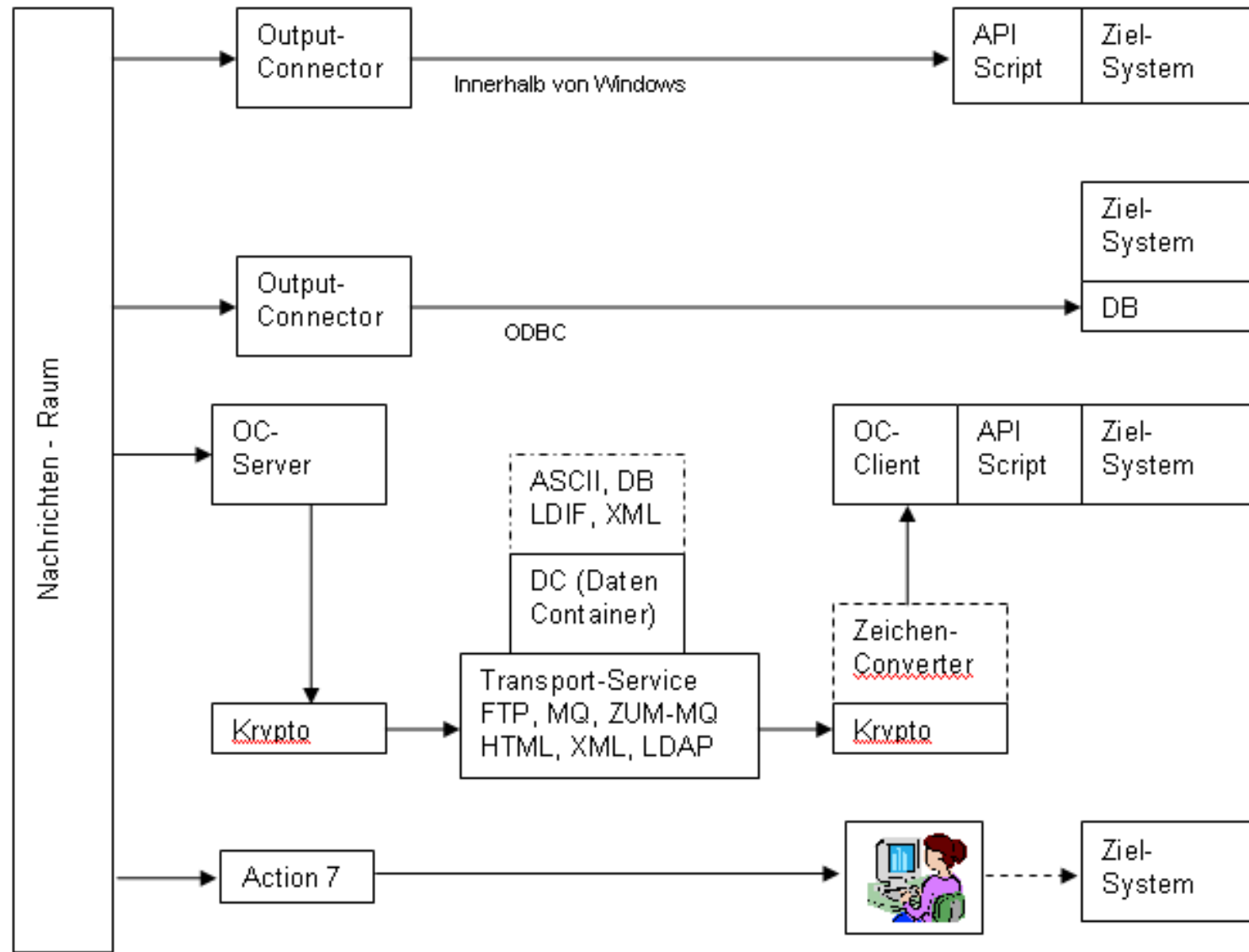


Technologie / asynchrones Messaging (USP)

- Dieses Prinzip ist ein **Alleinstellungsmerkmal** von **bi-Cube®** und die Basis der aktuellen **Technologie-Führerschaft** des iSM
- Abweichend vom klassischen Vorgehen, werden die Daten nicht direkt in die DB geschrieben, sondern Nachrichten von jedem System an jedes andere System in einen zentralen Nachrichtenraum (NR) geschickt.
- Jedes Zielsystem wird durch einen Output-Connector mit dem NR verbunden und mit den entsprechenden Nachrichten (Änderungsdaten) versorgt. Transaktionsstati sichern eine geordnete Verarbeitung.
- Diese sog. Messages stellen ein **bi-Cube®**-internes Protokoll dar.
- Jede Message durchläuft vor der Weiterverarbeitung einen Logik-Prozessor, der sog. Konsequenzen prüft. Im Ergebnis dieser Prüfung können diverse weitere Messages generiert werden, usw.



Technologie der Output-Connectoren



Unterstützte Verzeichnisdienste

(incl. Application Server):

Directory	Zugang
Microsoft Active Directory	Nativ Integration
Novell Directory Service	Nativ Integration
Novell Edirectory	Über LDAP
IPlanet Directory Service	Über LDAP
Sun ONE Directory Service	Über LDAP
IBM Security Directory	Über LDAP
Websphere	Über LDAP
Netscape Directory Service	Über LDAP
DirX	Über LDAP
Microsoft NT4 Domänen	Nativ Integration



Rollen-Modell und SoP (USP)

(Selbstorganisierendes Provisioning)

Die bi-Cube-Prozeßmodelle sind die Basis des SoP-Verfahrens und der Automatisierung der IT-Administration

Die Organisations- Fach- und Systemrollen werden durch logische Attribut- und Objektreferenzen weitgehend automatisch zugeteilt und auch wieder entfernt.

Veränderungsprozesse wie Mitarbeiter- Ein- und Austritt, OE-Wechsel, OE-Struktur- und Standortwechsel werden im Rollenmodell automatisch nachgezogen.

Die automatischen Prozesse können an geeigneten Stellen durch Genehmigungs- und Informations-Aktivitäten ergänzt werden



Reife eines Unternehmens für eine IPM-Lösung

IPM kann kein organisatorisches Chaos verwalten!!!!

- Unternehmensstrategie und Projektpositionierung muß passen
- Architekturverständnis
- Status der Organisation
- Modellierungsverständnis
- Umsetzbares Vorgehensmodell

Hierzu wird den Teilnehmern eine Checkliste übergeben (Bitte V-Card an der Anmeldung hinterlassen)



Rollen-Modell und SoP

(Selbstorganisierendes Provisioning)

Rollenmodellierung

- Organisations-, Fach- und System-Rollen
- Restriktions-Rollen (zur Einschränkung der Admins)
- Dynamische Systemrollen mit Access-Controls
- Rollenreferenzen (vereinfachte Rollenmodellierung)
- Synthetische Fach- und Systemrollen (USP)
- Security-Classification der Rollen (IKS) (USP)
- Mengenoperationen auf Rollen
- Mandanten- und Team-Rollen (USP)
- Störungsfreie Migrationsfähigkeit von direkter zu rollenbasierter Zuordnung von Berechtigungen (USP)
- Primary-Account (USP)



Zieldefinition

Konkreter Anlass zur Initialisierung des IPM-Projektes

- Unter diesem Gesichtspunkt können bestimmte Probleme bzw. Aufgaben für den IT-Bereich auslösender Faktor sein. Z.B. Ein Merger zwingt zur Integration zweier IT-Welten, Migration wichtiger Plattformen (NT -> w2k), kritische Analysen der IR oder WP, zentrale Compliance-Anforderungen z.B. SOX,...
- Neben diesen aktuellen Initialisierungen kann auch in der strategischen Planung der IT der Einsatz einer zentralen Plattform zur Verwaltung der User und deren Berechtigungen vorgesehen sein.



Problembereiche bei SoP – Prozessen

Bei den SoP- Prozessen sind komplexe Zusammenhänge zu beachten:

Rollenkonflikte (USP)

Zusammenfügen und Trennen von Systemberechtigungen, die aus verschiedenen Rollen dem User zugewiesen werden

Grundregel: Rollensystem überschreibt Direktzuweisung / sanfte Migration vom System- zum Rollenmodell

Rollenaktualisierung

Bei Änderungen von Rollen sind diese auf die zugewiesenen Rollen „durchzudrücken“

Attributindizierte Rollen (USP)

Grundlage der Automatisierung der IPM-Prozesse

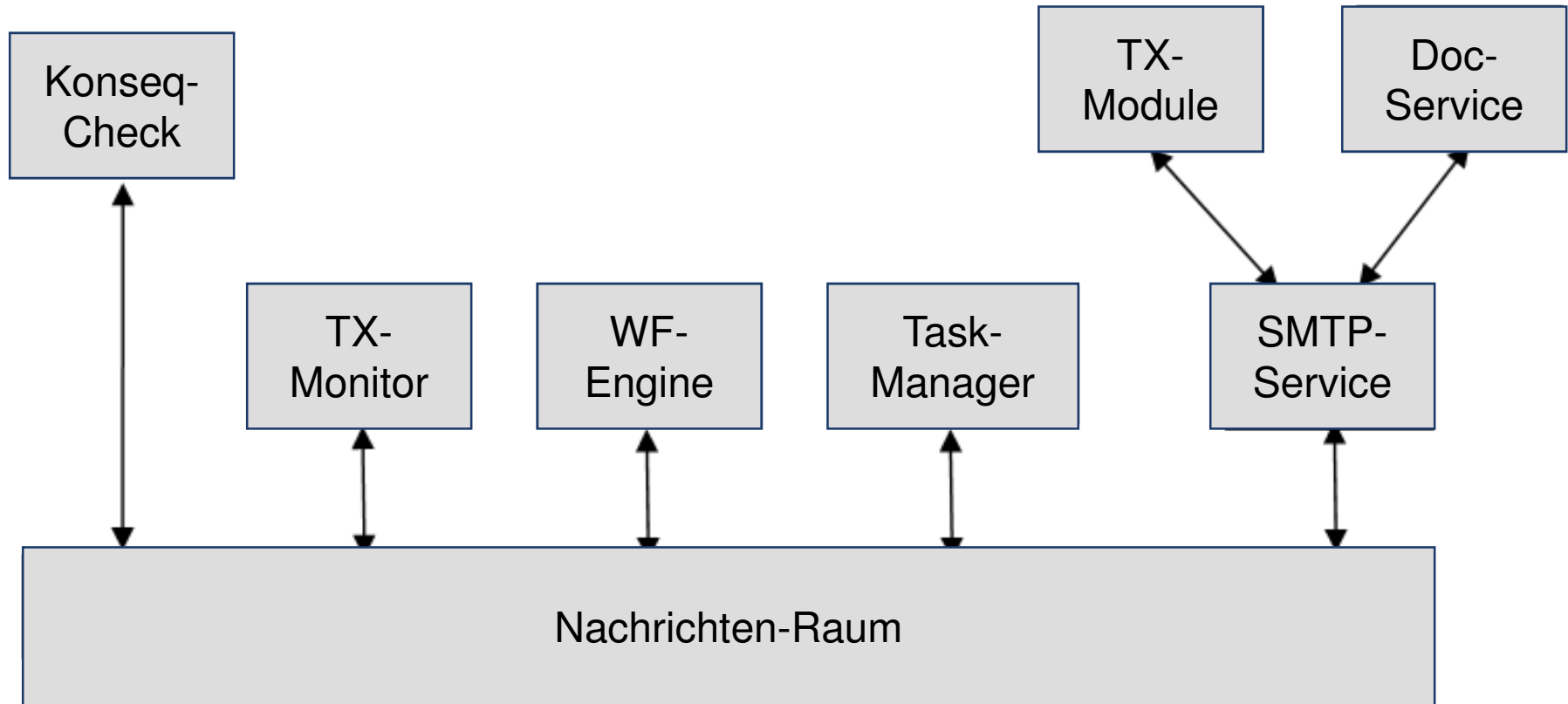
Rollenreferenzen (USP)

Basisrollen werden mit Spezialrollen verbunden und automatisch zugewiesen



Rollen-Modell und SoP

(Kollaboration der Komponenten)



Problembereiche bei SoP – Prozessen

Bei den SoP- Prozessen sind komplexe Zusammenhänge zu beachten:

- **Gleitende Übergänge / Wechselprozesse (USP)**
Bei einer Rollenänderung (z.B. durch OE-Wechsel) können die Berechtigungen nicht schlagartig wechseln (Vor- und Nachlaufzeiten u.a. konfigurierbare Regeln)
- **Wiedereintritt in Konzernstrukturen**
- **Transaktionsmanagement (USP)**
Transaktionen, die durch Attributänderungen getriggert werden, müssen bestimmte Änderungen so lange blockieren, bis die Transaktion beendet ist
- **OE-Kompetenzen**



Rollen und Teams (Projektorganisation) (USP)

Ziel:

- Berechtigungsvergabe an definierte temporäre Gruppen von Usern
- Zentrale Modellierung, dezentrales Provisioning

Regeln:

- Das Team wird mit einem Beginn- und einem Ablaufdatum versehen.
- Teammitglieder werden einer Position zugeordnet (Teamleiter, Stellvertreter...)
- Der Teamleiter fordert die User für sein Team an, vergibt Berechtigungen und steuert die Laufzeit des Teams
- User erhalten die Teamrollen bei Eintritt ins Team bzw. verlieren die Rollen bei Verlassen des Teams.



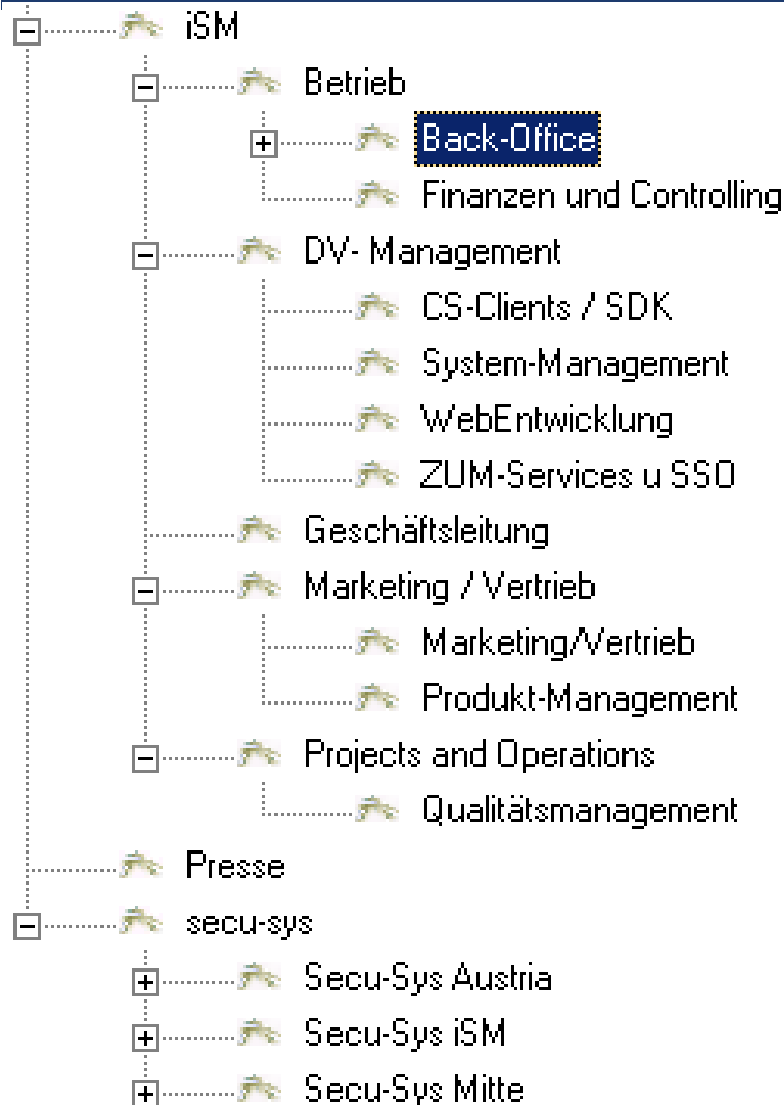
Dynamisches Filespace-Management (USP)

Dynamische Laufwerkszuordnung

- Automatische Generierung von Abtl. u Gruppen-LW
- Automatische Zuordnung von dyn- LW zu Usern
- Änderungsprozesse der OE generieren Änderungen bei den Dyn-LW
- Autom. Wechsel der dyn. LW bei OE-Wechsel des Users



Dynamisches Filespace-Management (USP)



Eigenschaften | User | User mit Stellen | Kostenstellen

Art der Organisationseinheit
Gruppe

Name der Organisationseinheit
Back-Office

Organisationseinheit: 00000011 Übergeordnete Org. Einheit: 00000006

weitere Eigenschaften

ADS Eigenschaften

- ADS Definitionen
 - mit dynamischen Laufwerken
 - Dyn.-Group-Drive
 - keine
 - Dyn.-Dep-Drive
 - keine

Funktionalität / weitere Komponenten

- **LDAP-Server**
für User- bzw. Unternehmensdaten
Verwaltung sekundärer Identifikationsmittel (ChipCard)
Synchronisation anderer LDAP-Devices (z.B. Firewall, RAS-Server)
- **Authentifikations-Server**
Soft-Token / SMS-Token
PKI-Integration (Entrust un Microsoft) Biometrie
duale Authentifikation und API auf Applikations-Servern
insbesondere für Web-Portale
- **Unterstützung Datenschutz (USP)**
X509 Standard Security Classification an User und Applikationen



Funktionalität / SSO

- versch. Single Sign-On Technologien
- User-Selbst-Registrierung / Synchronisation
- Lokales Profil (wichtig für Außendienst)
- Serverbasierter Desktop
- Wahlweise SSO in Windows-Desktop
- Token zur sicheren P to P Communication
- Mehrserver-Konfiguration möglich
- Starke Kryptierung/ Integration Biometrie
- Einsatz sekundärer Identifikationsmittel: Transponder /Chipcard / Zertifikate
- Zusatz-Services



Zusatzauthentifizierung in SSO

Mehrfache Sicherung durch zusätzliche Authentifizierung

Der gesamte SSO-Client oder einzelne besonders sicherheitsrelevante Systeme können durch zusätzliche hardwaregestützte Authentifizierungssysteme geschützt werden.

- **Chipkarte oder Fingerprint**

Ein System wird nur gestartet, wenn der Mitarbeiter sich mit seinem Fingerabdruck oder einer Chipcard zu erkennen gibt.

- **Security-Token, Digitale Signatur, RFID**
- **Besonderheit: aktive Authentifizierung**



SSO- Möglichkeiten des PW-Management

- Der User wechselt das PW im Zielsystem und synchronisiert es mit dem SSO-Client
- Der User wechselt das PW im Zielsystem und der SSO-Client fängt diese Eingabe ab und übernimmt sie.
- Der SSO-Client übernimmt den PW-Wechsel komplett automatisch auf dem Client durch Simulation der User-Interaction
- Der SSO-Client übernimmt den PW-Wechsel komplett automatisch auf dem Client durch Nutzung einer vom Zielsystem bereitgestellten API (z.B. SAP)
- Das SSO-System realisiert den PW-Wechsel serverseitig (z.B. RACF)
- Secu-Token (beste Lösung, erfordert Eingriff in Applikation)



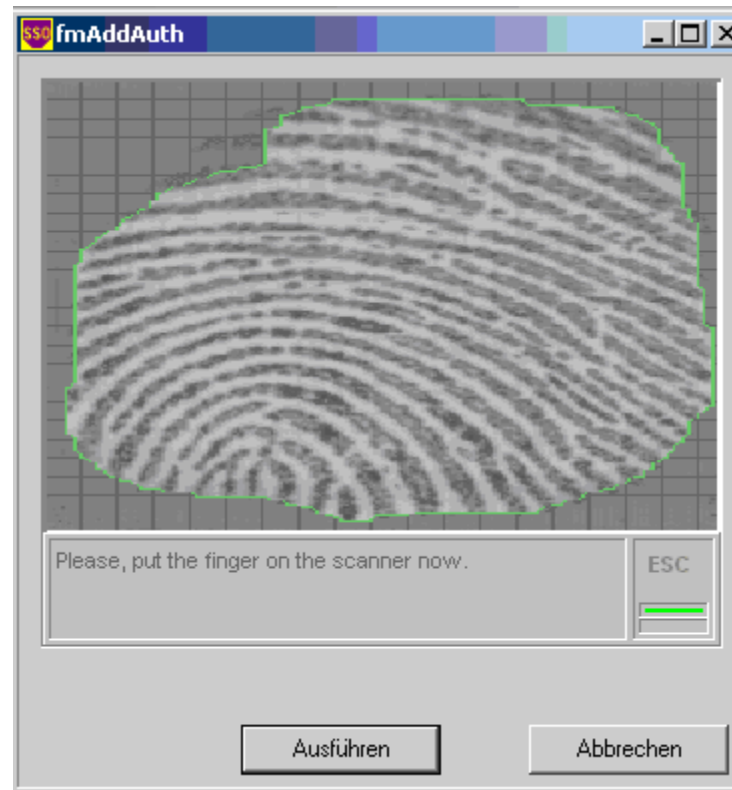
Paßwort-Management (USP)

- **Automatischer PW-Wechsel in Zielsystemen bei Einsatz der Connectoren**
- **PW-Self-Service über Web-Client**
- **UHD-Entlastung!!**

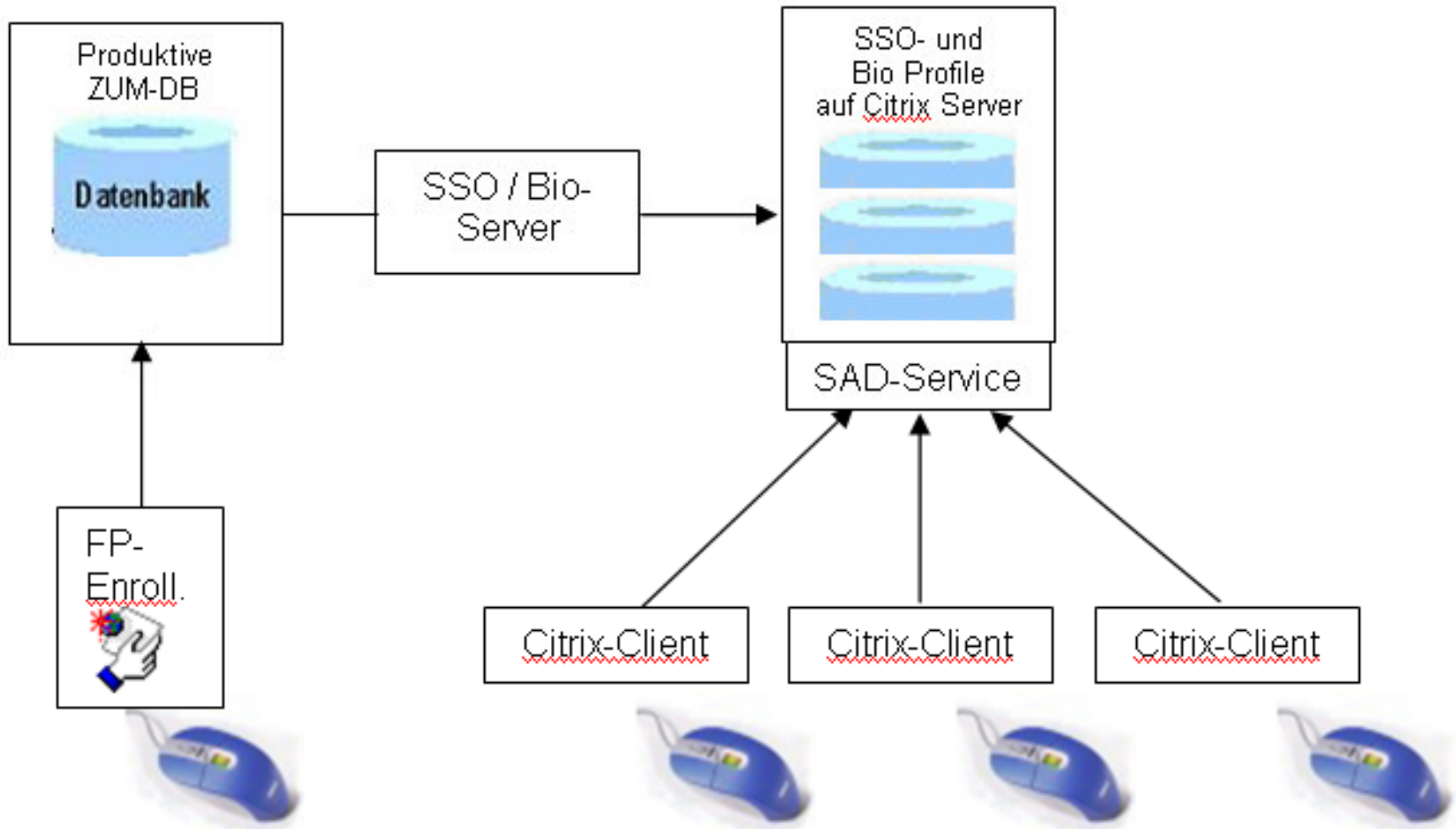


Bio-Logon

- **Anmeldung am Betriebssystem (iSM-Gina)**
- **Zusatzauthentifizierung im SSO**

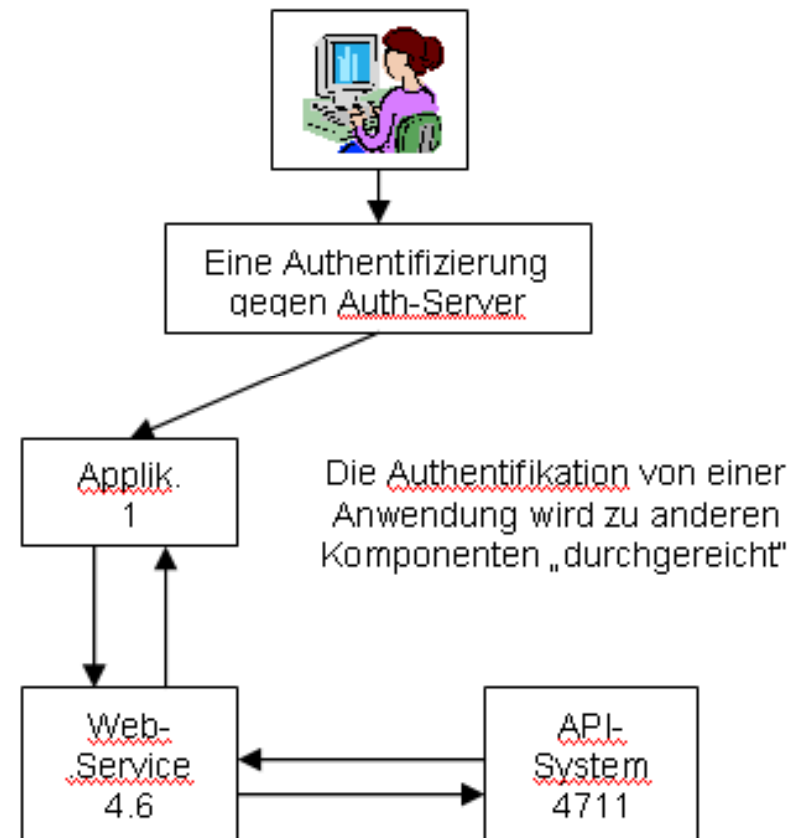
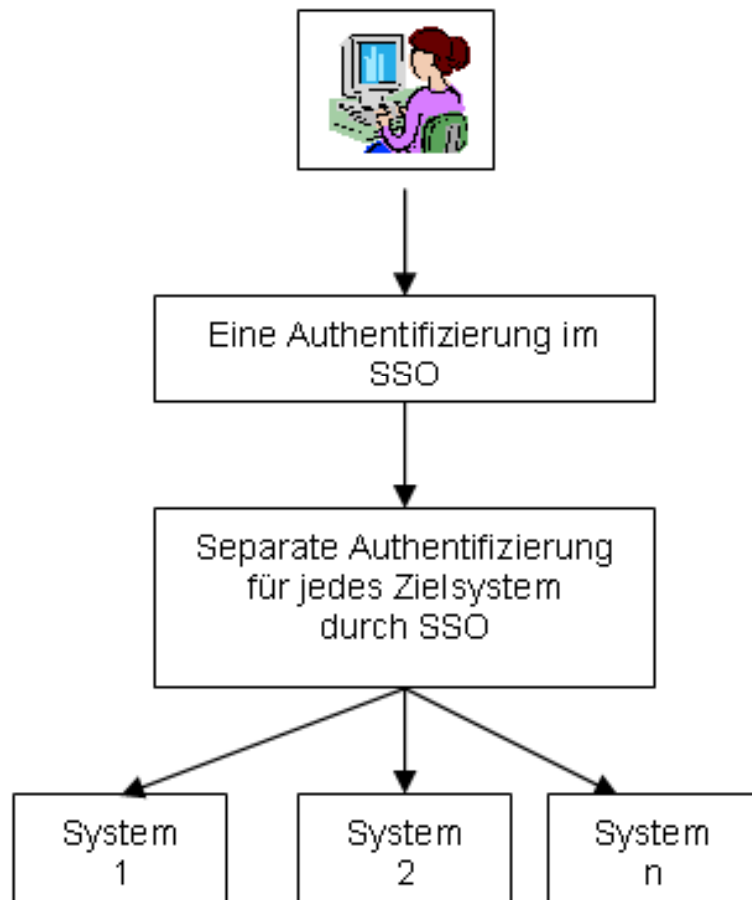


Eine Lösung: Biometrie, SSO und Citrix



SSO versus Federated Identity ?

Zwei Wege und teilweise auch 2 Ziele



bi-Cube[©] Professional – als online Access-Control-Server

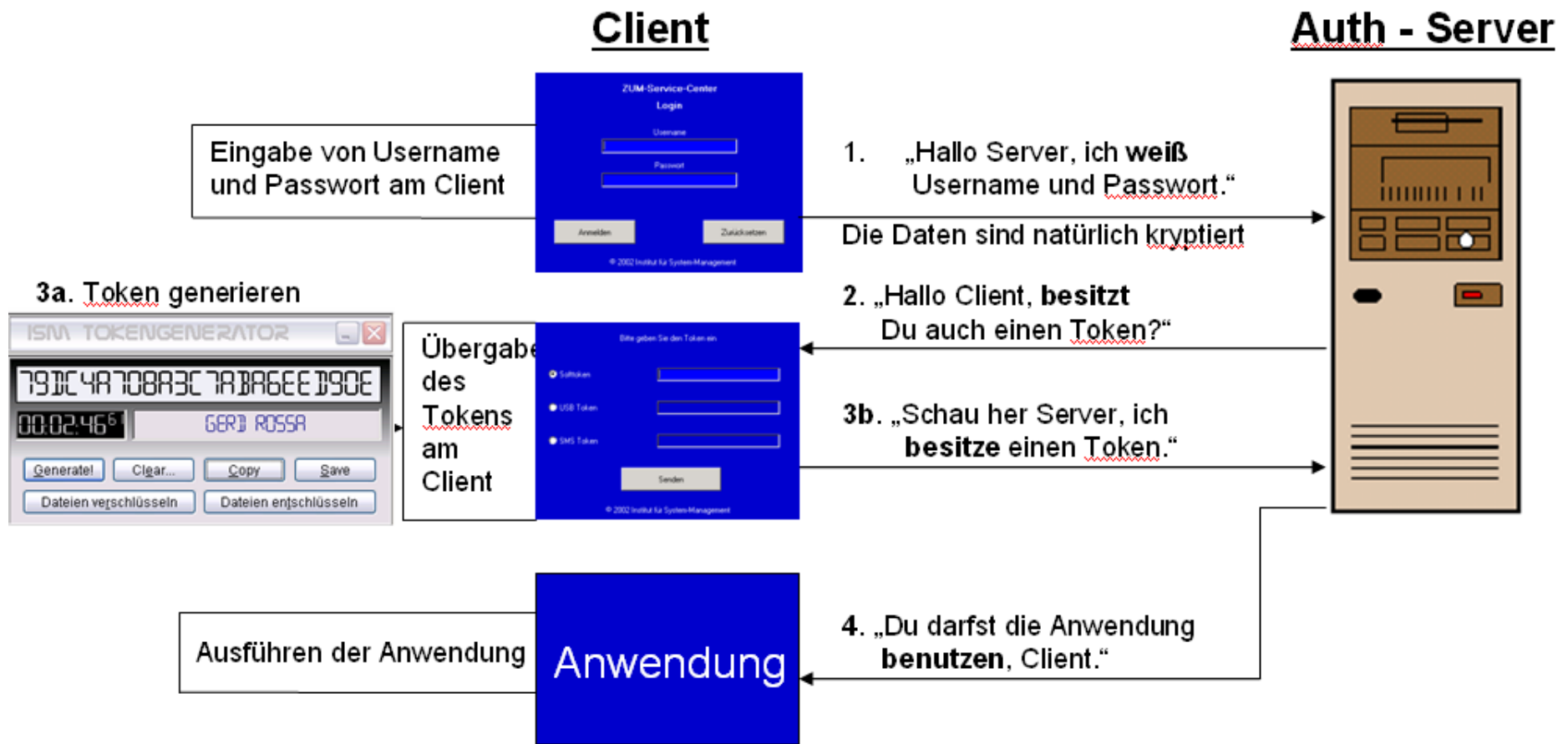
Autorisierung

Analog sind die Möglichkeiten der Unterstützung der Autorisierung durch **bi-Cube[©] Professional**

1. LDAP
Via LDAP kann das aktuelle Berechtigungsprofil eines Users für ein bestimmtes System abgefragt werden. (Proxy, Unix,..)
2. API
Dem Programmierer kann ein API bereitgestellt werden, das ein Berechtigungsprofil entweder zentral oder auch dezentral bereitstellt.
3. Access-Controls
Die engste Verbindung mit ZUM erfolgt auf der Basis der Access-Controls (AC).



bi-Cube[©] Token / Authentifikations-Server



bi-Cube[©] Token / Authentifikations-Server

Bitte geben Sie Ihr Token ein.

1. Tokenart wählen

Security-Token

SMS-Token

Handynummer

2. Token eingeben



bi-Cube® Professional als EAI oder „Datendrehscheibe“

Auf der Basis der Funktion des **bi-Cube**® als „Datendrehscheibe“ ergibt sich bereits hier ein erster Nutzen, indem die umfassende Datensammlung zu allen Usern anderen Systemen zur Verfügung gestellt werden kann.

Dazu gehören zum Beispiel:

- Datawarehouse
- Zeiterfassungs- und Zutrittssysteme
- Parkberechtigungen,
- Kantinenverwaltung, usw.

Viele dieser Systeme verwalten eigene Credentials, die vor allem beim Verlassen eines Mitarbeiters eine zeitnahe Information benötigen.



bi-Cube[®] Professional als Entry-Control-Server

Zutrittssteuerung

- Rollenbasiert
- Antragsverfahren
- Anbindung an konventionelle Zutrittssteuerungen
- Integration Biometrie



**Entry-Control
als integrierte
Profi-Lösung
(USP)**

Die „angenagelte“ Maus



bi-Cube® Professional–Zentralsystem (USP)

Zielstellung

- In einer Konzernstruktur mit „loser Kopplung“ und damit auch verschiedenen separaten IPM-Systemen ist ein Master -System zu installieren, das es gestattet, Cross-Ressourcen zu verwalten
- Es ist zu realisieren, daß einige Applikationen, auf verschiedenen Konzernunternehmen verteilt sind, aber bestimmten Mitarbeitern über den gesamten Konzern zur Nutzung bereitgestellt werden müssen.
- Weiterhin sollten alle Mitarbeiter konzernweit eine Identität haben, um Wechselprozesse zu unterstützen
- Dazu ist ein Master-IPM zu installieren, in dem alle User mit ihrer Verw-ID und den wichtigsten Stammdaten verwaltet werden.



Weitere Einsatzrichtungen

- **Asset – Management**
- **Standorte (in Bezug zu techn. Ressourcen)**
- **Integration USB-Blocker (USP)**
- **Lizenz – Kontrolle**
- **Adressverwaltung**
- **Geschäftsstellen (für die Finanzinstitute)**
- **Arbeitsplatzverwaltung**
- **Projekt – Controlling in SW-Entwicklung**

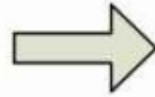


PKI in *bi-Cube*® Professional Umgebung

- Das *IPM*-System hat bei der PKI die Funktion der Verwaltung der Zertifikate im Sinne eines Ressourcenmanagements und der Zuordnung der Zertifikate samt geeigneter Zertifikatsträger zu einem User.
- Die Zuordnung eines Zertifikatsträgers (SmartCard oder USB-Token) erfolgt dabei weitgehend automatisiert über ein entsprechendes Organisations- und Rollenmodell. Die jeweilige PKI wird dabei aus Sicht des *ZUM* wie ein Subsystem betrachtet.
- Über eine geeignete Organisationslösung wird die gesicherte Übergabe des Zertifikats an den User abgewickelt.
- Erst durch die Integration in ein *bi-Cube*® Professional wird eine PKI wirtschaftlich betreibbar **(USP)**

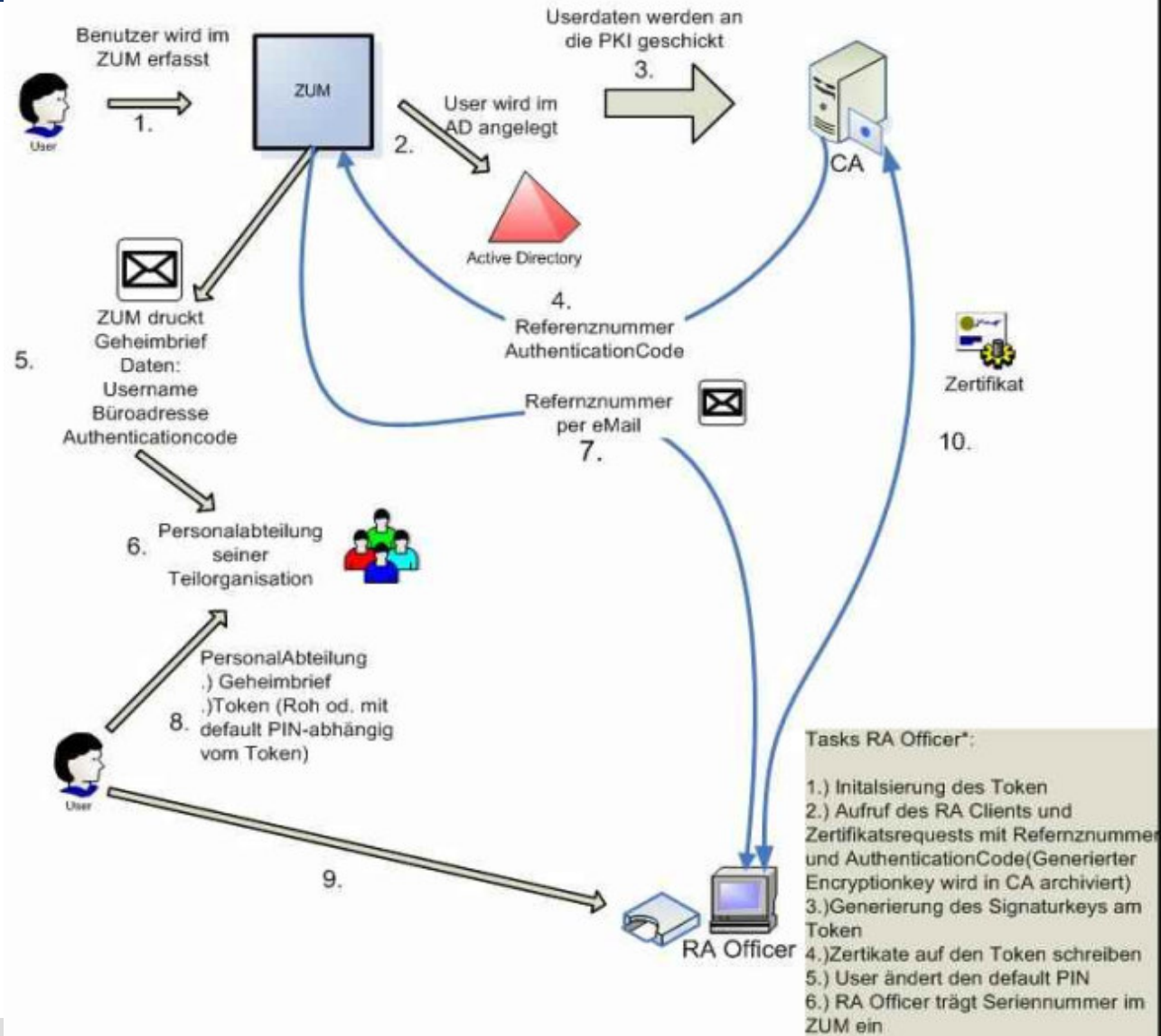


Tokenlieferung
Seriennummer



ZUM
Ressource
Manager

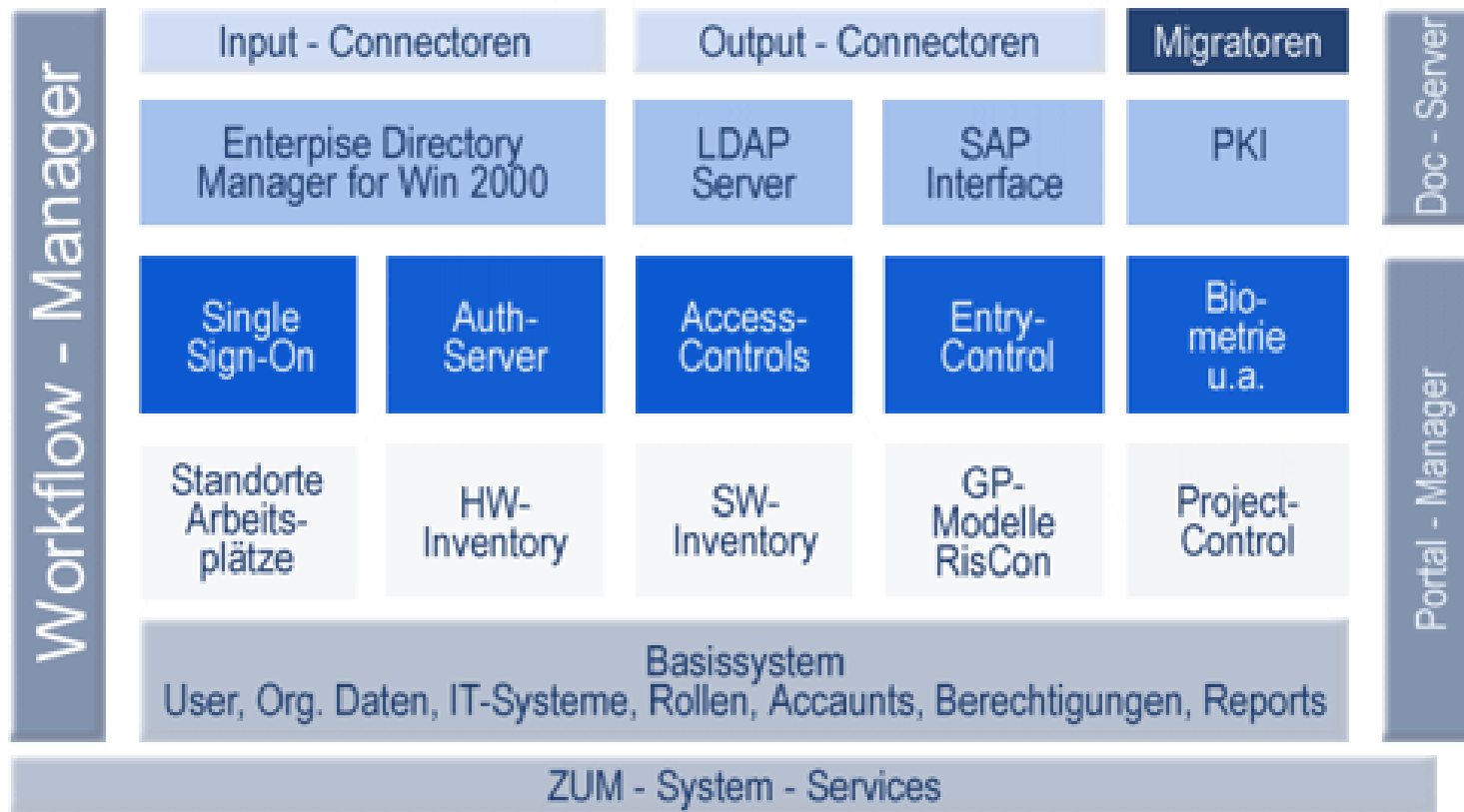
Input -> Personen
bestimter Rolle
Auditor -> Person mit
bestimmter Rolle
Check ob alle Token
erfasst sind



* Funktion der RA Officers wird durch
Innernrevision wahrgenommen



bi-Cube[©] Professional - Systemstruktur



Erreichbarer Nutzen und Effekte

direkter Nutzen

Wesentliche Reduzierung des Aufwandes in der Administration
Verringerung des Gefährdungspotentials

Prozess- Nutzen

Geordnete bzw. verbesserte Geschäftsprozesse
Automatisierung der IPM-Prozesse erhöht die Security

Compliance und IKS (USP)

durchgängige Nachvollziehbarkeit aller Aktionen und interne
Überwachung des Systems

Synergetischer Nutzen

Je mehr einzelne Komponenten im Rahmen eines Gesamtkonzeptes
„zusammenspielen“, um so geringer ist der Aufwand zur Implementierung
der einzelnen Komponenten

Nutzen neuer Funktionalität

Die neue Lösung ermöglicht Funktionen, die vorher nicht zu realisieren
waren



- Nachvollziehbarkeit aller Prozesse (SOX Support)
- Keine Berechtigungs-“Leichen“
- Nur aufgabenbezogene Berechtigungen
- Erhöhte Sicherheit im Access-Management
- Integration von PKI inkl. Verwaltung der Prozesse
- Integration von Sub-Directories, damit überall gleiche Berechtigungs-Regeln
- Gutes Rating im Risk-Management
(KONTRAG, SOX u. Basel II)
- Erhöhte Benutzersicherheit
(keine mehrfachen Passworte usw.)



Vorgehensmodell zur IPM-Einführung

Zieldefinition und Produktevaluierung

Proof of Concept oder Pilot

Ralisierung

Ein 2-Stufen-Konzept für die Umsetzung sichert kurzfristigen Nutzen und Raum für die Lösung offener Organisatorischer und konzeptioneller Fragen.

In Phase 1 wird das Kernsystem mit eindeutiger und unstrittiger Funktionalität realisiert

In Phase 2 werden die komplexeren Prozesse realisiert



Vorgehensmodell zur IPM-Einführung

1. Phase (beispielhaft – Dauer 4 Monate)

Produktiv

- Installation Kernsystem mit direkter Verwaltung der User im IPM, wenn das Interface zu SAP noch nicht steht
- Synchronisation der User im AD
- direkter Vergabe der Berechtigungen vor allem für Kernsysteme des Unternehmens
- Definition einiger Basisrollen incl. deren Antragsmöglichkeit im Web
- Nutzung erster Prozeßmodelle (Ein-, Austritt, allgemeiner Antrag)
- Einführung SSO / Auth. mit Biometrie an Windows PC

Konzeptionell

- Erarbeitung eines Fach-Rollen-Konzeptes
- Lösung diverser Org-Probleme (Betriebsrat, Personal,..)



Vorgehensmodell zur IPM-Einführung

2. Phase (beispielhaft - Dauer 10 Monate)

Produktiv

- Synchronisation mit Personal und anderen Org-Prozessen
- Weitere Funktionen im AD
- Übernahme weiterer Systeme in das Provisioning
- Weitere Rollen und Prozesse
- Einführung Interne Kostenverrechnung
- Einführung Lizenz-Management

Nutzung der zentral verfügbaren Daten und Konzepte für diverse andere Systeme. Z.B. für den Entwicklungsbereich



Vorgehensmodell zur IPM-Einführung

1. Phase (beispielhaft – Dauer 4 Monate)

Produktiv

- Installation Kernsystem mit direkter Verwaltung der User im IPM, wenn das Interface zu SAP noch nicht steht
- Synchronisation der User im AD
- direkter Vergabe der Berechtigungen vor allem für Kernsysteme des Unternehmens
- Definition einiger Basisrollen incl. deren Antragsmöglichkeit im Web
- Nutzung erster Prozeßmodelle (Ein-, Austritt, allgemeiner Antrag)
- Einführung SSO / Auth. mit Biometrie an Windows PC

Konzeptionell

- Erarbeitung eines Fach-Rollen-Konzeptes
- Lösung diverser Org-Probleme (Betriebsrat, Personal,..)



Vorgehensmodell zur IPM-Einführung

2. Phase (beispielhaft - Dauer 10 Monate)

Produktiv

- Synchronisation mit Personal und anderen Org-Prozessen
- Weitere Funktionen im AD
- Übernahme weiterer Systeme in das Provisioning
- Weitere Rollen und Prozesse
- Einführung Interne Kostenverrechnung
- Einführung Lizenz-Management

Nutzung der zentral verfügbaren Daten und Konzepte für diverse andere Systeme. Z.B. für den Entwicklungsbereich





Besuchen Sie
das iSM im Internet:

[www. Secu-Sys .de](http://www.Secu-Sys.de)

[www. *bi*-Cube .de](http://www.bi-Cube.de)