



Secu-Sys
Group



bi-Cube

IPM Komponentensystem (Identity und Provisioning- Management)

Ein Erfahrungsbericht

© iSM Gerd Rossa CEO

Gliederung

- Motivation und Zielstellung
- Technologie und Architektur
- Funktionalität
- Implementierung
- ROI-Betrachtung
- Am Beispiel: Generali und e-plus

Situation heute

Beide Partner sind zufrieden und leben voll die IPM Lösung

Generali

- Die Generali administriert von einem Zentrum (Wien) aus alle Unternehmen in Osteuropa und 14 deutsche Konzernunternehmen (AMB) mit ca. 50.000 Usern
- Schwerpunkt: Ressourcenverwaltung des ADS über alle Domänen hinweg mit Integration der Filertechnologie
- User- und Rechtemanagement am Host
- Verwaltung der Organisationsstrukturen und eines fachlichen Rollenmodells
- Alleine in Österreich Rezentralisierung der Administration von 70 auf 5 Administratoren
- Zentrales Ressourcenmanagement dieser IT-Struktur und Komplexität nur mit ZUM (Zentrales User-Management) möglich. (Z.B. alleine in D 1.4 Mio Filespacezuordnungen)
Adminaufwand auf 30% reduziert.
Zufriedene IR und WP

Situation heute

Beide Partner sind zufrieden und leben voll die IPM Lösung

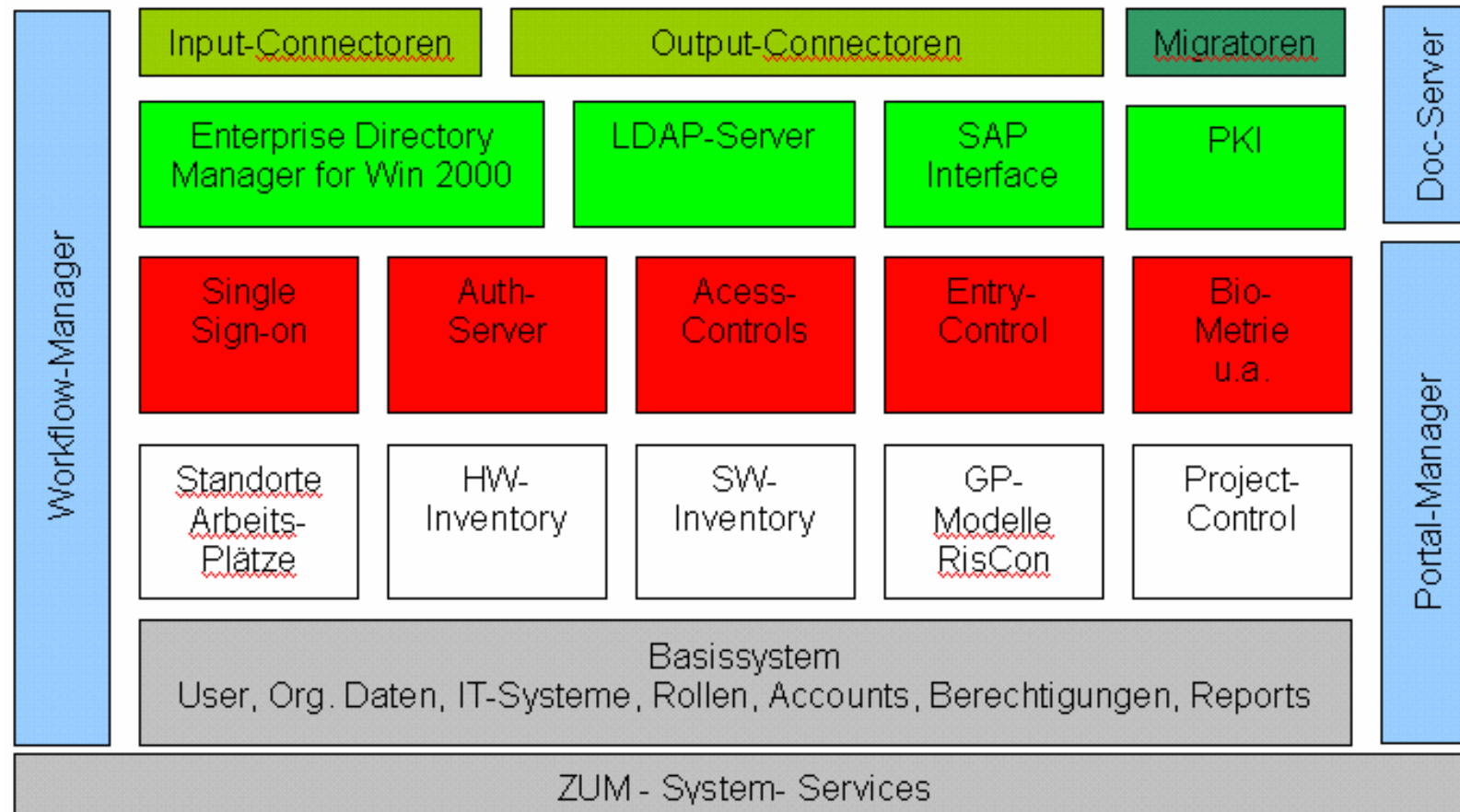
E-plus

- Von Beginn an die Berechtigungsvergabe nur über Rollen.
- Automatisierung durch Workflow
- 70% der „Glattläufer-Rollen“ werden vollautomatisch zugeordnet.
- Automatische Wechselprozesse z.B. OE-Wechsel = Wechsel der Rollen
- Auflösung von Rollenkonflikten
- ROI von unter 2 Jahren
- - etwa 5000 User an 14 Standorten deutschlandweit.
- - über 400 UNIX Server, deren Accounts automatisch von ZUM verwaltet werden.
- - in 2 Domänen werden Windows-Accounts automatisch verwaltet.
- - über 100 globale Zugriffsgruppen werden automatisch von ZUM im Active Directory Usern zugewiesen oder entzogen.
- - über 1000 aktive Systeme.
- - stark gesunkene Aufwände in der Windows Useradministration.
- - 2 ZUM-Administratoren.
- - konsistente, revisionssichere Erfassung aller Systemberechtigungen der User.
- - Löschung aller Berechtigungen eines Users, der das Unternehmen verlässt, durch Mitarbeiteraustritt-Workflow,
- - performantes, skalierbares Frontend für alle User bei E-Plus (ZIC).

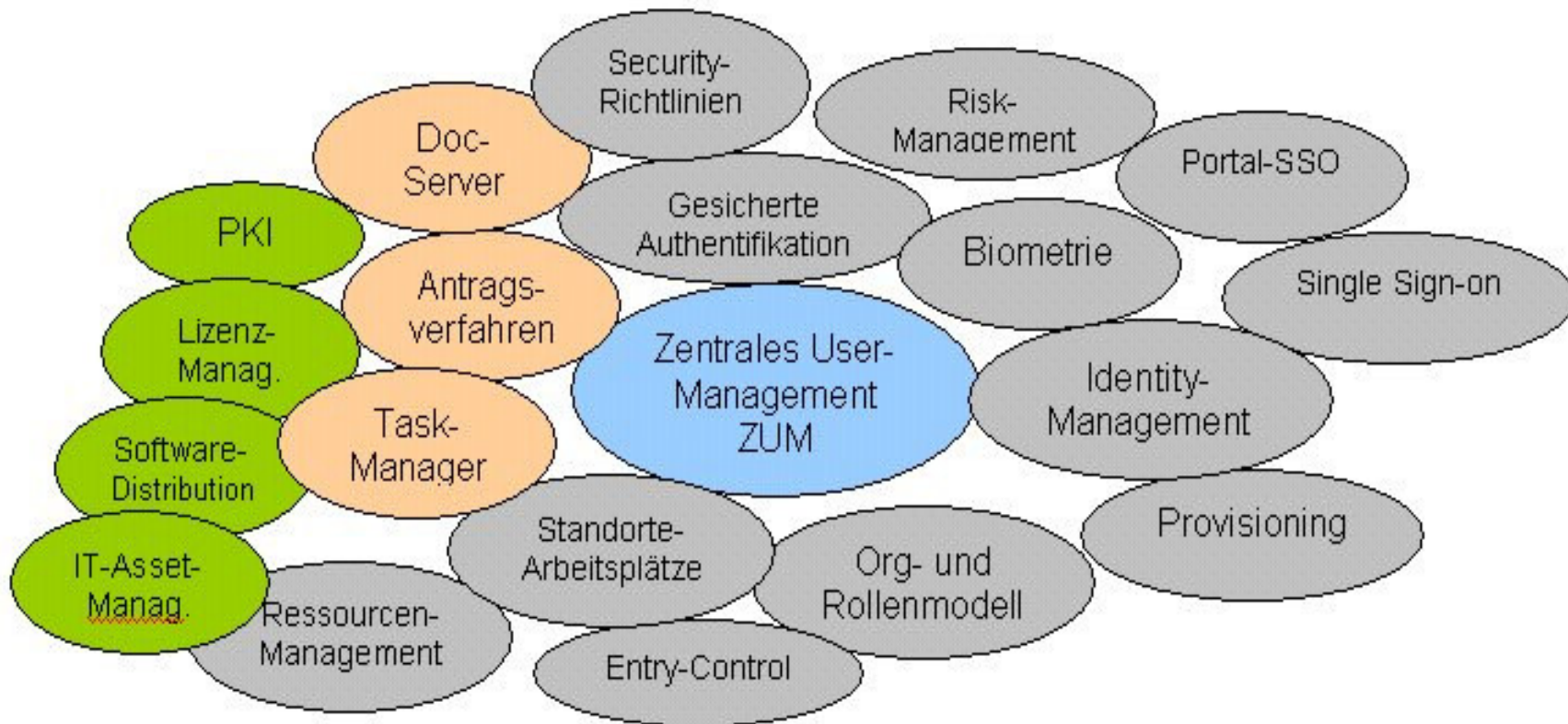
Der Weg dahin - Anforderungen

- Die Architektur sollte offen sein, um unabhängig von evtl. beigestellten Verwaltungstools eigene Komponenten einbinden zu können.
- Es soll modular strukturiert und trotzdem weitgehend out of the box einsetzbar sein
- Das Datenmodell soll diese Flexibilität und Offenheit unterstützen. Es muß effektive Strukturen für Metadaten zur Unterstützung des Customizing anbieten.
- Die Datenverwaltung soll durch ein etabliertes DBS realisiert werden und damit einer internen Weiterentwicklung offen stehen.

bi-Cube - Systemstruktur



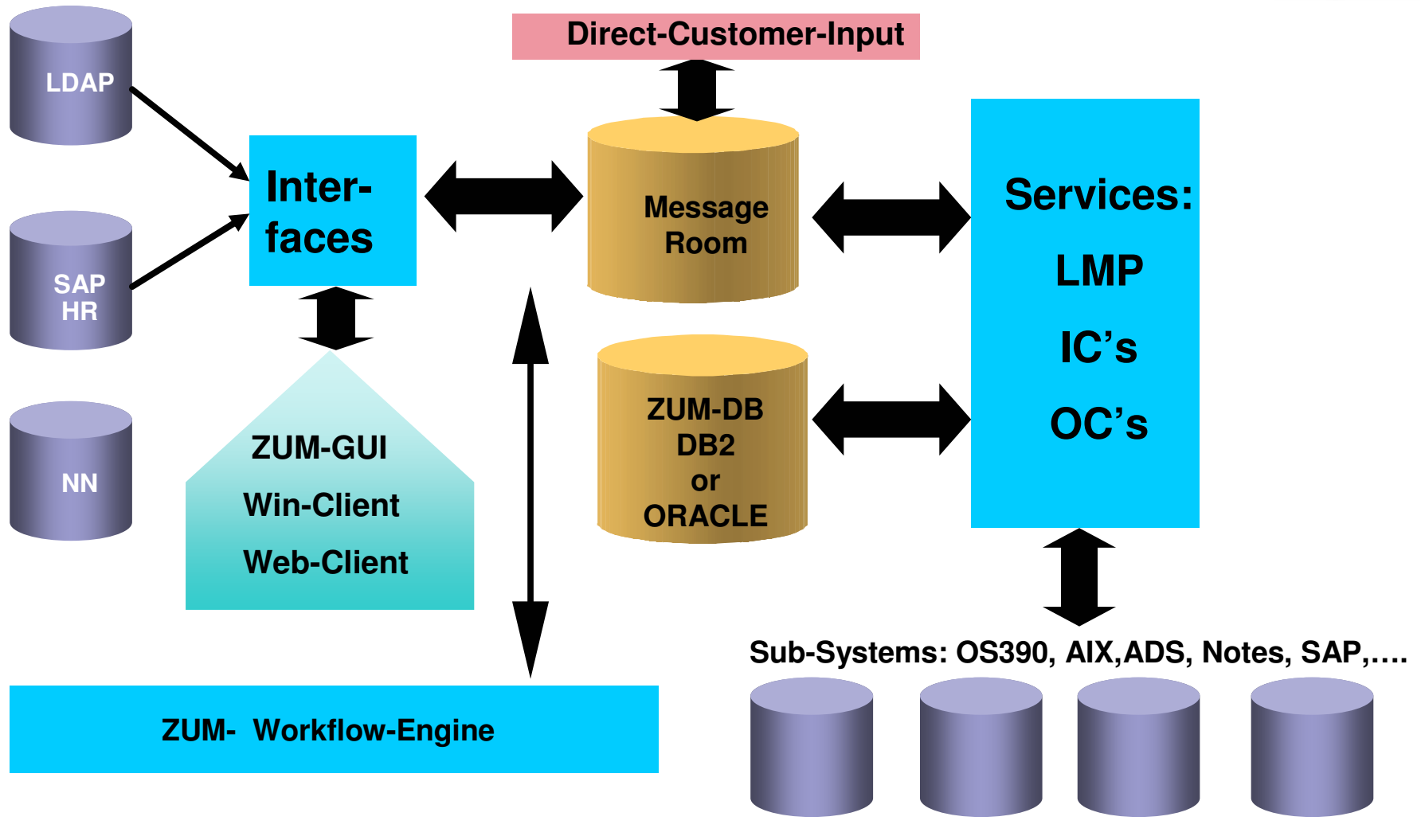
bi-Cube – Funktions-Komponenten



Technologie / asynchrones Messaging

- Dieses Prinzip ist ein Alleinstellungsmerkmal von **bi-Cube** .
- 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.

bi-Cube - System-Architektur



Funktionalität / Userverwaltung

- **User-Zuordnungen**
Funktionen / KSt. / Organisationseinheit /
Standort / Arbeitsplätze
Rollen
Teams
- **Berechtigungen**
Berechtigungen für Standardsysteme
Berechtigungen für Fachapplikationen
Berechtigungen im e-Business
Applikationen ohne Authentisierung
- **Ressourcen** (via *bi-Cube* ins ADS und win 2000)

Funktionalität / Userverwaltung

- **Vordefinierte Abläufe in der GP-Modellierung für:**
 - Antrag für Systemberechtigungen
 - Antrag für Rollenzuteilung
 - Automatische Berechtigungsvergabe für neue Mitarbeiter
 - Supportanfrage an NBV (Nutzer- u Berechtigungsverwaltung)
 - Automatisches Mitarbeiteraustrittsverfahren
 - PKI - Integration
 - Antrag auf einen Arbeitsplatz bzw. Änderung der Arbeitsplatzausstattung
 - Rollenbasierter Antrag auf eine Zutrittsberechtigung

Funktionalität / weitere Komponenten

■ LDAP-Server

für User- bzw. Unternehmensdaten

Verwaltung sekundärer Identifikationsmittel (ChipCard)

Synchronisation anderer LDAP-Devices (z.B. Firewall, RAS-Server)

■ PKI (ist erst durch ZUM sinnvoll nutzbar / Aufwand)

Tokenverwaltung / Zuordnung im Workflow

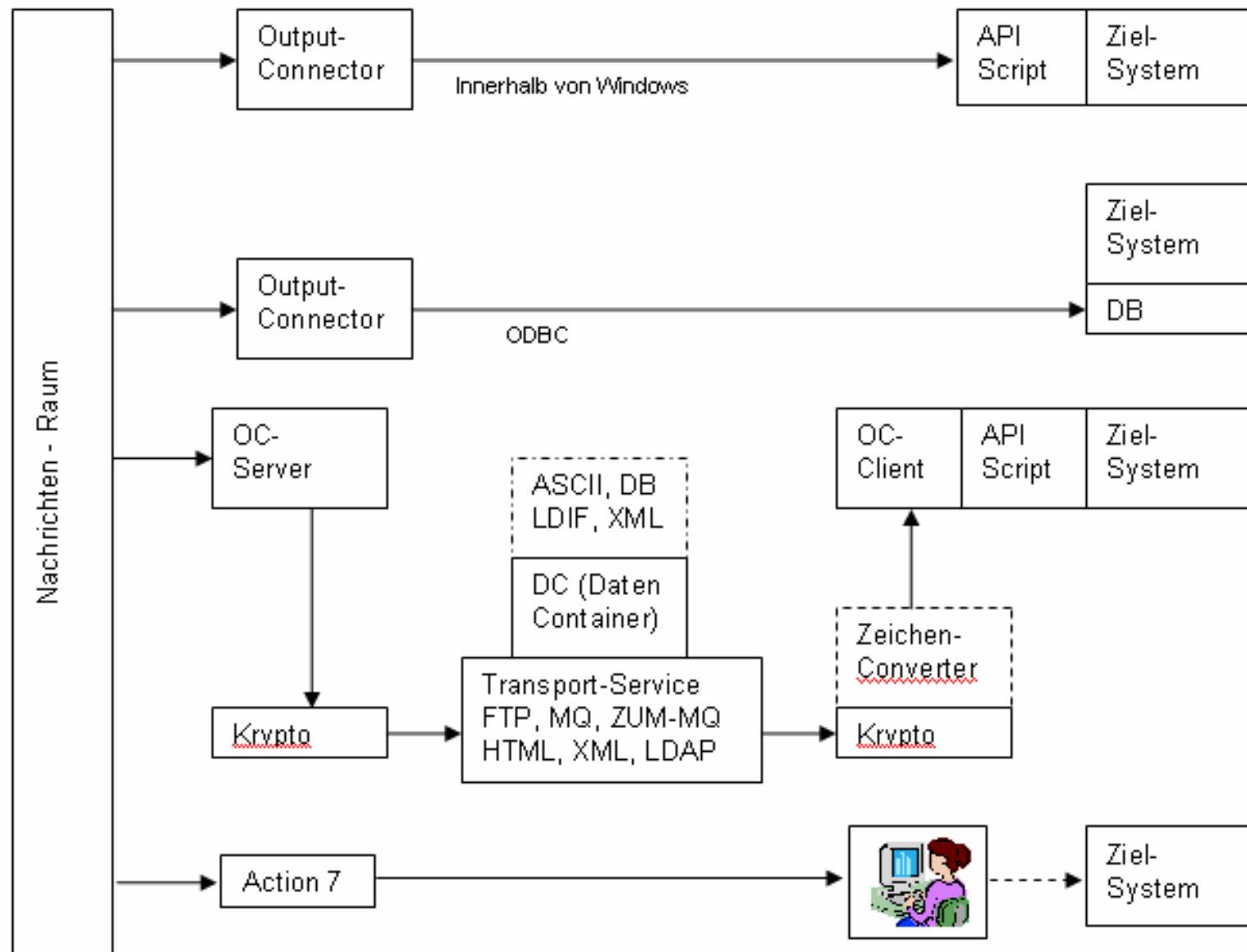
FallBack Lösung bei fehlendem Token

Integration mit Zutritt

■ Unterstützung Datenschutz

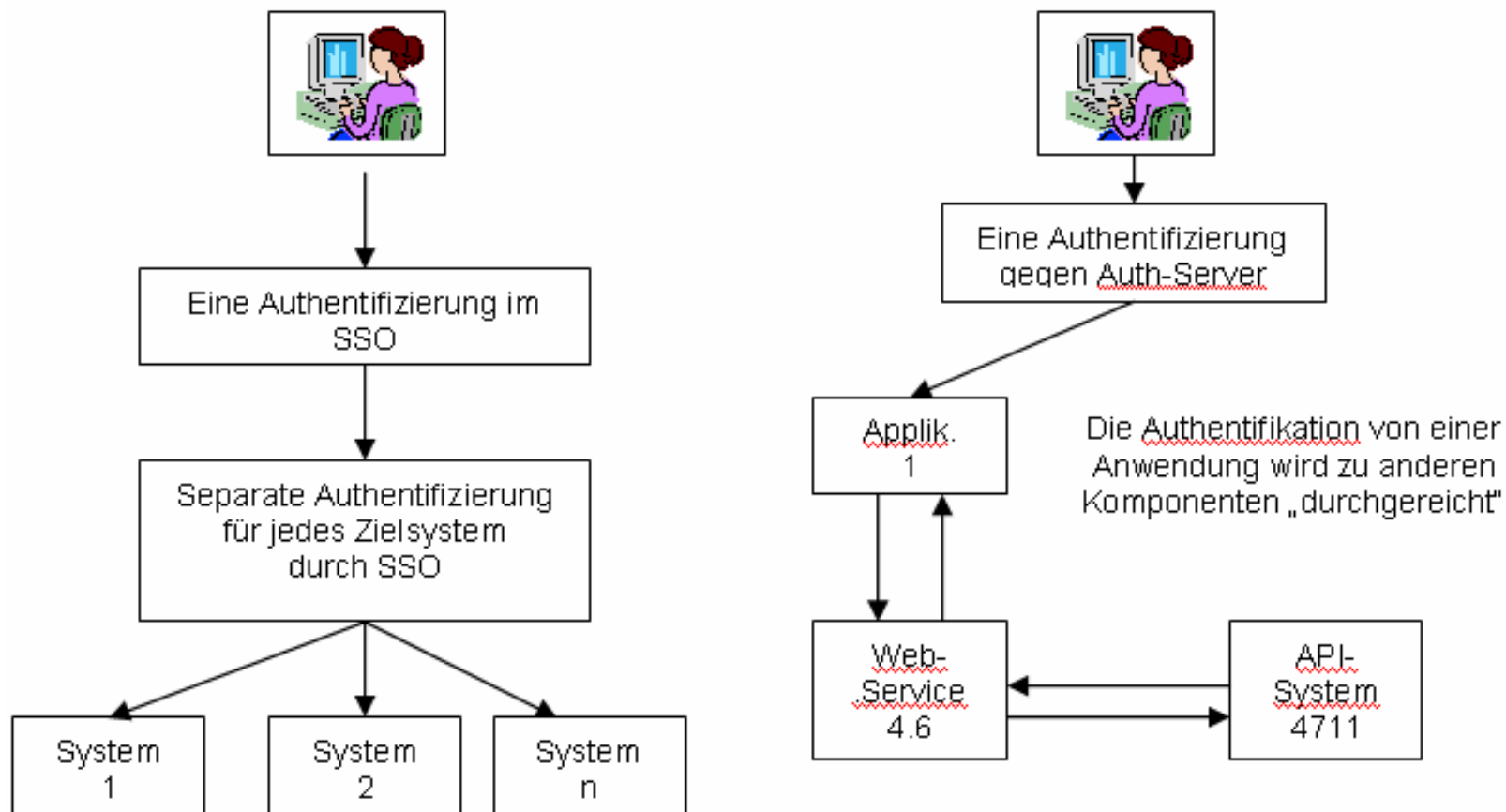
X509 Standard Security Classification an User und Applikationen

Technologie der Output-Connectoren



SSO versus Federated Identity ?

Zwei Wege und teilweise auch 2 Ziele



Funktionalität / SSO

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

Funktionalität / SSO

- Weitere Funktionen:
- Integration in das automatische Antragsverfahren
- Temporäres Sperren von Usern bzw. einzelnen Berechtigungen ohne dies in den Sub-Systemen nachzuziehen
- Aufgabenbezogenen Desktop des Users generieren
- User-Selbst-Registrierung zur sanften Migration der Accounts
- PW-Anlernen
- Integrierte Datei-Verschlüsselung
- SSO-Pro als Applikation Launcher zur Verwaltung differenzierter Systemumgebungen
- Personifiziertes SSO (individuelle Nutzung der SSO-Funktion)

Federated Identity und *bi-Cube CTT*

- **Federated Identity** (ein neuer Hype und ein anderes SSO...)
- **Ziel:** Gemeinsame zentrale Verwaltung aller User (Interne, Externe, Kunden, Lieferanten,..) und Rechte
Schwerpunkt: Portalintegration / Application Launching

Lösung: Web-Identitäten durchreichen zu Webservices und internen Applikationen

Ansätze: SAML 1.1, Liberty Alliance ID-FF und WS-Security ..

Problem1: zusätzlich „alte“ Verfahren: Kerberos, Secu-Token

Problem2: Session Transfer und Control / LogOut

Problem3: Identität ist noch keine Autorisierung

bi-Cube-Ansatz: intern ein Cross-Transfer-Token, das die Umsetzung in und zwischen den Standards und Verfahren realisiert, gleichzeitig trägt es Rolleninformationen

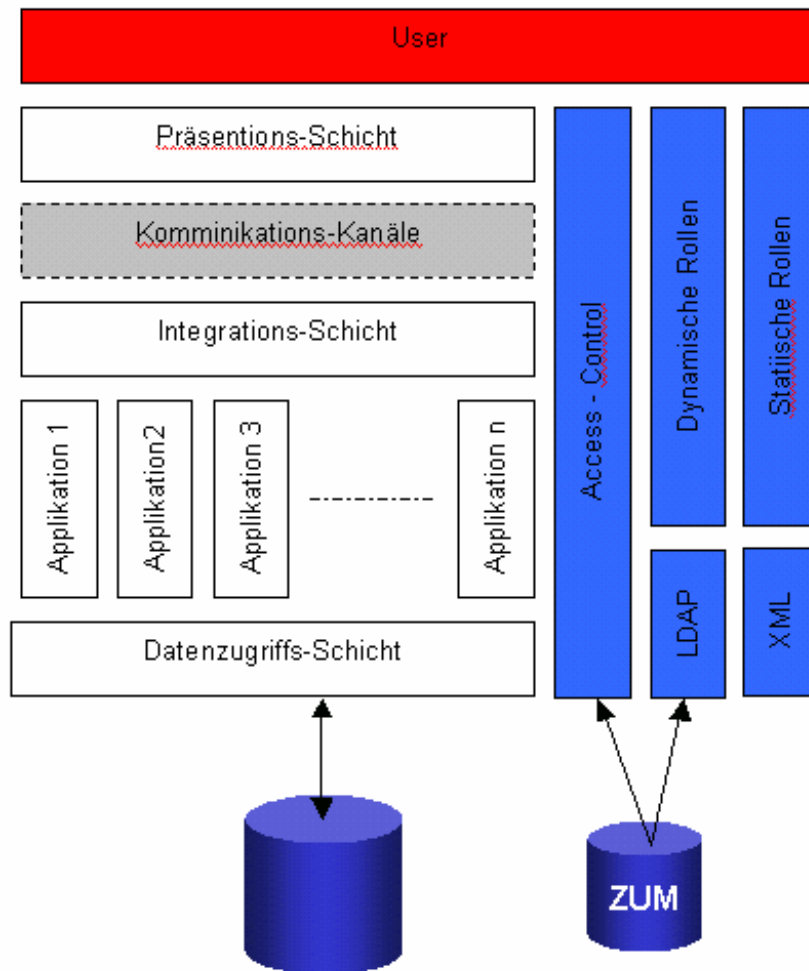
Dieses CTT wird Partnern ohne SAML als SAML-Bridge zur Integration in eigene Anwendungen angeboten

Federated Identity und *bi-Cube CTT*

Kampf der Giganten und keine Rettung für den Anwender

- Microsoft und IBM (WS-Federation) gegen Liberty (SUN)
- Unabhängiger Standard SAML von beiden nur partiell unterstützt
- Liberty Alliance nur für Browser-basierte Authentifizierung
- Die ganze Entwicklung noch recht am Anfang: Kontroll-Strukturen und Transaktions-Sicherheit fehlen
- Mit dem *bi-Cube CTT versuchen wir eine einsatzfähige und offene Lösung zu schaffen, die Standards berücksichtigt*

bi-Cube – als Access-Control-Server



Der Access Control-Server stellt seine Dienste in verschiedenen Ebenen zur Verfügung:

1. Definition von Berechtigungsstrukturen in ZUM und deren Übergabe an die Zielsysteme
2. Online Authentifizierung
3. Steuerung der program to program communication
4. online Authentifizierung
5. **Federated Identity Funktionen incl. Session-Control-Vector**

bi-Cube Einführungsstrategie

■ **Einführungsschritte (nach *bi-Cube* -Logik)**

1. Implementierung der User-Identität !!!
Übernahme und Verwaltung der Userdaten /
Anbindung an Personalverwaltung (evtl. andere
Quellen: RACF, LAN, Notes..)
2. Bereitstellung der Organisationsdaten / Pflegeprozeß
dazu
3. Modellierung und Übernahme der wichtigsten
Systeme (AD/w2k, Notes, RACF, SAP..??)
4. Implementierung Rollensystem (Anleihe an SAP u.a.)
5. Ersteinsatz Antragsverfahren

bi-Cube Einführungsstrategie

Einführungsschritte / projektgetrieben

1. Unterstützung WinTel-Plattform / AD Migration
2. Unterstützung laufender Projekte mit sachlichem Bezug zu ZUM
3. Andere tangierende Projekte ?
4.

Einführungsschritte / strukturgetrieben

1. zuerst die Unternehmen/OE mit den größten Effekten
2. zuerst Einheiten mit guten organisatorischen Bedingungen, um schnell einen Effekt zu erreichen

bi-Cube -typischer Zeitrahmen

Jahr 1

Wichtigste Etappe: User-Identität

(30.000 User aus 70.000 Accounts ermitteln)

alle User im AD verwalten / Ressourcenzuordnungen (1,4 Mio)

die definierten wichtigsten Systeme in ZUM verwaltet

die Verwaltungsprozesse in Bezug auf Personal neu definiert

die in bestehenden Systemen modellierten Rollen (Tätigkeiten, Gruppen / Profile) werden in ZUM-Rollen portiert

der Antrags-Workflow zumindest in der halbautomatischen Betriebsart in Nutzung genommen werden

Neuordnung der Administration (von 70 auf 5 Admins)

bi-Cube -typischer Zeitrahmen

Jahr 2

Weitere Konzern-Unternehmen werden übernommen
Töchter in anderen Ländern integrieren (Unicode)

Weitere Systeme werden in *bi-Cube* verwaltet

Der Einsatz von Output-Connectoren wird erweitert
um weitere Prozesse zu automatisieren.

Breitere Nutzung des Antragsverfahrens

Weitere Prozesse werden automatisiert:

Berechtigungsvergabe für neue User

Anträge für Systeme und Änderungen

Datenübergabe an andere Systeme (im Sinne EAI)

Nutzensarten

direkter Nutzen

Wesentliche Reduzierung des Aufwandes in der Administration
Verringerung des Gefährdungspotentials

Prozess- Nutzen

Geordnete bzw. verbesserte Geschäftsprozesse

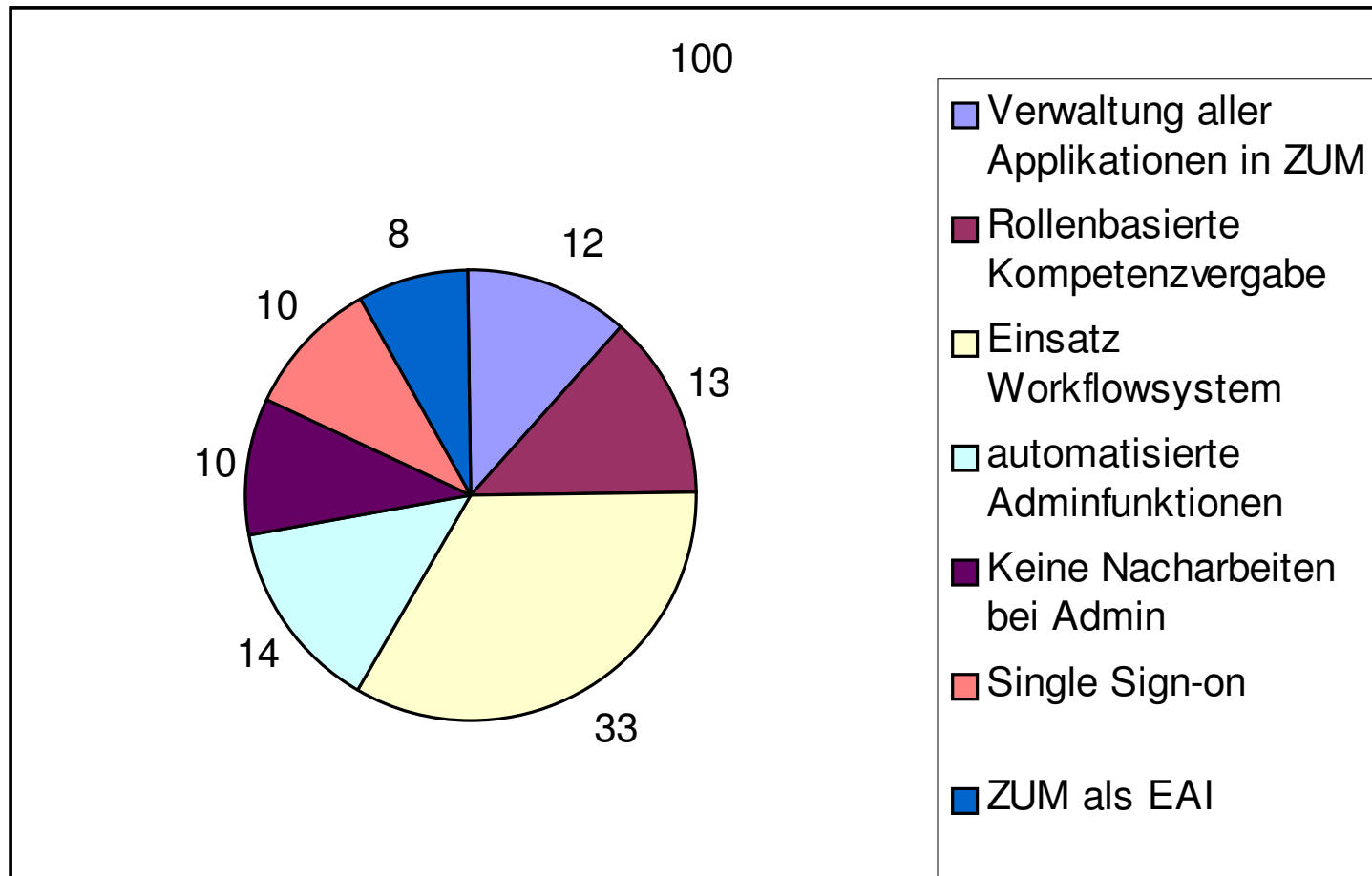
Synergetischer Nutzen

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

Einfluß der einzelnen Maßnahmen auf den zu erreichenden Rationalisierungseffekt



Mitbewerber

Keine wirklichen im deutschsprachigen Raum
(Betasystem / SAM von Systor)

Am „dichtesten auf den Fersen“ ist **Business Layers**
(**Netegrity**)

auch objekt-relationaler Ansatz aber nicht die Flexibilität
(asynchrones Messaging) und nicht die funktionelle Breite
(z.B. kein ADS, ecter Workflow, schwaches Rollensystem,
usw...)

Andere partiell nur immer mit Teilbereichen:

IBM (Access 360, Tivoli), CA, Sun (Waveset), Bull / Evidian
(SSO), Siemens (DirX, BMC (CONTROL-SA),...)

U S P

Technologie, asynchrones Messaging

Offene Architektur

Modularität bei Funktionsbreite

Einheitlicher konzeptioneller Ansatz

Spezielle Funktionalität für Finanzwirtschaft
(als Erweiterung nicht als Einschränkung)

Praktischer Nachweis einer kurzen und effektiven
Einführungsphase