FSP CONSULTING & IT-SERVICES

Die Rollen der User –

Revisionssichere und rollenbasierte Benutzerrechteverwaltung

Kurzvorstellung FSP GmbH

- FSP steht für Financial Services Partner
- Sitz des Unternehmens ist Köln
- 35 erfahrene Mitarbeiter

- IT-Consulting & Development
- Produkte & Lösungen
- Business Consulting

Leistungsschwerpunkte der FSP GmbH

Business Consulting

- Prozessoptimierung
- Dokumenten- & Workflowmanagement
- Migrations-Konzeption
- Rollen & Rechte Konzeption
- Projektmanagement / Coaching
- Testmanagement

IT-Consulting & Development

- Architekturberatung Anwendungssysteme
- Anwendungsintegration
- Anwendungs- und Datenmigration
- IT-Projektmanagement / Coaching
- Change & Configuration Management
- Individuelle Softwarelösungen

Eigene Produkte & Lösungen

- IPS – Anbindung GDV-Branchennetz
- ORG – Benutzerrechteverwaltung
- MPF – Integrationsframework für Datenaustausch
- FAS – Entwicklungsframework für Application Server
- SWT – Entwicklungsumgebungen für Mainframe

Kunden (Auszug)

Warum revisionssichere und rollenbasierte Benutzerrechteverwaltung?

Die präzise und effiziente Zuweisung der Berechtigungen über Rollen

Schont Ressourcen

- Verringert Warte- und Ausfallzeiten bei Neueinstellungen und Abteilungswechseln
- Erhöht Produktivität durch Fokussierung auf das Kerngeschäft
- Senkt die Benutzeradministrationskosten
- Reduziert Sicherheits- und Haftungsrisiken durch klare Prozesse

Themenüberblick

- Revisionssicherheit: Definition, Nutzen
- Rollenkonzept
  - Was sind Rollen?
  - Revisionssicherheit und Rollenkonzeption
  - Vorgehensweise bei Einführung eines Rollenkonzepts
  - Umsetzung von Revisionssicherheit und Rollenkonzept
- Effiziente Administration von Berechtigungen
  - Anforderungen
  - Herkömmliche und zentrale rollenbasierte Administration
  - ROI (Teilaspekt)
  - Darstellung einer rollengestützten Administration
  - Übersicht: Produktkategorien und Anforderungen
  - Schema einer Produktvergleichsmatrix
- Zusammenfassung

Revisionssicherheit

Was bedeutet „revisionssicher“?

Der Begriff ist u. a. herleitbar aus HGB, AO und GoBS:

Sicher, unverändert, vollständig, ordnungsgemäß, verlustfrei, reproduzierbar, datenbankgestützt recherchierbar (Definition aus den GDPdU)

Weitere Kriterien:

Betriebssicherheit, Investitionssicherheit, Migrationssicherheit, Informationssicherheit, Datensicherheit (vor Verlust und Veränderung), Zugriffssicherheit

Revisionsrelevante Fragestellungen:

- Welche Rechte hatte Nutzer X zum Zeitpunkt Y? **Historisierung mit Zeitpunkt- und Zeitraumbetrachtung**
- Wer hat wann welchen Nutzer warum mit welchen Rechten ausgestattet? **Historisierung**
- Wann hat Nutzer X (in welchem Umfang) Gebrauch von welchen Rechten gemacht bzw. einen Verstoß gegen seine Rechte versucht? **Logging**

Revisionssicherheit: Nutzen und Notwendigkeit

Revisionssicherheit

- Grundlage zur Nachvollziehbarkeit/Beweisbarkeit von Vorgängen, die in elektronischer Speicherform vorliegen (steuerliche Gesichtspunkte, Betrugsfälle, Fehler, Klagen gegen oder durch Kunden bzw. Geschäftspartner)
- Erfüllt gesetzliche Bestimmungen und Normen wie §93 AktG/§43 GmbHG, CG-Kodex, Basel II, IFRS-Vorgaben (EU-Norm ab 2005) oder Sarbanes-Oxley Act durch Messbarkeit und Belegbarkeit operativer Risiken
- Reduziert Risiken der Unternehmenshaftung und der persönlichen Haftung für operative Verantwortliche wie Geschäftsführer / Vorstände

Rollenbasierte Benutzerrechteverwaltung

Was ist eine Rolle?

Aufgabenbeschreibung, die entsprechende Vollmachten enthält;

IT-technisch betrachtet: Objekt als Ordner zur Gruppierung von Kompetenzen

Wozu Bündelung von Rechten in Rollen?

Ermöglicht die Hinterlegung von Regeln für Mitarbeiter mit gleichartiger Aufgabenstellungen

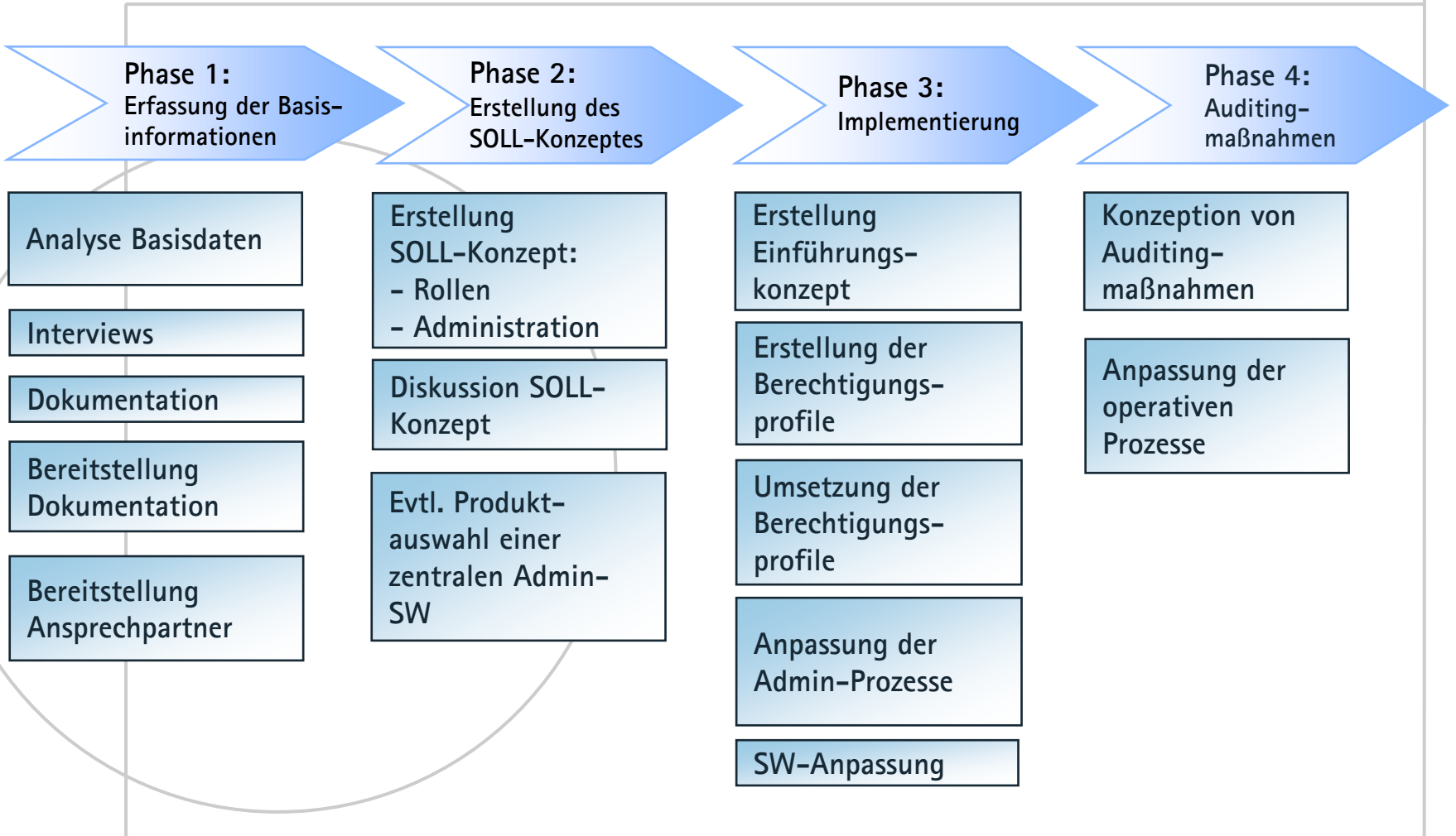
- Zeit- und Kostenersparnis bei der Administration: Automatisierbarkeit
- Verbesserte Kontrolle, Fehler- und Risikominimierung
- Delegierte Administration möglich: Mehrstufige Genehmigungsverfahren
- Nutzbarkeit der strukturierten Rollen- /Rechteinformation für z.B. Vorgangssteuerung

Revisionssicherheit und Rollen

Vorteile durch Rollenbildung

- Im Gegensatz zur Vergabe von Einzelberechtigungen spart die Rechtevergabe über Rollen Zeit und vermindert Fehler: Kostenvorteil und Risikoreduzierung für das Unternehmen
- Deutlich geringerer Einarbeitungsaufwand für Administratoren und beantragende Abteilungen in die Einzelrechte notwendig, weil die Rollen bereits die notwendigen Daten enthalten
- Zuweisung von Rechten zu Nutzern wird dezentralisierbar und nachvollziehbar
- Hohe Transparenz und schnelle Überprüfbarkeit des Status Quo der Berechtigungen möglich: Automatisierbare Audits und Policies
- Berechtigungsverwaltung in heterogenen IT-Landschaften mit ihrer Vielzahl an Systemen ist auf diese Weise effizient durchführbar

Vorgehen bei der Rolleneinführung



Beispielabteilung mit Rollen (Stellen)

Rolle/Stelle	Einzel-freigabe	Gegen-zeichnung	Systemzugriff					
			CICS	SAP	Partner	AD-Info	HR	Test
GB A Abteilungsleiter		50.000 €	X	X	X	X	X	
GB A Gruppenleiter	50.000 €	50.000 €	X	X	X	X	X	X
GB A Sachbearbeiter Standard			X		X			
GB A Sachbearbeiter Standard + Lst (2)	2.000 €		X		X			
GB A Sachbearbeiter Standard + Lst (5)	5.000 €		X		X			
GB A Sachbearbeiter erweitert			X	X	X			
GB A Sachbearbeiter erweitert + Lst (2)	2.000 €		X	X	X			
GB A Sachbearbeiter erweitert + Lst (5)	5.000 €		X	X	X			
GB A Sachbearbeiter erweitert + Lst (20)	20.000 €		X	X	X			
GB A Sachbearbeiter erweitert + Lst (20) + GGZ	20.000 €	20.000 €	X	X	X			
GB A Aussendienstbetreuer			X		X	X		
GB A Koordinator	2.000 €		X		X		X	X

abteilungsspezifisch

Rolle umfasst Einzelrechte in diesen Systemen

Effiziente Administration von Zugriffsrechten

Anforderungen an die Administration:

- Sicherheit
- Transparenz des Gesamtprozesses
- Schnelligkeit
- Automatisierbarkeit (Reduzierung von manuellen Eingriffen)
- Kostengünstigkeit im Gesamtprozess
- Anpassbarkeit und Erweiterbarkeit (Investitionssicherheit, Skalierbarkeit)

Herausforderungen an die Zugriffsadministration:

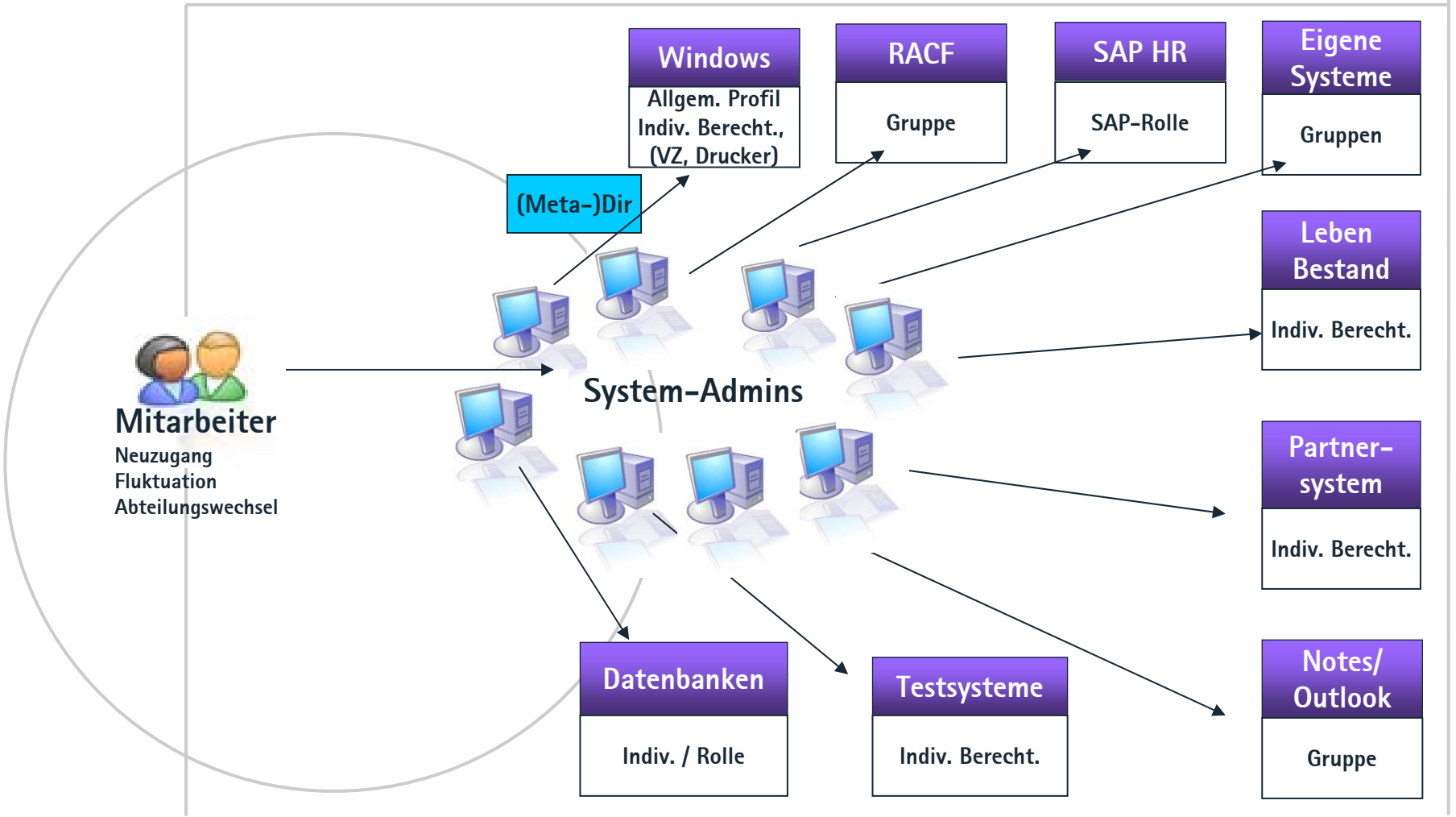
- Einführung zusätzlicher neuer Systeme
- Fusionen

} Immer mehr heterogene Systeme

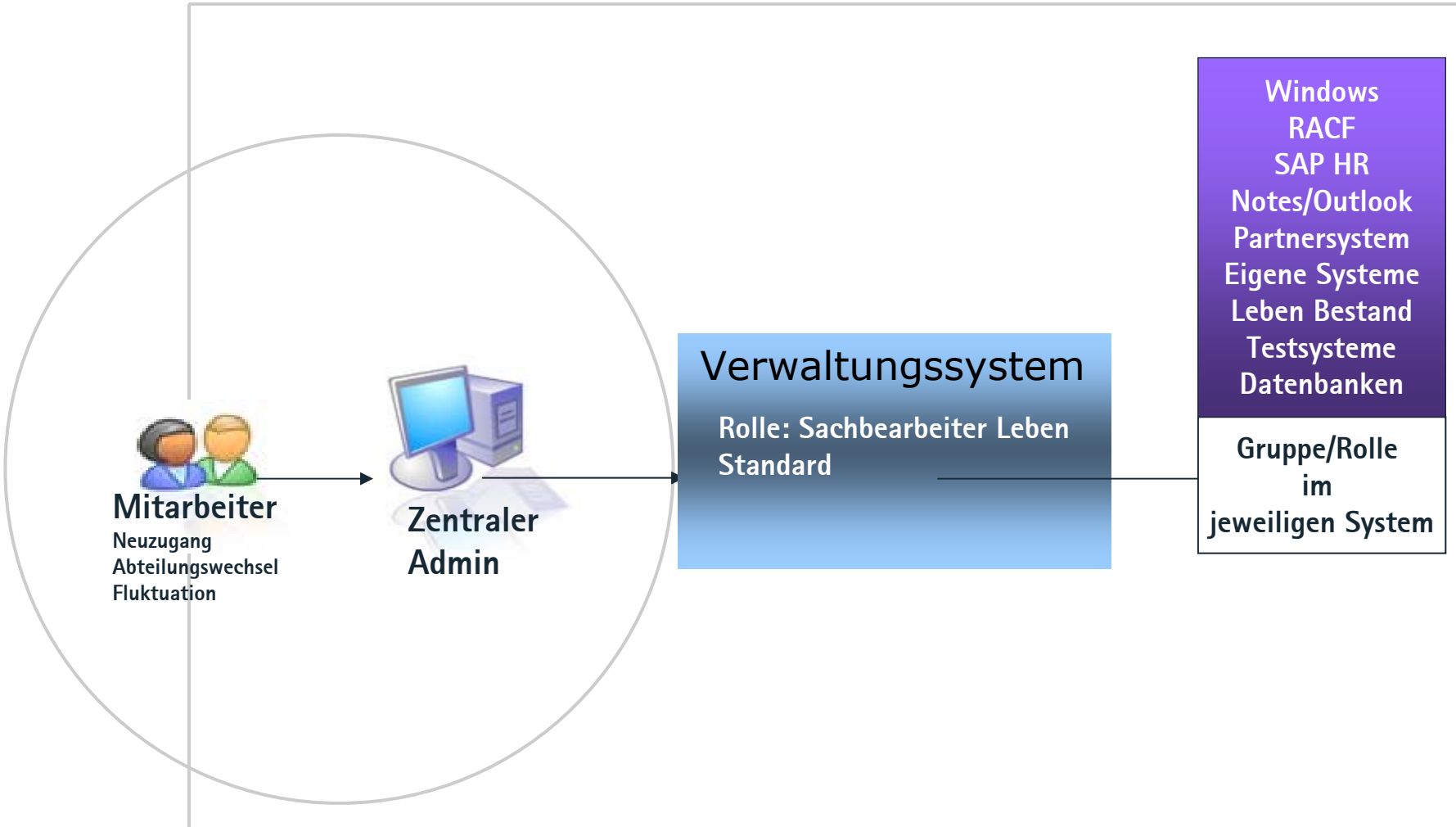
- Anbindung von Kunden
- Anbindung Außendienstorganisationen
- Anbindung von Partnern/Zulieferern

} Übergang vom weitgehend geschützten internen Netzwerk zum Internet

Herkömmliche Berechtigungsverwaltung



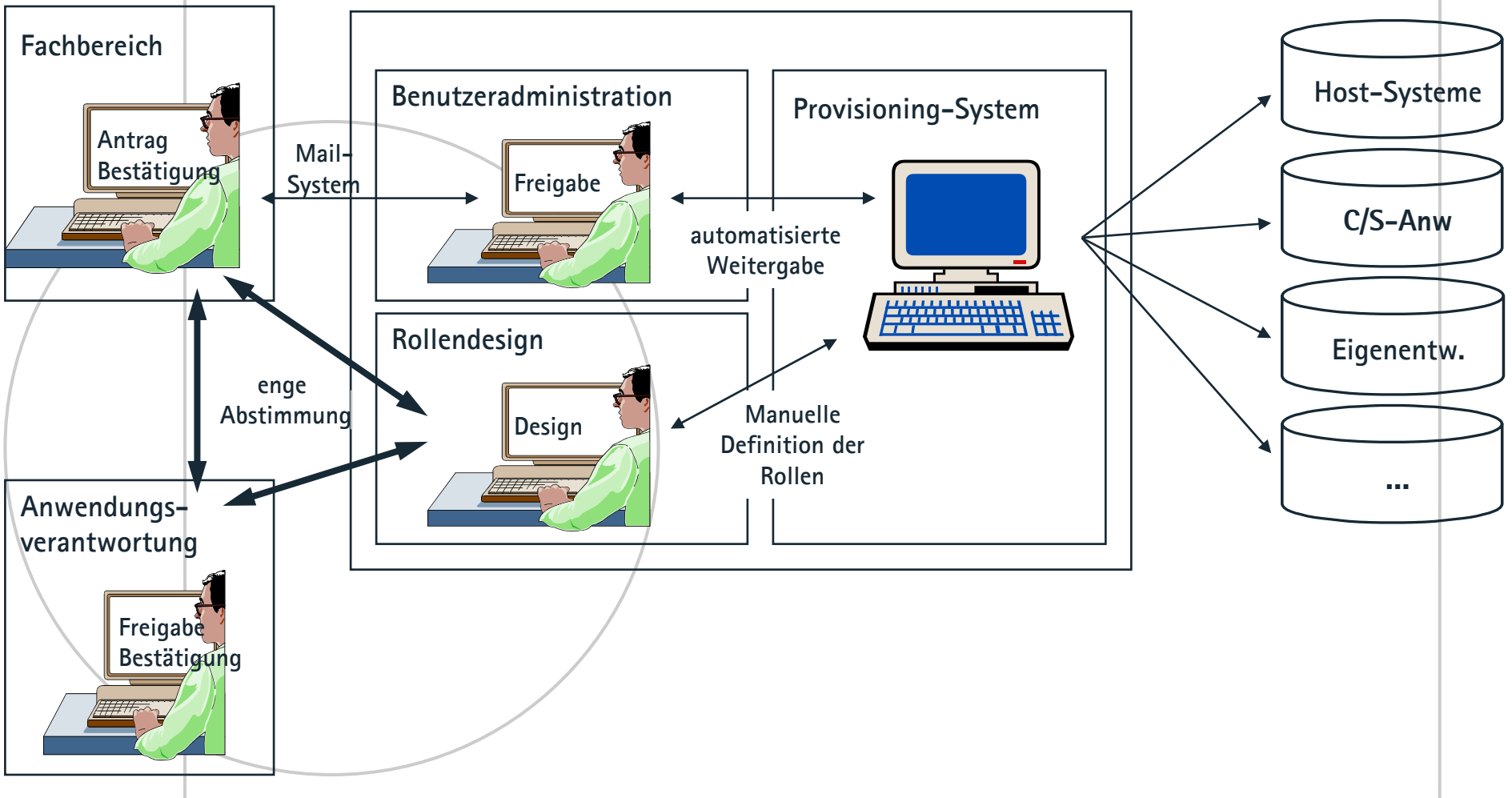
Die Lösung: zentrale rollenbasierte Berechtigungsverwaltung



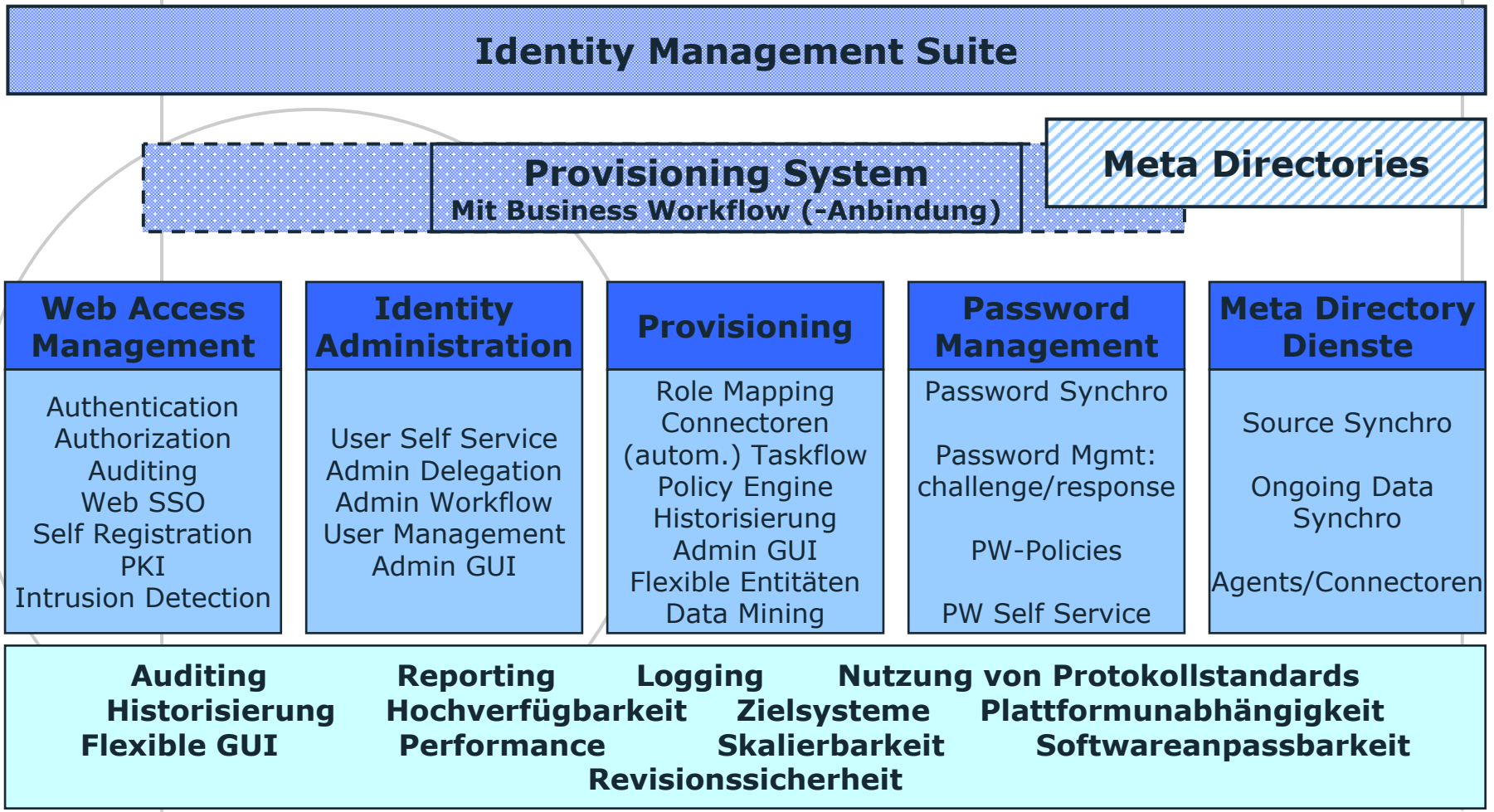
ROI auf Jahresbasis (Teilaspekt anhand eines Beispiels)

	ohne Rollen	mit Rollen	Kommentar
Vorgaben			
Anzahl Angestellte	5000	5000	
Anzahl Vollzeit-Administratoren	8	4	
Lohnkosten Angestellte/Stunde	28 €	28 €	
Quote Neu./Versetz./Fluktuation	6% / 12% / 6%	6% / 12% / 6%	
Zeitbedarf Neu./Änd./Löschen	12% / 20% / 1%	2% / 2% / 1%	
Ausfallzeit bei Neueinstellung	24h	0* - max. 8h	"0": Vorausadministration
Ausfallzeit bei Versetzung	16h	0* - max. 8h	"0": Vorausadministration
Kostenblöcke			
Lohnkosten Admins	124.000 €	62.000 €	
Prod.ausfall bei Neueinstellung	205.000 €	0 - 68.000 €	
Prod.ausfall bei Versetzung	273.000 €	0 - 137.000 €	
			jährl. Kostenvorteil
laufende Gesamtkosten	602.000 €	62.000 - 267.000 €	**533.000** €

Beispielprozess rollenbasierter Berechtigungsvergabe



Leistungsvergleich IMS – Provisioning System – Metadirectory



Definieren Sie Ihre Anforderungen – Die Auswahl ist groß

	Identity Management Suite			Provisioning Software			Metadirectory		
	Produkt A	Produkt B	Produkt C	Produkt D	Produkt E	Produkt F	Produkt G	Produkt H	Produkt I
Workflow	WF-Mgmt	Admin-WF	Schnittstelle	WF-Mgmt	Schnittstelle	WF-Mgmt	WF-Mgmt	nein	nein
Protokolle	LDAP	LDAP/X.500	LDAP	LDAP	LDAP	LDAP	LDAP, X.500	LDAP	ActiveX,...
Zertifizierung / eingesetzte Standards	X.509, 3 DES	X.509, SAML	X.509, SSL	DSML, SSL	SAML, X.509	X.509, 3 DES	DSML, SSL	DSML, X.509	X.509
Datenbasis	zentral	zentral	de-/zentral	de-/zentral	de-/zentral	zentral	de-/zentral	eigene	eigene, NDS
Deployment Platform	nur WIN	WIN, Solaris	WIN	jede J2EE	jede J2EE	WIN, Unix	WIN, Solaris	auf Anfrage	nur WIN
Betriebssysteme, unterstützte Applikationen, Message-Systeme, Datenbanken, Directories, Berechtigungssysteme (z.B. RACF)									
Administration	de-/zentral	de-/zentral	de-/zentral	de-/zentral	de-/zentral	de-/zentral	zentral	de-/zentral	de-/zentral
Antragstellung automatisierbar	nein	ja	nein	ja	ja	nein	nein	nein	nein
Audit-und Reporting-Funktionen	eigene	eigene	Schnittstelle	eigene	Schnittstelle und eigene	Schnittstelle und eigene	Auditing	Schnittstelle	eigene
Historienfunktion	X	eingeschr.	?	time stamp	X	time stamp	nein	nein	nein
Data Mining Funktionen			X	X					
RBAC-Fähigkeit	X	X	X	eigene	eigene	X	nein	nein	nein
Policy-Hinterlegung	PW	Admin	Workflow	PW, Admin	Admin	Workflow	für User	nein	Group-Pol.
SSO	X	Web-SSO	X	Web-SSO	X	Partner	Partner	nein	mit Kerberos
Password-Management	X	X	X	Self Service	Synchro	Synchro		Synchro	
Recovery System	MultiMaster	P2P	MultiMaster	MultiMaster	?	?	MultiMaster	MultiMaster	MultiMaster
Skalierbarkeit	5 Mio User	12 Mio User	1 Mio User	mehrere Mio	2 Mio User	100000 User	mehrere Mio	mehrere Mio	mehrere Mio
Hochverfügbarkeit	3-Tier	RAC-Support	?	?	?	?	3-Tier	RAC-Support	...
Zusatzleistungen	...	...	...	...	...	...	...	...	...
Preis (Produkt, Integration...)	?	?	?	175000$	300000$	600000$	auf Anfrage	0 + X	0 + X

Zusammenfassung

Die präzise und effiziente Zuweisung der Berechtigungen über Rollen

Schont Ressourcen

- Verringert Warte- und Ausfallzeiten bei Neueinstellungen und Abteilungswechseln
- Erhöht Produktivität durch Fokussierung auf das Kerngeschäft
- Senkt die Benutzeradministrationskosten
- Reduziert Sicherheits- und Haftungsrisiken durch klare Prozesse

FSP unterstützt Sie gerne

- Fachliche und technische Beratung im Bereich Rollen-Rechte
- Auswahl des für Sie passenden Security-Produktes

Vielen Dank für Ihre Aufmerksamkeit

Frank Böhm
Geschäftsführer FSP

www.fsp-gmbh.com

Abkürzungsverzeichnis

AD	Aussendienst
AktG	Aktiengesetz
AO	Abgabenordnung
CG-Kodex	Corporate Governance Kodex
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (Verordnung seit 1.1.2002)
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchungssysteme
HR	Human Resources
IFRS	International Financial Reporting Standards
PKI	Public Key Infrastructure (Verschlüsselungskonzept)
PW	Password
ROI	Return on Investment
SSO	Single Sign On