

**Erläuterungen  
zu einer**

**Dienstvereinbarung zur Einführung  
und Betrieb eines  
Identitätsmanagement**

**an der  
Universität Duisburg – Essen**

**Burkhard Wald**

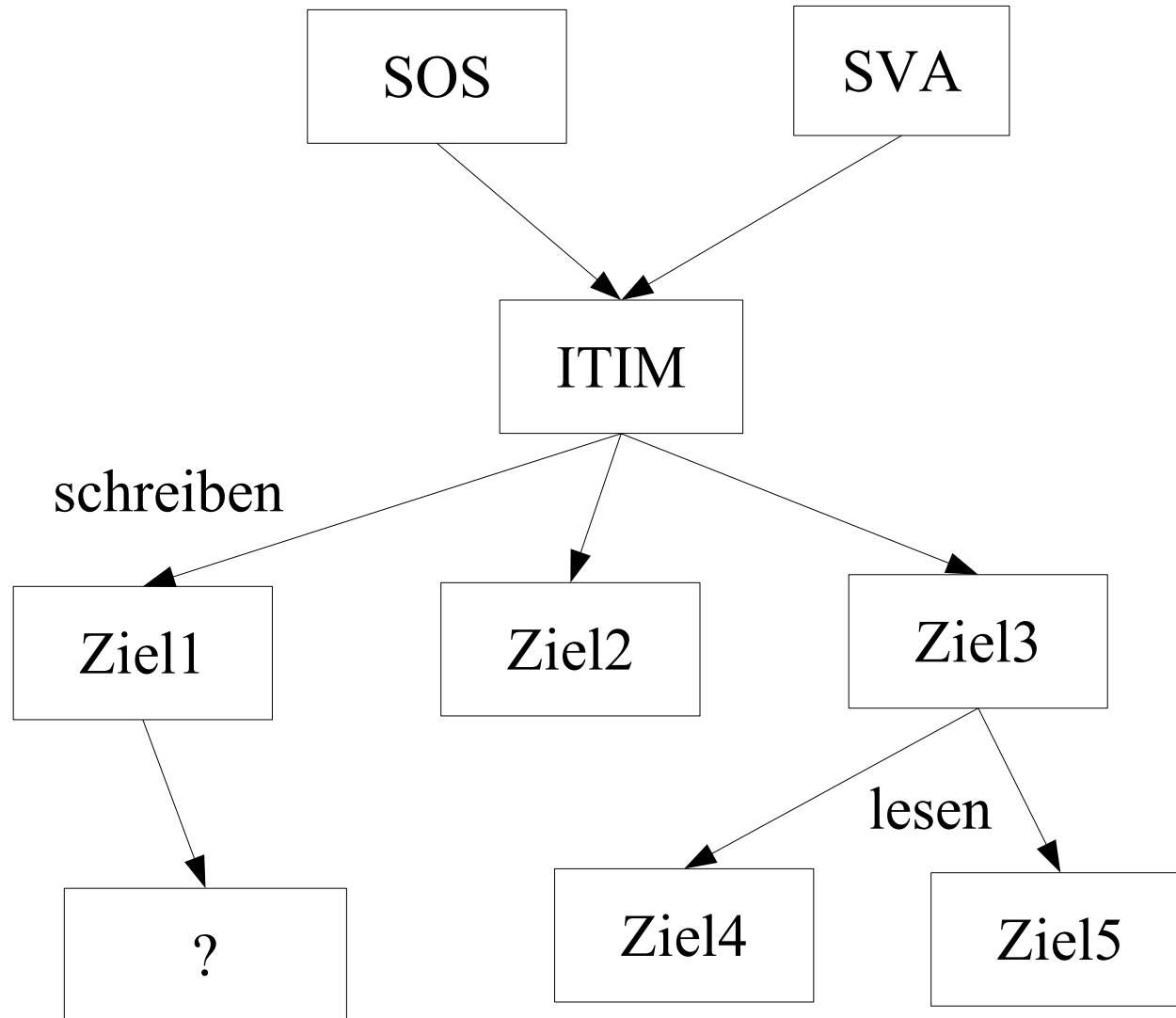
# Vorbemerkung

- Die Universität Duisburg Essen
- Das Zentrum für Informations- und Mediendienste
- Meine Person
- Das Identitätsmanagementprojekt
  - Vorgängersysteme Duisburg und Essen
  - Neukonzeption auf Basis von IBM/Tivoli
  - Integration Duisburg/Essen
  - Mischbetrieb Alt und Neu

# Problem: Mitarbeiterdaten

- HRZ - Verwaltung
- Verwaltung – Personalverwaltung
- ZIM – Personalverwaltung
- Personalräte
- Dienstvereinbarung
- Mitarbeitererklärung
- Datenschutzbeauftragter (Vorabkontrolle)

# Architektur



# Architekturprinzipien

- Kein Zurückschreiben in die Quellsysteme
- Kein Zugriff auf IM von Außen.
- Agenten auf den Zielsystemen (als Slaves)
- Alle Aktivitäten gehen von IM aus

# Vorgespräche mit Personalräten

- Grundsätzlich keine Ablehnung
- Allgemeines Gemeckere
  - Macht man die Welt nicht mit Gewalt kompliziert?
  - Wieso ist das nicht schon längst alles vom Himmel gefallen?

# Ernst zu nehmende Bedenken

- Freibrief, dass Mitarbeiterdaten nach belieben verteilt werden dürfen.
- Befürchtung, dass Hierarchien abgebildet werden.
- Wer entscheidet, wer welche Ressourcen bekommt?
- Wird hier eine Genehmigung erteilt, für etwas, das nachträglich ohne Genehmigung ständig erweitert wird.

# Klares Bekenntnis zu ...

- IM ist Infrastruktur die
  - Daten sammeln und verteilen möchte.
  - ständig neue Systeme anschließen will.
- IM schafft eine integrierte IT-Welt, wie sie bisher an der Hochschule nicht vorhanden war.
- Dafür müssen Grundregeln vereinbart werden.
- Problematiken der Zielsysteme müssen ausgegrenzt werden.



# Abgrenzung IM und Zielsysteme

- Zielsysteme sollen Personendaten nicht neu erfassen sondern von IM erhalten.
- Zielsysteme haben aber eigene Aufgaben und Begründungen.
- Die Frage, ob Zielsysteme gesondert genehmigt werden müssen, wird in der Dienstvereinbarung nicht berührt.
- Dazu sollen weder neue Regeln geschaffen werden, noch bestehende Regeln außer Kraft gesetzt werden.

# Prinzip Offenheit

- Es geht nicht darum alles im Voraus festzulegen und sich genehmigen zu lassen.
- Handlungspielraum erhalten
- Grundsätze festlegen
- Grundsatz Dokumentationspflicht
- Das betrifft die Administrationskonzepte
- Das betrifft die Zielsysteme

# Administrationskonzepte

- Objekte
  - Personen
  - Services
  - Prozesse
- Bereiche
  - zentral
  - dezentral
- Hotline, Helpdesk
- Systemadministration

# Dokumentation Zielsysteme

- Beschreibung
- Ziele
- Weitergegebene Daten
- Administration
- Aussagen zum Datenschutz
  - Wer kann welche Daten sehen
- Regeln und deren Begründung
  - Wer wird automatisch, wer darf freiwillig?

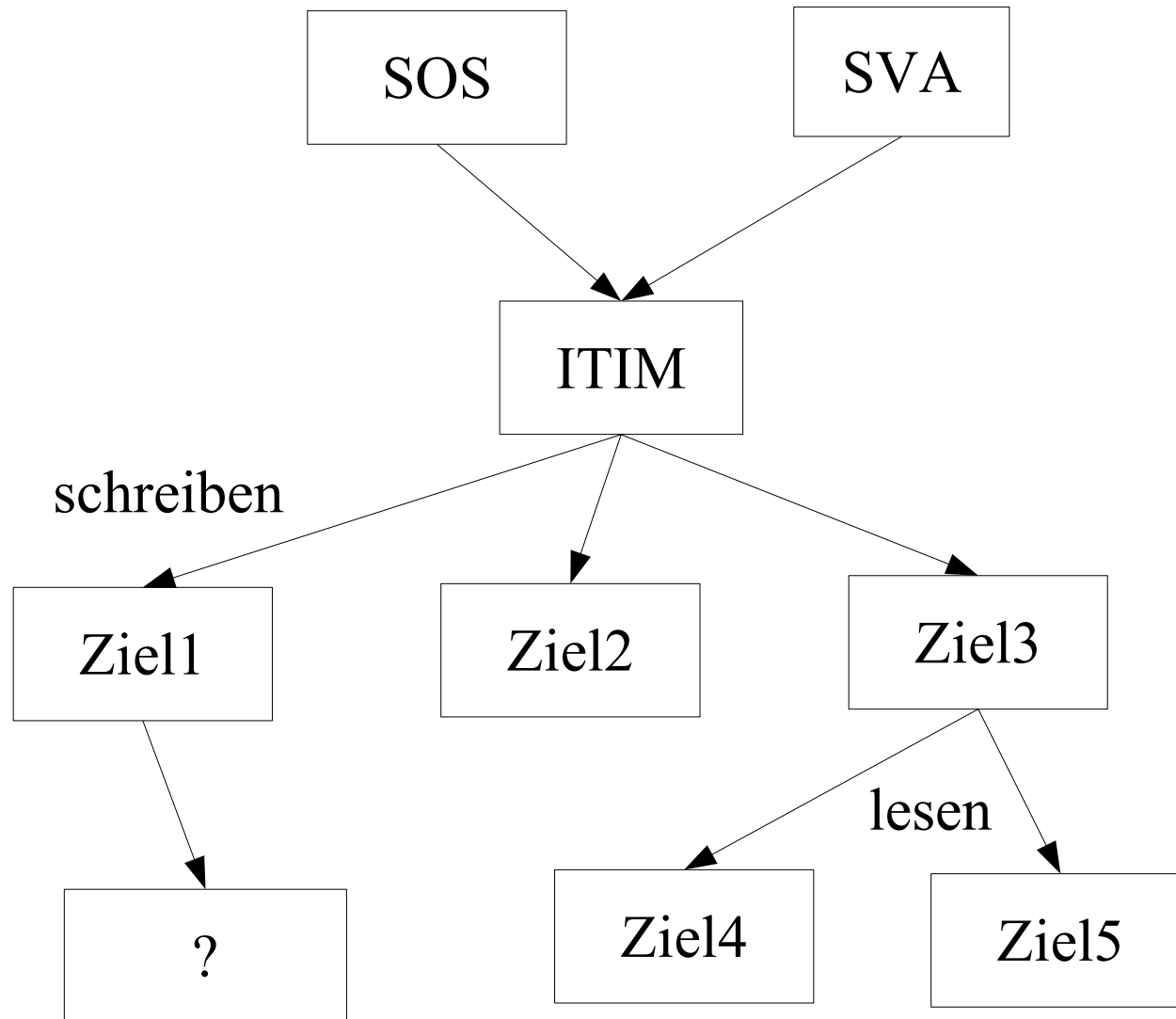
# Dienstvereinbarung besteht aus ...

- Eigentliche Dienstvereinbarung (Ziele, Grundregeln)
- Beschreibung des Systems (Architektur, Konzepte)
- Aktuell praktiziertes Administrationskonzept
- Je Zielsystem eine Dokumentation nach Vorgabe

# Und nun?

- Dienstvereinbarung ist kein Freibrief
- Wie kommt man in der Praxis damit zurecht.
- Arbeitsauftrag an die Kollegen, die IT-Systeme verantwortlich betreiben
  - Ziele formulieren
  - Betriebs- und Administrationskonzepte formulieren
- Ständig neue Anfragen und Erwartungen
- Wie wird der Personalrat unser Handeln beäugeln?

# Architektur



# Verzeichnisdienste als Zielsysteme

- Policy eines Verzeichnisses
  - Ziele
  - Öffentlichkeit, Zugriffsarten
  - Administration
  - Anforderungen an abfragende Systeme
- Z.B. Active Directory
  - Authentifizierung
  - Groupware (Exchange)



# Zusammenfassung

- Trennung zwischen Identitätsmanagement und Zielsysteme
- Dienstvereinbarung für Identitätsmanagement – nicht für die Systeme, die Identitätsmanagement nutzen werden.
- Offenheit und Dokumentationspflicht
- Verweise:
  - <http://www.uni-duisburg-essen.de/zentralverwaltung/dienstvereinbarung.shtml>