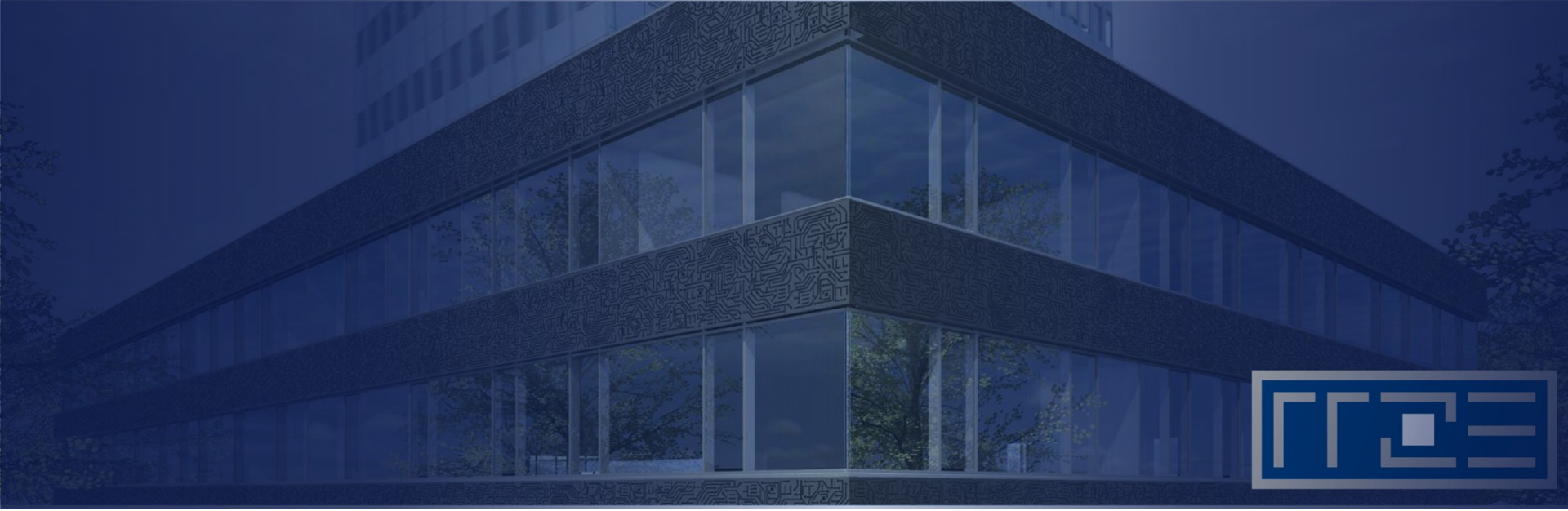


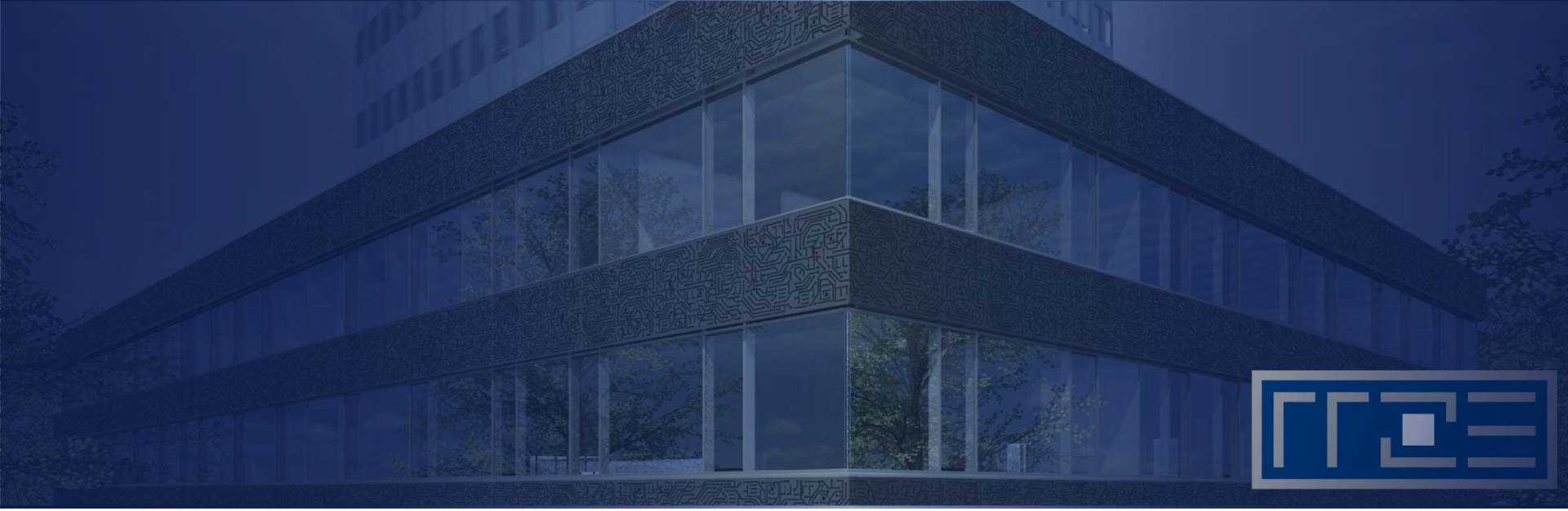
Das Regionale RechenZentrum Erlangen (RRZE)

IAM, Personalrat und Dienstvereinbarung

Tradition und **Moderne** in der
Zusammenarbeit, bei Dokumenten
und Dokumentationen

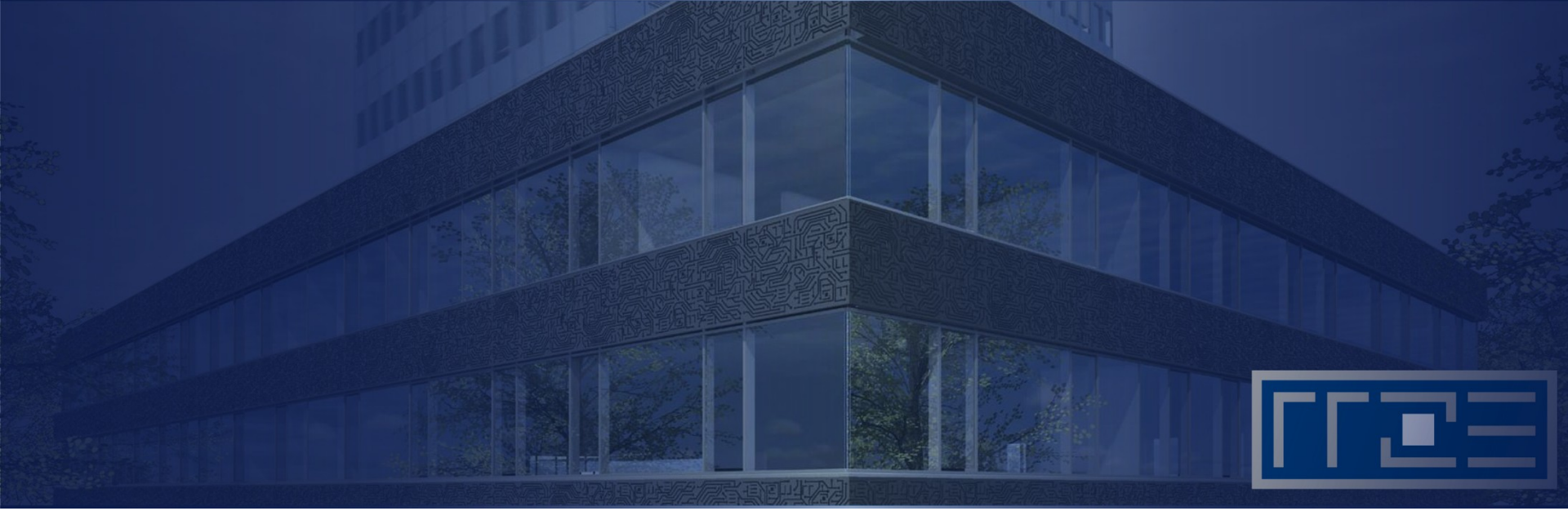
Dr. P. Reiß, F. Tröger

FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG



Agenda

1. Rahmenbedingungen und Rechtliches
2. Online-Dokumentation
    - Berechtigte und Berechtigungen
    - Datenfluss: Systeme, Entitäten, Attribute
3. Demonstration des Systems



Agenda

1. Rahmenbedingungen und Rechtliches
2. Online-Dokumentation
    - Berechtigte und Berechtigungen
    - Datenfluss: Systeme, Entitäten, Attribute
3. Demonstration des Systems

Rahmenbedingungen

content provided by 

- Keine Landesdienstvereinbarung zum Thema IdM im Freistaat Bayern
- IdM fällt in die Zuständigkeit des Gesamtpersonalrats (FAU hat auch „lokale“ Personalräte)
- Aktueller Stand des IdM wurde in den vergangenen 5 Jahren einmal jährlich dem GPR präsentiert
- Einführung der FAUcard führte zu „Zwangsnutzung“ des IdM für alle Beschäftigten der FAU
- Damit auch prominent auf der Agenda des GPR und Bedarf für Dienstvereinbarung (DV) erkannt
- Abhängigkeitsgeflecht:
  - Zeiterfassung hängt von FAUcard ab
  - FAUcard hängt von IdM ab
  - IdM Kern-Dienstvereinbarung (Show Stopper!)

Vorgehen

- Kontaktaufnahme durch Technologie-Ausschuss des GPR
  - Gewährung von Einsicht in Konzeption und Funktionsweise
  - Gemeinsames Abstecken der Grenzen des IdM
  - Erste Ideen für Regelungsinhalte

- Erster Entwurf einer DV
  - Nicht zustimmungsfähig, da Materie zu komplex für GPR als Gesamtgremium
  - Technologie-Ausschuss des GPR sollte tieferen Einblick erhalten

Vorgehen (2)

content provided by 

- Detaillierte Diskussion mit Technologie-Ausschuss, Datenschutzbeauftragten und ständigem Vertreter des Kanzlers (als Vertreter der Uni-Leitung)
  - Systembeschreibung
  - Berechtigte und Berechtigungen
  - Text der eigentlichen Dienstvereinbarung
  - Dauer bisher ca. 9 Monate

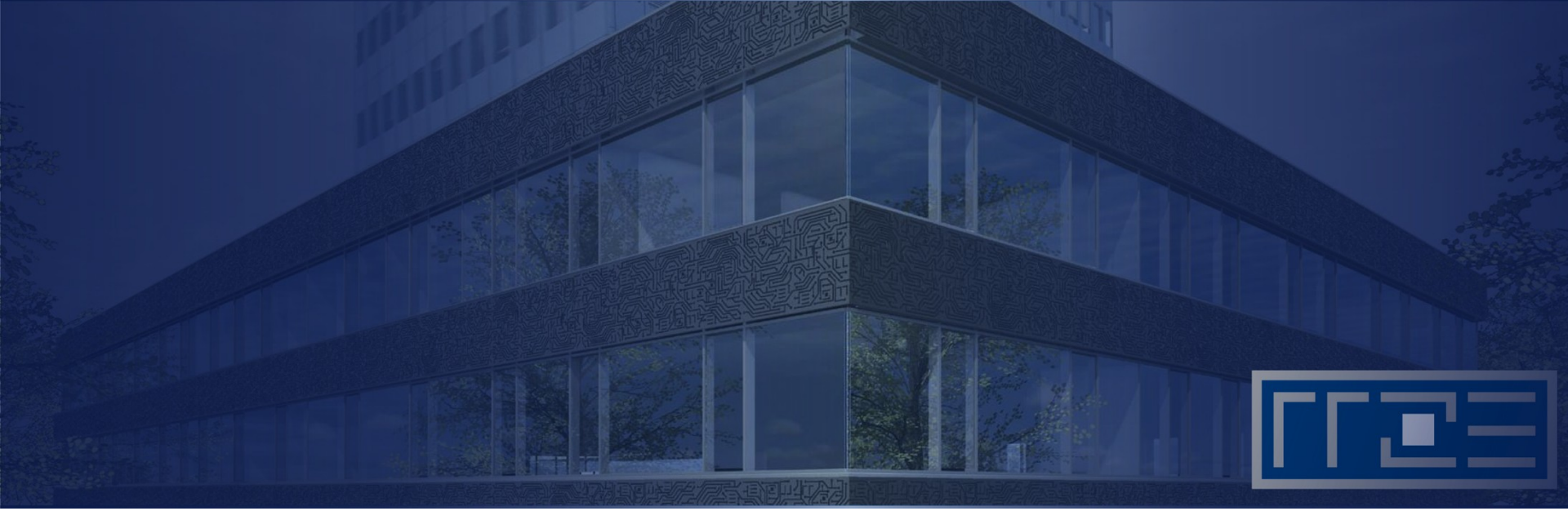
Online-Anlagen

- Alle Fakten zum IdM in der Dienstvereinbarung selbst zu formulieren ist schlechter juristischer Stil
  - Anlagen notwendig
- Anlagen
  - Systembeschreibung
  - Berechtigte und Berechtigungen
  - Details zu Datenflüssen

- Idee: Warum alle Informationen zum laufenden System bei jeder Änderung ausdrucken und GPR + DSB formal zur Kenntnis bringen?

  Besser:

  Direkte Leseberechtigung für GPR und DSB im IdM!



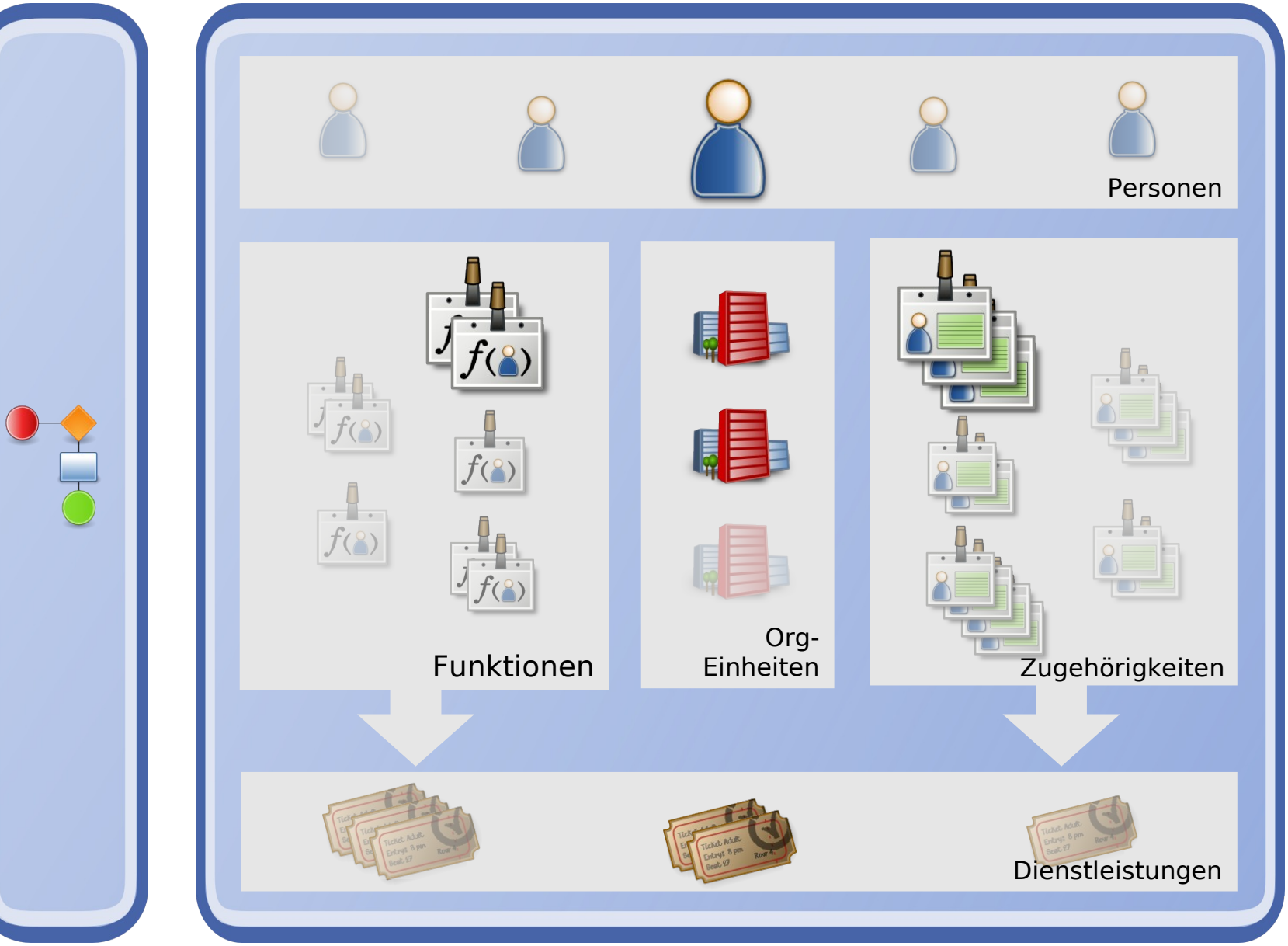
Agenda

1. Rahmenbedingungen und Rechtliches
2. Online-Dokumentation
    - Berechtigte und Berechtigungen
    - Datenfluss: Systeme, Entitäten, Attribute
3. Demonstration des Systems

Online-Doku: Berechtigungen

- IdM-Administratoren benötigen Zugang zu vertraulichen Informationen der Mitarbeiter

- Je nach Arbeitsgebiet
  - Gesamtsicht (IdM-Kernteam)
  - Teilsicht (Dienstleistungs-Administratoren)

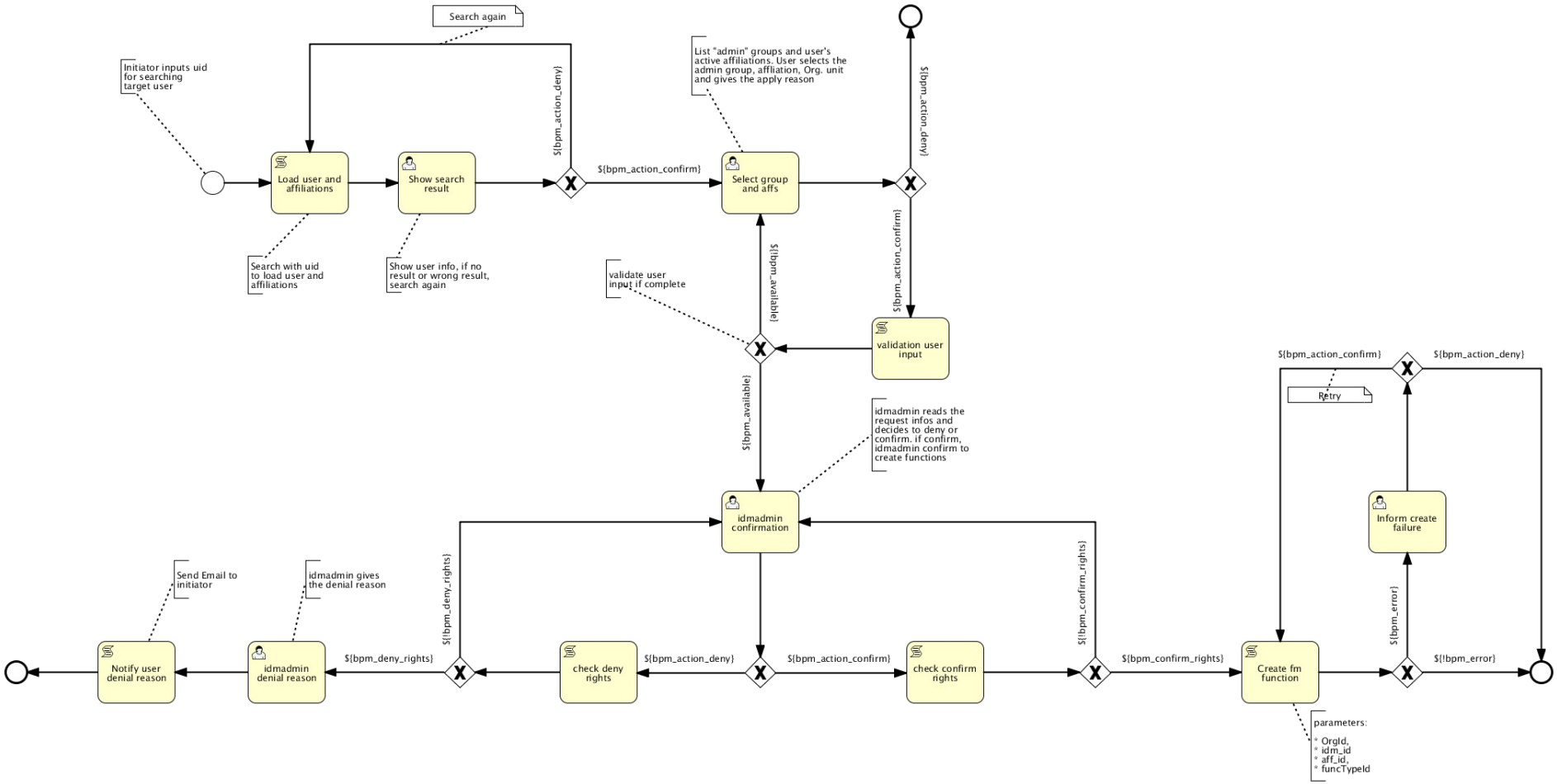

Personen
Funktionen
Org-
Einheiten
Zugehörigkeiten
Dienstleistungen

Online-Doku: Berechtigte

- Admin-Gruppen
  - Aufräumen alter Gruppen
    - Mitgliedschaften „auf Zuruf“ eingetragen
    - Fehlende Begründungen (nur via E-Mail)
  - Mitgliedschaft in neuen Gruppen durch Workflow
    - Beantragen der Mitgliedschaft mit Begründung
    - Prüfung des Antrags und ggf. Bestätigung durch zweite Person (Vier-Augen-Prinzip)
  - Mitgliedschaft ist an IdM-Funktion (FM) geknüpft
    - Endet automatisch
    - Keine „Admin-Leichen“ mehr

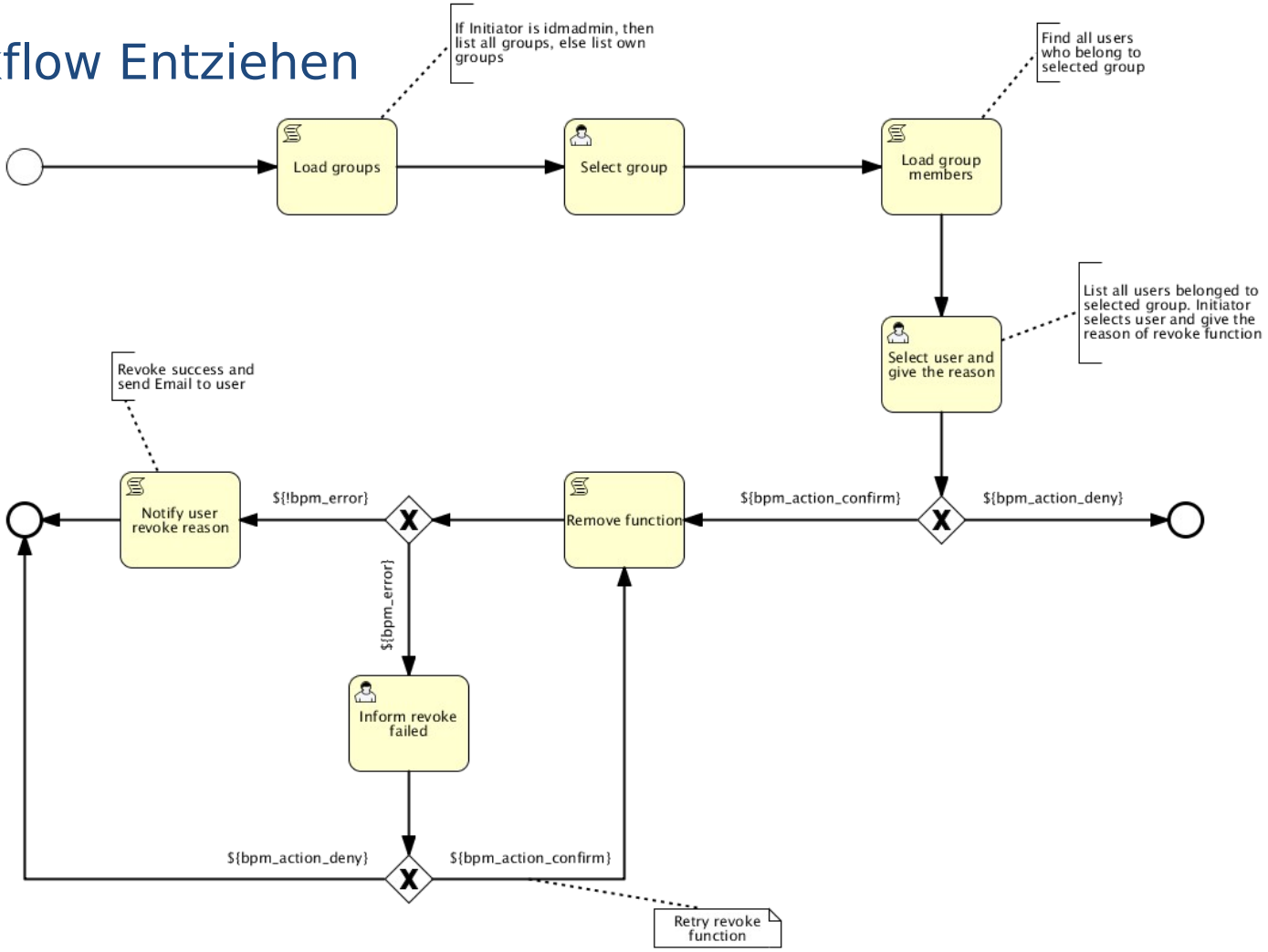
Online-Doku: Berechtigte

- Workflow Beantragen



Online-Doku: Berechtigte

- Workflow Entziehen



Online-Doku: Berechtigte (2)

- Der GPR erhält
  - online Antworten auf ...
    - Welche Admin-Gruppen gibt es?
    - Wer ist Mitglied?
    - Warum ist jemand Mitglied?
    - Welche Berechtigungen resultieren aus der Mitgliedschaft?
  - E-Mail-Benachrichtigungen bei
    - Hinzufügen einer Mitgliedschaft
    - Entfernen einer Mitgliedschaft

FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

Regionales RechenZentrum Erlangen

Regionales RechenZentrum Erlangen ■ Martensstraße 1 ■ 91058 Erlangen

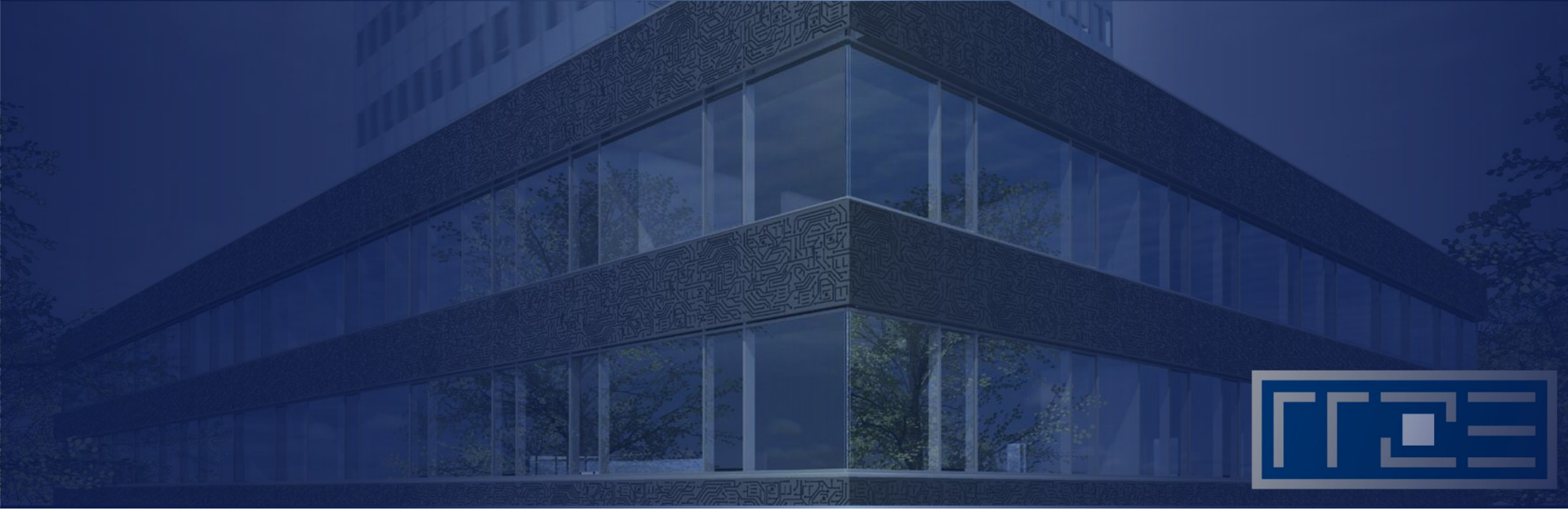
Der IT-Dienstleister der FAU

linuxadmin

Beschreibung	Beschäftigte, die die Linux-basierten Systeme am RRZE administrieren
Berechtigungen	Die 3 Mitglieder der Admingruppe "linuxadmin" haben Zugriff auf folgende Bereiche: • IdM-Portal » Administration » Systemadministratoren (Attributliste) Es existieren keine Einschränkungen auf bestimmte Benutzergruppen, d.h. die aufgelisteten Attribute sind bei Mitarbeiter-, Studenten- und Sonstigeneinträgen einsehbar.

Gruppenmitglieder

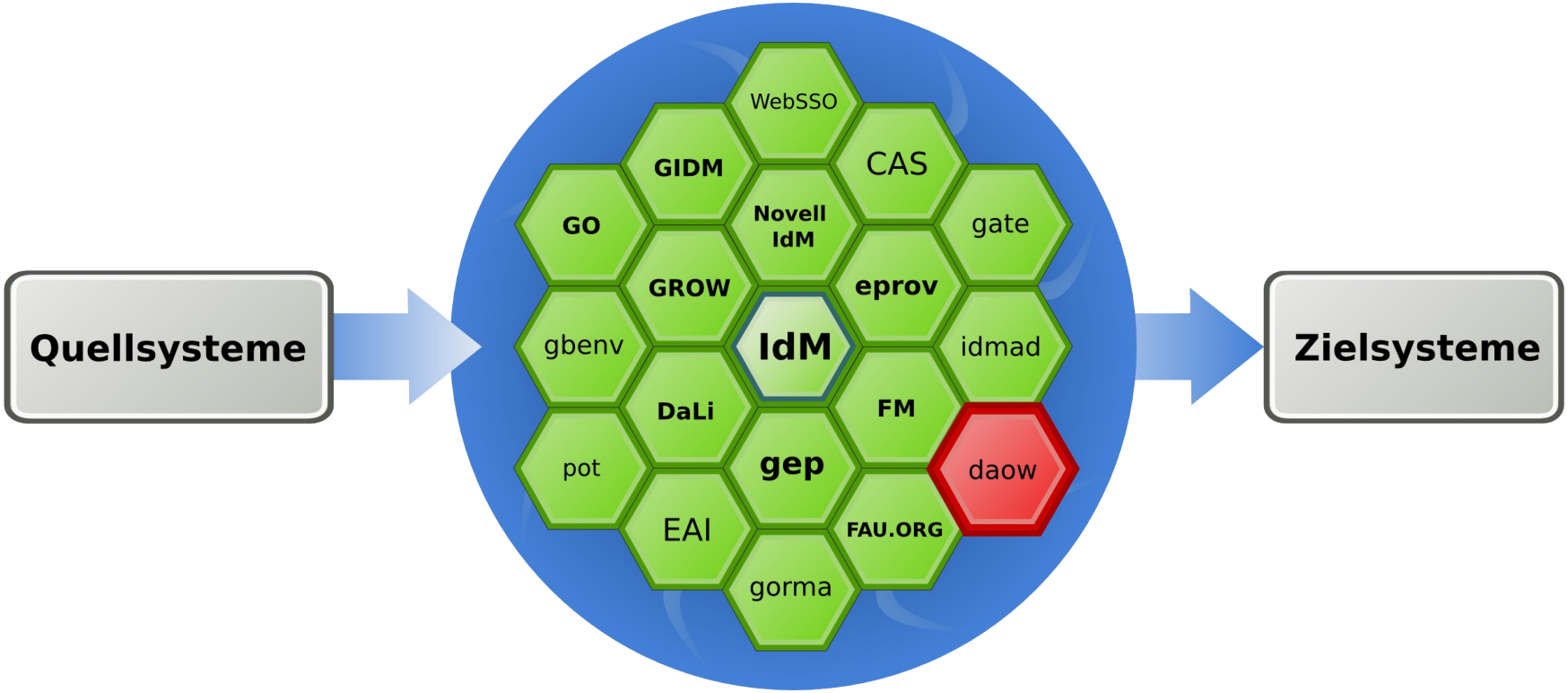
	Name	OE	Antragssteller	Grund
[redacted]	[redacted]	[1011126000] Zentrale Systeme	[redacted]	Frau [redacted] administriert die Linux-Systeme am RRZe und benötigt für die Kontrolle der Schnittstelle zwischen IdM und Linux Zugriff.
[redacted]	[redacted]	[1011126000] Zentrale Systeme	[redacted]	Herr [redacted] ist Abteilungsleiter "Zentrale Systeme am RRZE und administriert zudem die Linux-Systeme am RRZE und benötigt für die Kontrolle der Schnittstelle zwischen IdM und Linux Zugriff.
[redacted]	[redacted]	[1011126000] Zentrale Systeme	[redacted]	Herr [redacted] administriert die Linux-Systeme am RRZe und benötigt für die Kontrolle der Schnittstelle zwischen IdM und Linux Zugriff.



Agenda

1. Rahmenbedingungen und Rechtliches
2. Online-Dokumentation
    - Berechtigte und Berechtigungen
    - Datenfluss: Systeme, Entitäten, Attribute
3. Demonstration des Systems

dataflow

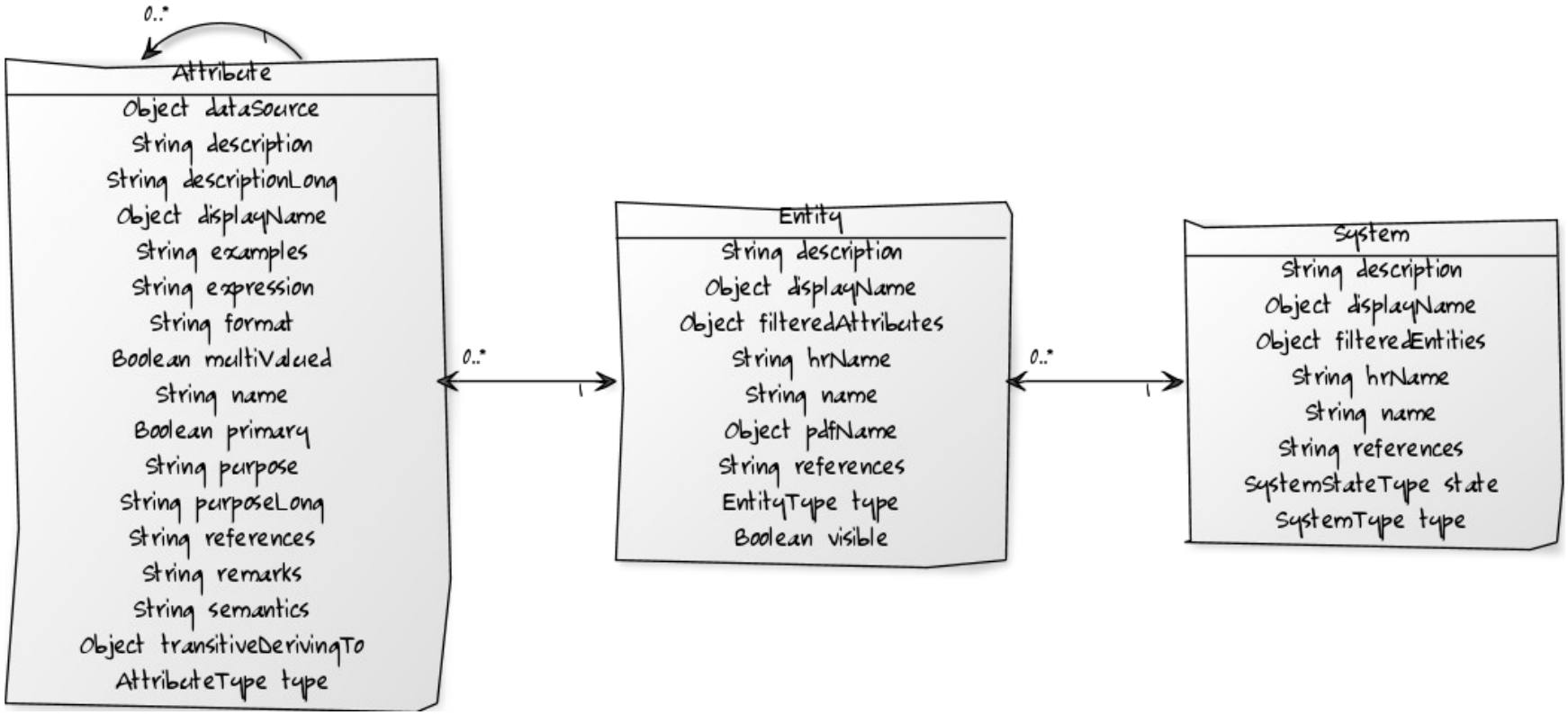

Quellsysteme
WebSSO
GIDM
CAS
GO
Novell IdM
gate
GROW
eprov
gbenv
IdM
idmad
DaLi
FM
pot
gep
daow
EAI
FAU.ORG
gorma
Zielsysteme

Online-Doku: Elemente

- Systeme
  - Quellsysteme (nur IdM-Schnittstelle!)
  - Kernsysteme (IdM)
  - Zielsysteme (nur IdM-Schnittstelle!)
- Entitäten
  - Tabelle/View in DBMS (z.B. HIS SOS)
  - LDAP-Objekt im IdM
  - WebService-Aufruf
  - XML-Dokument (z.B. VIVA)
- Attribute
  - Spalte einer Tabelle
  - LDAP-Attribut
  - Methodenparameter
  - XML-Element

Online-Doku: Datenmodell

- Einfaches Datenmodell:
  - Attribut, Entität, System



Online-Doku: Datenfluss

- Attribute
  - „abgeleitet von“-Abhängigkeit zwischen Attributen
  - … dadurch zwischen Entitäten
  - … dadurch zwischen Systemen
  - „Quellsystem“ und „Zielsystem“ ergibt sich aus Abhängigkeiten

- Abhängigkeiten
  - Zeigen den **möglichen** Datenfluss
  - Wertbildung nur informell beschrieben
    (z.B. Geburtsdatum: 15.06.1986 → Volljährig: ja)

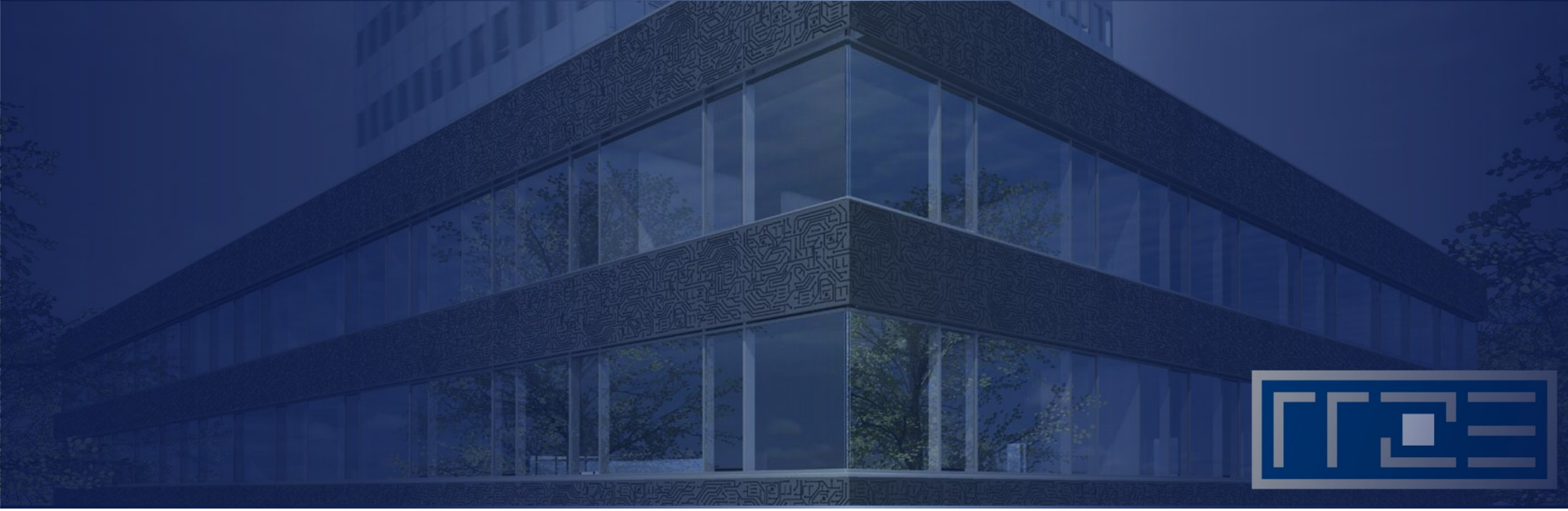
Online-Doku: **dataflow**

- Der GPR erhält
  - online Antworten auf ...
    - Welche Systeme, Entitäten und Attribute gibt es?
    - Woher stammen Informationen?
    - Wohin fließen Informationen?
    - Warum wird ein Attribut benötigt?
  - Änderungenverfolgung
  - Wöchentliche E-Mail-Benachrichtigungen
  - PDF-Exporte

Online-Doku: Fazit und Ausblick

- Version für Abschluss Dienstvereinbarung online
- Unterzeichnung steht noch aus

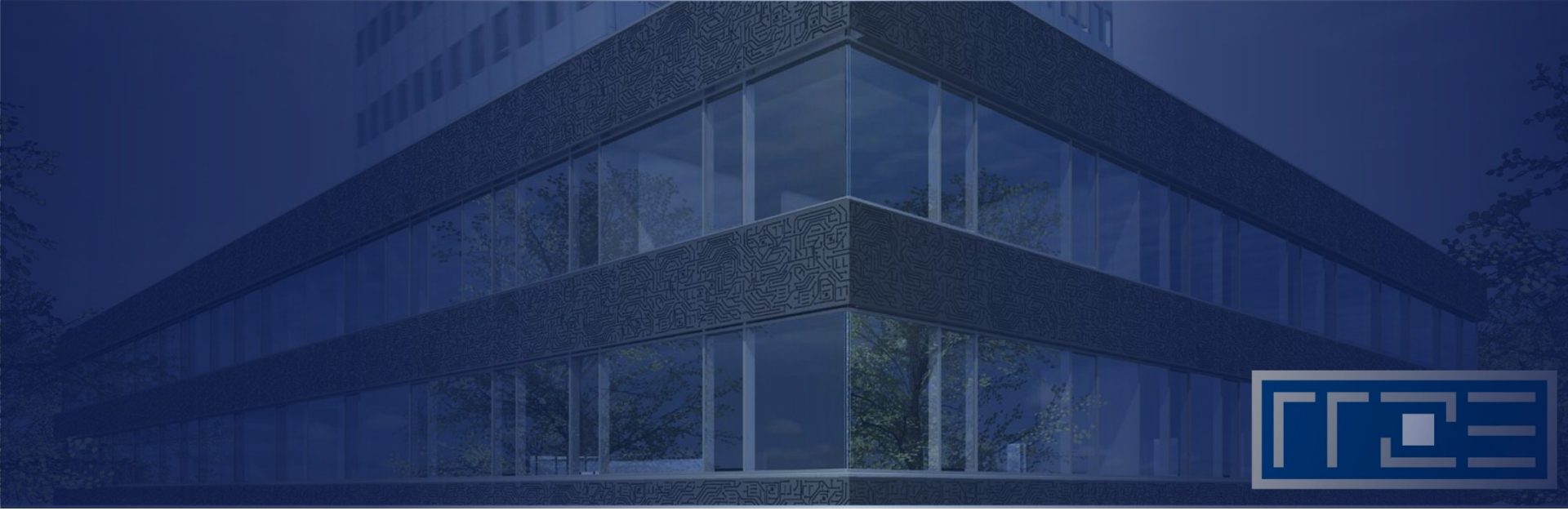
- Weitere Visualisierungen in Planung
  - Stärkere Nutzung bei der Entwicklung
- Abfrage der nutzbaren Attribute direkt aus daow
  - IdM-Umsetzung nur mit den dokumentierten Attributabhängigkeiten möglich
    d.h. Berechnung von Attributwerten nur mittels der „abgeleitet von“-Attributen
- Wöchentliche E-Mail mit Änderungen



Agenda

1. Rahmenbedingungen und Rechtliches
2. Online-Dokumentation
    - Berechtigte und Berechtigungen
    - Datenfluss: Systeme, Entitäten, Attribute
3. Demonstration des Systems

    Live-Demo oder Hotel?



Herzlichen Dank!

Regionales RechenZentrum Erlangen (RRZE)
Martensstraße 1, 91058 Erlangen
http://www.rrze.fau.de