

Paradigmenwechsel im Access Management

Organisationsübergreifende Autorisierung und
Rechteverwaltung

security Essen 2010 – security-forum - 06.10.2010

Michael Gröne

groene [at] internet – sicherheit . de

Institut für Internet-Sicherheit – if(is)

Fachhochschule Gelsenkirchen

<https://www.internet-sicherheit.de>



if(is)
internet-sicherheit.

Agenda

Worum geht es?

Berechtigungsmanagement heute

Warum ein Umdenken?

ABAC/PBAC Ansatz

ABAC/PBAC Umsetzung

Zukunft

Worum geht es?

→ Wie lassen sich Privilegien mit ABAC verwalten?

Privilegienmanagement vs. Berechtigungsmanagement

■ IAM & GRC

- Identity and Access Management (IAM)
- Governance, Risk and Compliance Management (GRC)

■ Identitätsföderation (Identity Federation)

- → **Organisationsübergreifend**; dynamisch, bspw. Service-orientierte Ansätze wie SOA oder SaaS Cloud Computing
- → Erfordert **Umdenken** bzgl. Autorisierung und Access Control

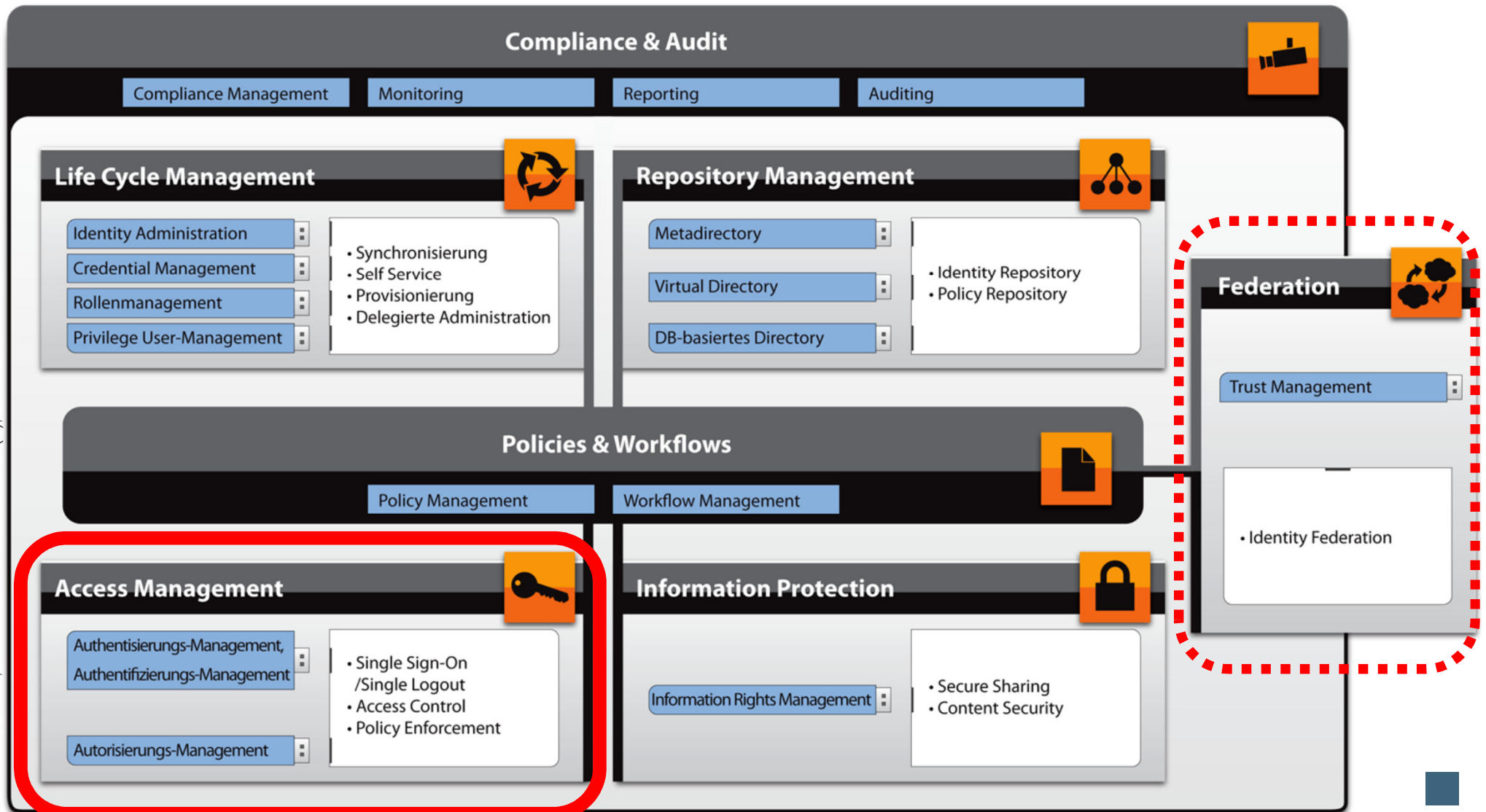
■ Policy- oder **Attribut-Based Access Control (ABAC)**

■ ABAC + GRC → **Paradigmenwechsel**

■ Einbeziehung von Risiken → **Risk-Adaptable Access Control**

Worum geht es?

→ Föderiertes Identity and Access Management

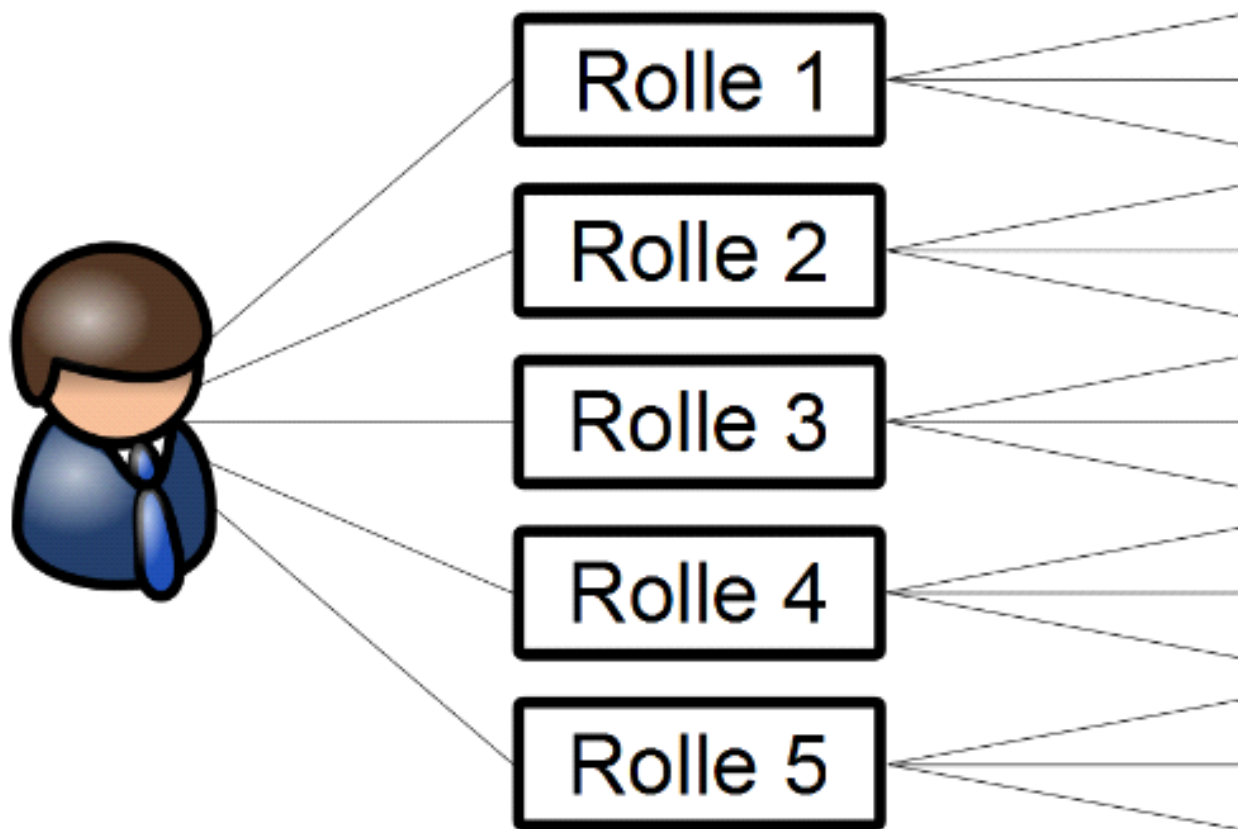


Berechtigungsmanagement heute

→ Rollen-basiertes Privilegienmanagement

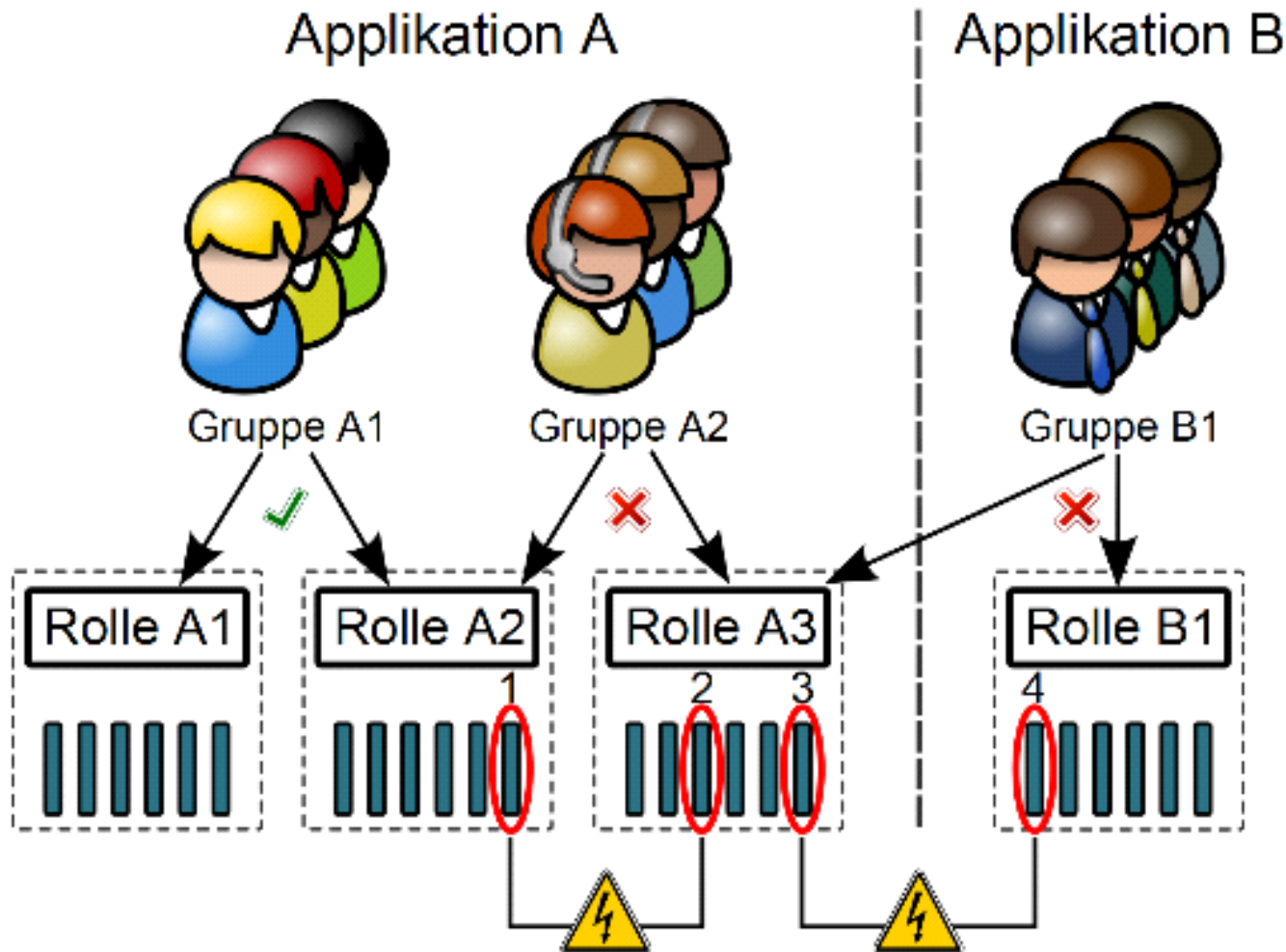
Role-Based Access Control

Nutzer -> Rollen -> Berechtigungen



Warum ein Umdenken?

→ RBAC + Funktionstrennung: Kaum zu lösen

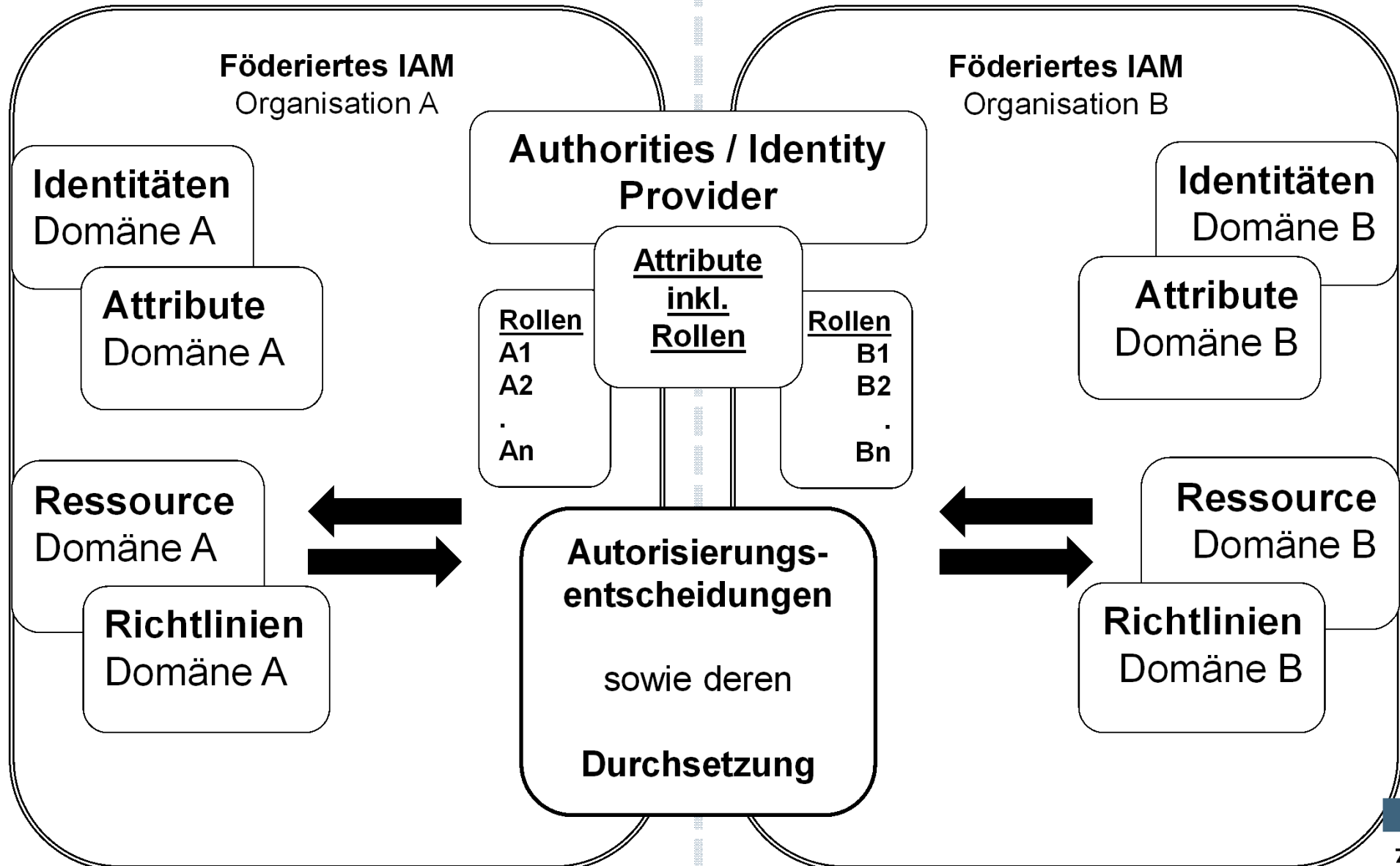


Verletzung der Funktionstrennung
(Privilegienkombinationen 1+2 & 3+4 dürfen nicht auftreten)

.....a never-ending Sudoku....

Warum ein Umdenken?

→ Föderiertes Identity and Access Management



Warum ein Umdenken?

→ Notwendigkeit eines neuen Ansatzes

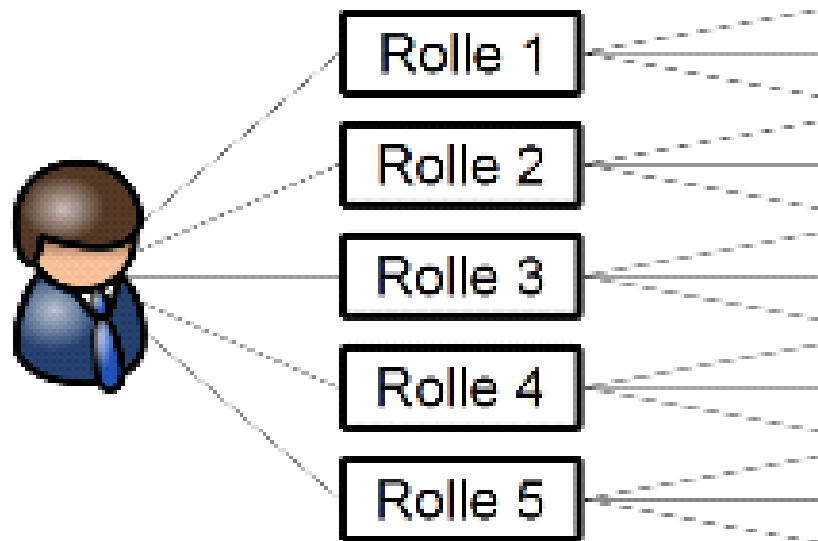
Notwendigkeit der Nutzung von Richtlinien- und Attribut-basiertem Access Control

- RBAC-Autorisierungsentscheidungen nur **grobgranular**, **Kontext** kann **nicht einbezogen** werden
- Rollenbasierter Ansatz **schwer umzusetzen**, **unüberschaubare Risiken** in Identitätsföderationen
 - Explosion der Rollenzahl
 - Überberechtigung
- Privilegienmanagement statisch, **nicht dynamisch** an den IT-Ressourcen
 - Zeiträume bis zum Inkrafttreten von Änderungen oft zu lang (Tage...)
 - Untragbar in einer SOA

ABAC/PBAC Ansatz → Weit mehr als RBAC

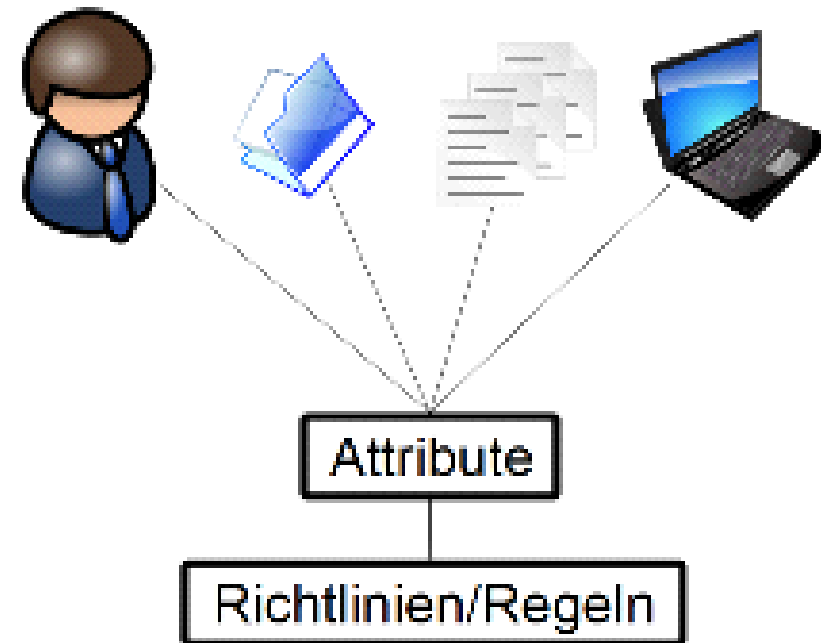
Role-Based Access Control

Nutzer → Rollen → Berechtigungen



Attribute-Based Access Control

Subjekt + Aktion + Resource + Umgebung



ABAC/PBAC Ansatz

→ Anwendungsfallbeispiel

Beispiel für die Notwendigkeit von ABAC:

- **Fall:**
 - „Ein **Patient**, der mit einer **heiklen Erkrankung** gerade in das **Krankenhaus** eingeliefert wird, in dem seine **Exfrau** praktiziert, und der Patient die Details seiner Krankheit nicht mit ihr teilen möchte.“
- **Richtlinie bzw. Gesetzgebung:**
 - „Ein **Arzt** darf die **Patientengeschichte** ausschließlich derjenigen Patienten einsehen, die **nicht explizit** eben jenen davon **ausgeschlossen** haben.“

(bspw. in den USA per Gesetz möglich)

ABAC/PBAC Ansatz

→ Richtlinien

Beispiel für eine Zugriffsrichtlinie auf Organisationsebene:

- „Ein **Arzt** darf auf **Patientenakten** während **normaler Arbeitszeit** **zugreifen** und diese **ändern** falls sein Name in einer **Liste** der bevorzugten Doktoren der Medizin in der Patientenakte steht, vorausgesetzt der **Zugriffspunkt** befindet sich innerhalb des Krankenhausnetzwerks.“

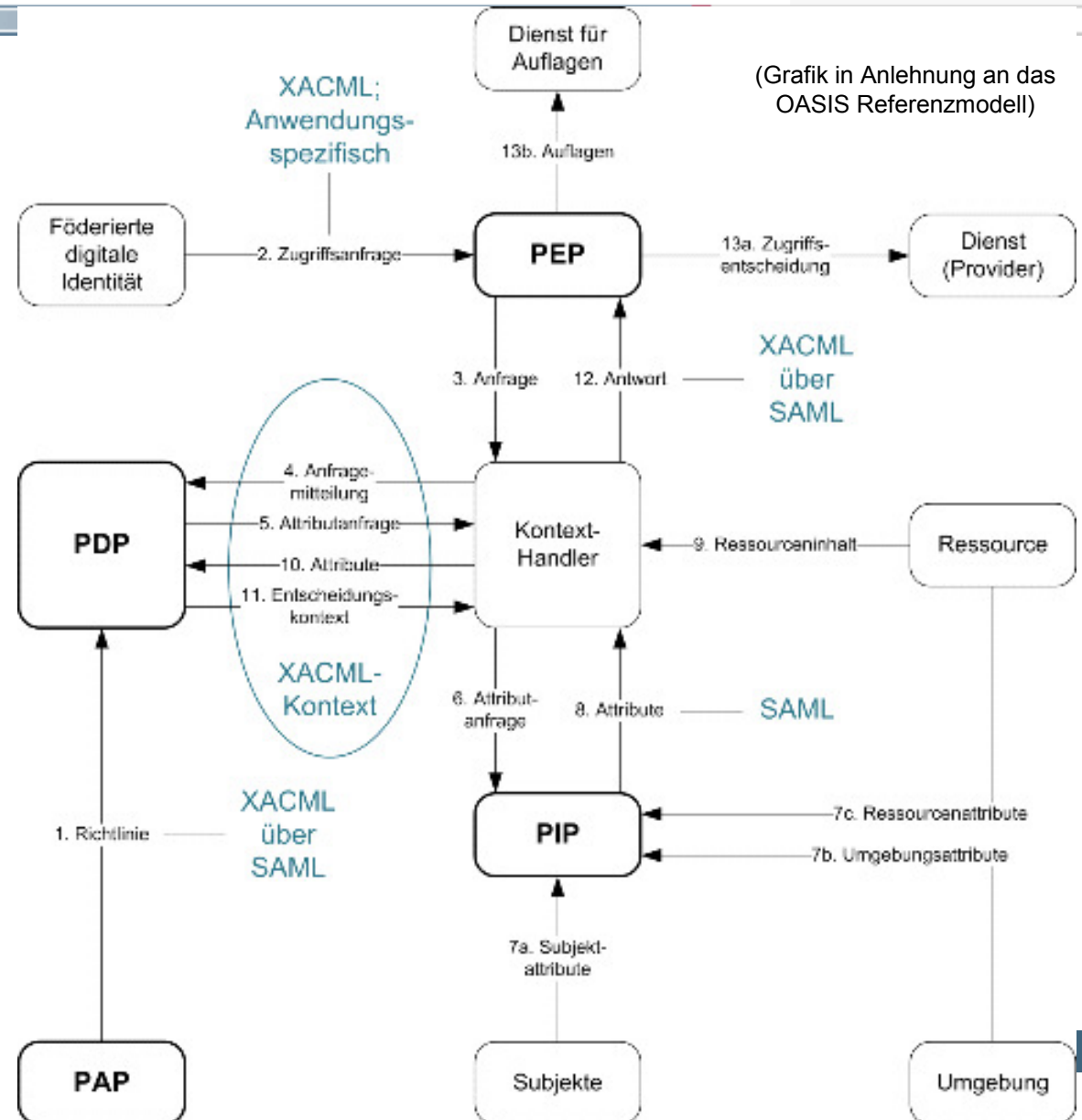
Subjekt	Aktion	Ressource	Umgebung	Zugriff erlaubt?
Dr. med. Freud möchte zugreifen und ändern...	... eine Patientenakte... (mit zugelassenen Ärzten; Dr. med.: Parkinson; Freud)	... auf dem PC in seinem Büro am Dienstag um 14:20 Uhr.	Ja (Umgebung ist ok und Name des Arztes steht auf der Liste, etc.)

ABAC/PBAC Umsetzung

→ Standardkonformes Komponentenmodell

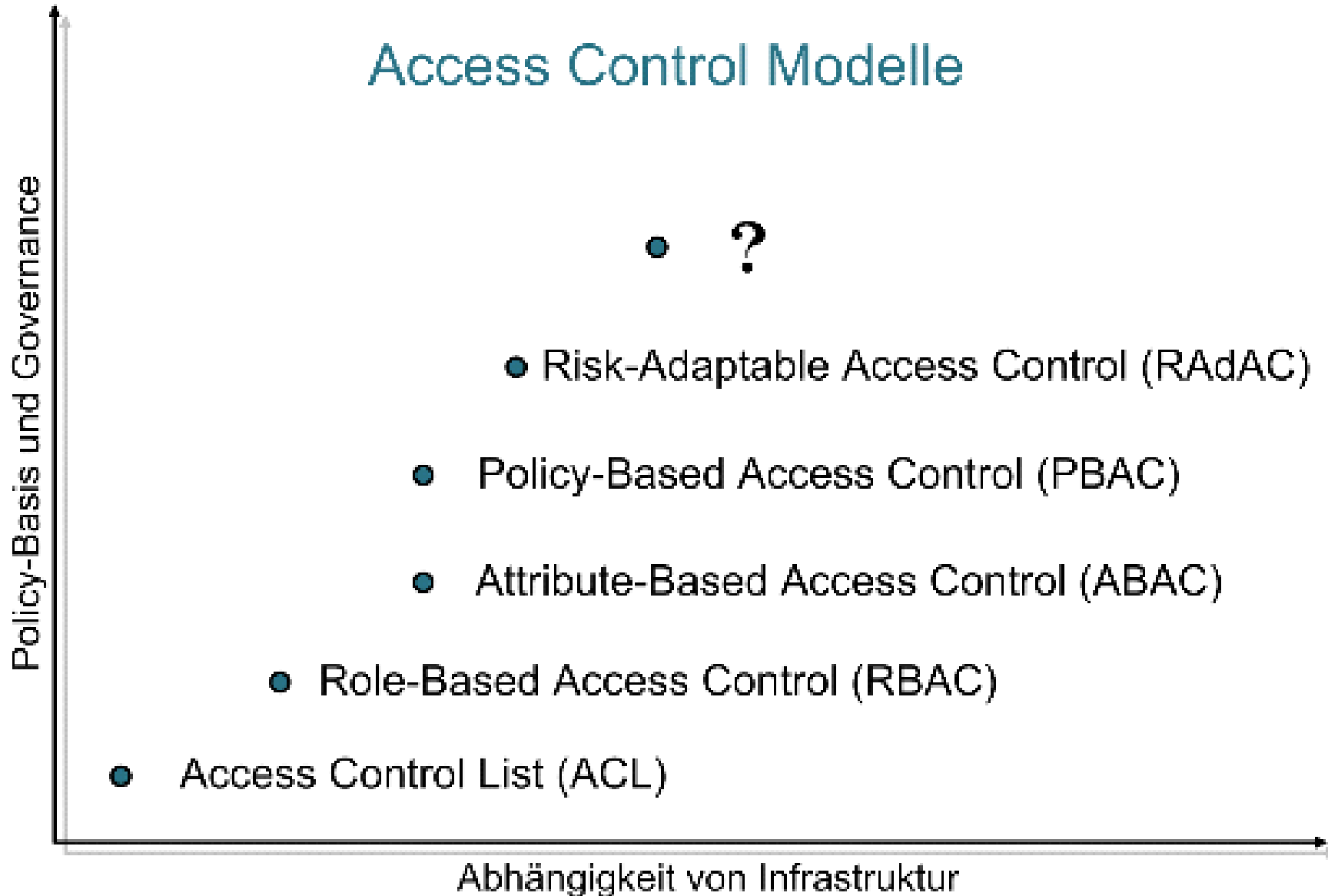
OASIS eXtensible Access Control Markup Language (XACML)

- Auslagerung der Entscheidung in PDP
- zentralisierte als auch verteilte Umgebungen
- Zusätzlich notwendig:
 - Attribut-Management
 - „mächtige“ Richtlinieneditoren (umfangreiche Prüffunktionen, etc.)



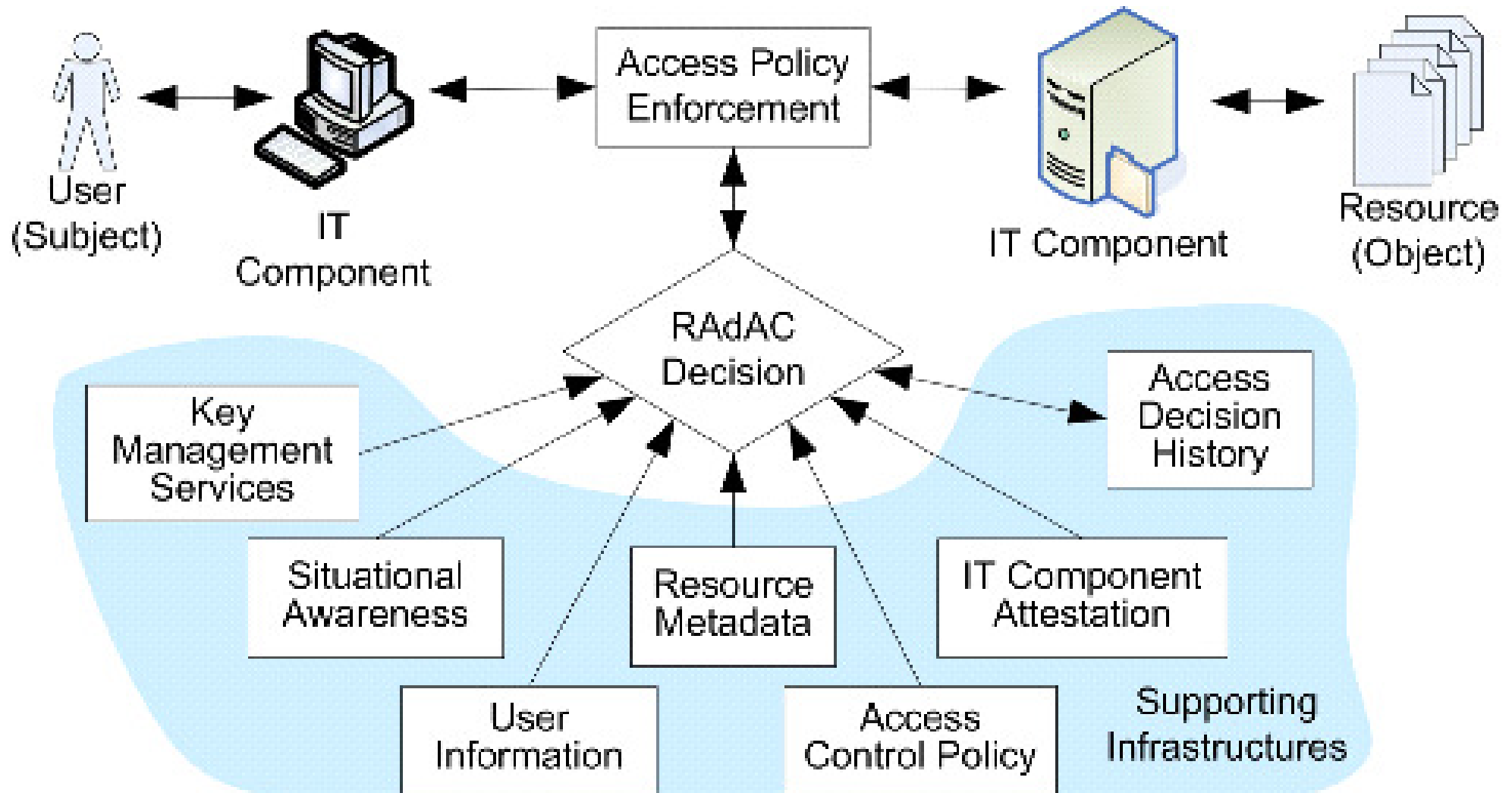
Zukunft

→ Mehr Möglichkeiten, mehr Abhängigkeiten



Zukunft (optionale Folie)

→ RAdAC und unterstützende Infrastruktur



Paradigmenwechsel im Access Management

Organisationsübergreifende Autorisierung und
Rechteverwaltung

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Michael Gröne

groene [at] internet – sicherheit . de

Institut für Internet-Sicherheit – if(is)

Fachhochschule Gelsenkirchen

<https://www.internet-sicherheit.de>



if(is)
internet-sicherheit.