



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Zugriffsschutz und Identitätsmanagement

Prof. Dr. (TU NN)

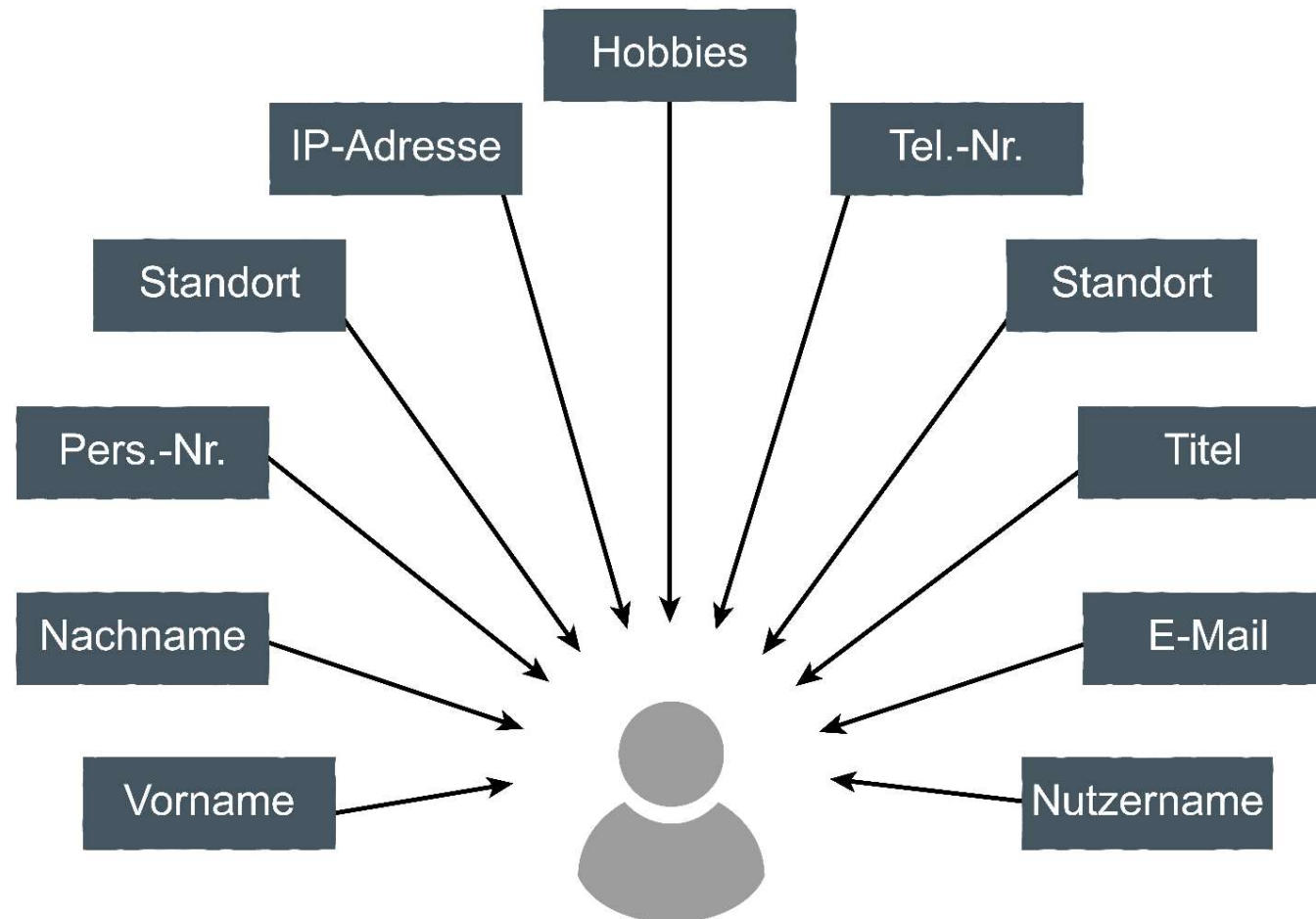
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
<http://www.internet-sicherheit.de>

if(is)
internet-sicherheit.

Definitionen

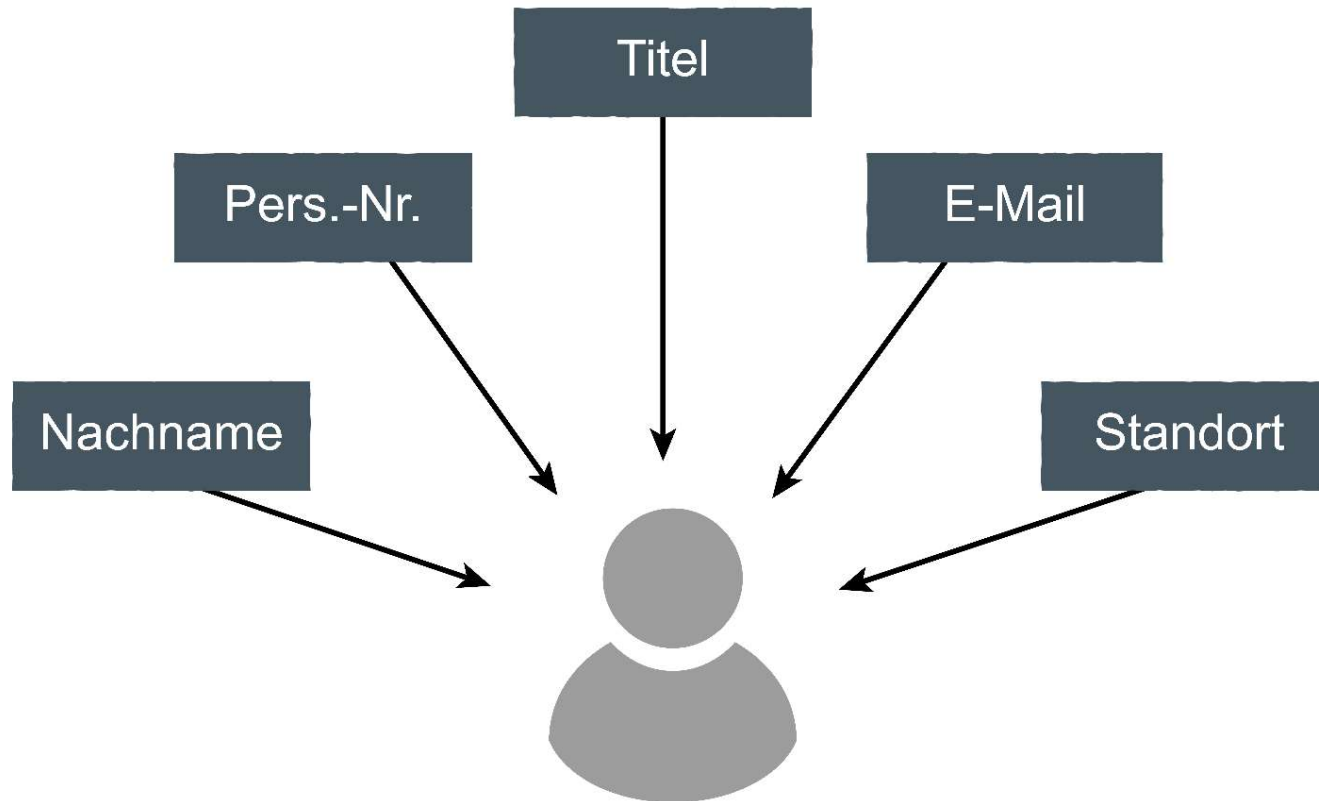
→ Entität



- Eine **Entität** (Person, IT-System etc.) setzt sich zusammen aus der sie **beschreibenden Attribute**.

Definitionen

→ Digitale Identität



- Eine **digitale Identität** ist die **Teilmenge der Attribute einer Entität**, welche diese Identität in einem bestimmten Kontext im Unterschied zu anderen Entitäten **eindeutig bestimmbar** machen.

Definitionen

→ Identity and Access Management

- In der Fachwelt hat sich bisher keine einheitliche Auffassung, was exakt unter **Identity and Access Management** zu verstehen ist, durchgesetzt.
- In der Mehrheit der Definitionen bezieht sich der Begriff **Identity and Access Management (IAM)** im Kern auf
 - die Kombination von Verfahren der **Organisationsführung** einerseits
 - und **Technologie** andererseits,
- welche es Organisationen durch eine breite Palette von Prozessen und Funktionalitäten erlauben
 - die **Einhaltung gesetzlicher Vorschriften**
 - sowie die **Integrität, Vertrauenswürdigkeit und Verfügbarkeit von Informationen**
- gewährleisten zu können.

Definitionen

→ Identity and Access Management

- **Definition des Instituts für Internet-Sicherheit – if(is):**
 - Der Begriff **IAM** beschreibt jeglichen Einsatz von digitalen Identitäten, deren Attributen, sowie deren Berechtigungen und schließt die Erzeugung, Nutzung, Pflege und Löschung dieser digitalen Identitäten mit ein.
- Das **Ziel** ist es,
 - **vertrauenswürdige,**
 - **Identitätsbezogene und**
 - **regelkonforme Prozesse**
- durchzusetzen, die **unabhängig von Organisationen und Plattformen** standardisiert nutzbar sind.

Keinen Einsatz eines IAMs → Die Probleme

- Erhöhte Kosten
- Komfortverlust
- Steigender Administrationsaufwand
- **Fehlende Kontrolle**
- Informations- bzw. Datenverlust
- **Unüberschaubare Sicherheitsrisiken (Überberechtigung ...)**
- Sicheres organisationsübergreifendes Arbeiten unmöglich

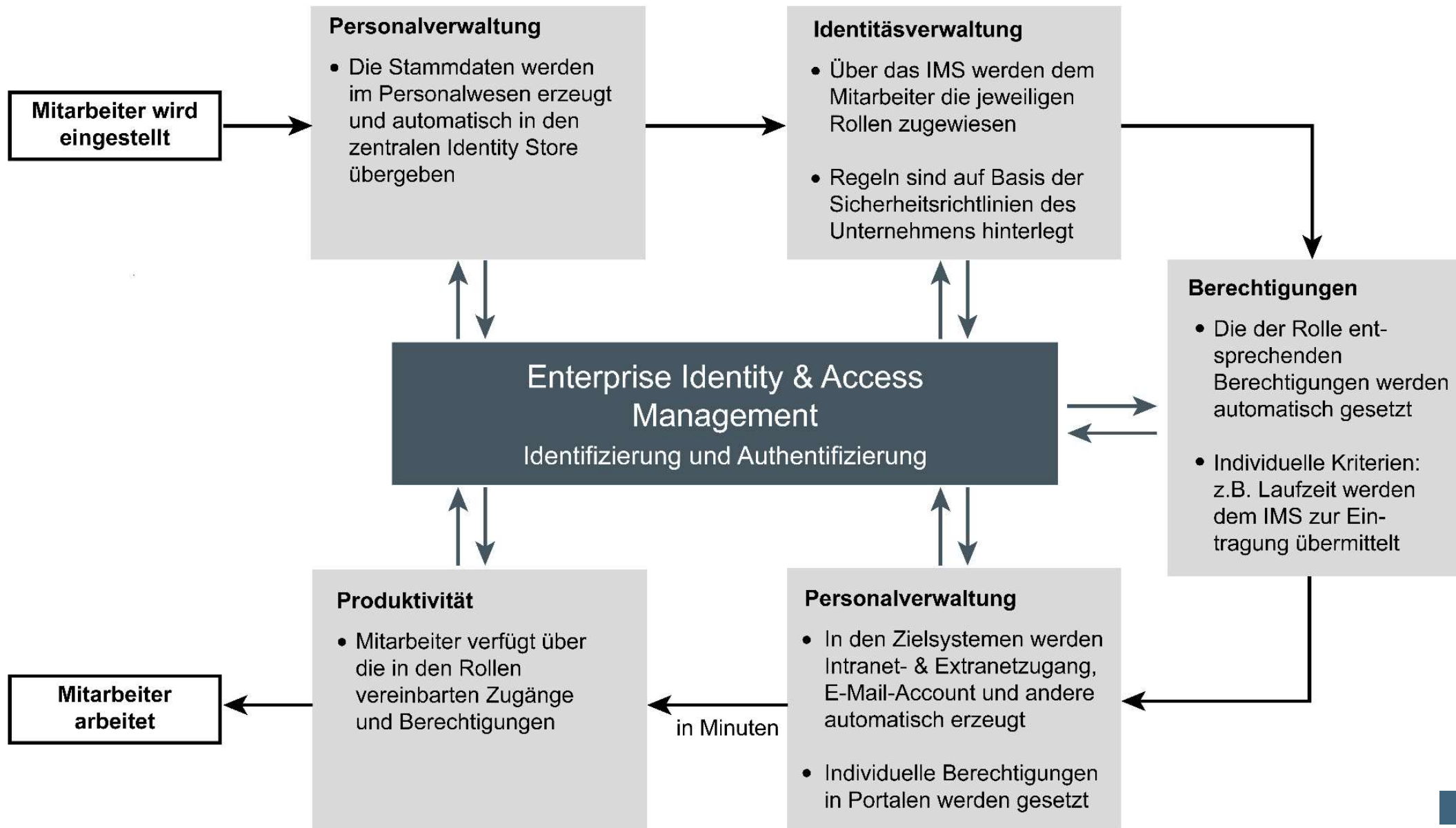
Notwendigkeit

→ Zusammenarbeit mit Partnern

- Organisationen sind auf Zusammenarbeit mit Partnern angewiesen, dies verlangt nach
 - Sicherem Austausch von identitätsbezogenen Daten
 - Vertrauensverhältnissen
 - Verwendung einheitlicher Standards
 - Koppelung von Geschäftsprozessen
 - Need-to-Share Prinzip
 - Sicheres Einbinden externer Personen in interne IT-Systeme
- Cloud Computing benötigt technische Aspekte zur
 - Weitergabe von Identitäten
 - Authentifizierung und Autorisierung

Anforderungen

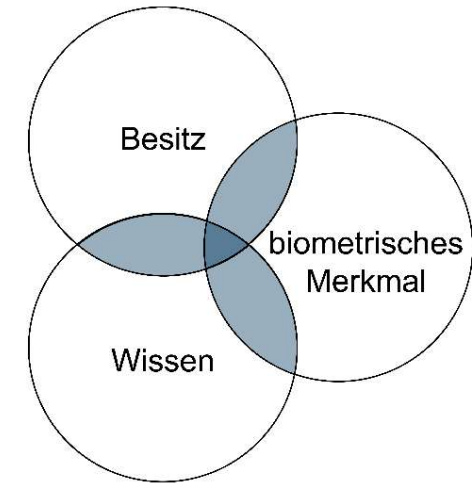
→ Beispiel



Key Concepts

→ Anforderungen an ein IAM-System

- **Sichere und komfortable Authentifizierung (MFA)**
- Strukturierte Identitäts-Datenspeicherung und -verwaltung
- Zusammenführung von Identitätsdaten
- Identitäten über ihren gesamten Lebenszyklus begleiten
- **Vermeidung von Überberechtigungen**
- Schutz von Informationen und Zugriffen (**Verschlüsselung**)
- Organisationsübergreifende Nutzung von Identitäten
- **Vertrauen zwischen Diensteanbietern herstellen**

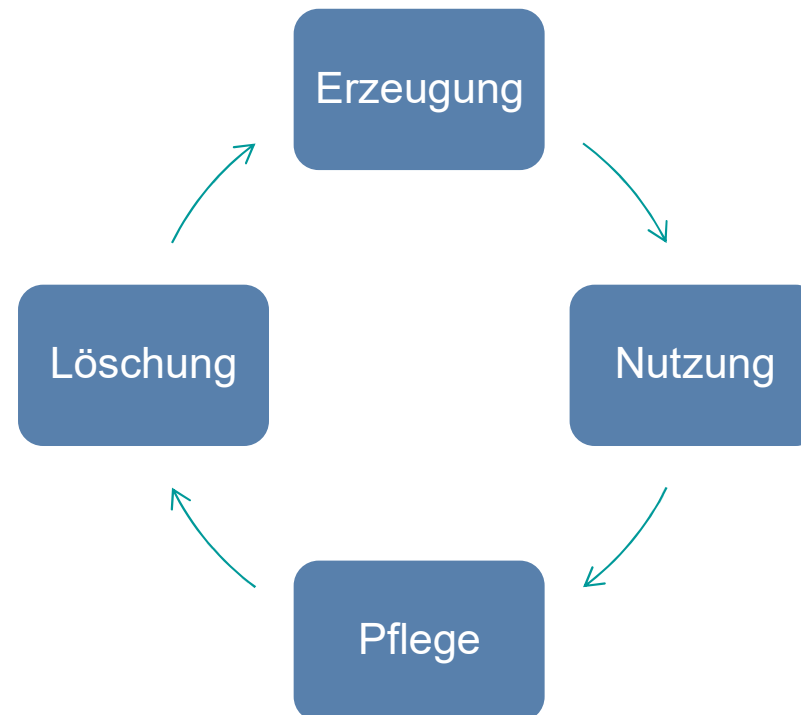


Stand der Technik ... IT-Sicherheitsgesetze

Key Concepts

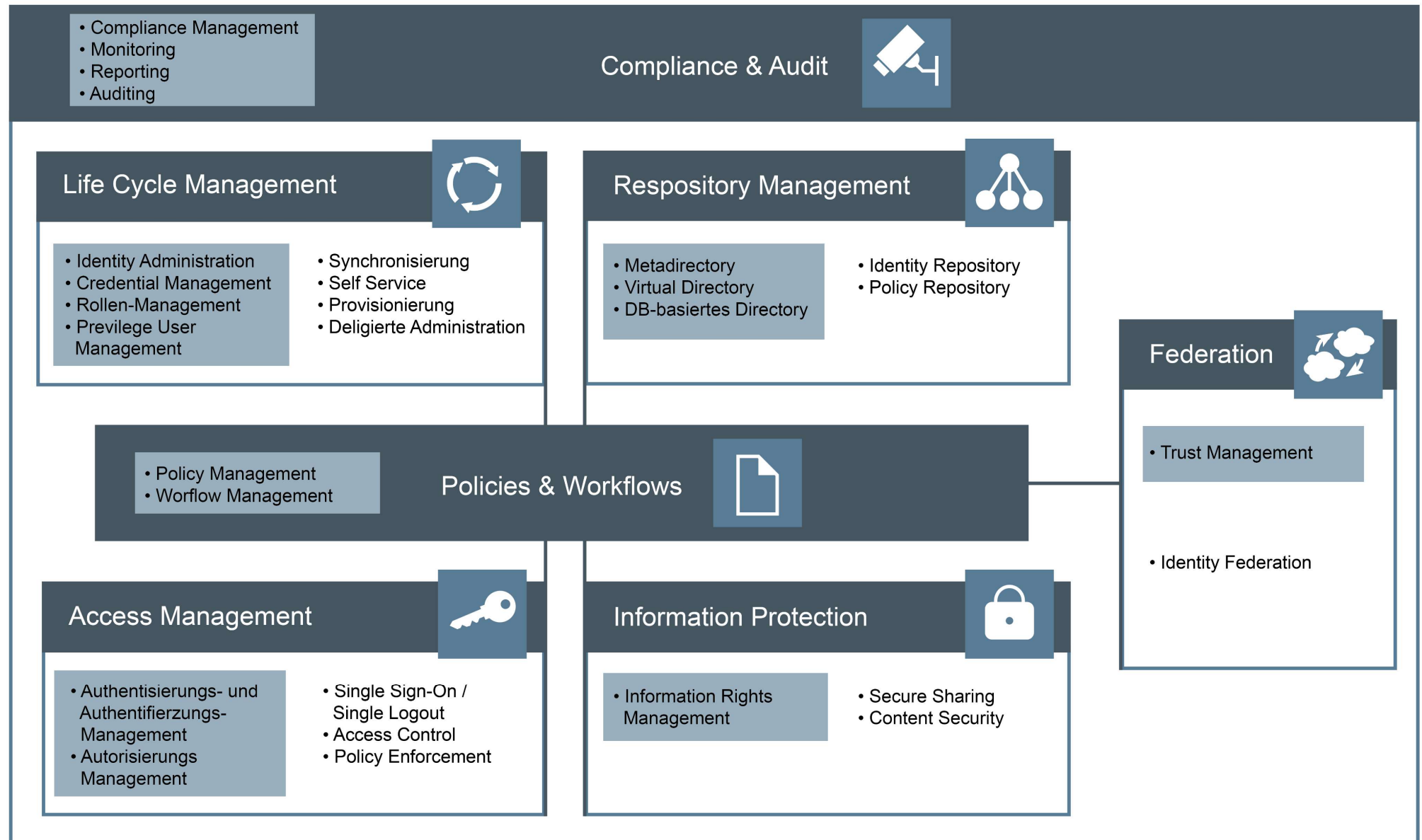
→ Anforderungen

- Identity and Access Management soll:
 - digitale Identitäten und ihren gesamten Lebenszyklus verwalten
 - insbesondere, deren vertrauenswürdige Attribute sowie Berechtigungen



IAM-Modell

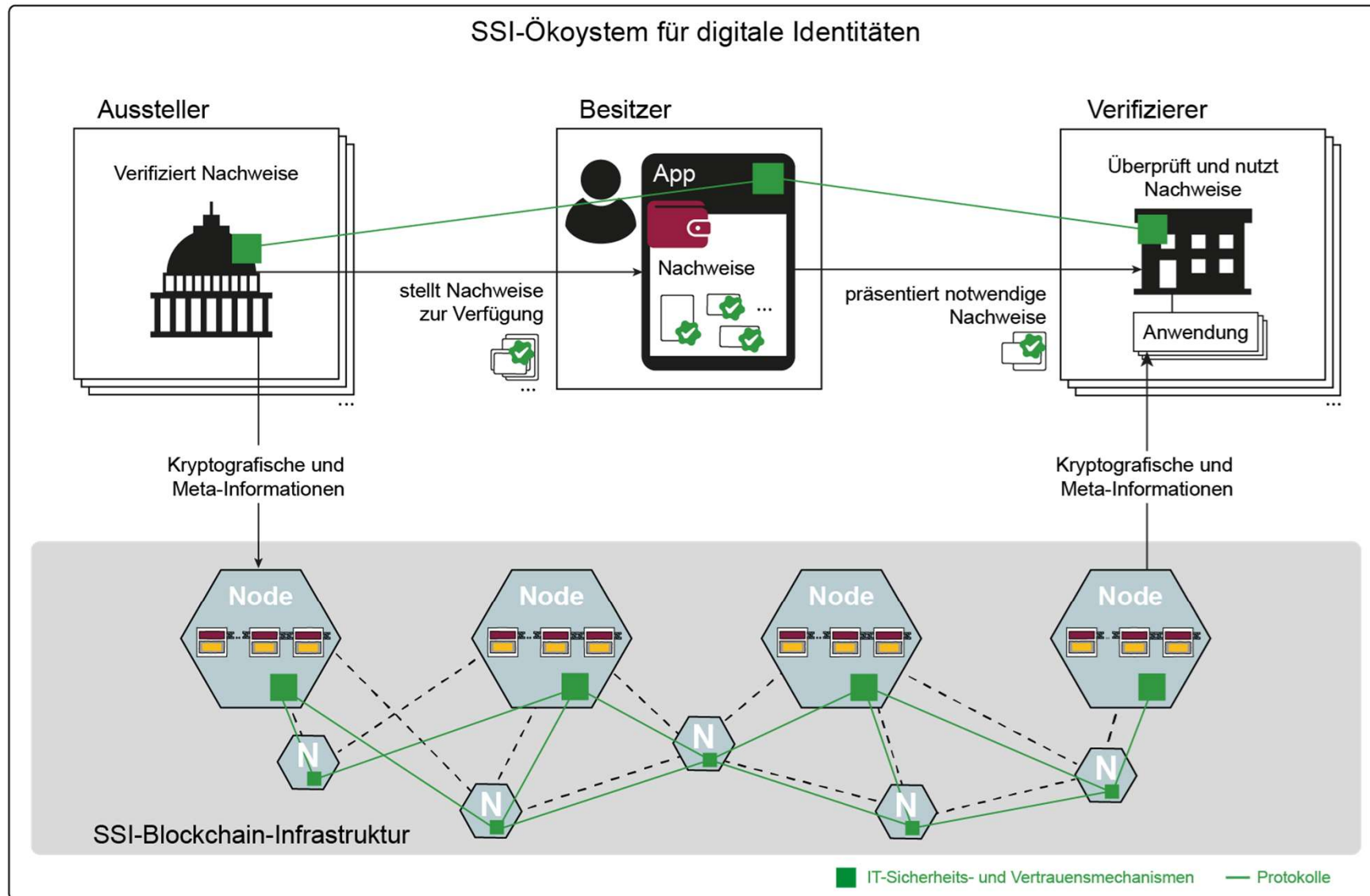
→ Referenz-Modell



Self-Sovereign Identity

→ Architektur

- Im SSI-Ökosystem spielen **drei Akteure eine Rolle**, die gemeinsam einen Vertrauensdienst – zum Beispiel die SSI-Blockchain-Infrastruktur - nutzen.



- Identity and Access Management Systeme (IAMS) **vereinfachen** den Umgang mit digitalen Identitäten, ihren **Attributen** und **Berechtigungen** enorm.
- IAM ist ein sehr **komplexes Thema** – Ein **Modell** bringt unterschiedliche Module in **Einklang**
- Zunehmend wird es wichtiger, **Authentikationsverfahren** zu verwenden, die in der globalen handelnden Gesellschaft über staatliche Grenzen und Verantwortungsbereiche hinaus verwendet werden können.
- In der Zukunft wird ein **neues Identitätsparadigma** eine wichtige Rolle spielen.

Von „Enterprise-Centric-Identity“ zu „User- Enterprise-Centric-Identity“



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Zugriffsschutz und Identitätsmanagement

Prof. Dr. (TU NN)

Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
<http://www.internet-sicherheit.de>

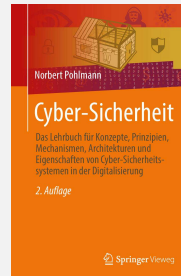
if(is)
internet-sicherheit.

Wir empfehlen

Cyber-Sicherheit

Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2022

<https://norbert-pohlmann.com/cyber-sicherheit/>



7. Sinn im Internet (Cyberschutzraum)

<https://www.youtube.com/cyberschutzraum>



Master Internet-Sicherheit

<https://it-sicherheit.de/master-studieren/>



Glossar Cyber-Sicherheit

<https://norbert-pohlmann.com/category/glossar-cyber-sicherheit/>



It's all about Trust!

<https://vertrauenswuerdigkeit.com/>



Quellen Bildmaterial

Eingebettete Piktogramme: Institut für Internet-Sicherheit – if(is)

Besuchen und abonnieren Sie uns :-)

WWW

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

Facebook

<https://www.facebook.com/Internet.Sicherheit.ifis>

Twitter

https://twitter.com/_ifis

<https://twitter.com/ProfPohlmann>

YouTube

<https://www.youtube.com/user/InternetSicherheitDE/>

Prof. Norbert Pohlmann

<https://norbert-pohlmann.com/>

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
<https://www.it-sicherheit.de/>

Literatur

→ Artikel / Bücher

N. Heibel, M. Linnemann, N. Pohlmann: „Dokumente sicher im Griff: Sicheres Enterprise Rights Management“, IT SECURITY, März/April, 02/2008

<https://norbert-pohlmann.com/wp-content/uploads/2015/08/220-Dokumente-sicher-im-Griff-Sicheres-Enterprise-Rights-Management-Prof-Norbert-Pohlmann.pdf>

S. Feld, N. Pohlmann: „Security analysis of OpenID, followed by a reference implementation of an nPA-based OpenID provider“. In Proceedings of the ISSE 2010 - Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe 2010 Conference, Eds.: N. Pohlmann, H. Reimer, W. Schneider; Vieweg-Teubner Verlag, Wiesbaden 2010

<https://norbert-pohlmann.com/wp-content/uploads/2015/08/264-Security-analysis-of-OpenID-followed-by-a-reference-implementation-of-an-nPA-based-OpenID-provider-Prof-Norbert-Pohlmann.pdf>

O. Achten, S. Feld, N. Pohlmann: „Identity Management als fortwährender Prozess – Mit Sicherheit zum Ziel“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 1/2010

<https://norbert-pohlmann.com/wp-content/uploads/2015/08/253-Identity-Management-als-fortwährender-Prozess-Mit-Sicherheit-zum-Ziel-Prof-Norbert-Pohlmann.pdf>

M. Gröne, N. Pohlmann: „Föderierte Autorisierung und ein Umdenken im Privilegienmanagement – Organisationsübergreifend arbeiten – aber sicher!“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 5/2010

<https://norbert-pohlmann.com/wp-content/uploads/2015/08/267-Föderierte-Autorisierung-und-ein-Umdenken-im-Privilegienmanagement---Organisationsübergreifend-arbeiten---aber-sicher-Prof-Norbert-Pohlmann.pdf>

N. Pohlmann: "Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, ISBN 978-3-658-25397-4; 594 Seiten, Springer-Vieweg Verlag, Wiesbaden 2019

<https://norbert-pohlmann.com/cyber-sicherheit/>