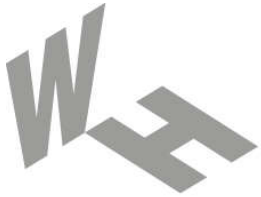


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

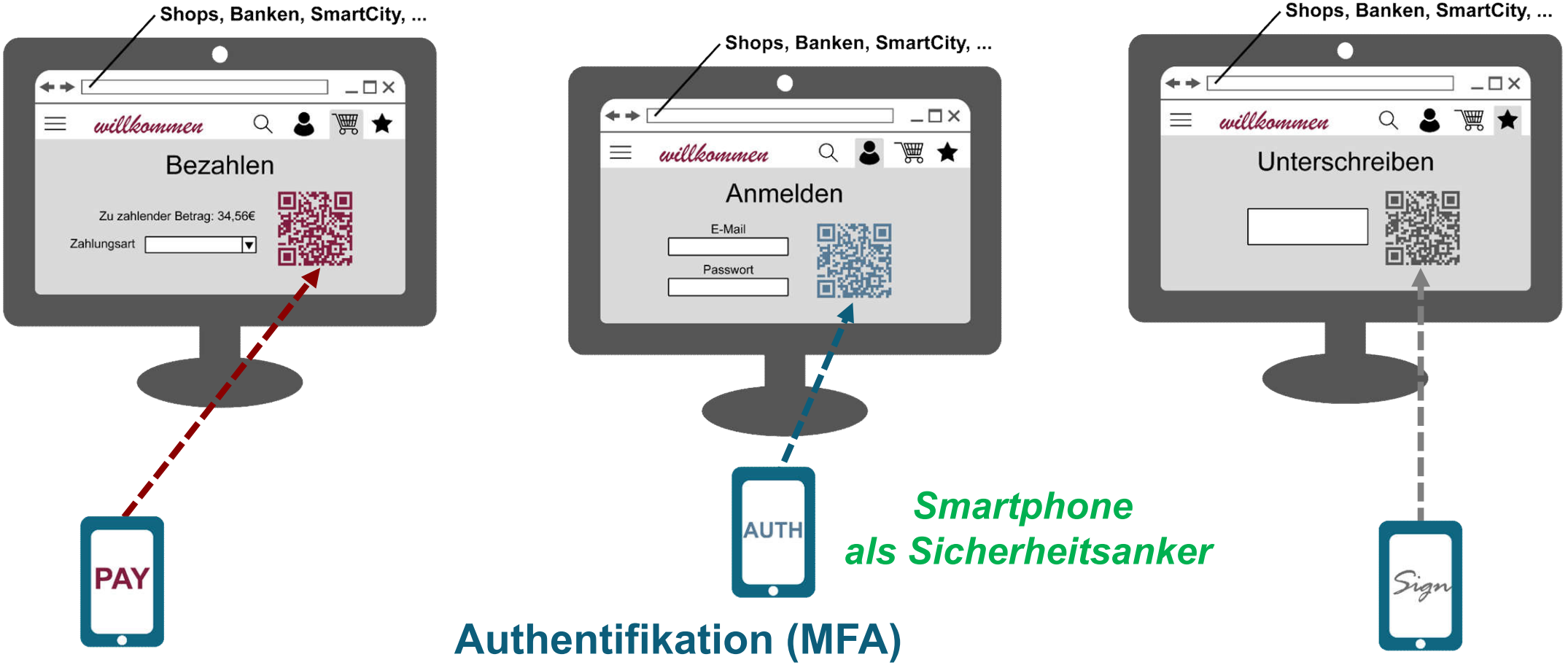
Smart Authentifikation, Identifikation und digitale Signaturen → als Grundlage zukünftiger Ökosysteme

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is) internet-sicherheit.

Zukünftiges Ökosystem
→ Sichtweise



Smartphone als Sicherheitsanker

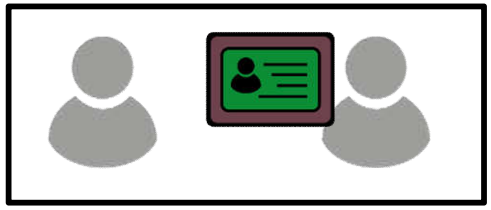
Payment
- Coin (Blockchain)
- Eilüberweisung **(PSD2)**
- Payment-Broker
- …

Authentifikation (MFA)
- **Challenge-Response (PKI-basierend)**
- Passwort / PIN
- **Biometrie** (Fingerabdruck, Gesichtserkennung, …)
- *IT-System-Signatur (HW und SW)*
- *Umgebung (GPS, WLAN, …)*

Signatur
- Transaktionen
- AGBs
- Verträge
- Anträge
- … (**eIDAS**)

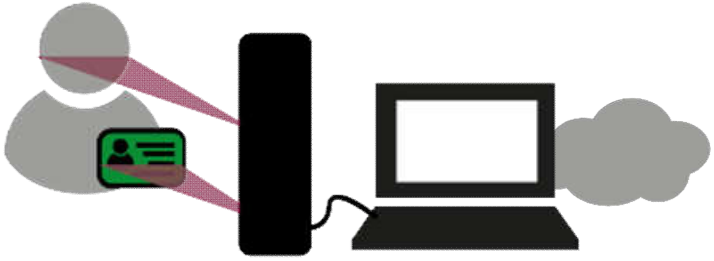
Identifikationsverfahren
→ Übersicht der Verfahren mit PA

Vorlage eines Personalausweises

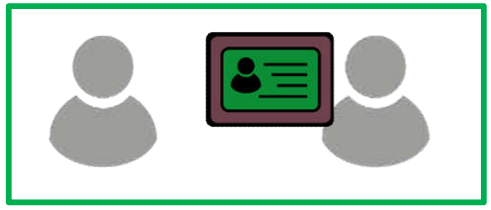


eID Verfahren des elektronischen Personalausweises

VideoIdent



PostIdent



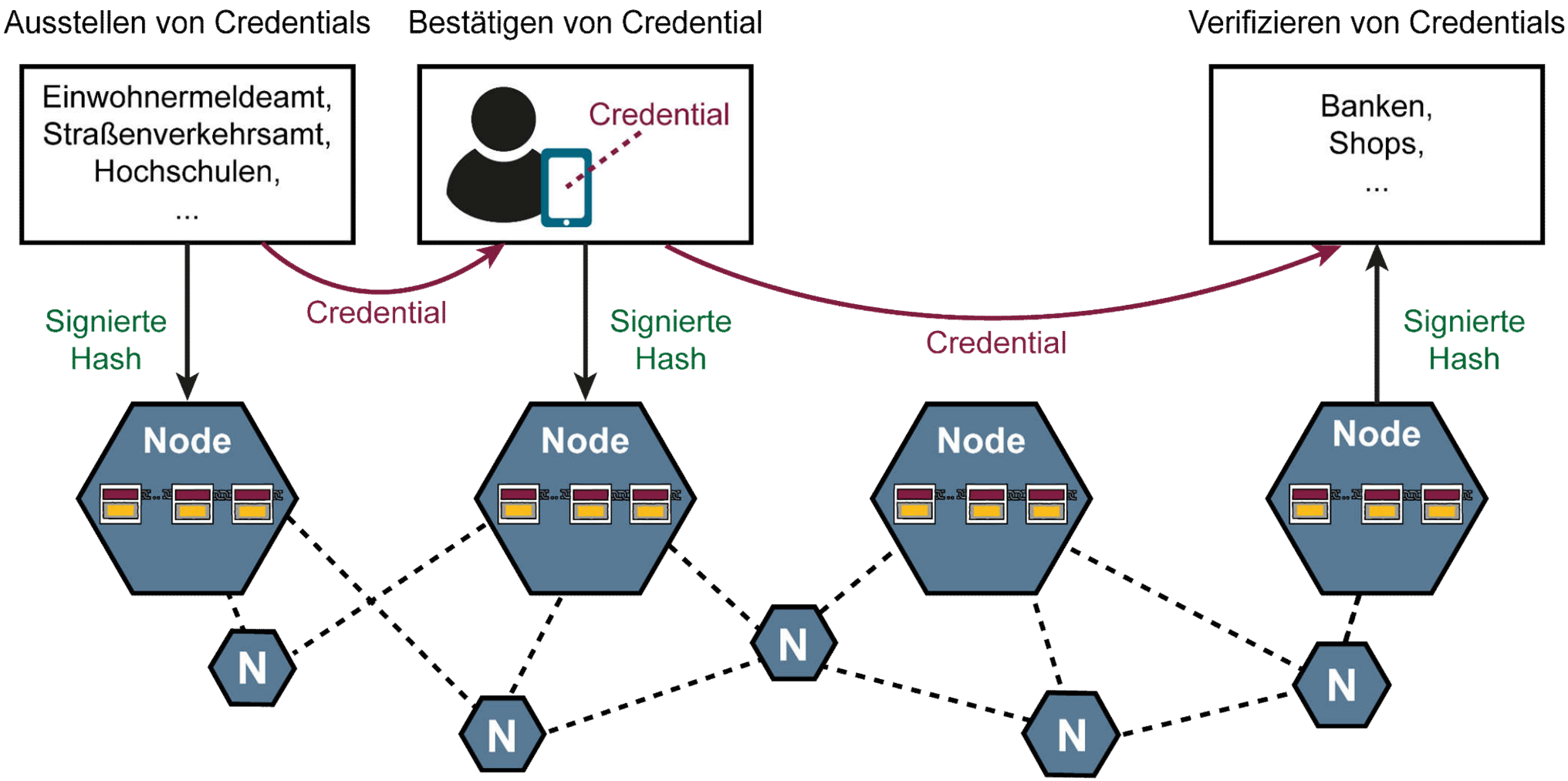
	Personal -ausweis	Video-Ident	Post-Ident	eID
Medienbruchfreiheit	-	+	-	+
Terminbindung	-	+-	-	+
Kosten	+-	+	+	+
Nutzerkreis	+	+	+	-

Identifikationsverfahren
→ Weitere Verfahren

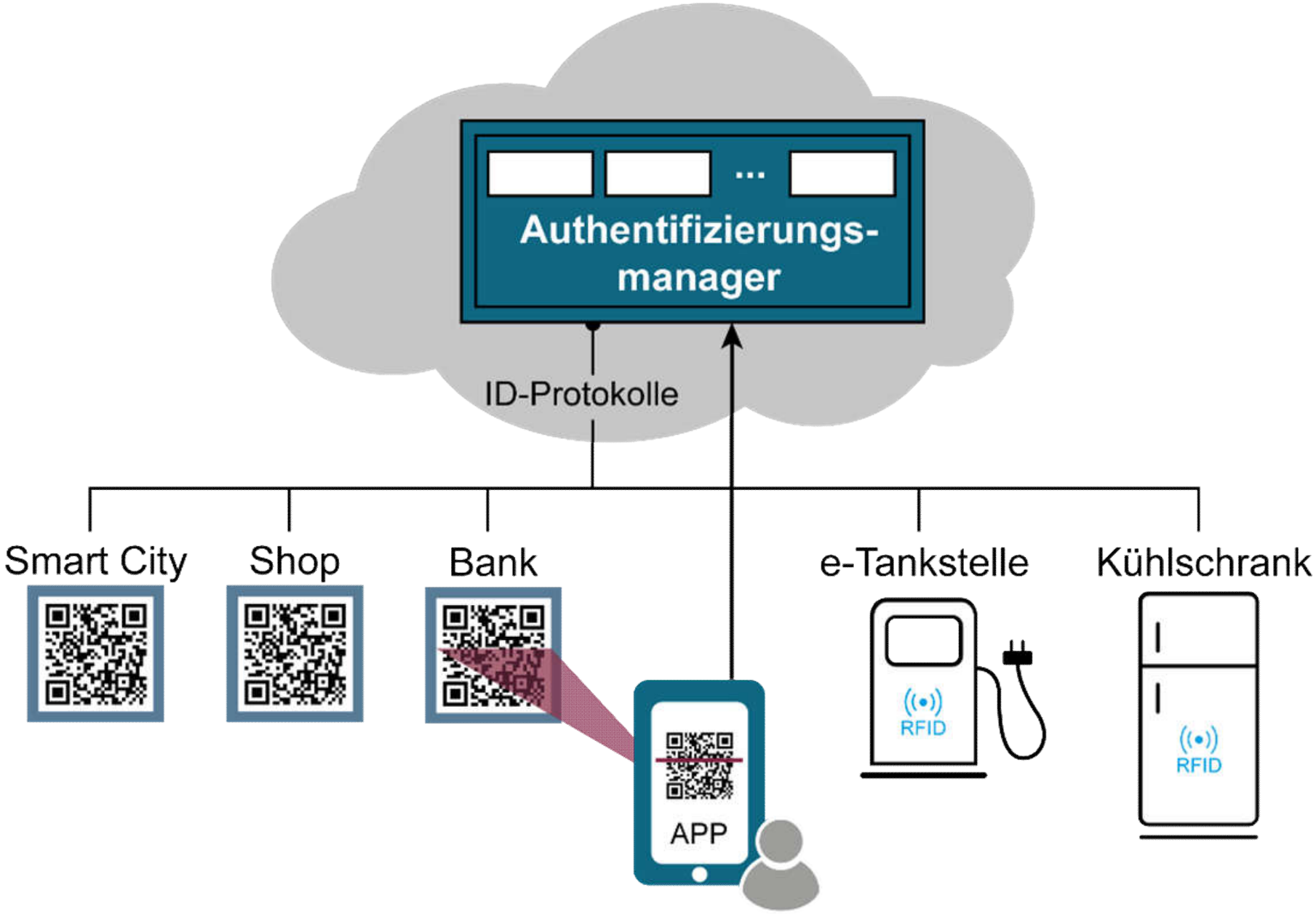
„Positive Erfahrung“
(erfolgreiche Zahlungen, Kreditwürdigkeit, Verhalten (Bestellung, Lieferung), …)

SocialIdent

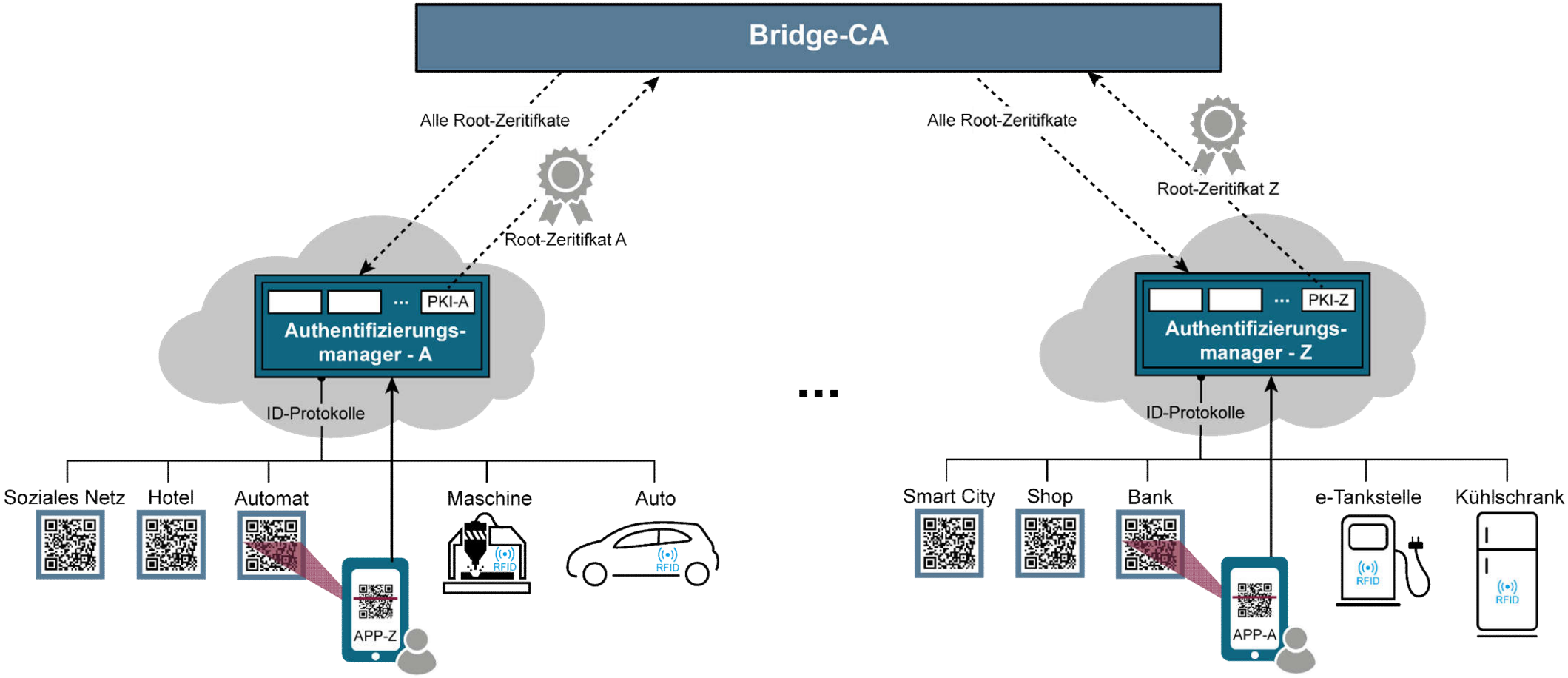
Self-Sovereign Identity (Blockchain)
→ Identifikations-/Credential Broker



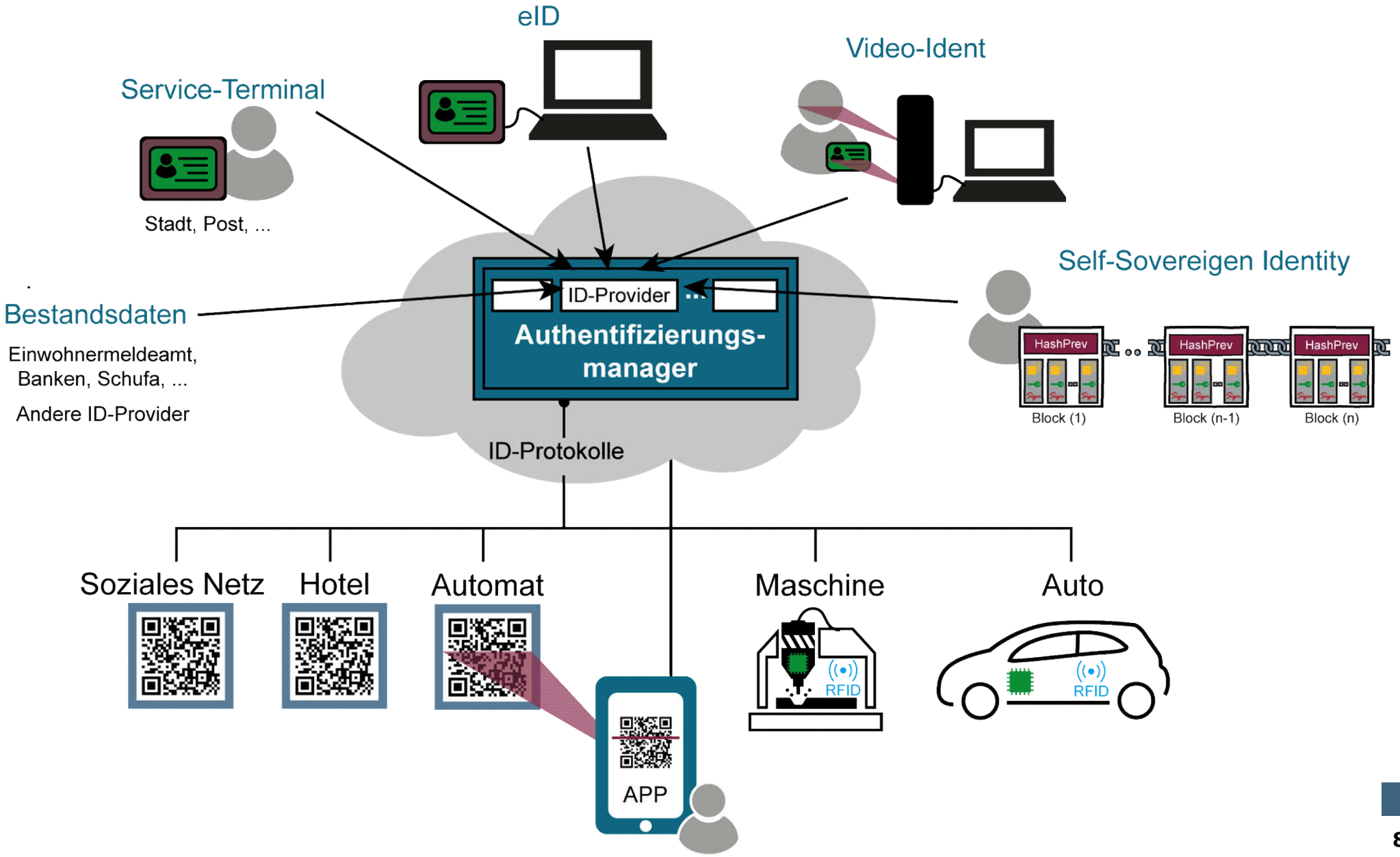
Lösung der XignSys
→ Idee XignQR



XignQR
→ **Bridge-CA** (PKI-basierend)



XignQR
→ ID-Provider



Bedarf an Forschung und Entwicklung
→ Standards

- **Frameworks im Sinn von Standards für**
  - Identitätsmanagement
  - Authentifikation
  - Signatur
  - Payment

  mit einer **einfachen** und **standardisierten Einbindung** und **Nutzung**.

- **Austausch von Identitäten zwischen ID-Provider**
  - Definition von Datenstrukturen, Schnittstellen und Vertrauenslevel
  - **sID4X - Secure ID for the Internet of Everything**
    (VDI DIN-Connect Projekt – XignSys – siehe in der Anlage)

Bedarf an Forschung und Entwicklung
→ Self-Sovereign Identity (Blockchain)

- **Sicherheit** der **Schlüssel** und **Credentials**
  (Sicherheitsanker – Speicherung, Verteilung, Einbindung, …)
- **Vertrauliche Übertragung** der **Credentials**
  (Verschlüsselung – Infrastruktur, …)
- **Lebensdauer** einer **Decentralized Identifier** (DID) und **Credentials**
  (Krypto-Agilität planen, Hard-Fork organisieren, …)
- **Vertrauenslevel** für verschiedene Credentials
  (hoheitlich, freie Wirtschaft, …)

Digitale Identitäten
→ Zusammenfassung

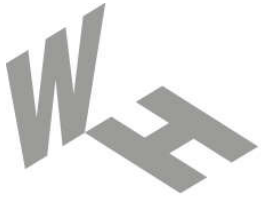
- **Einfache Abläufe** (QR-Code) *und*
  vertrauenswürdige Sicherheitsanker (Smartphone)
  *(**Akzeptanz** und **Vertrauen**)*

- **PKI-basierende Lösung** für Challenge-Response, Signatur und Payment
  *(**gesetzliche Anerkennung** - eIDAS) und **Interoperabilität** - Bridge CA)*

- **Hohe Anwendung und Nutzung** von Identifikation, Authentifikation, Digitale Signatur, Payment, …
  *(**Ökosystem aufbauen** (EU, international)*
  *mit **vertrauenswürdiger Infrastruktur**)*

- **Zusammenarbeit und Austausch der ID-Provider**
  *(**schnelle Verbreitung von Identitäten mit hohem Vertrauenslevel**)*

- **Frameworks für die Schaffung von Standards**
  *(**einfache Einbindung** und **Nutzung** sowie **rasche Verbreitung**)*



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Smart Authentifikation, Identifikation und digitale Signaturen → als Grundlage zukünftiger Ökosysteme

Digitale Identitäten für mehr Vertrauen im Internet

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is) internet-sicherheit.

Secure ID for the Internet of Everything
→ VDI DIN-Connect Projekt

- Fragestellungen des **VDI DIN-Connect** Projekts

sID4X

  - Welche **technischen Anforderungen** müssen für den sicheren und nachweislichen Austausch von **Attributen, einer digitalen Identität**, erfüllt sein? *(für Web- und IoT Services)*

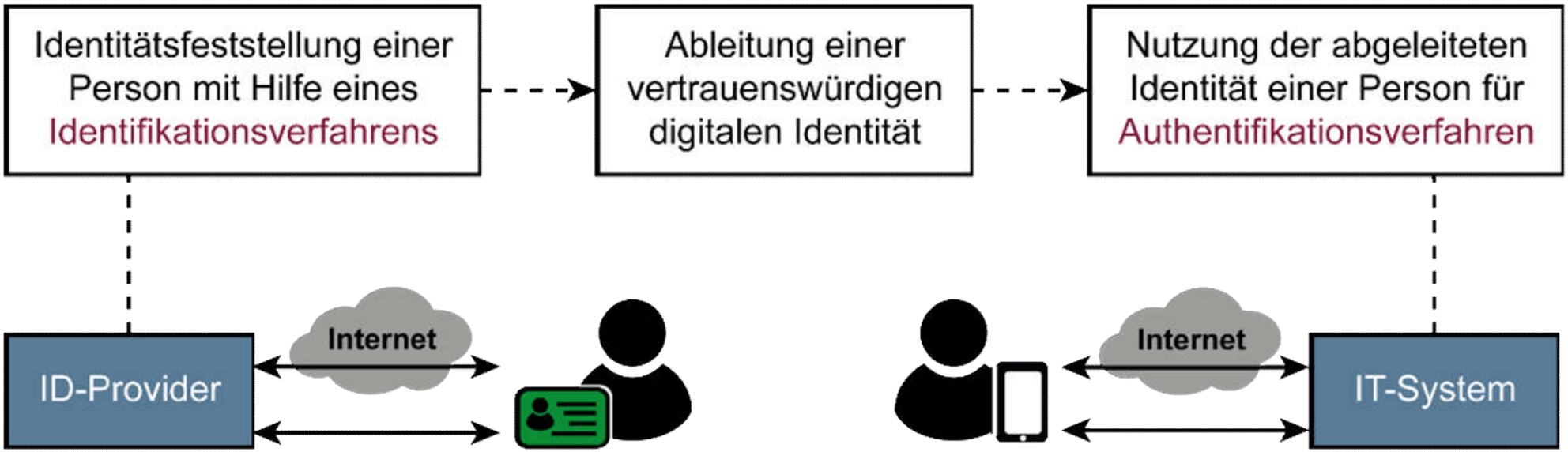
  - **Infrastruktur**, ***Verschlüsselung***, **Mechanismus zur Bestimmung von Vertrauens- und Sicherheitsniveaus**, ***Interaktion des Nutzers mit dem System*** *(Schnittstelle)*

  - **Protokolldefinition** zwischen der Kommunikation von Identity Provider zu Identity Provider und Identity Provider und Service

  - Berücksichtigung aktueller Protokolle, Technologien und Infrastruktur

  - **Ziel: Interoperabilität von Identity Systemen**

Ableitung einer vertrauenswürdigen → digitalen Identität



Anhang / Credits

Wir empfehlen

- **Kostenlose App securityNews**

securityNews

- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/channel/UCEMkHjW9dHcWfek_En3xhjg
-
- **Cybärcast – Der IT-Sicherheit Podcast**
  https://podcast.internet-sicherheit.de/

- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/

Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

Google+
https://plus.google.com/107690471983651262369/posts

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

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

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:

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

A. González Robles, N. Pohlmann: „Identity Provider zur Verifikation der vertrauenswürdigen digitalen Identität". In Proceedings der DACH Security 2014 Konferenz – Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven, Hrsg.: Peter Schartner, Peter Lipp; syssec Verlag, 2014

M. Hertlein, P. Manaras, N. Pohlmann: „Bring Your Own Device For Authentication (BYOD4A) – The Xign–System". In Proceedings of the ISSE 2015 - Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe 2015 Conference, Eds.: N. Pohlmann, H. Reimer, W. Schneider; Springer Vieweg Verlag, Wiesbaden 2015

M. Hertlein, P. Manaras, N. Pohlmann: „Die Zeit nach dem Passwort - Handhabbare Multifaktor-Authentifizierung für ein gesundes Eco-System", DuD Datenschutz und Datensicherheit – Recht

N. Pohlmann, R. Riedel: „Risikobasierte und adaptive Authentifizierung". In Proceedings der DACH Security 2018 Konferenz, syssec Verlag, 2018

Siehe: https://norbert-pohlmann.com/artikel/