

# OpenID trifft nPA

## Sichere Authentisierung im Internet

CeBIT 2011, Hannover  
Heise Forum – Sicherheit und IT-Recht  
Dienstag, 1. März 2011

Sebastian Feld, M.Sc.  
feld [at] internet-sicherheit [dot] de

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



if(is)  
internet-sicherheit.

- **Institut für Internet-Sicherheit**
- **Motivation**
- **Grundlagen**
  - OpenID
  - Neuer Personalausweis (nPA)
- **nPA-basierter OpenID-Provider**
- **Fazit**

- **Institut für Internet-Sicherheit**
- **Motivation**
- **Grundlagen**
  - OpenID
  - Neuer Personalausweis (nPA)
- **nPA-basierter OpenID-Provider**
- **Fazit**

### ■ Wer wir sind

- Eine innovative, unabhängige und wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen

### ■ Unsere Aufgaben

- Forschung, Entwicklung und anwendungsbezogene Lehre auf dem Gebiet der Internet-Sicherheit

### ■ Unser Team

- Ca. 50 wissenschaftliche Mitarbeiter, Diplomanden und Studenten

### ■ Unser Ziel

- Mehrwert an Vertrauenswürdigkeit und Sicherheit im Internet herstellen



### ■ Trusted Computing

- Sichere Betriebssysteme
- Network Access Control



### ■ Internet-Frühwarnsysteme

- Internet-Analyse
- Strukturelle Analyse des Internets



### ■ E-Mail-Sicherheit

- Anti-Spam
- E-Mail-Verlässlichkeit



### ■ Identity Management

- Neuer, elektronischer Personalausweis
- Studie IdMS-Konzept



### ■ Sonstige

- Mobile Security, VoIP, Web Services Security, Marktplatz IT-Sicherheit, Awareness

- Institut für Internet-Sicherheit
- **Motivation**
- Grundlagen
  - OpenID
  - Neuer Personalausweis (nPA)
- **nPA-basierter OpenID-Provider**
- **Fazit**



# Motivation

## → Das heutige Internet

- **Authentisierung im Internet**
  - Heutzutage: Login bei fast jedem Dienst nötig
  - Passwortverfahren: Viele Nachteile und Probleme
- **Digitale Identitäten**
  - Abbild der realen Welt: Soziale Netzwerke, ...
  - Notwendig: Möglichst sicherer Beweis der Identität
- **Vielfältige Technologien**
  - Passwort Safe, Single Sign-On (SSO), Starke Authentisierung, ...
  - Hier: Web SSO + Starke Authentisierung

# Motivation

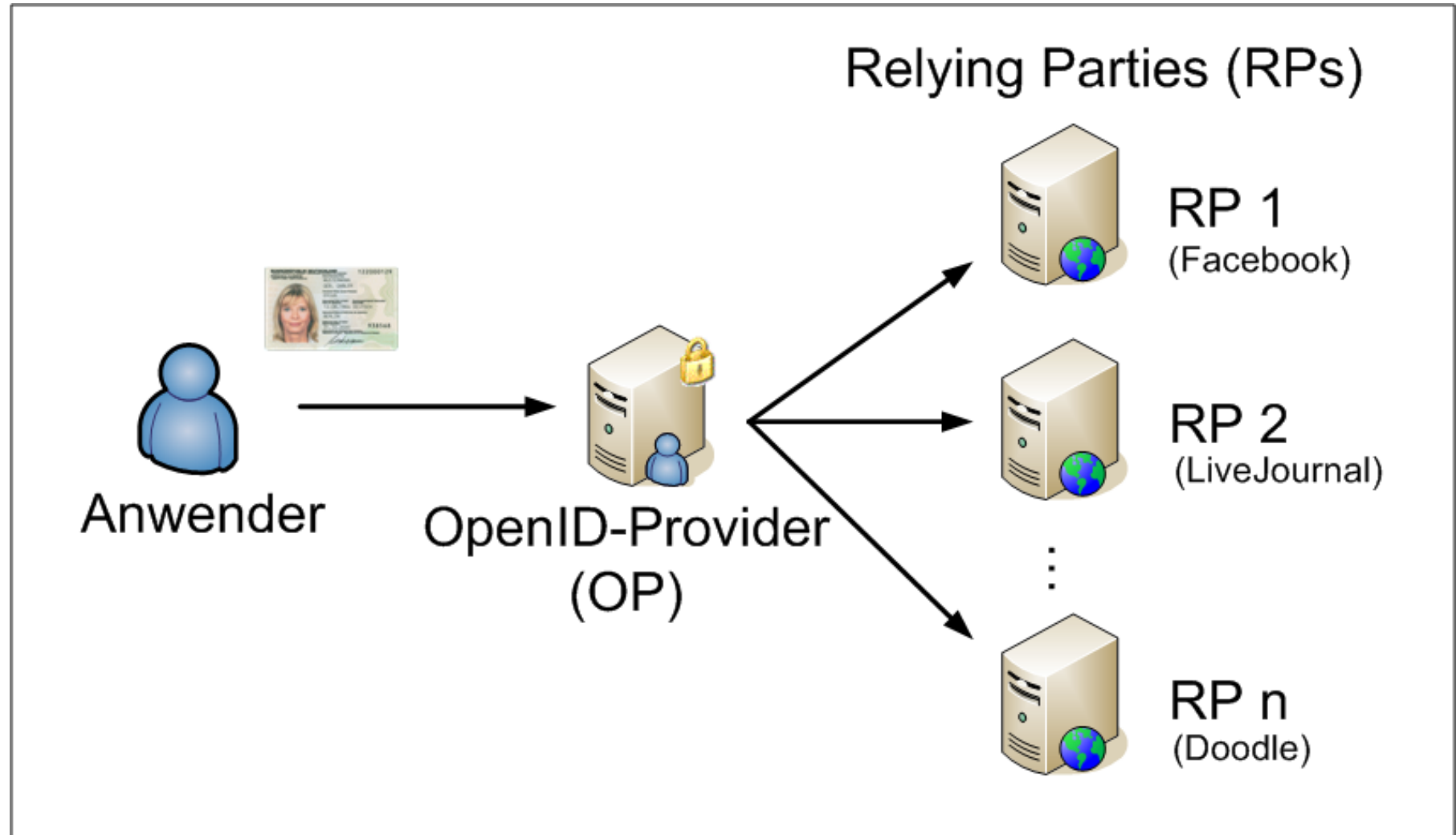
## → Kombination zweier Technologien

- **OpenID**
  - Recht junges Protokoll für Single Sign-On (SSO) im Internet
  - Viele Vorteile und Möglichkeiten, aber auch Herausforderungen und Probleme
  - Insbesondere: Phishing und Profilbildung
- **Neuer Personalausweis (nPA)**
  - Ausweis mit integriertem kontaktlosen Chip
  - Gegenseitige Authentisierung stellt einen Gewinn für vielfältige Anwendungen dar
- **Motivation**
  - Verbindung gegenwärtig vollkommen getrennter Themenbereiche
  - Kombination generiert wechselseitig Mehrwerte

- **Institut für Internet-Sicherheit**
- **Motivation**
- **Grundlagen**
  - **OpenID**
  - **Neuer Personalausweis (nPA)**
- **nPA-basierter OpenID-Provider**
- **Fazit**

# Grundlagen

## → OpenID: Gesamtbild



# Grundlagen

## → OpenID: URL-basierter Ansatz

Username:

Passwort:

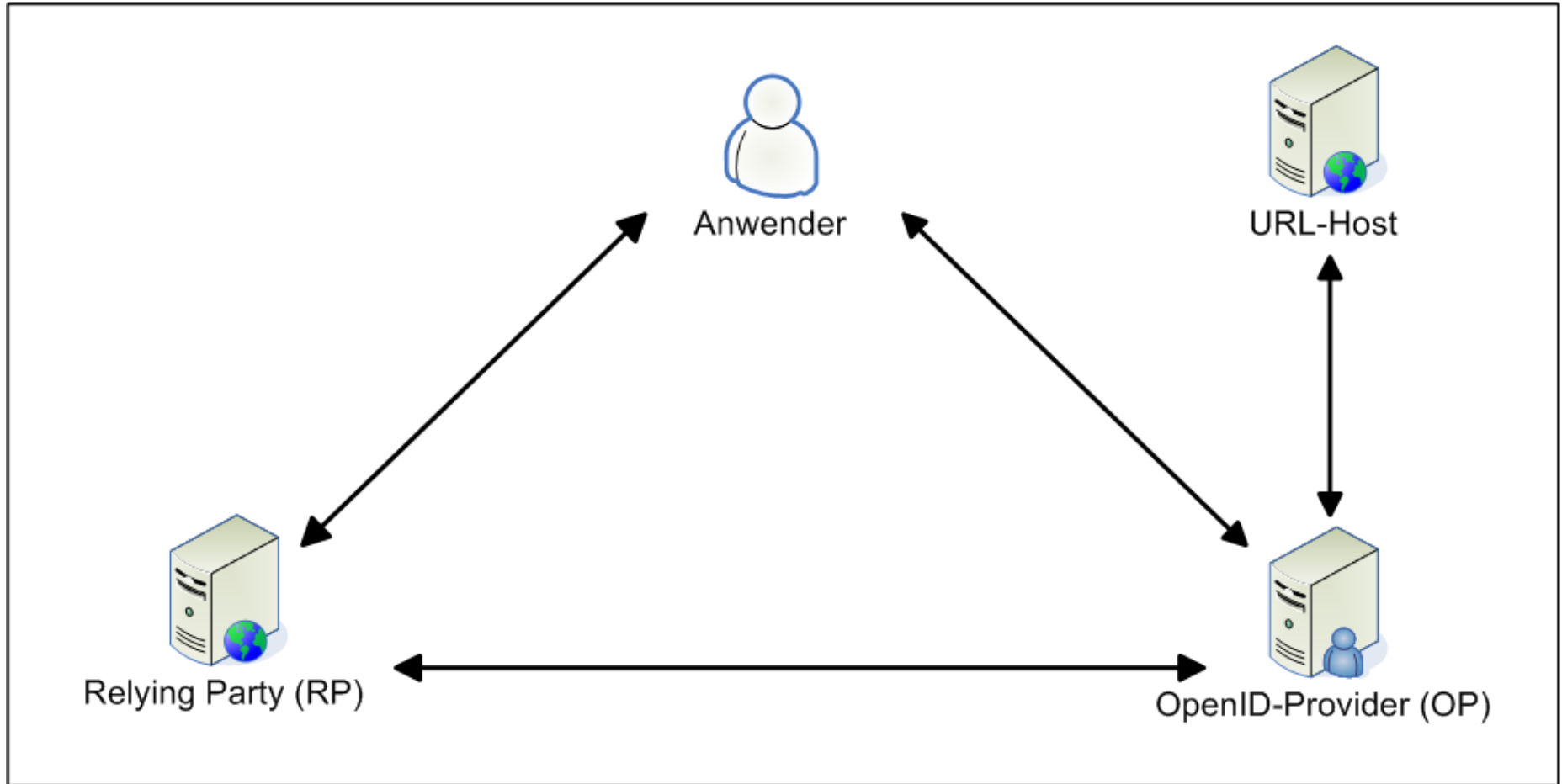
Login

OpenID URL:

Login

# Grundlagen

## → OpenID: Protokollablauf



# Grundlagen

## → OpenID: Überblick

### ■ Web Single Sign-On (Web-SSO)

- URL-“Besitz“ bestimmt Identität
- Dezentraler Mechanismus
- Identitätenverwalter frei wählbar

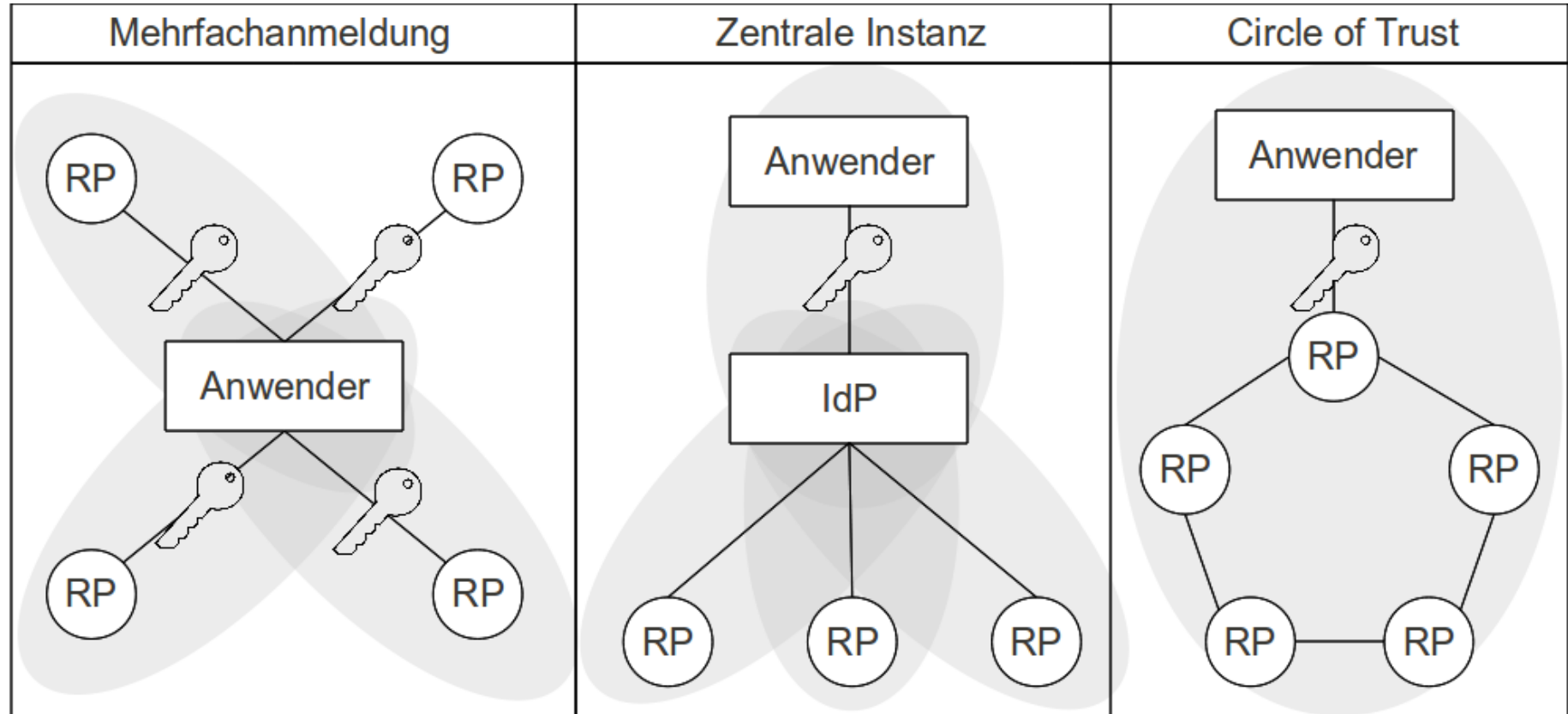
<https://openid.internet-sicherheit.de/sfeld>

### ■ Art der Authentisierung

- Im Standard nicht spezifiziert
- Verantwortung liegt beim Identitätenverwalter (und Anwender)
- ~~Benutzername/Passwort~~      Digitale Zertifikate

### ■ Anwendungsbereich

- Im Privatumfeld, aber auch
- im Geschäftsbereich denkbar



- **Institut für Internet-Sicherheit**
- **Motivation**
- **Grundlagen**
  - OpenID
  - **Neuer Personalausweis (nPA)**
- **nPA-basierter OpenID-Provider**
- **Fazit**

# Grundlagen

## → Neuer Personalausweis (nPA)

### ■ Ausprägung des nPAs

- Kontaktloser Chip (ähnlich ePass)
- Kryptoprozessor
- Kartenlesegerät
- Bürgerclient      AusweisApp
- Freischaltung durch PIN



### ■ Drei elektronische Funktionalitäten

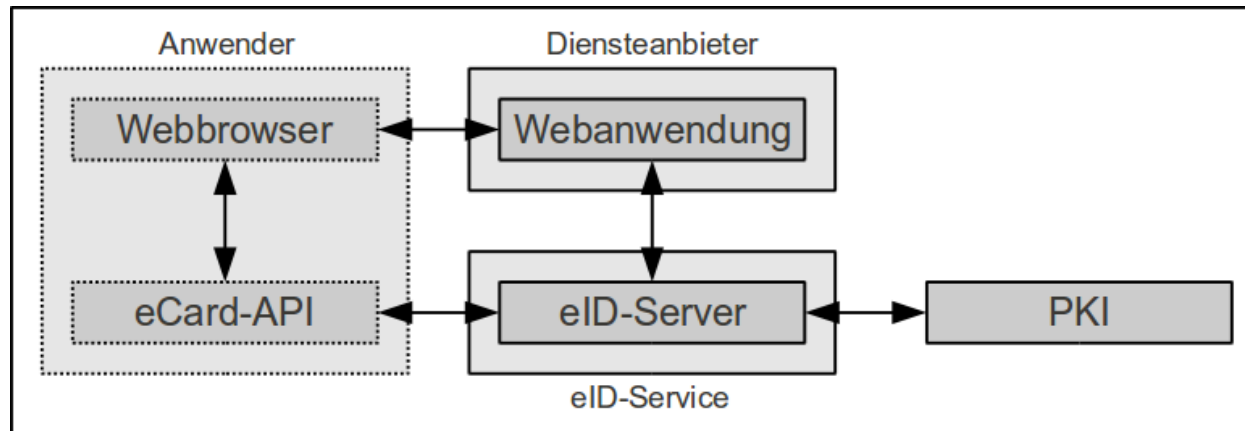
- ePass      hoheitlich
- Online-Authentisierung      eBusiness & eGovernment
- Qualifizierte, elektronische Signatur      eBusiness & eGovernment

# Grundlagen

## → Online-Authentisierung (eID-Funktion)

### ■ Funktionalität

- Identitätsfeststellung / authentische Übertragung von Attributen
- Gegenseitige Authentisierung wie in der realen Welt



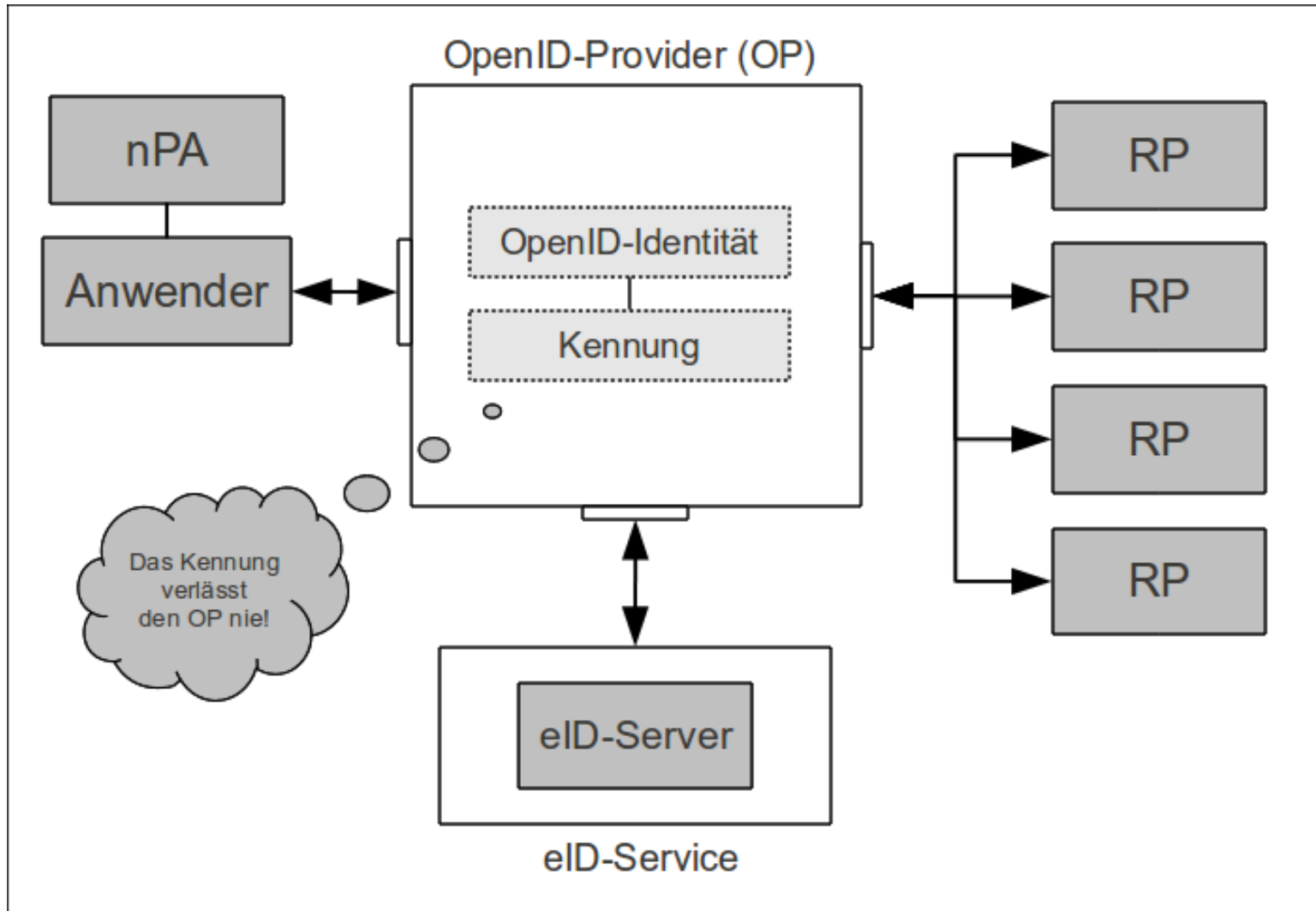
### ■ „Wiedererkennen eines bereits registrierten Anwenders“

- Verwendung der Seriennummer rechtlich nicht zulässig
- Lösung: Dienste- und kartenspezifische Kennung

- **Institut für Internet-Sicherheit**
- **Motivation**
- **Grundlagen**
  - OpenID
  - Neuer Personalausweis (nPA)
- **nPA-basierter OpenID-Provider**
- **Fazit**

# nPA-basierter OpenID-Provider

## → Grobkonzept und Schnittstellen



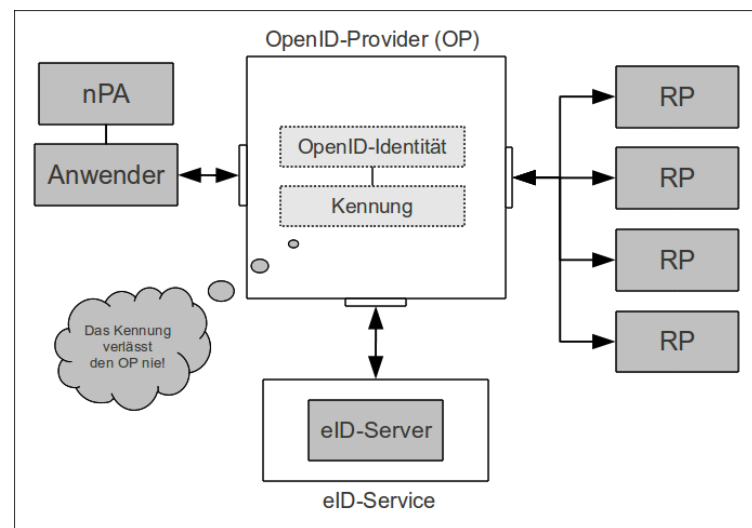
# nPA-basierter OpenID-Provider → 2 grundlegende Ideen

## ■ Beweis des URL-Besitzes

- Starke Authentisierung statt Passwortverfahren (Phishing)
- Verknüpfung der Kennung mit OpenID-Identität

## ■ Proxy-Funktionalität

- Gewisse „Internationalisierung der eID-Funktion
- Erweiterte Nutzungsmöglichkeit des nPAs



# nPA-basierter OpenID-Provider → Mehrwerte

- **Genereller Mehrwert durch OpenID**
  - Zentralisierung: Identität, Informationen, Berechtigungsnachweis
  - Sicherung: Bewusstere Wahl bei Identitätenverwalter/ Auth.Methode
- **OpenID-Protokoll wird sicherer gestaltet**
  - Anwender kann keine schwachen Passwörter mehr wählen
  - Haupt-Problem Phishing ist nicht mehr gegeben
  - Authentisierung des OpenID-Providers (durch eID-Funktion)
- **Mehrwert für Anwender und Dienste**
  - Bereitgestellte Infrastruktur für Web-SSO und Multi-Faktor-Auth.
- **Aus Sicht des neuen Personalausweises**
  - Gewisse „Internationalisierung“ der eID-Funktion
  - Proxy-Funktion ermöglicht Einsatz des nPAs im persönlichen Umfeld

- **Institut für Internet-Sicherheit**
- **Motivation**
- **Grundlagen**
  - OpenID
  - Neuer Personalausweis (nPA)
- **nPA-basierter OpenID-Provider**
- **Fazit**

# Fazit

## → Zusammenfassung und Ausblick

### ■ Zusammenfassung

- Wachsende Bedeutung: Identity Management im Internet
  - Notwendigkeit des sicheren Identitätsnachweis (Authentisierung)
- Kombination von OpenID und der eID-Funktion
  - Kompensation der Schwächen von OpenID
  - Generierung verschiedener Mehrwerte
- Erster seiner Art: OpenID-Provider mit nPA-Unterstützung

### ■ Ausblick

- Schnelle Entwicklung von Web-Standards und „sozialen“ Protokollen
  - OpenID Connect
- Seit November 2010: Ausgabe des nPAs
  - Noch sehr wenige Möglichkeiten / Diensteanbieter



Fachhochschule  
Gelsenkirchen

# OpenID trifft nPA

**Sichere Authentisierung im Internet**

CeBIT 2011, Hannover  
Heise Forum – Sicherheit und IT-Recht  
Dienstag, 1. März 2011

Halle 9  
Stand D06

**Vielen Dank für Ihre Aufmerksamkeit!**  
**Bestehen Fragen ?**

**Sebastian Feld, M.Sc.**  
**feld [at] internet-sicherheit [dot] de**

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

**if(is)**  
internet-sicherheit.