

# Lessons Learned

## Ein OpenID-Provider unterstützt den neuen Personalausweis

CeBIT 2011, Hannover  
Heise Future Talk  
Freitag, 4. 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.

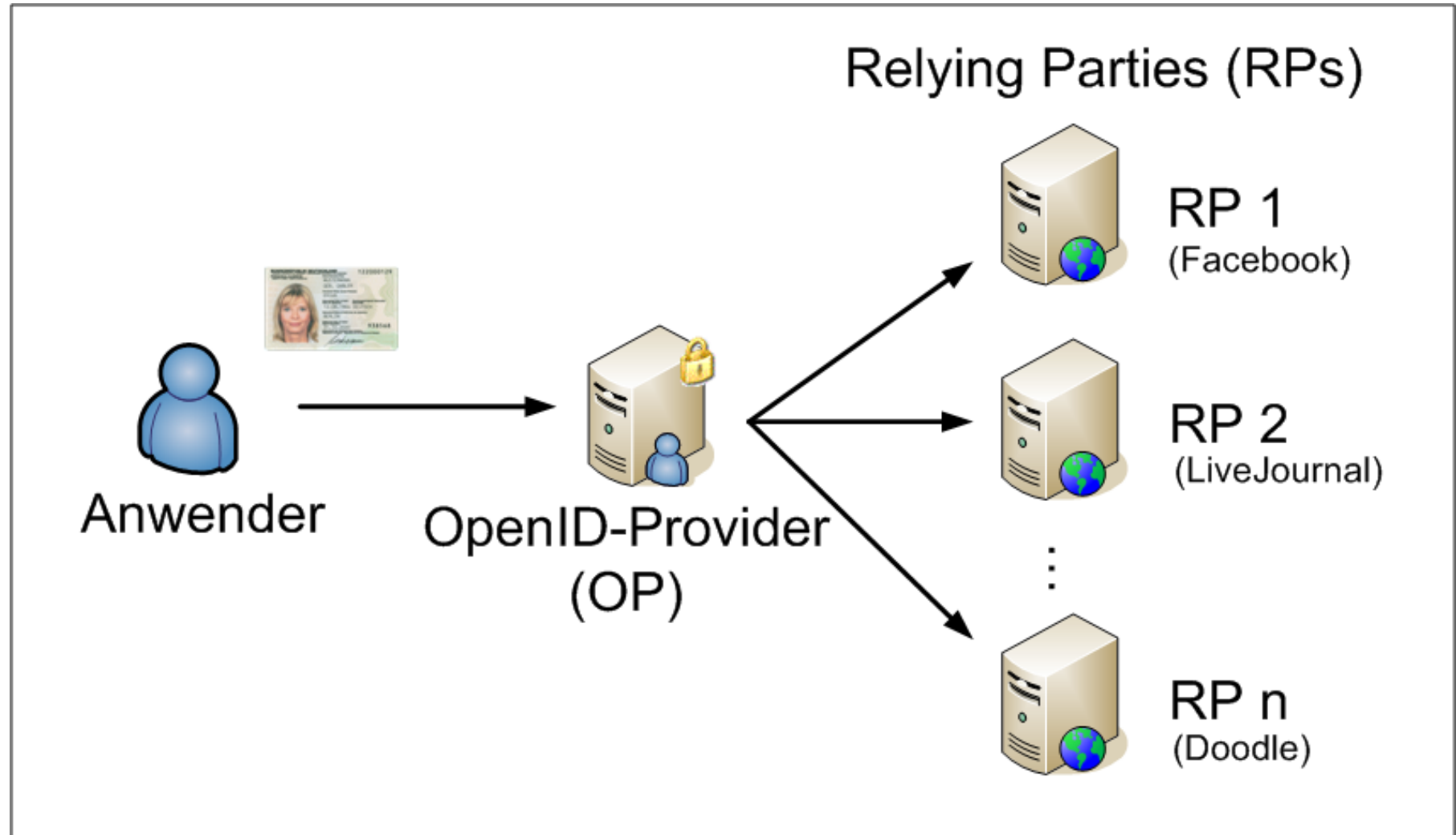
- **Motivation**
- **Grundlagen**
  - OpenID
  - Neuer Personalausweis (nPA)
- **nPA-basierter OpenID-Provider**
- **Sicherheitsbetrachtung von OpenID**
- **Fazit**

# Motivation

- **OpenID**
  - 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
  - Vermutung: Kombination generiert wechselseitig Mehrwerte

# Grundlagen

## → OpenID: Gesamtbild



# 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

### ■ Nutzen

- Einmaliger Login mit OpenID
- Anschließende Nutzung aller Dienste mit OpenID-Unterstützung

# Grundlagen

## → Neuer Personalausweis (nPA)

### ■ Ausprägung des nPAs

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



### ■ Drei elektronische Funktionalitäten

- ePass
- Online-Authentisierung
- Qualifizierte, elektronische Signatur

hoheitlich

eBusiness & eGovernment

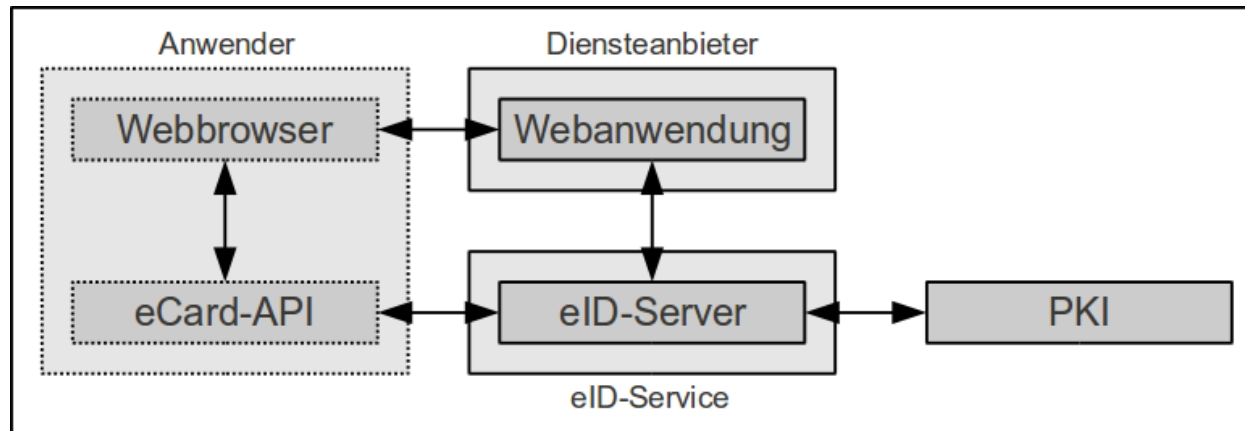
eBusiness & eGovernment

# Grundlagen

## → Online-Authentisierung (eID-Funktion)

### ■ Funktionalität

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

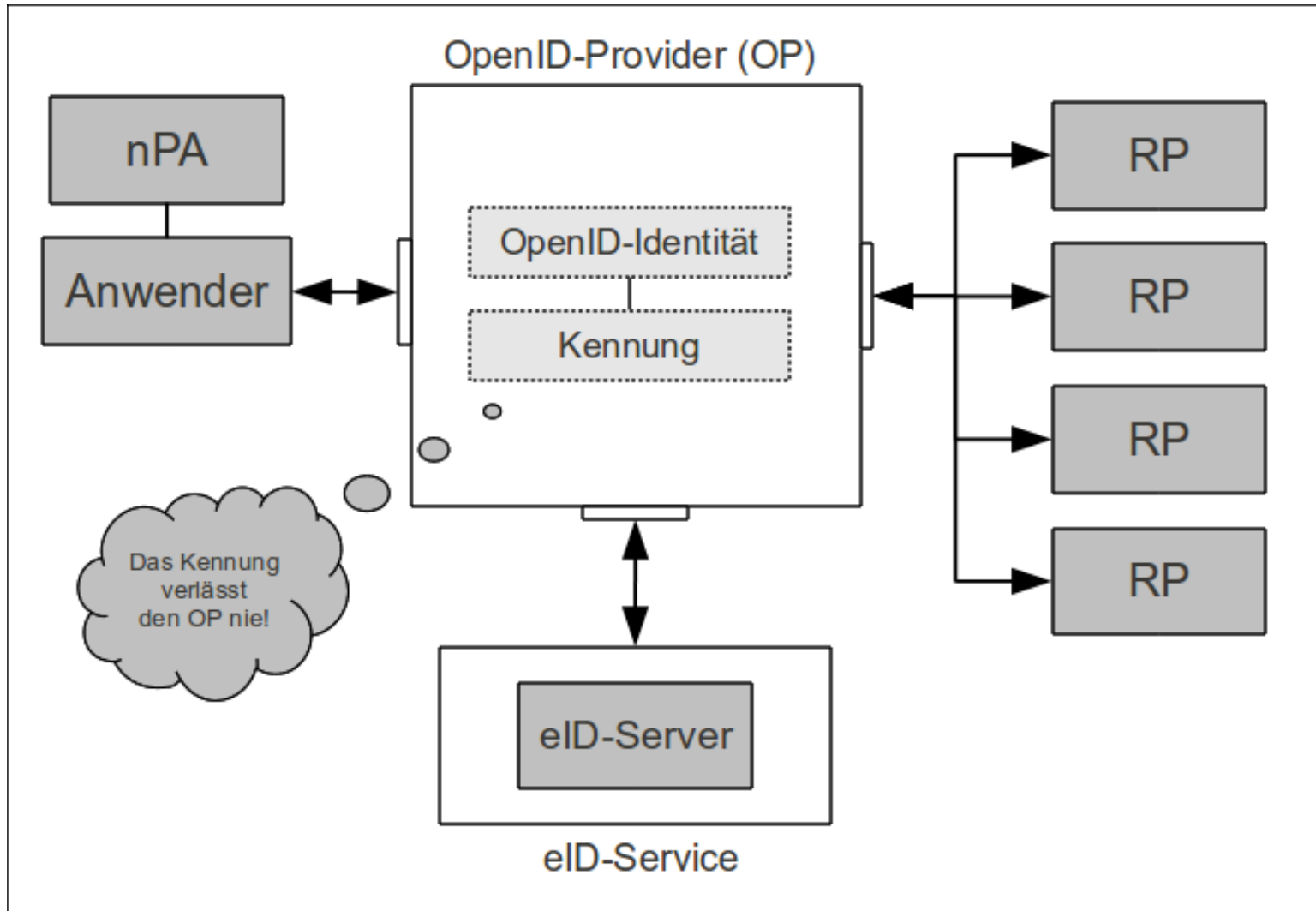


### ■ „Wiedererkennen eines bereits registrierten Anwenders“

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

# nPA-basierter OpenID-Provider

## → Grobkonzept und Schnittstellen



# 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

# Sicherheitsbetrachtung von OpenID

## → Motivation

### ■ Problematik

- OpenID ist ein lebendiges Protokoll, viele Tests und Untersuchungen
- Ergebnisse und Informationen sehr dezentral und schwer zu erfassen
  - Einzelne Aspekte in Blogeinträge
  - Viele Ideen in Blogkommentare
- Viel Literatur zu Schwachstellen, wenig Informationen zur Behebung

### ■ Lösungsvorschlag

- Sicherheitsbetrachtung über Grenzen der Spezifikation hinweg
- Strukturierte Aufbereitung
- Integration von Handlungsempfehlungen
- Kurze Diskussion der Restrisiken

### ■ Aspekte beziehen sich auf...

- Die Spezifikation von OpenID
- OpenID als Web-basierte Technologie
- OpenID als SSO-System
- „Soziale“ Probleme

### ■ Erkenntnisse

- Viele Aspekte können durch den Einsatz des nPAs behoben werden
- Einige Handlungsempfehlungen auf gewisse Weise widersprüchlich (Abwägung zwischen Sicherheit und Komfort)

## ■ **OpenID-Protokoll**

- Schlank, aber: Der Teufel steckt im Detail
- Viele Funktionen im Internet statt in der Spezifikation beschrieben

## ■ **nPA-basierter OpenID-Provider**

- Erstmalige Verknüpfung von OpenID und nPA generiert Mehrwerte
- Durch Programmierung wird der Aufwand nachvollziehbar

## ■ **Sicherheitsbetrachtung von OpenID**

- Probleme auf verschiedenen Ebenen
- Nicht zuletzt: Faktor Vertrauen
- Ergänzung des praktischen und theoretischen Teils

## Lessons Learned

### Ein OpenID-Provider unterstützt den neuen Personalausweis

CeBIT 2011, Hannover  
Heise Future Talk  
Freitag, 4. 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.