

# Ein OpenID-Provider mit Proxy-Funktionalität für den nPA

→ D-A-CH Security 2010

Sebastian Feld, Norbert Pohlmann  
[feld | pohlmann] @ internet - sicherheit . de

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



if(is)  
internet-sicherheit.

# Agenda

→ Ein OpenID-Provider mit Proxy-Funktionalität für den nPA

- Motivation
- OpenID
- Sicherheitsbewertung
- Neuer Personalausweis (nPA)
- OpenID-Provider (OP) mit nPA-Unterstützung
- Zusammenfassung

# Motivation

→ Ein OpenID-Provider mit Proxy-Funktionalität für den nPA

## ***Identitäten im Internet immer wichtiger***

- Identifikator mit Attributen und Informationen einer Person
- Notwendigkeit: Möglichst sichere Gestaltung des Beweises der Identität
- Verstreute, redundante Identitäten mit versch. Identifikatoren und Passwörtern

## ***Offene Standards für Single Sign-On im Internet***

- OpenID als einfache Möglichkeit
- Schwächen des Protokolls müssen kompensiert werden

## ***Einsatz starker Authentisierung***

- eID-Funktion des neuen Personalausweises (nPA)
- Generierung von Mehrwerte in verschiedener Hinsicht



### *Web Single Sign-On*

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

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

### *Art der Authentisierung*

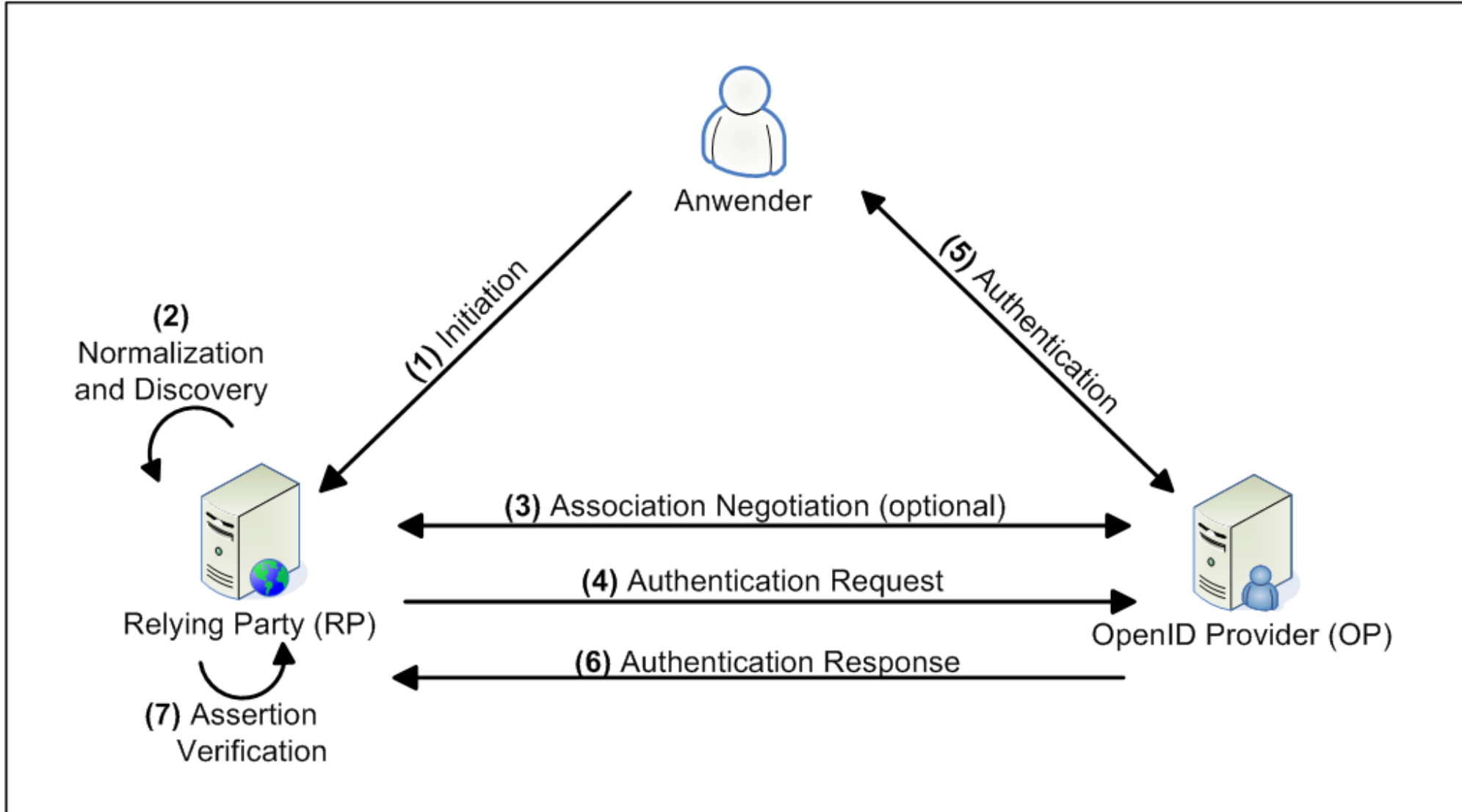
- Im Standard nicht spezifiziert
- Liegt beim Identitätsverwalter
- ~~Benutzername/Passwort~~      Digitale Zertifikate

### *Nutzen*

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

# OpenID

## → Protokollablauf



# Sicherheitsbewertung (1/2)

## → Schritte 0-4

### ***Identifier Creation***

- Vorsicht bei Wahl eines vertrauenswürdigen OPs / Eingabe persönlicher Informationen

### ***Normalization/Discovery***

- Definition von Zeit- und Datenlimits für Discovery-Prozess
- Einschränkung der Protokolle und Ports

### ***Association Negotiation***

- Forcierte Nutzung einer Transportverschlüsselung (SSL/TLS)
- Definition von Beschränkungen und Limits zur Vorbeugung von DoS-Angriffen

### ***Authentication Request***

- Gezielte Einschränkung des Realms
- Nicht anbieten/nutzen: „Automatisiertes Vertrauen“
- Prüfung der return\_to-URL

# Sicherheitsbewertung (2/2)

## → Schritte >4

### ***Authentication***

- Einsatz starker Authentisierung zur Verhinderung von Phishing
- Löschung temporärer Daten über verwendete Dienste und Frequenz der Nutzung

### ***Authentication Response***

- Einsatz von Nonces und Timestamps gegen Replay-Angriffe
- Problem: Angreifer kann „schneller“ als das Opfer sein

### ***Assertion Verification***

- Signaturprüfung und Nachhalten der Nonces
- Prüfung, ob OP autorisiert zur Ausgabe von Assertions ist

### ***Weitere Angriffe, Bedenken und Ideen***

- Angriffe auf die Namensauflösung (→ Starke Authentisierung)
- ...

# Neuer Personalausweis (nPA) → Überblick

## Ausprägung des nPA

- Kontaktloser Chip, RF-Lesegerät
- Bürgerclient AusweisApp + PIN



## Drei elektronische Funktionalitäten

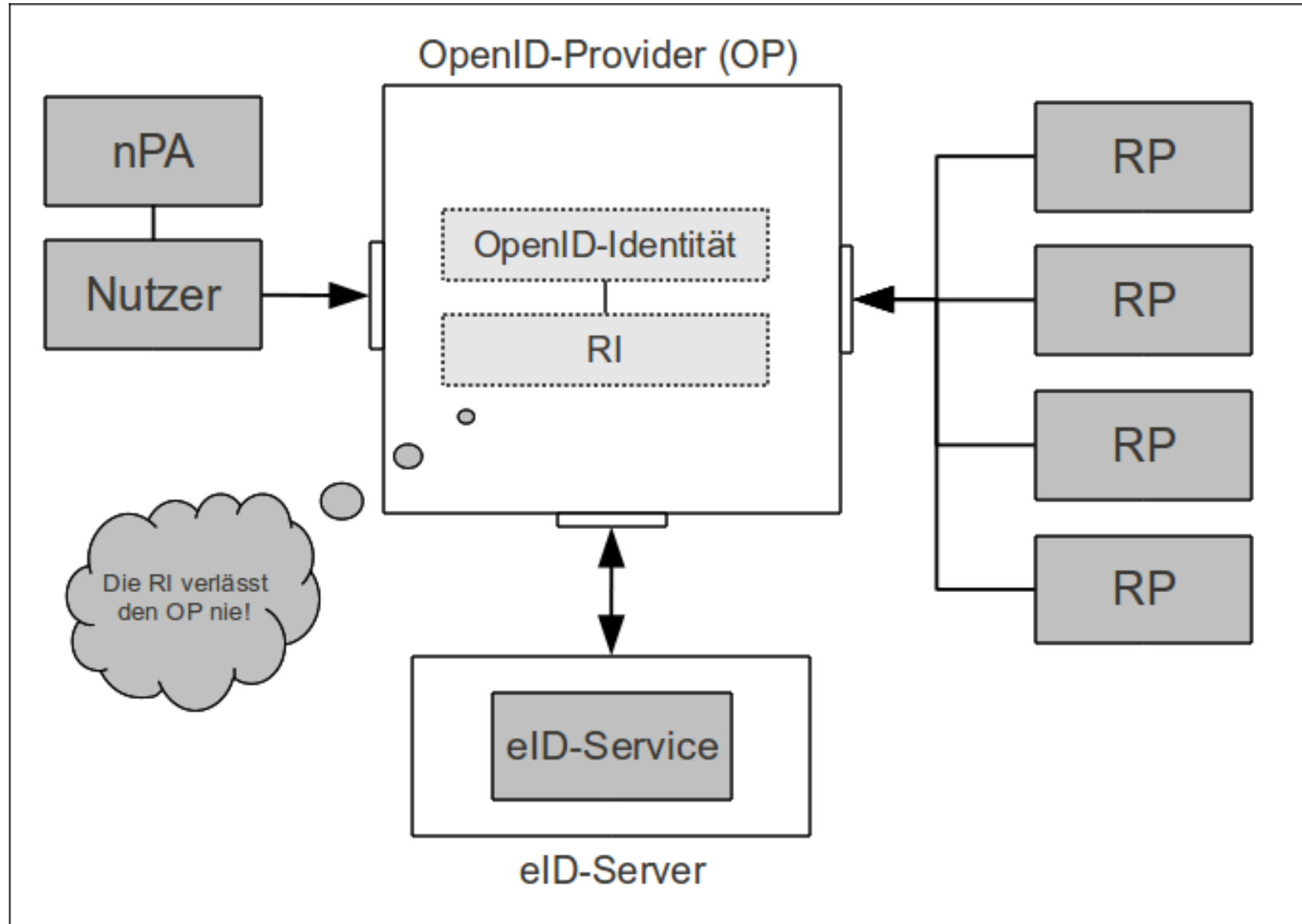
- ePass hoheitlich
- Online-Authentisierung eBusiness & eGovernment
- Qualifizierte elektronische Signatur eBusiness & eGovernment

## Restricted Identification (RI)

- Innerhalb eines Sektors ist die RI jedes Chips eindeutig
- Es ist praktisch (rechnerisch) unmöglich, die RI eines Chips zwischen zwei Sektoren zu verbinden

# OP mit nPA-Unterstützung

## → Konzept und Schnittstellen



# Zusammenfassung

## → Mehrwerte eines OPs mit nPA-Unterstützung

### ***Genereller Mehrwert durch OpenID***

- Zentralisierung: Identität, Informationen, Credentials
- Sicherung: Bewusstere Wahl bei Identitätsverwalter / Authentisierungsmethode

### ***OpenID-Protokoll wird sicherer gestaltet***

- Nutzer kann keine schwachen Passwörter mehr wählen
- Haupt-Problem Phishing ist nicht mehr gegeben
- Authentisierung des OpenID-Providers (durch eID-Funktion)

### ***Mehrwert für Nutzer und Dienste***

- Bereitgestellte Infrastruktur für Web-SSO und Multi-Faktor-Authentisierung

### ***Aus Sicht des neuen Personalausweises***

- Gewisse „Internationalisierung“ der eID-Funktion
- Proxy-Funktion ermöglicht Einsatz des nPA im persönlichen Umfeld

# Ein OpenID-Provider mit Proxy-Funktionalität für den nPA

→ D-A-CH Security 2010

Vielen Dank für Ihre Aufmerksamkeit  
Fragen ?

Sebastian Feld, Norbert Pohlmann  
[feld | pohlmann] @ internet - sicherheit . de

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



if(is)  
internet-sicherheit.