

Security analysis of OpenID, followed by a reference implementation of an nPA- based OpenID provider

Sebastian Feld, Norbert Pohlmann

Institute for Internet-Security, if(is)
Gelsenkirchen University of Applied Sciences
{feld | pohlmann}@internet - sicherheit . de

Agenda

- Motivation
- OpenID
- Security evaluation
- German new electronic identity card (nPA)
- OpenID provider (OP)
- Summary and Outlook

Motivation

Access information for IT systems

- Services (on the Internet): First Login, then utilization
- More and more in private and business environment
- User name and password: The „password dilemma“

Different approaches for remedy

- Password Safe, Single Sign-On, Strong Authentication, ...
- This talk: Web SSO + Strong Authentication
 - OpenID
 - German new electronic identity card (nPA)

OpenID: Overview

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

At a glance...

- URL-based, decentralized, open
- Type of authentication is not specified

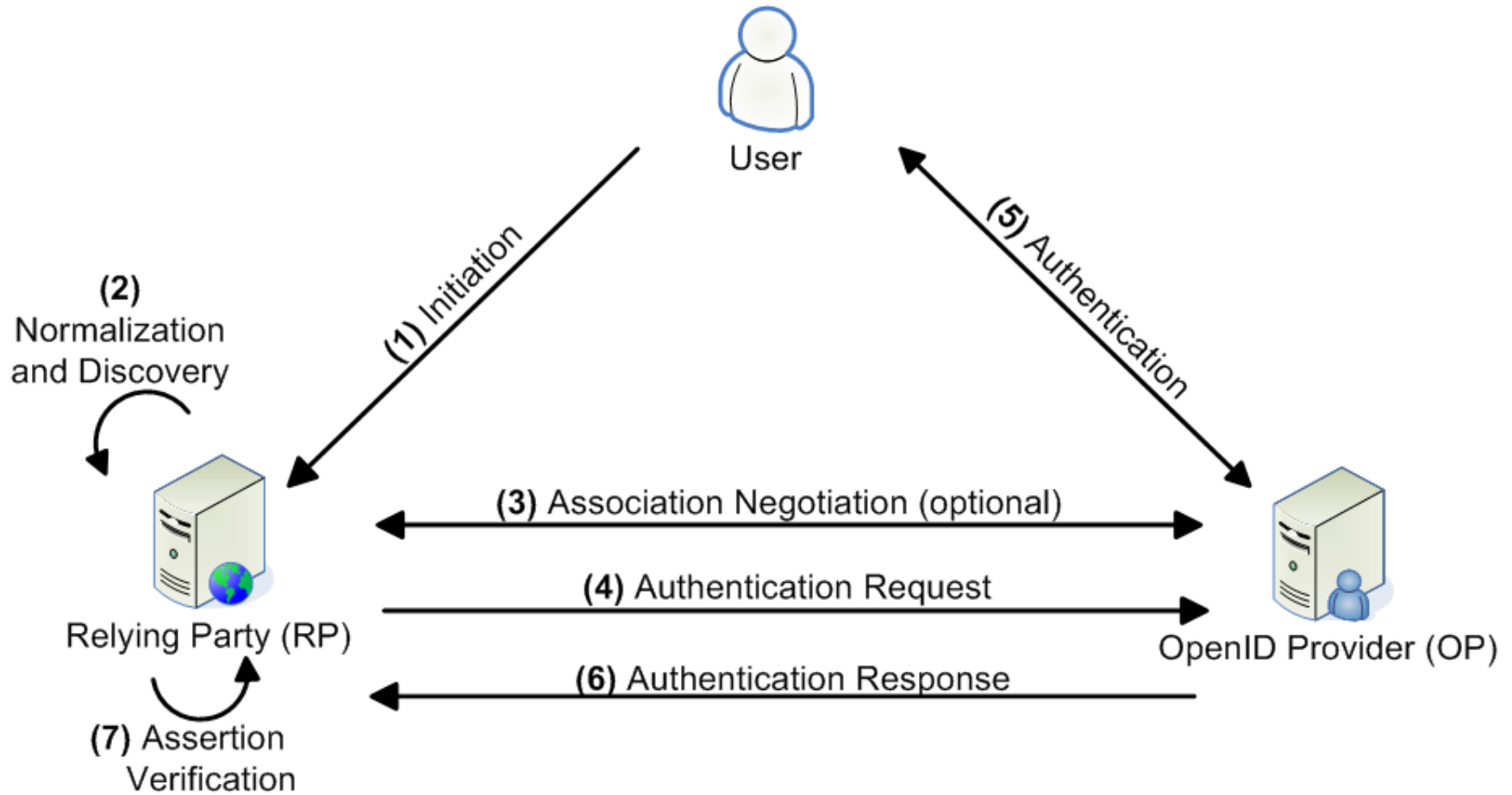
Benefit

- One-time login with OpenID identity
- Subsequent use of any OpenID-supporting services

Possible fields of application

- Personal websites
- Commercial service provider
- Business environment

OpenID: Course of the protocol



Security evaluation (1/2)

Central issue 1: Phishing

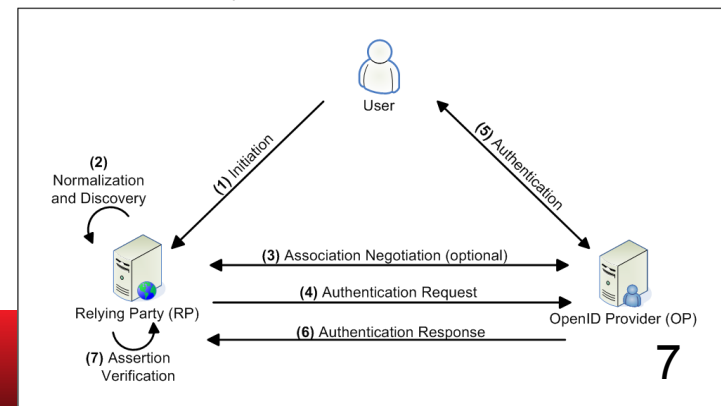
- Authentication Request: Simple HTTP redirect
- Relying Party sends user to fake OpenID provider
- Strong Authentication as a remedy

Central issue 2: Profiling

- OpenID provider (OP): Central authority for the user's logins
 - Knowledge of the services utilized
 - Knowledge of the frequency of use
- Temporary data unavoidable
- Human factor ,trust', mandatory policies, certification, ...

Security evaluation (2/2)

- Choice of the OP: Different aspects of trust
- Entering personal information: full profile vs. pseudonym
- DoS attack on RP (Discovery)
- MITM attack (Association)
- Overly-generalized Realm (Authentication Request)
- Replay attack (Authentication Response)
- OP-Discovery (Assertion Verification)
- Attacking the DNS (Discovery and Redirects)



nPA: Overview

Motivation

- Introduction: November 1, 2010
- Supports the Federal Government's eCard strategy

Basic goal

- Expand the conventional use to the electronic world
- Secure and legally binding communication on the Internet

Three electronic functions

- ePass
- eID feature (Online Authentication)
- Qualified electronic Signature (QES)



nPA: Restricted Identification (RI)

Recognition of an already registered user

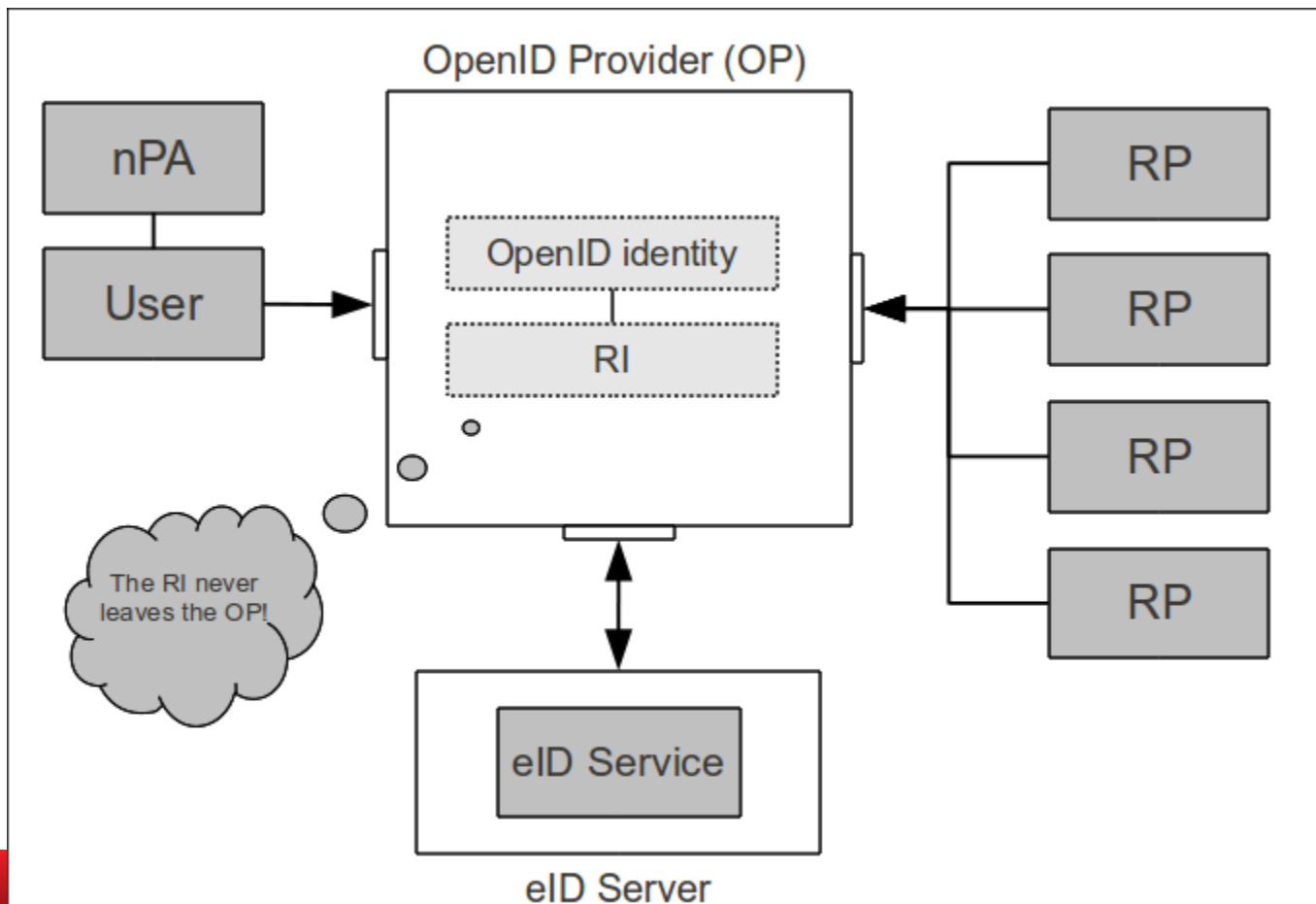
- nPA's specification provides recognition
- Identification using serial number is legally not permitted
- Sector-specific identification

Two special properties

1. RI of a chip is unique within a sector
 - Recognizing a user without knowing the actual identity
2. Practical impossibility to connect the chip's RI between two sectors
 - No association of persons beyond application boundaries

OP: Fundamental Concept

1. Proof of the possession of a URL
2. Proxy functionality for the new German identity card



OP: Added value (1/2)

Overall

- Proof of identity only at a single point
 - More conscious choice of OP
 - concentrated effort for secure configuration

Perspective: OpenID

- Non-specified authentication made more secure
 - Weak passwords and Phishing no longer possible
 - Authentication of the OpenID provider

OP: Added value (2/2)

Perspective: User

- Provided infrastructure for Web SSO and Strong Authentication
- RI never leaves the OP
 - Data avoidance and data economy are met

Perspective: nPA

- Certain „internationalization“ of the eID feature

Perspective: Service Provider

- “Outsourcing” of authentication
- Use of the nPA’s eID function via the proxy functionality

Summary and Outlook

Summary

- Growing importance: Identity Management on the Internet
 - Need for secure proof of identity
- Combination of OpenID and the eID feature
 - Compensating the weaknesses of OpenID
 - Generating added value
- First of its kind: OpenID provider with nPA support

Outlook

- Rapid development of web standards and „social“ protocols
 - OpenID Connect
- November 1, 2010: Issue of the nPA
 - Difficult estimation of reaction and acceptance

Security analysis of OpenID, followed by
a reference implementation of an nPA-
based OpenID provider

Any questions?

Sebastian Feld, Norbert Pohlmann

Institute for Internet-Security, if(is)
Gelsenkirchen University of Applied Science
{feld | pohlmann}@internet - sicherheit . de