

Authentication in the Cloud using OpenID and the German ID card

**The European e-Identity Management Conference
Session: Identity in the Cloud
Tallinn, Estonia, 9th June 2011**

Sebastian Feld, M.Sc.

Norbert Pohlmann, Prof. Dr. (TU NN)

[feld|pohlmann] @ internet - sicherheit . de

Institute for Internet Security – if(is)

University of Applied Sciences, Gelsenkirchen

<https://www.internet-sicherheit.de>

if(is)

- Institute at the FHGe
- Established 2005, ~ 50 employees
- Research, development, teaching

Research areas (selection)

- IdM study, IT-AmtBw
- Residual risk analysis German ID card, BMI
- Internet Key Figure System, BMWi
- FISHA project, EU funded
- Internet Early Warning, Trusted Computing, Mobile Security, Live Hacking Shows, Penetration Testing, ...

Motivation

OpenID

German new electronic identity card (nPA)

nPA-based OpenID Provider

Excursus: Trust Framework

Conclusion

Motivation

OpenID

German new electronic identity card (nPA)

nPA-based OpenID Provider

Excursus: Trust Framework

Conclusion

Motivation

Digital emigration

- Outsourced infrastructure, services, but identities as well
- Private and business environment (Public/Private Cloud)
- Accessing information or services: First login, then utilization

Two problems

- Lots of identities (identifier, credentials, information)
- Identities getting more valuable and thus more worthy of protection

Different approaches

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

Motivation

OpenID

German new electronic identity card (nPA)

nPA-based OpenID Provider

Excursus: Trust Framework

Conclusion

OpenID: Overview

At a glance ...

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

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

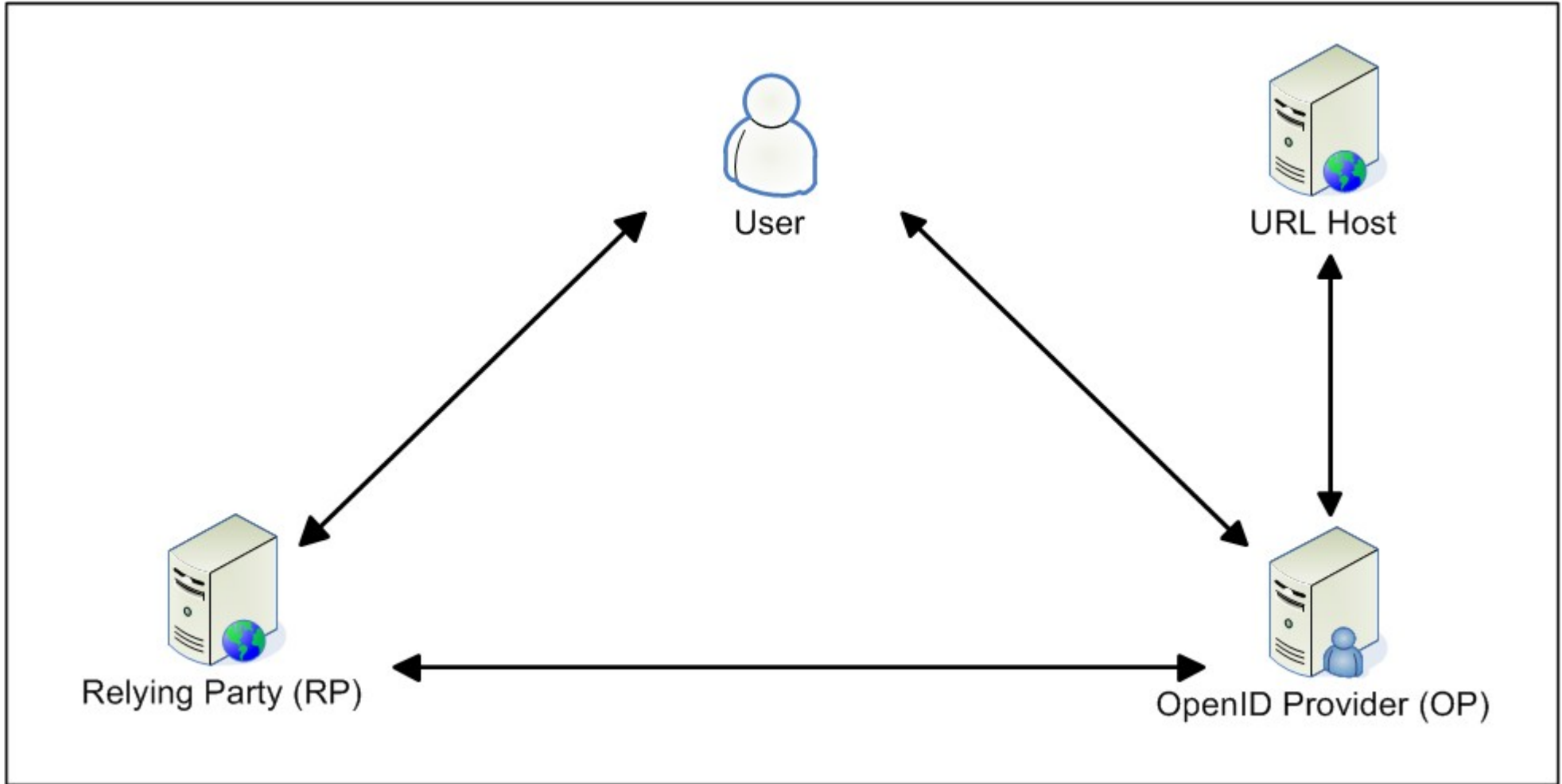
Benefit

- One-time login with OpenID identity
- Subsequent use of any OpenID-supporting services
- Authentication in the Cloud

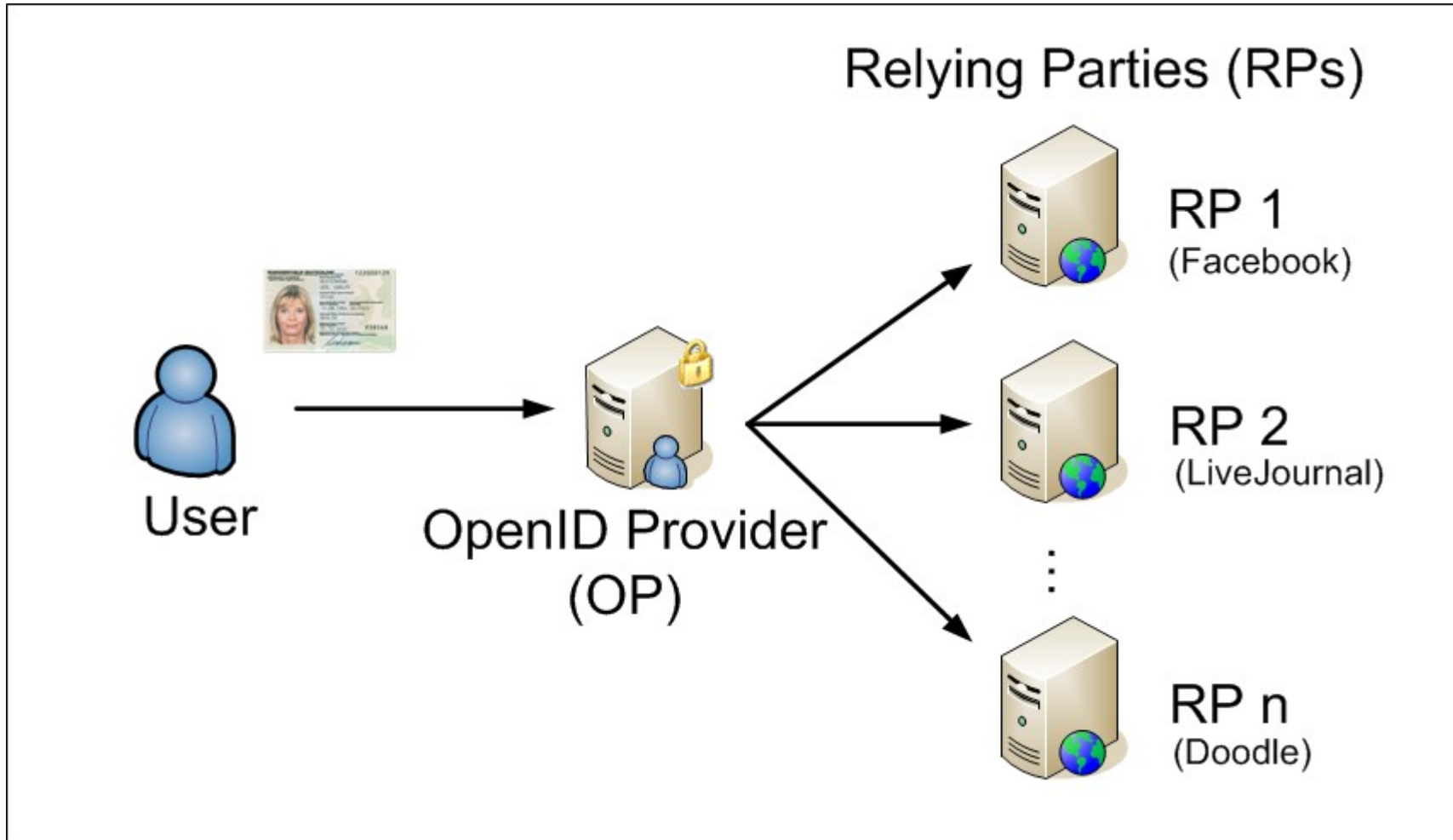
Possible fields of application

- Personal websites
- Commercial service provider (eGovernment as well)
- Business environment (e.g. Private Cloud)

OpenID: Course of the protocol



OpenID: Overall picture



Agenda

Motivation

OpenID

German new electronic identity card (nPA)

nPA-based OpenID Provider

Excursus: Trust Framework

Conclusion

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

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

Motivation

OpenID

German new electronic identity card (nPA)

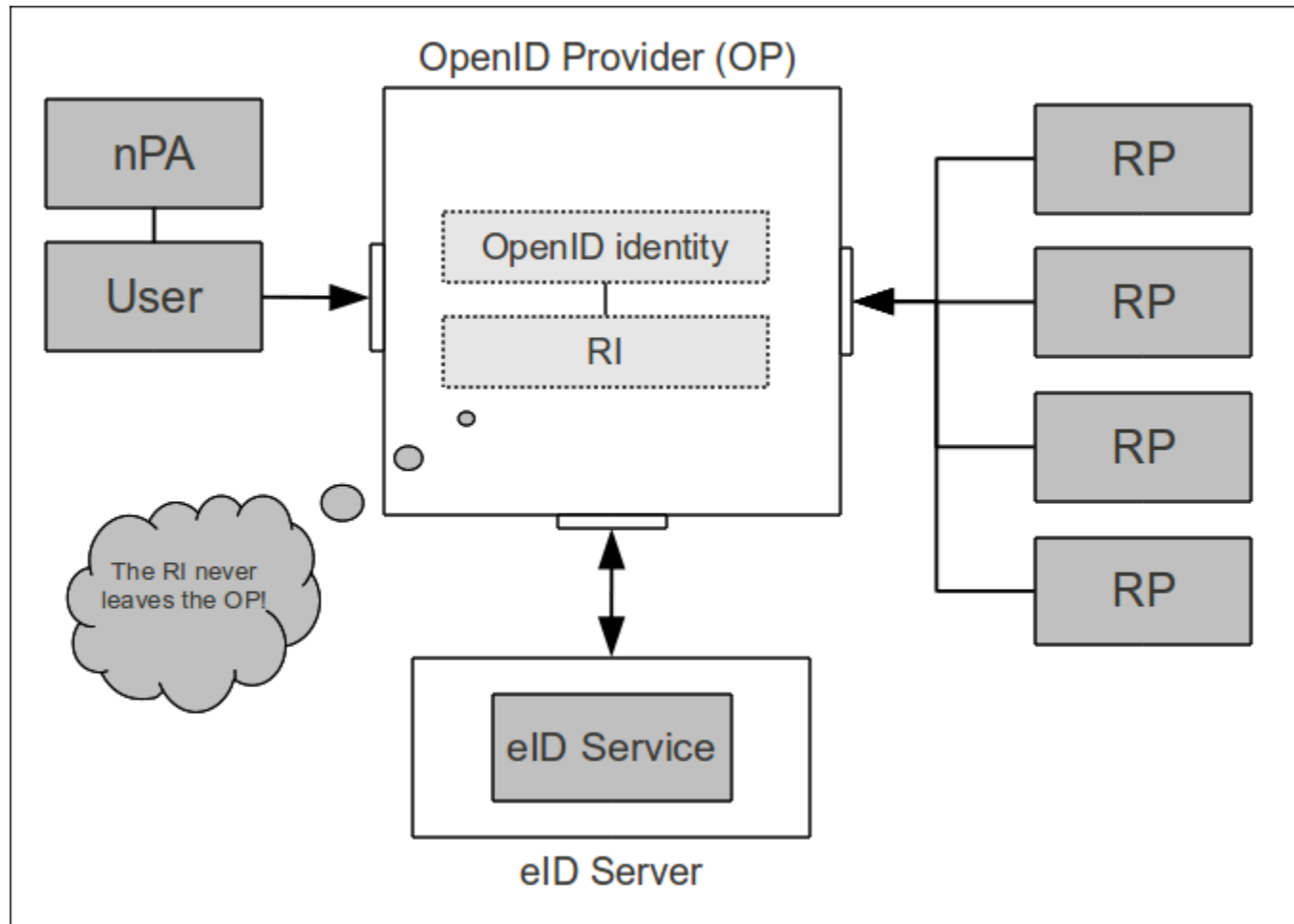
nPA-based OpenID Provider

Excursus: Trust Framework

Conclusion

nPA-based OP: Fundamental Concept

1. Make proof of identity more secure
2. Provide proxy functionality for the new German ID card



nPA-based OP: Added value (1/2)

Overall

- Proof of identity only at a single point
 - More conscious choice of identity provider
 - 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

nPA-based 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: (Cloud) Service Provider

- „Outsourcing“ of authentication
- Use of the nPA's eID function via the proxy functionality

Motivation

OpenID

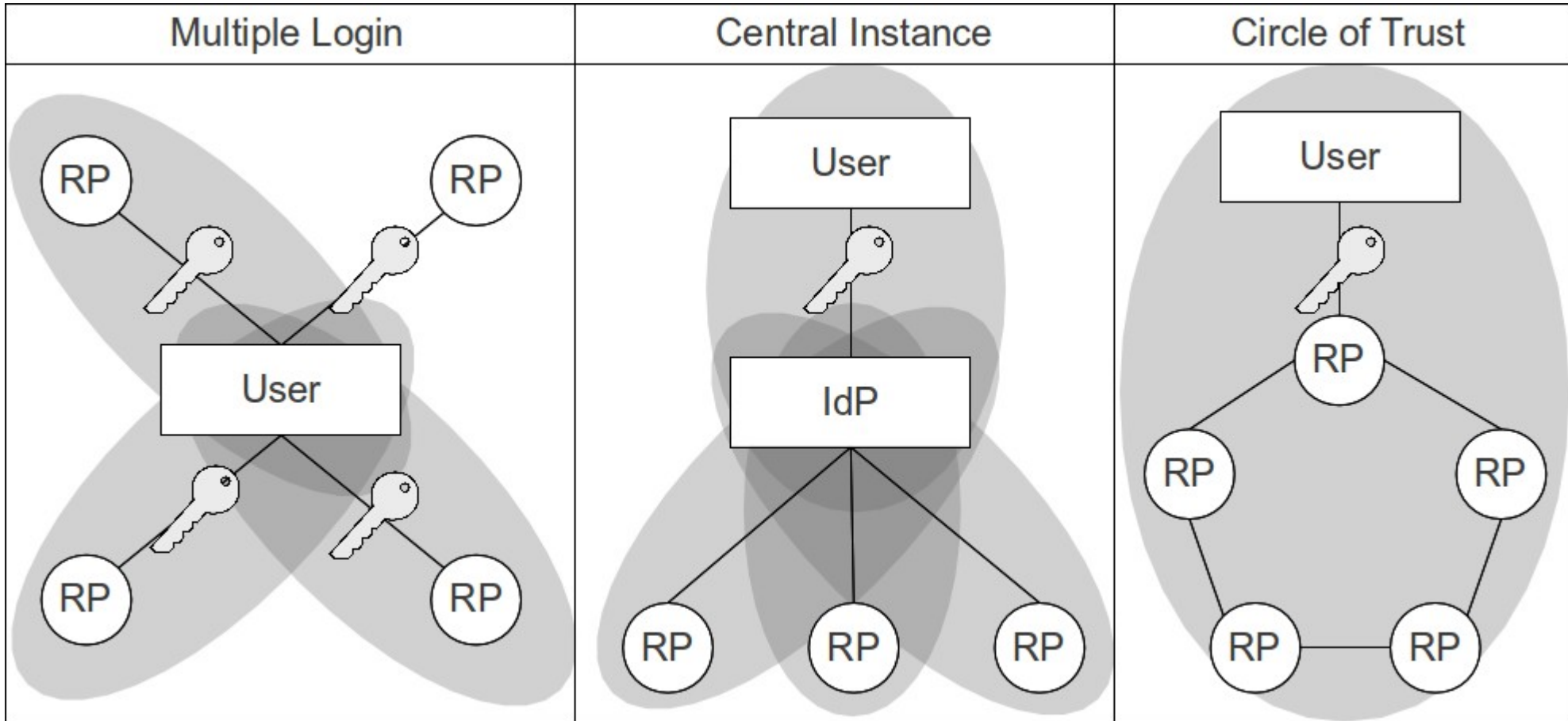
German new electronic identity card (nPA)

nPA-based OpenID Provider

Excursus: Trust Framework

Conclusion

Excursus: Trust Framework (1/3)



Excursus: Trust Framework (2/3)

Lots of problems/questions

- Relying Party (RP)
 - Authentication's level of assurance (LOA)?
 - Accurate attributes? Authoritative identity provider?
- Identity Provider (IdP)
 - Accurate information about the user?
 - RP's use of information in accordance with contract?
- User
 - IdP and RP trustworthy? Respecting the privacy?
- In general
 - All parties keeping the requirements and contracts?
 - How reliable are the parties?

Excursus: Trust Framework (3/3)

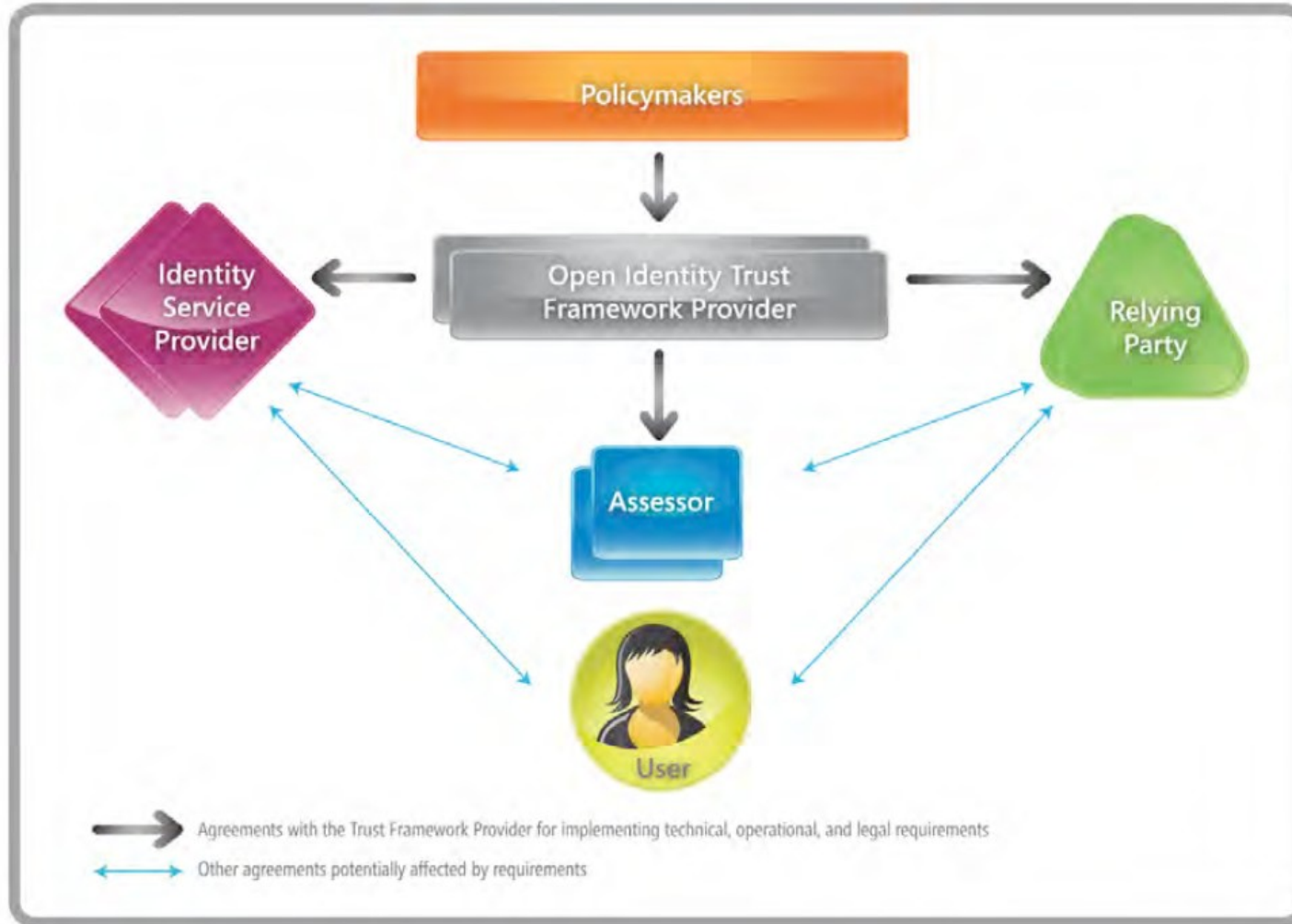


Figure 2, „The participants in an OITF for identity information“,
in „The Open Identity Trust Framework (OITF) Model“,
Maler, Nadalin, Reed, Rundle, Thibeau, March 2010

Agenda

Motivation

OpenID

German new electronic identity card (nPA)

nPA-based OpenID Provider

Excursus: Trust Framework

Conclusion

Conclusion

OpenID protocol

- Growing importance: Identity Management on the Internet
 - Need for secure proof of identity

New German ID card

- Necessary step towards a digital future (including identities)
- Issue of the nPA since November 2010
 - Difficult estimation of reaction and acceptance (until now/still)

nPA-based OpenID provider

- First of its kind
- Combination of OpenID and the eID feature
 - Compensating the weaknesses of OpenID
 - Generating added value

Trust Frameworks

- Potential of OpenID is far from exhausted
- Problem: Factor Trust!
- Much work in National / European Frameworks

Any questions?

Authentication in the Cloud using OpenID and the German ID card

**The European e-Identity Management Conference
Session: Identity in the Cloud
Tallinn, Estonia, 9th June 2011**

Sebastian Feld, M.Sc.

Norbert Pohlmann, Prof. Dr. (TU NN)

[feld|pohlmann] @ internet - sicherheit . de

Institute for Internet Security – if(is)

University of Applied Sciences, Gelsenkirchen

<https://www.internet-sicherheit.de>