re:claimID

IETF 104 PEARG

Martin Schanzenbach

25.3.2019

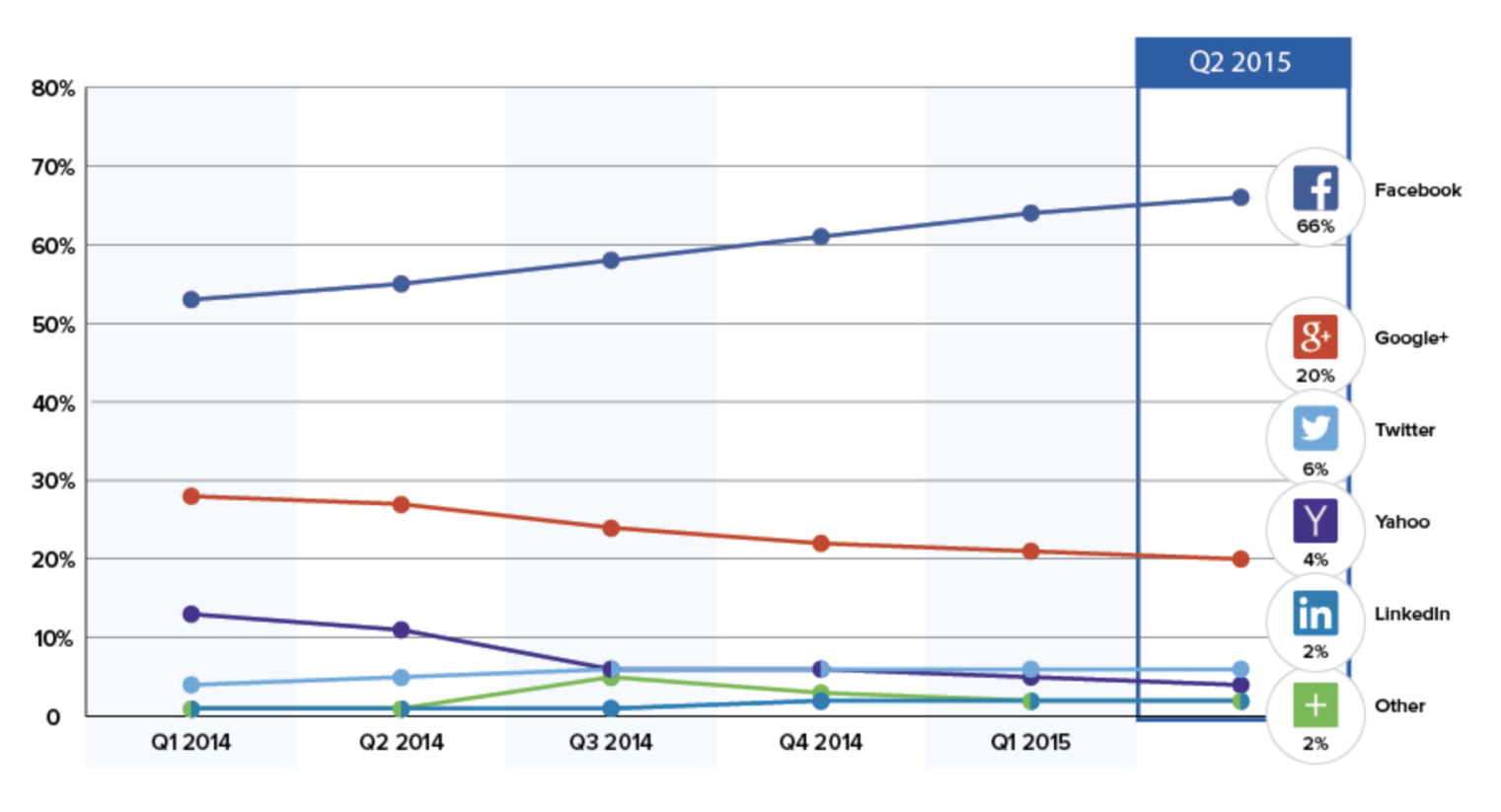
Fraunhofer AISEC

GNUnet

Motivation

Motivation

Identity Provider Market:



Source: `http://www.gigya.com/blog/the-landscape-of-customer-identity-q2-2015/`

Motivation

Issues:

1. **Privacy** concerns:
    - Targeted advertisement, opinion shaping.
    - "Public safety": Mass surveillance and data collection.

Motivation

Issues:

1. **Privacy** concerns:
    - Targeted advertisement, opinion shaping.
    - "Public safety": Mass surveillance and data collection.
2. **Liability** risks:
    - Data loss through leaks or hacks may result in existential legal implications (GDPR)

Motivation

Issues:

1. **Privacy** concerns:
   - Targeted advertisement, opinion shaping.
   - "Public safety": Mass surveillance and data collection.
2. **Liability** risks:
   - Data loss through leaks or hacks may result in existential legal implications (GDPR)
3. **Oligopoly**:
   - "There can be only one (two)"
   - IdP market tends to degenerate.
   - Federation not widely used.

Approach

Primary objective: We must enable users to exercise their right to digital self-determination:

Approach

Primary objective: We must enable users to exercise their right to digital self-determination:

1. Avoid third party services for identity management and data sharing.

Approach

Primary objective: We must enable users to exercise their right to digital self-determination:

1. Avoid third party services for identity management and data sharing.
2. Open, free service which is not under the control of a single organization, consortium or business.

Approach

Primary objective: We must enable users to exercise their right to digital self-determination:

1. Avoid third party services for identity management and data sharing.
2. Open, free service which is not under the control of a single organization, consortium or business.
3. Free software.

Approach

Primary objective: We must enable users to exercise their right to digital self-determination:

1. Avoid third party services for identity management and data sharing.
2. Open, free service which is not under the control of a single organization, consortium or business.
3. Free software.

$\Rightarrow$ Empower users to **reclaim** control over their digital identities.

Introducing re:claimID

What does an IdP do?

1. Identity provisioning and access control
    - Management of identities and personal data by user.
    - Facilitate sharing of identity data with third parties.
    - Enforce authorization decisions of user.

What does an IdP do?

1. Identity provisioning and access control
    - Management of identities and personal data by user.
    - Facilitate sharing of identity data with third parties.
    - Enforce authorization decisions of user.

2. Identity information verification:
    - “this is Alice’s email address”: Email provider.
    - “this user is living in Germany”: Sovereign state.

What does an IdP do?

1. Identity provisioning and access control
    - Management of identities and personal data by user.
    - Facilitate sharing of identity data with third parties.
    - Enforce authorization decisions of user.

2. Identity information verification:
    - “this is Alice’s email address”: Email provider.
    - “this user is living in Germany”: Sovereign state.

What does an IdP do?

1. Identity provisioning and access control
    - Management of identities and personal data by user.
    - Facilitate sharing of identity data with third parties.
    - Enforce authorization decisions of user.

2. Identity information verification:
    - “this is Alice’s email address”: Email provider.
    - “this user is living in Germany”: Sovereign state.

What does an IdP do?

1. Identity provisioning and access control
   - Management of identities and personal data by user.
   - Facilitate sharing of identity data with third parties.
   - Enforce authorization decisions of user.

   $\Rightarrow$ **re:claimID**
2. Identity information verification:
   - "this is Alice's email address": Email provider.
   - "this user is living in Germany": Sovereign state.

   $\Rightarrow$ **Out of scope**

In a nutshell

re:claimID = Decentralized directory service + Cryptographic access control

Scope

- Decentralized directory service
  - Secure **name system** with open name registration.
  - Idea “borrowed” from NameID.
  - Our implementation uses the **GNU Name System (GNS)**

Scope

- Decentralized directory service
  - Secure **name system** with open name registration.
  - Idea "borrowed" from NameID.
  - Our implementation uses the **GNU Name System (GNS)**

  $\Rightarrow$ For detailed info on GNS see talk by Christian Grothoff at DINRG!

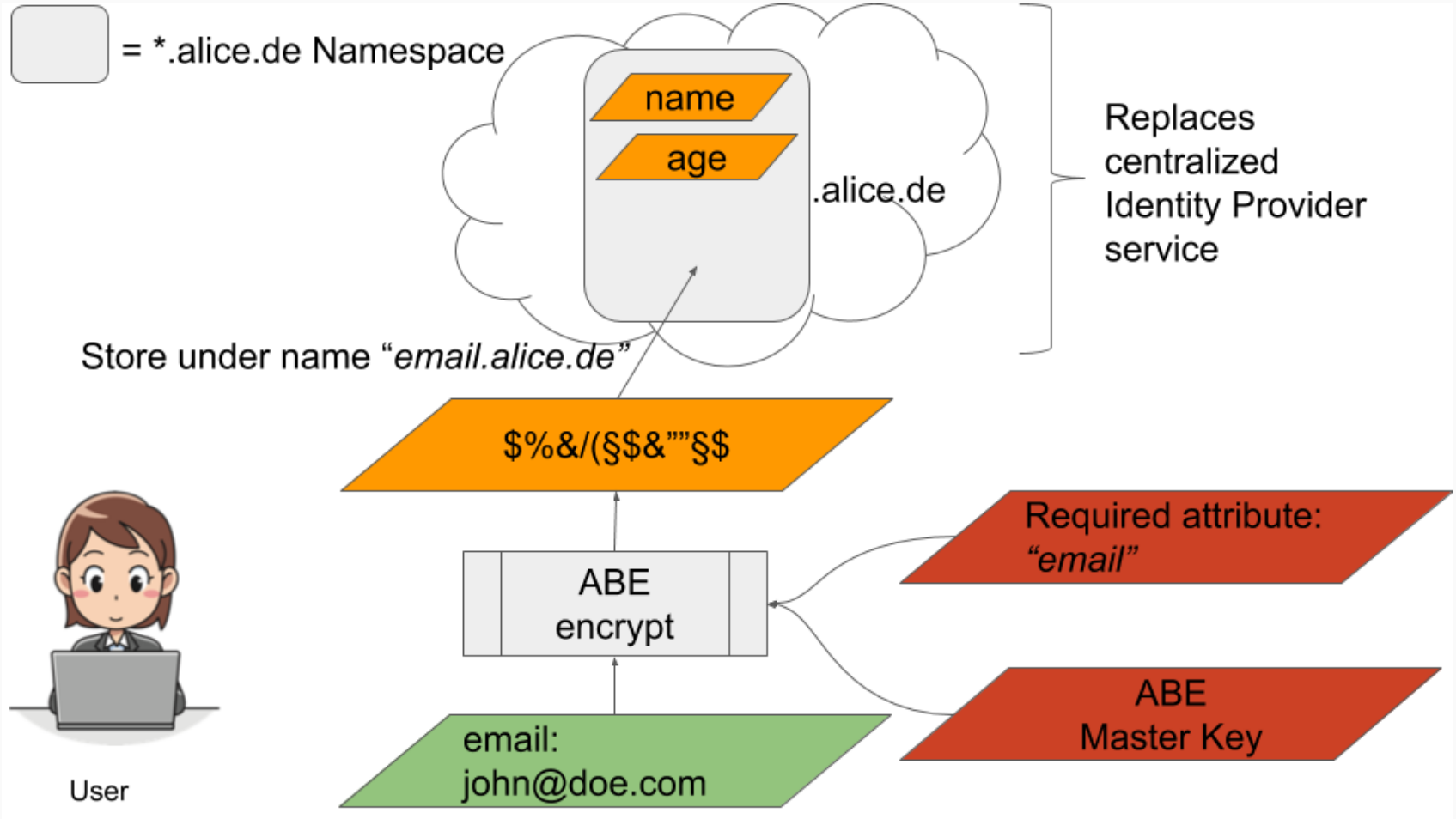
Scope

- Decentralized directory service
  - Secure **name system** with open name registration.
  - Idea "borrowed" from NameID.
  - Our implementation uses the **GNU Name System (GNS)**

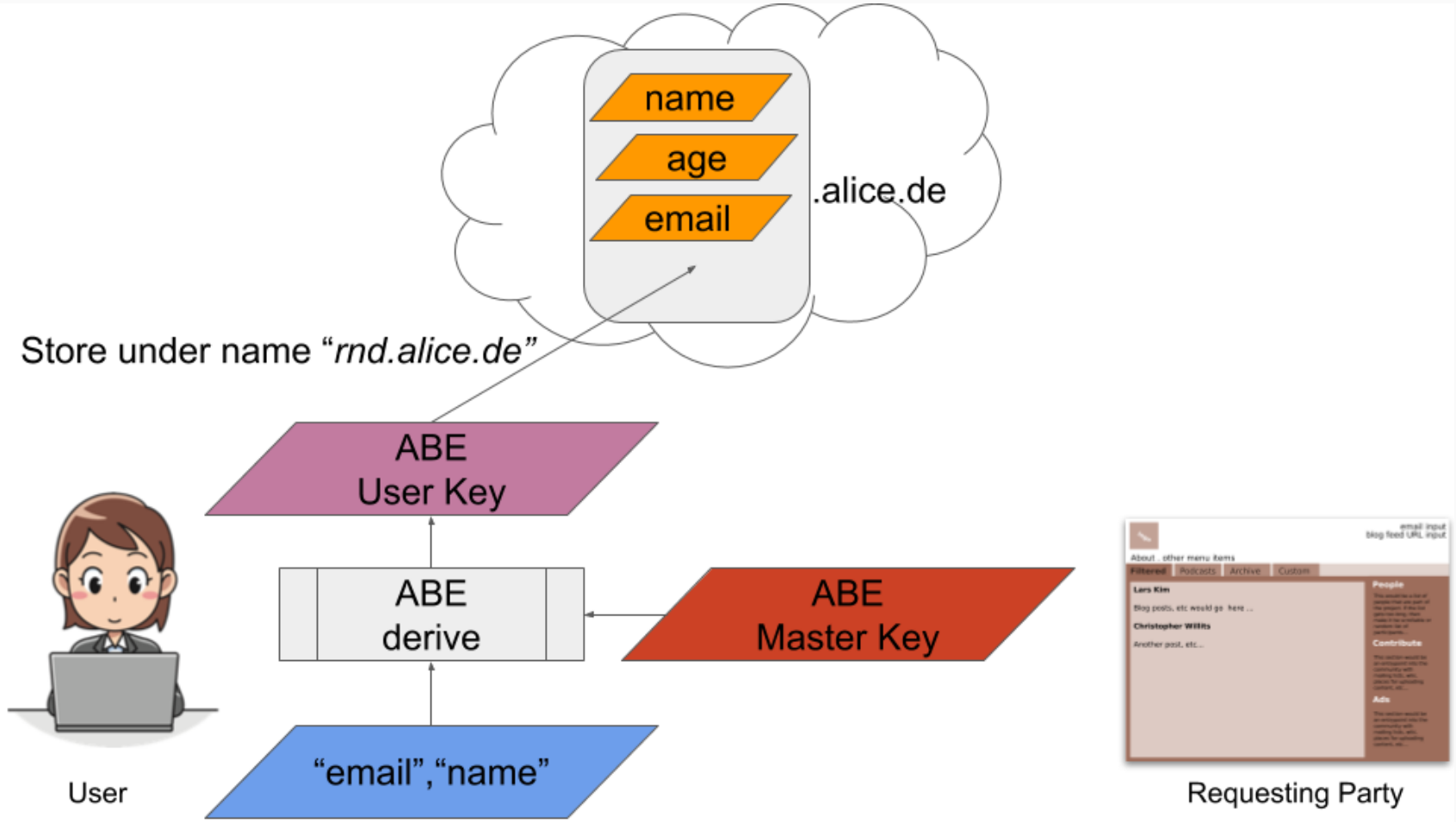
  $\Rightarrow$ For detailed info on GNS see talk by Christian Grothoff at DINRG!
- Cryptographic access control layer
  - Built using **attribute-based encryption**.
  - Protects identity data from unwanted disclosure and allows users to enforce access control.

Example

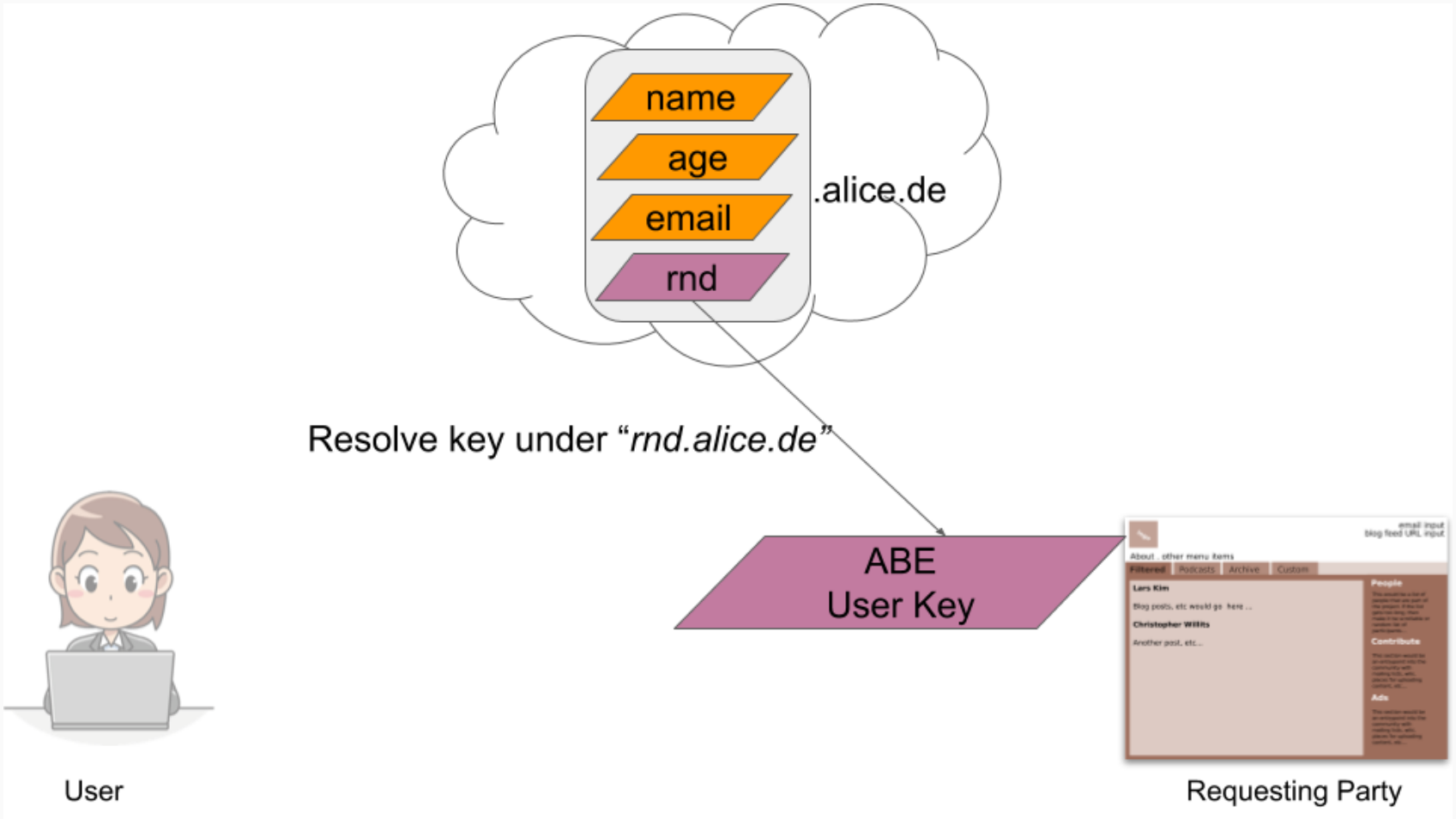
Publish attributes



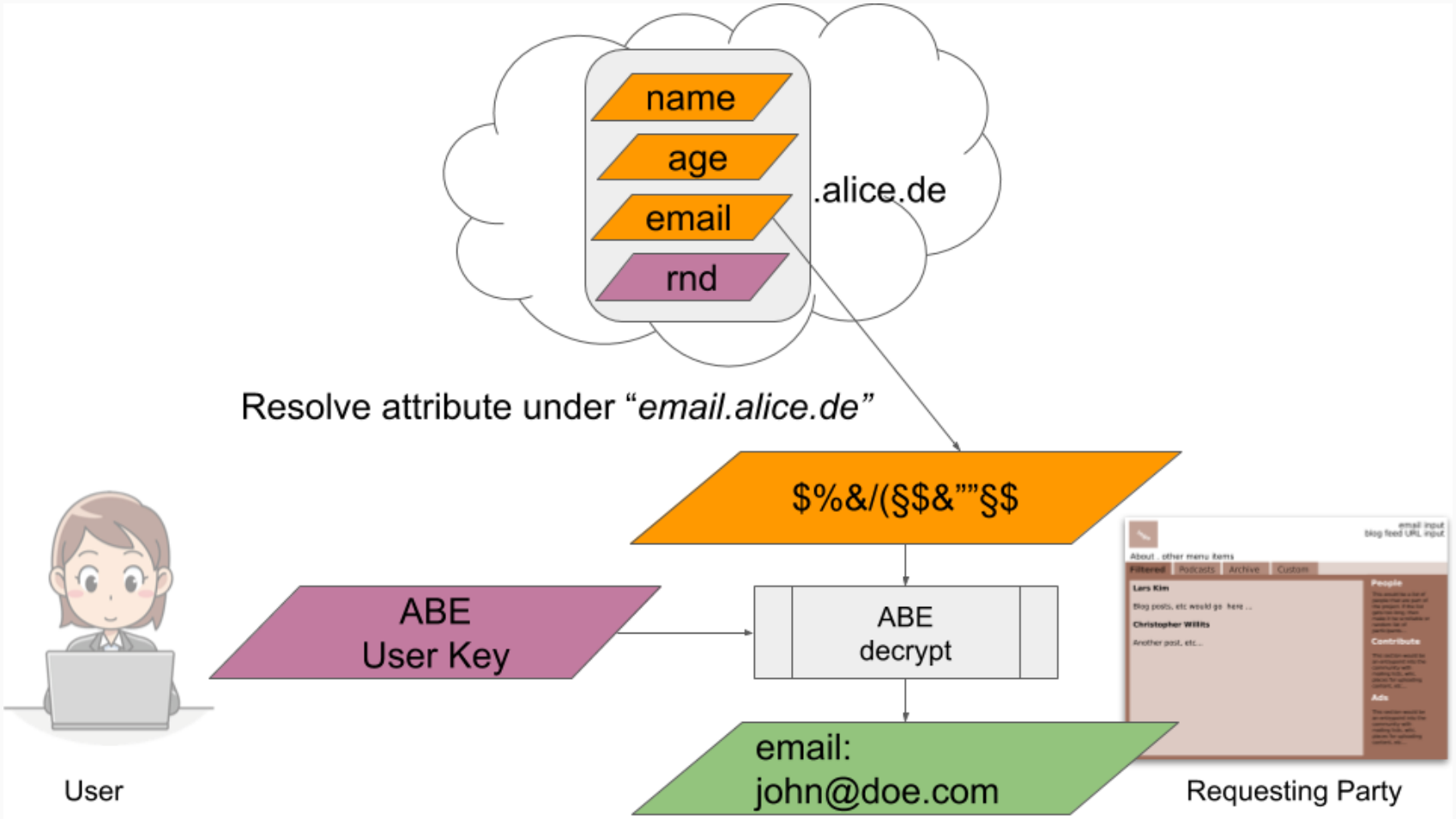
Publish keys



Retrieve keys



Retrieve and decrypt attributes



Authorization protocol and key transfer

re:claimID

OpenID Connect

Summary

Status

- Implementation part of GNUnet.
- Functional proof-of-concept on gitlab.
- Roadmap:
  - User-friendly packaging
  - Dissemination by integration into products (via OIDC)
  - Documentation
  - “1.0” by end of 2019
- Links:

`https://reclaim-identity.io`

`https://gitlab.com/reclaimid`

`https://gnunet.org`

Questions?

schanzen@aisec.fraunhofer.de

GPG: 6665 201E A925 7CC6 8FDE 77E8 8433 5131 EA3D ABF0

– or –

schanzen@gnunet.org

GPG: 3D11 063C 10F9 8D14 BD24 D147 0B09 98EF 86F5 9B6A

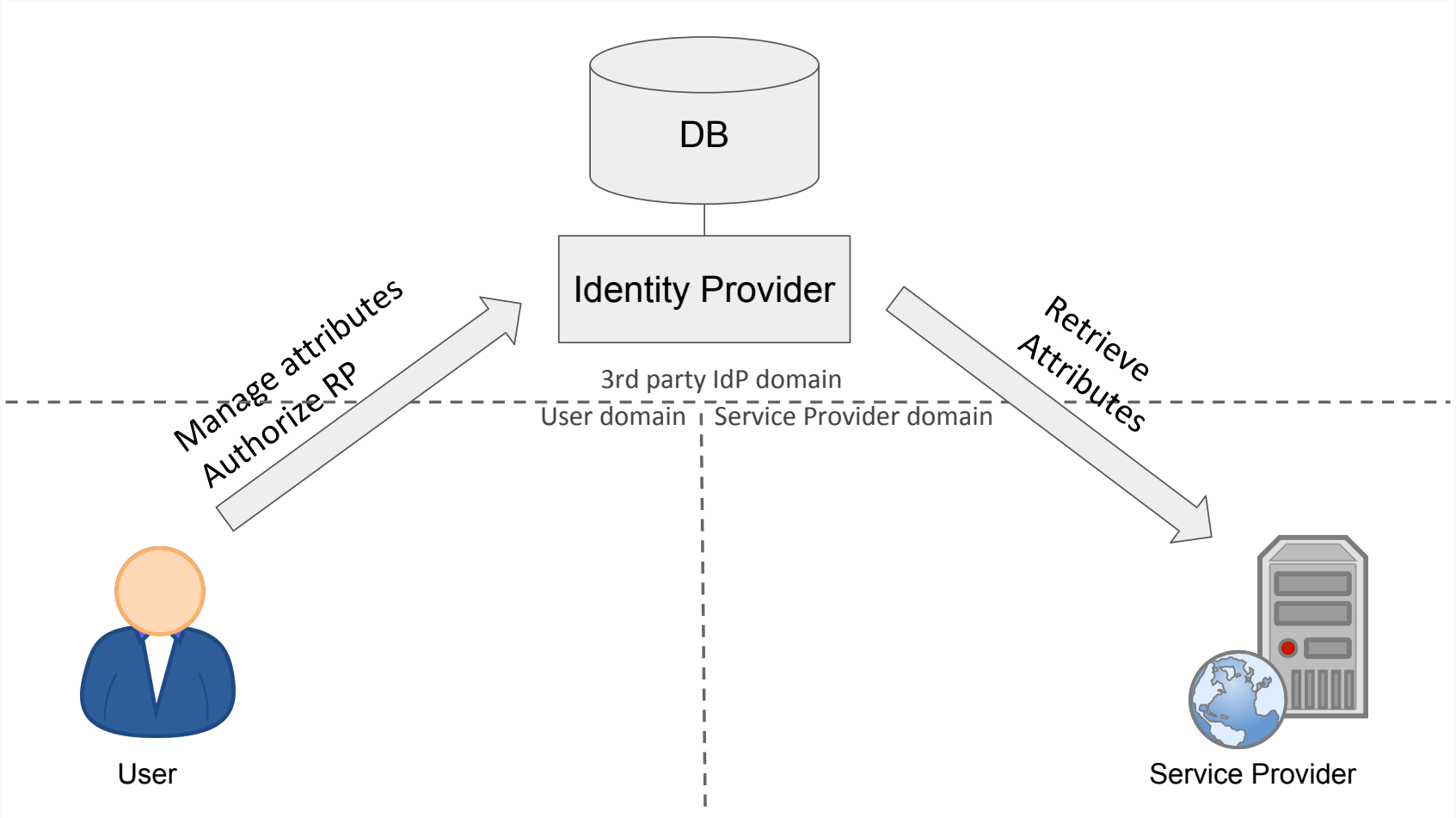
References

1. Matthias Wachs, Martin Schanzenbach and Christian Grothoff. *A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System*. **13th Intern ational Conference on Cryptology and Network Security**, 2014.

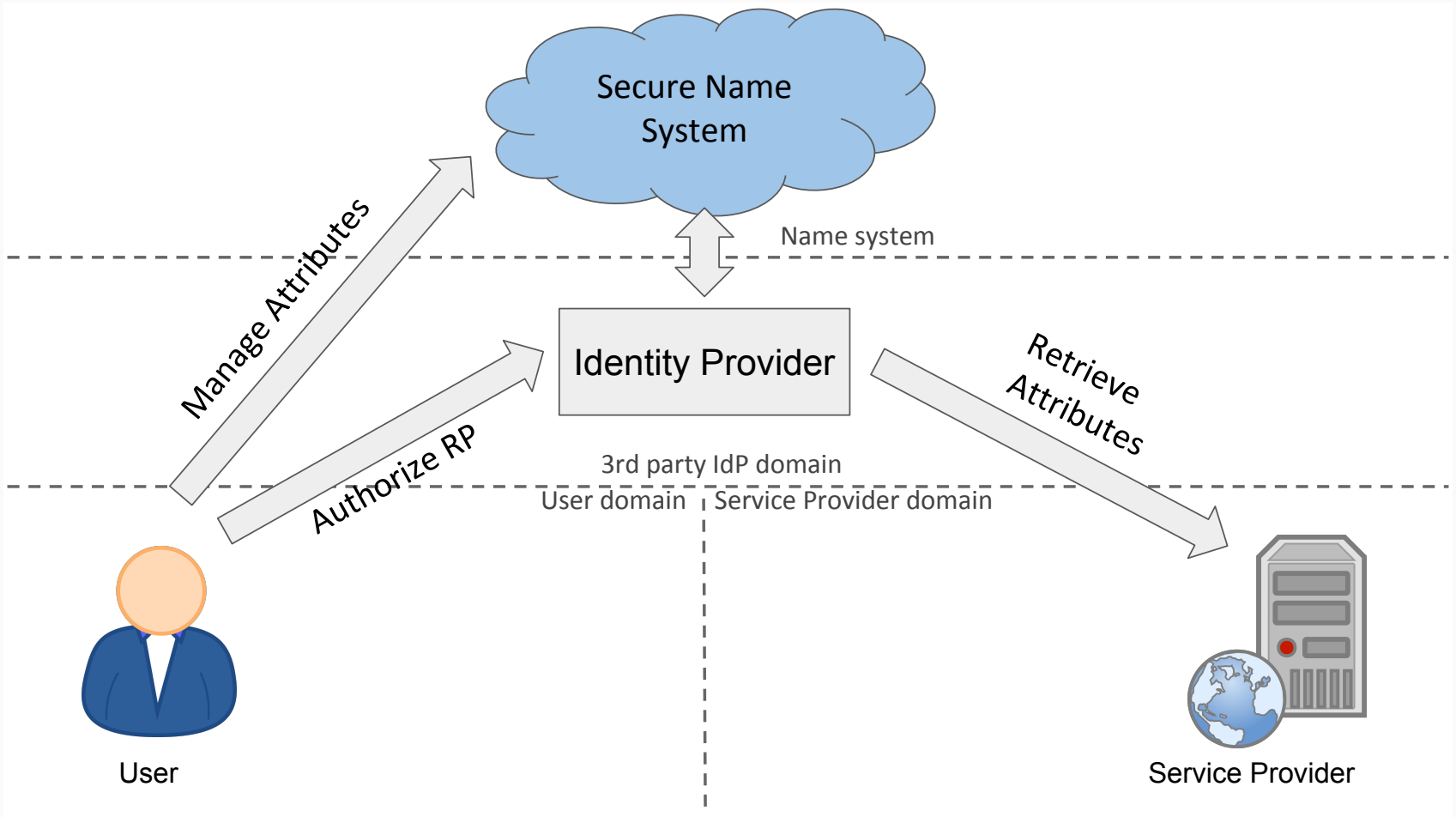
2. Martin Schanzenbach, Georg Bramm, Julian Schtte. *reclaimID: Secure, Self-Sovereign Identities Using Name Systems and Attribute-Based Encryption*. **17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom)**, 2018

3. J. Bethencourt, A. Sahai, and B. Waters. *Ciphertext-policy attribute-based encryption.*. **IEEE Security and Privacy, 2007. SP07.**

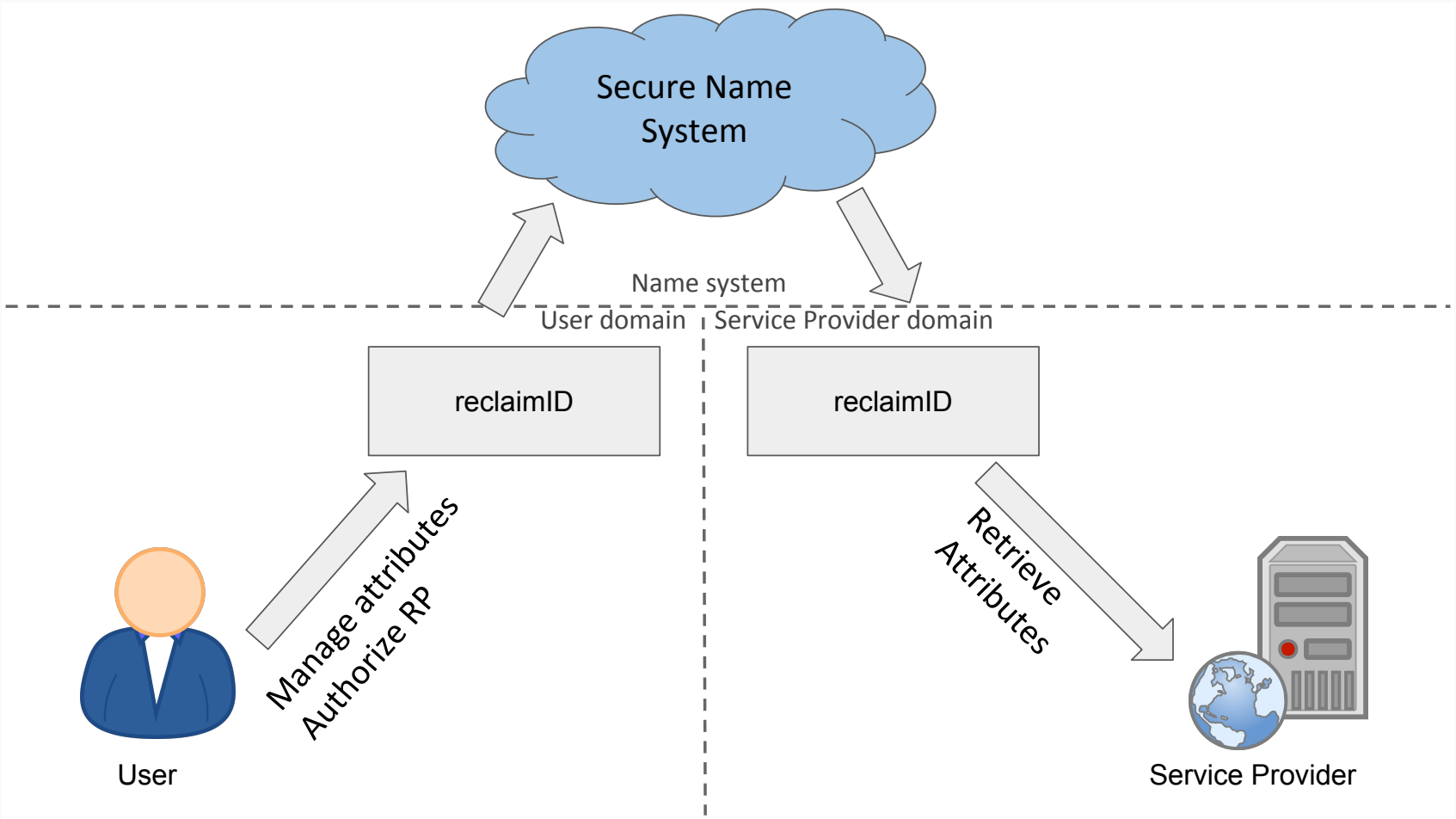
Centralized Storage, centralized IdP



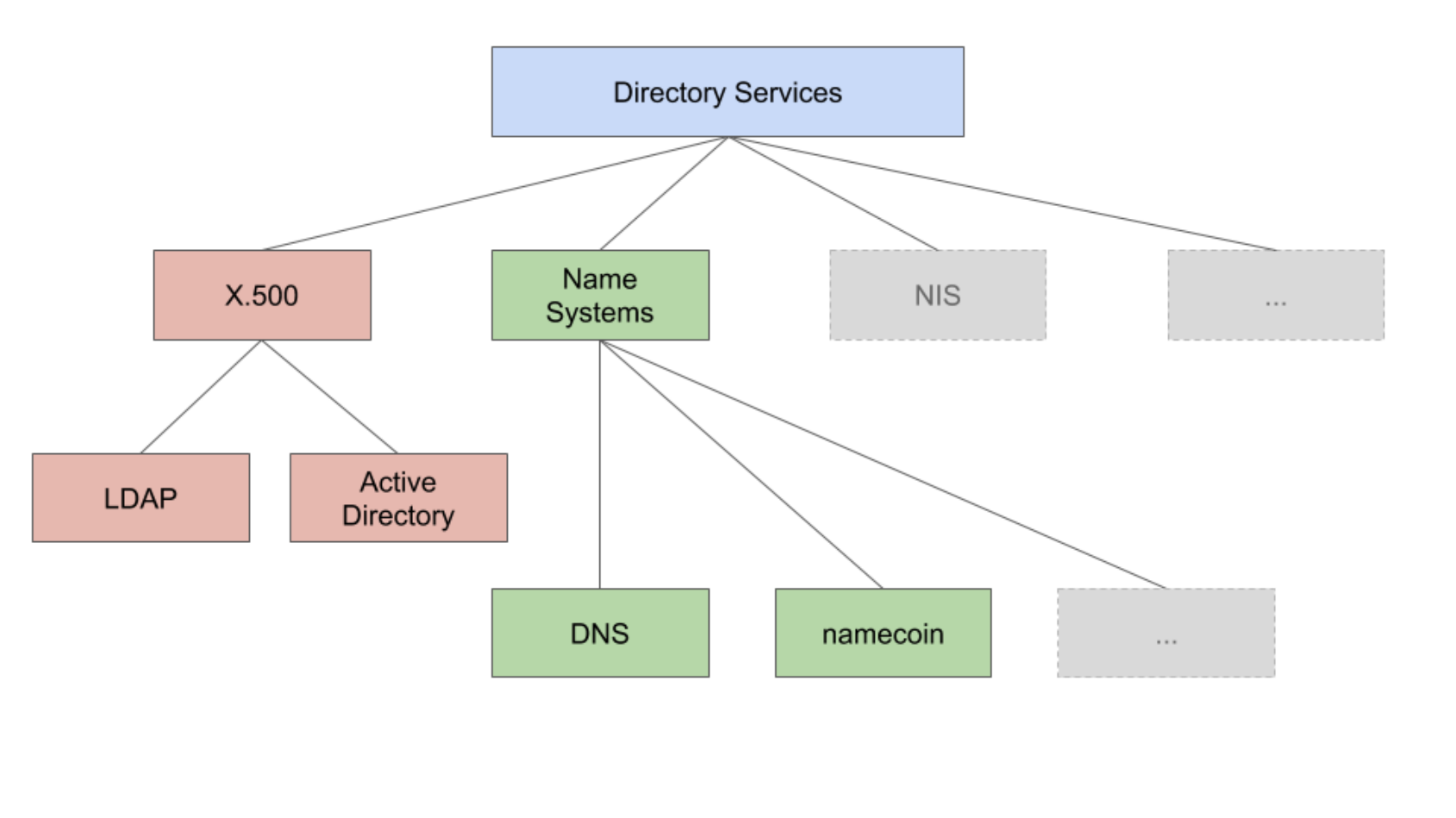
Decentralized Storage, centralized IdP



reclaimID

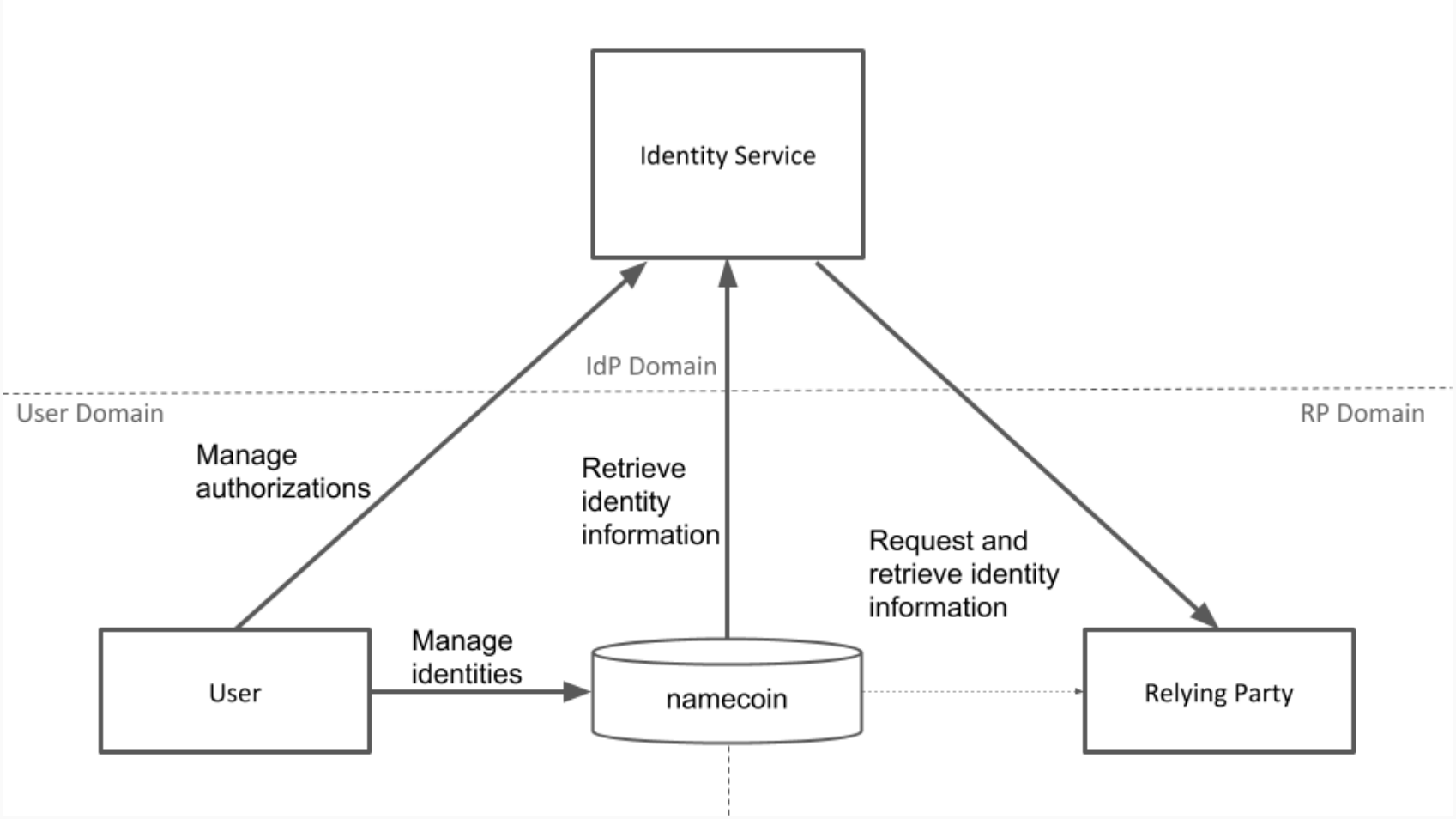

Secure Name System
Name system
User domain
Service Provider domain
reclaimID
reclaimID
Manage attributes
Authorize RP
Retrieve Attributes
User
Service Provider

Directory services



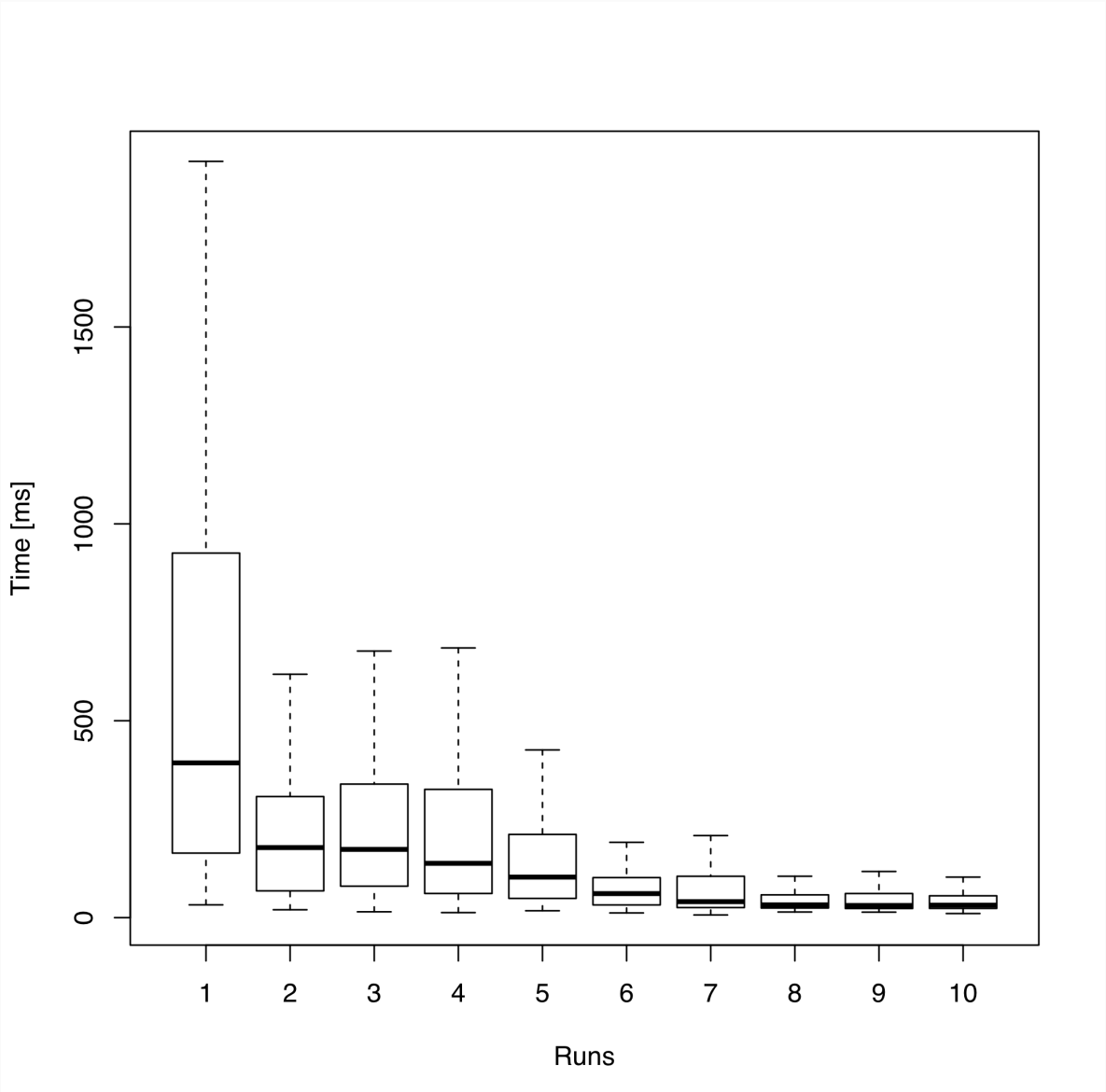
NameID

NameID:



Performance

Impact of name system caches on successive attribute resolution.



Performance

Attribute resolution performance depending on network size.