Motivation
Identity Provider Market:

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.
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.

⇒ Empower users to reclaim control over their digital identities.
**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.
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.
**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.
**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.

⇒ 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.
   ⇒ re:claimID

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

= *.alice.de Namespace

Store under name "email.alice.de"

Replaces centralized Identity Provider service

$%%&/(§§&”§$ %

Required attribute: "email"

User

email: john@doe.com

ABE encrypt

ABE Master Key
Publish keys

Store under name “rnd.alice.de”

User

“email”, “name”

ABE User Key

ABE derive

ABE Master Key

name

age

e-mail
Retrieve keys

Resolve key under “rnd alice.de”
Retrieve and decrypt attributes

Resolve attribute under “email.alice.de”

User

ABE User Key

email: john@doe.com

Requesting Party
Authorization protocol and key transfer

re:claimID

OpenID Connect
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


Centralized Storage, centralized IdP

User

Service Provider

3rd party IdP domain

User domain

Service Provider domain

Identity Provider

Manage attributes

Authorize RP

Retrieve Attributes

DB
Decentralized Storage, centralized IdP

Managing Attributes

Name system

Identity Provider

Authorize RP

Retrieve Attributes

User domain

Service Provider domain

3rd party IdP domain
NameID:

Identity Service

User Domain

IdP Domain

RP Domain

User

Manage authorizations

Manage identities

Retrieve identity information

namecoin

Request and retrieve identity information

Relying Party
Performance

Impact of name system caches on successive attribute resolution.
Attribute resolution performance depending on network size.