IETF 104 PEARG

Martin Schanzenbach
25.3.2019
Motivation
Motivation

Identity Provider Market:

Issues:

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

\[ \text{re:claimID} = \text{Decentralized directory service} + \text{Cryptographic access control} \]
Decentralized directory service

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

e-mail: john@doe.com

ABE encrypt

ABE Master Key

$%&/(§§§”§§$
Publish keys

Store under name “rnd.alice.de”

User

“email”, “name”

Requesting Party

ABE
User Key

ABE
derive

ABE
Master Key

name
age
email
.alice.de
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
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


Centralized Storage, centralized IdP

- User
- Service Provider
- Identity Provider
- DB
- Manage attributes
- Authorize RP
- Retrieve Attributes
- 3rd party IdP domain
- User domain
- Service Provider domain
Decentralized Storage, centralized IdP
Directory services

- X.500
  - LDAP
  - Active Directory
- Name Systems
- NIS
- DNS
- namecoin
  - ...
  - ...
NameID:

- User
  - Manage identities

- Identity Service
  - Manage authorizations
  - Retrieve identity information

- namecoin
  - Request and retrieve identity information

- Relying Party

User Domain

IdP Domain

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

![Attribute retrieval performance (Median)](image)