Rich Identity Provisioning

Agenda

• Introduction
• Research questions
• Related work
• RIP architecture
• Open source components
• Conclusion
Rich Identity Provisioning

introduction: trigger

Digital identity: business

Digital identity: web shop

Digital identity: social
Rich Identity Provisioning

introduction: trigger

Digital identity: business
- colleagues
- business card

Digital identity: web shop
- name
- address
- bank

Digital identity: social
- friends
- photos
Rich Identity Provisioning

**introduction: trigger**

Digital identity: business
- colleagues
- business card

Digital identity: web shop
- name
- address
- bank

Digital identity: social
- friends
- photos
Rich Identity Provisioning

introduction: trigger

Identity Provider A

Digital identity: business

Identity Provider B

Digital identity: web shop

Identity Provider C

Digital identity: social
Rich Identity Provisioning

Research Questions

1. What architecture fits best to a user-centric identity provisioning system regarding Web access?

2. What open source components fit into such a system?
Reports on issues regarding Identity provisioning

- User-centric: Data-store architecture
- Security: Trusted module (SmartCard)
- Privacy: Cross-layer privacy

Project:
- Global architecture $\iff$ answer research questions
Rich Identity Provisioning

RIP Architecture

SP resources

User

RIP Architecture

Access & Policy services
- Protocols

Data Storage services
- Identity
- Policy
- Audit
- Synchronization
- Virtualization

Identity Data services
- inControl
- Audit

Identity Provider (IdP)
Rich Identity Provisioning

RIP Architecture

- IdP
- SP
- TTP audit
- PDS
- context
- managed
- personal
- Virtual device
- SmartCard
- sync
- policy
- audit

UvA-SNE-RP2 presentation
Rich Identity Provisioning

RIP Architecture

- Minimal disclosure
  - private information

- Rich sharing
  - personal information

Using Ontologies (Vocabularies)
- FOAF
Rich Identity Provisioning
Open source components

<table>
<thead>
<tr>
<th>Implementation</th>
<th>Identifier used</th>
<th>Minimal Disclosure</th>
<th>Rich Sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td>BrowserID</td>
<td>e-mail address</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>SQRL</td>
<td>site-specific key</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>TiQR</td>
<td>QR code</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>U-prove</td>
<td>key</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>OpenID</td>
<td>URI</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>WebFinger</td>
<td>e-mail address</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>WebID</td>
<td>URI</td>
<td></td>
<td>√</td>
</tr>
</tbody>
</table>
RIP Architecture fits to a user-centric identity provisioning system
- User controls personal digital identities
- IdP selection context-based

Open source components that fit into the architecture
- Minimal disclosure
- Rich sharing