Digital Delegation of Rights

Prof. Dr. Reinhard Riedl
Bern University of Applied Sciences

Digital Identity = Union of all data related to a person

Conflict of interest
• Citizen: data control & free usage
• State/Company: data integration & control of usage
4-Qualities of Digital Identity

- Global & universal usage
- Coverage of all rights and duties
- Guaranteed transparency
- Support for business models

Big Picture: Systemic Development
Holistic Goal

- Enabled information orientation through transparent resource integration
  - Individually → Digital Identity
  - Representation layer → Portals & SOA
  - Process layer → POA
  - Application- and data layer → EAI-Kernel

- Sustainable solutions today and tomorrow, which do not create a legacy for the day after tomorrow

General Requirements

- Conceptual unification
  - Role concepts
  - Differing life-cycles
  - Trustworthy anonymity

- Openness
  - Mapping to different legal contexts
  - Integration with other communication channels
  - Sufficient capabilities for control
General Requirements II

• Feasibility
  – Benefits for all stakeholders
  – Low costs & low requirements for devices
  – Interoperable with existing security and identity management systems

• Usefulness
  – Non-repudiation and revocation
  – Fair distribution of risks & clear allocation of tasks
  – Guaranteed security & privacy
  – Online and offline usage
  – Failure tolerance

Delegations
Criteria
Raffael Schweizer, Beat Perjes, Monika Weber, Reinhard Riedl

- Solution Architecture
  - Technological independence, extensibility / adaptability, integration with existing systems, distribution of tasks, performance, scalability, security, privacy protection, offline usability
- Functionality
  - Compliance (issuance and control), possibility for fine-grained restrictions, transfer, anonymity, non-repudiation
- Economic Aspects / Maintenance
  - Costs, availability, risks

Solution 1

Electronic Register

CA & Directory Service  \[\rightarrow\] Service Provider
Validation, Certificate

Register  \[\rightarrow\] Principal
Validation, Correctness

Communication / Revocation

Principal  \[\rightarrow\] Procurator
Communication / Revocation

Own certificate and reference to mandate
Solution 2

Credentials from Principal

CA & Directory Service

Service Provider

Validation Correctness, Certificate and credential

Revocation Credential

Principal

Signed credential

Procurator

Solution 3

Credentials from 3rd Party

CA & Directory Service

Service Provider

Validation Correctness, Certificate and credential

Request / Revocation

Principal

Signed credential

Procurator
Solution 4

Separate Certificates

CA & Directory Service

Service Provider

Validation
Correctness, Certificate and credential

Request / Revocation

New pair of keys

Principal

Procurator

Signed delegation key

Evaluation

Raffael Schweizer, Beat Perjes, Monika Weber, Reinhard Riedl

<table>
<thead>
<tr>
<th></th>
<th>Register</th>
<th>Credentials from Principal</th>
<th>Credentials from 3rd Party</th>
<th>Separate PK-Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>OK</td>
<td>NOT</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>Sophisticated Rights</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>Revocation</td>
<td>OK</td>
<td>Part. OK</td>
<td>OK</td>
<td>NOT</td>
</tr>
<tr>
<td>Anonymity</td>
<td>Part. OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>Transfer</td>
<td>OK</td>
<td>NOT</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>N-times Usage</td>
<td>Part. OK</td>
<td>Part. OK</td>
<td>Part. OK</td>
<td>NOT</td>
</tr>
<tr>
<td>Automated Transfer</td>
<td>OK</td>
<td>NOT</td>
<td>OK</td>
<td>NOT</td>
</tr>
<tr>
<td>Technological Feasibility</td>
<td>Part. OK</td>
<td>Part. OK</td>
<td>Part. OK</td>
<td>NOT</td>
</tr>
<tr>
<td>Economic Feasibility</td>
<td>OK</td>
<td>Part. OK</td>
<td>OK</td>
<td>Part. OK</td>
</tr>
<tr>
<td>User acceptance / Usability</td>
<td>Part. OK</td>
<td>Part. OK</td>
<td>Part. OK</td>
<td>NOT</td>
</tr>
</tbody>
</table>
Case Study
Raffael Schweizer, Beat Perjes, Monika Weber, Reinhard Riedl

• Usage of credentials from 3rd party for e-banking and tax counselors
  – Feasible
  – Many special cases
    • E.g. accounts across multiple identities, restriction of actions, late execution, anonymous procurators, OFX, mandates beyond death, etc..
    • E.g. joint declaration by a married couple, correspondence, failure management during processes, automated and real-time processing, certification of tax-office, etc.

Conclusion

• Systematic problem classification missing
• No knowledge about non-trivial applications
• No “best” solution
• Electronic registers and credentials from 3rd parties work quite well
• Design decisions have considerable implications
  – as far as e-government is concerned, the people should have the possibility to vote on these decisions (Swiss opinion)