Exploiting the Cloud: Lifelong Privacy-Preserving Data Storage

Katrin Borcea-Pfitzmann, Stefan Köpsell
TU Dresden

Privacy in „My Life“
Privacy throughout “My Life” – Stages of Life (SoL)

- Nonage
- Legal Age
- Adulthood
- Retirement
- Legal Guardian

Delegation:
- Mandatory
- Discretionary

Privacy throughout “My Life” – Areas of Life (AoL)

- Past
- Now
- Future

Various partial identities

Establishment

Evolvement

Termination
Focal Points of the Presentation

- Third year focal prototype
  - challenge we were faced:
    - develop a prototype considering timespan of 80 - 100 years
    - limited possibilities of predicting technology development
  - Lifelong personal data management demonstrator

- Delegation
  - important concept to tackle with stages of life
  - challenging in the context of privacy protection for law and technology development

Delegation

“… [a] data subject needs to be represented by another natural person who exercises the right on behalf of the data subject concerned during certain phases of life.“ [D1.3.1]

- means to cope with changing abilities and willingness to manage privacy
- delegation based on
  - legal provisions
  - explicit consent
Delegation requirements

- mechanisms for issuance of mandate for proxy and related activities including revocation
- support of “proxy credentials”
- mechanisms to trace proxy actions
- mechanisms to stipulate conditions and preferences
- mechanisms to protect the proxy’s privacy

Lifelong Personal Data Management Demonstrator

- useful area of public interest
  - most “normal” users are familiar with the concept
  - enhancement of existing idea
- lifelong privacy aspects:
  - everyday work with AoLS
  - everyday work with different SoLS
  - everyday work with partial identities (pIDs)
- combination with ideas and concepts from a couple of prototypes
Objectives of Demonstrator

- protection of user against unwanted data loss during his lifetime
  - redundancy and physical distribution
- assurance of lifelong confidentiality of user’s data
  - encryption
- delegation of access rights to user’s backup data
  - specific conditions
- distribution of the backup data according to different areas of life
  - privacy management in advanced way

Features of the Demonstrator

![PrimeLife Backup Tool](image)
Features: Setting up a Delegation

Features: Delegation/Collective Decision
Summary & Lessons Learned 1\|2

- highly complex research area
- interdisciplinary approach
- two-fold problem field:
  - long-term security
  - minimization of disclosure of personal data & identity management
- domain-/application-/user-specific

---

Summary & Lessons Learned 2\|2

- design of privacy-respecting applications requires thorough contemplations:
  - the full lifespan of users meaning
    - dynamics in life conditions, aims, attitudes
    - changes in abilities and willingness to manage privacy
    - possible influences of privacy-related decisions for contexts other than the “current”
- delegation scenarios are crucial as
  - interests of all involved parties regarding their privacy and expected service/functionality have to be met
  - law has to be fulfilled
Thank you for your attention!

References

[D1.3.1] K. Borcea-Pfitzmann (ed.): Scenario, Analysis, and Design of Privacy Throughout Life Demonstrator. PrimeLife Deliverable D1.3.1, February 2011