Enforcement of Privacy-compliant Delegation of Personal Data

Sven Wohlgemuth, Isao Echizen, Noboru Sonehara, Günter Müller
National Institute of Informatics, Tokyo, Japan
University of Freiburg, Germany

Personalized Services and Business Processes

Service providers act as data consumers and data providers
• Data consumers collect, use, and store the user’s personal data
• Data providers disclose/delegate personal data to service providers
• Privacy promise: Service providers handle personal data according to the agreed-upon privacy policy between users and service providers
• Examples: Customer relationship management and medical services with electronic health record

Identity Management and Delegation

• Privacy by non-linkable credentials
• All credentials and pseudonyms are based on secret key
• All-or-nothing delegation: Loss of control

No Control on the Delegation of Personal Data

Digital Watermarking and Delegation
• Copyright protection by labeling digital content
• Symmetric watermarking scheme: Both service providers get the same watermark: Non-distinction of last data provider

Controllable Delegation of Personal Data by DREISAM & DETECTIVE

DREISAM: Non-linkable Delegation of Rights
• Authorization: Delegation of access rights to user’s data
• PKI-based protocols with cryptographic commitments and zero-knowledge proof for non-linkability
• Proxy credentials instead of sharing secret key

DETECTIVE: Documenting Delegations of Personal Data
• Ex-post enforcement by identifying last data provider
• Linking the identities of data provider and consumer by cryptographic commitments and digital watermarking
• Verification by user due to delegated rights as watermarking key

Evaluation: Proof-of-concept implementation for medical services with electronic health records