User-Centric Secure Data Sharing
Exploration of Concepts and Values

Jan Grashöfer, Alexander Degitz, Oliver Raabe
Traditional Data Collection

Portability? Access Control?
Traditional Data Outsourcing & Sharing

User

Telemetry Data Storage Provider

Upload Data

Access
Revocation

Trust???

Logical Access Control

Retrieve Data

Power Supplier

Insurance Company

Manufacturer
Secure Data Sharing (SDS) ∈ Outsourcing

User

Telemetry Data Storage Provider

Logical Access Control

Upload Data

Key Distribution

Retrieval Data

Manufacturer

Insurance Company

Power Supplier

Key Distribution

 Outsourcing
User-Centric Secure Data Sharing (UC-SDS)

Our Goals:

- Enable the user to control access to his/her data cryptographically
  - Combined approach of elements of
    - Secure Data Sharing (SDS), transferring control to the user
    - Secure Data Outsourcing (SDO), in particular Access Pattern Confidentiality

Research questions:

- Is UC-SDS technically feasible?
- How is UC-SDS influenced by values?
- Can values be balanced by a user?
Methodology

Example Scenario & Building Blocks

Constraints

Legal Considerations

Design Space Exploration

Individual Values

Societal Values

User-Centric Value Balancing

Appropriateness → Optimization Problem → Appropriateness
Secure Data Sharing (SDS)

- **Cryptographic Access Control**
  - Granting & revocation of access rights

- **Traditional Cryptography**
  - Symmetric & asymmetric encryption primitives
  - Client-side key management → e.g. Lockboxes
  - Trust anchors: PKI

- **Proxy Re-Encryption (PRE)**
  - Re-Encryption without plain text access
  - Trust anchors: PKI, Proxy

- **Attribute Based Encryption (ABE)**
  - Attributes bound to users by Attribute Authorities (AA)
  - Trust anchors: PKI, AA, Proxy

Increasing # of trust anchors
Secure Data Outsourcing (SDO)

- How to query encrypted data efficiently?
  - Confidentiality-Preserving Indices (CPI)

- **Threat:** Inference attack based on
  - stored data
  - access patterns

- **Goals:**
  - Fast Index Access (FIA)
  - Low Information Leakage (LIL)

- SDO using a Mediator → trusted environment
- SDO Mechanisms:
  - Retrieval of dummy elements
  - Node shuffling
Societal Values: Codified in law (e.g., Charter of the Fundamental Rights of the European Union, Grundgesetz: Grundrechte)

Legal Considerations

- **Economic perspective:**
  - "Data Ownership" (ito: physical possession)
    - Personal data = privacy
    - Ownership = transferable
  - Data subject cannot waive fundamental rights (informational self-determination)

- **Access Right** (origin: competition law)
  - GDPR: "free flow of data" & "right to data portability"

- **Data Protection perspective:**
  - GDPR: "data minimization" & "privacy by design"

- **Example Scenario:** "fair and undistorted competition", "consent", "standardized access" & "free choice" (C-ITS, re-use of vehicular data)

- **Adequate approach:** User-enforced cryptographic access control
  → UC-SDS

GDPR: European General Data Protection Regulation
C-ITS: Cooperative Intelligent Transport Systems
Methodology

- **Design Space Foundations:**
  - **Legal Framework:** fair and undistorted competition, consent, standardized access, free choice
  - **Data Model:** Relational database
  - **Attack Model:** *honest but curious* attacker

- Security & Functionality Requirements
Design Space

SDS Strategy

Mediator Placement

User operated
External SP
Manufacturer
Everywhere

Traditional
PRE
ABE

Re-Encryption Proxy Placement

External SP
Manufacturer

SP: Service Provider
Exemplary Design

- **User**
  - Upload Data (encrypted)
  - Access Revocation

- **Mediator**
  - Re-Enc. Proxy
  - Telemetry Data

- **Manufacturer**
  - Retrieve Data (encrypted query)

- **Insurance Company**

- **Power Supplier**
Methodology

Example Scenario & Building Blocks

Legal Considerations

Constraints

Design Space Exploration

Societal Values

Individual Values

User-Centric Value Balancing
Consideration of Individual Values

Discussion & Future Work

- Establish a comprehensive scenario
  - Driver ≠ owner, frequently changing
  - Balancing of manufacturer role (control vs. legitimate demands)

- Further investigation of Data Models
  - Standardization → Portability
  - Database vs. Streaming paradigm

- Address practical usability
  - Design & evaluate UI for Access Control management
    - User-centricity limits acceptable complexity

- Legal Perspective
  - Reuse of competition law (Access Right)
  - From data minimization to user-controlled access

User-centricity = value-laden decision!
Summary

- UC-SDS can be realized by combining SDS and SDO.
- In accordance to societal values, individual preferences can be transformed to access control decisions/policies.
- A UC-SDS system can be designed with respect to societal and individual values: