Enforcement of Privacy-compliant Delegation of Personal Data

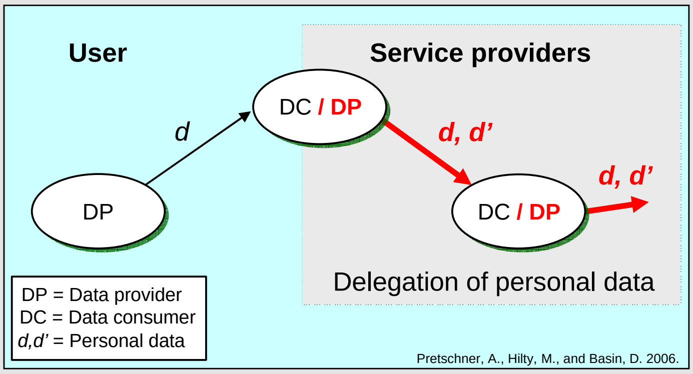
Sven Wohlgemuth Isao Echizen Noboru Sonehara Günter Müller

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



DP = Data provider
DC = Data consumer
d,d' = Personal data

Pretschner, A., Hilty, M., and Basin, D. 2006.

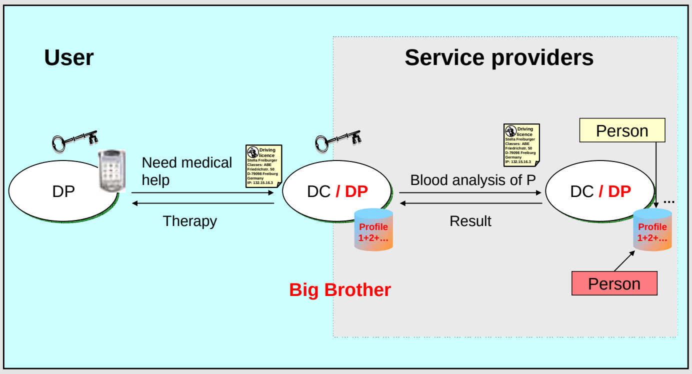
No Control on the Delegation of Personal Data

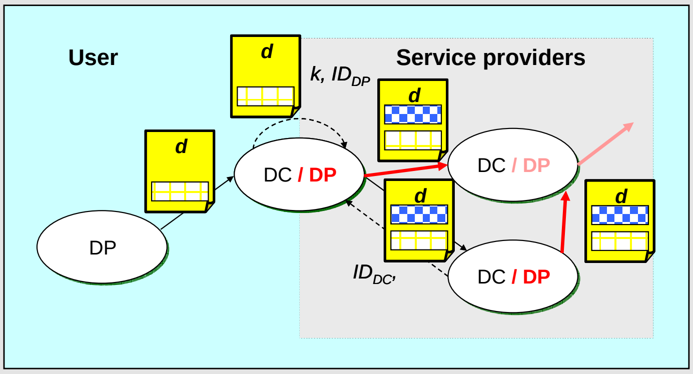
Identity Management and Delegation

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

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**





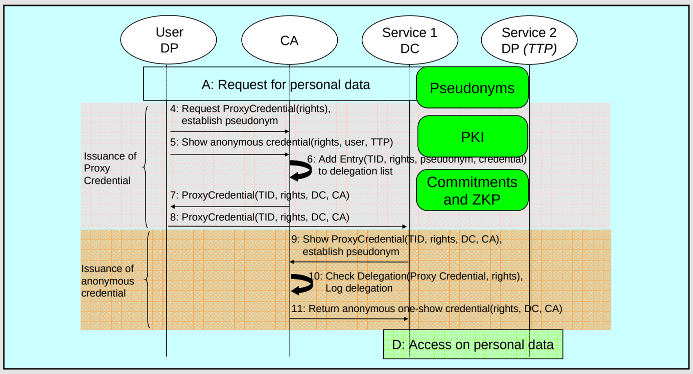
Controllable Delegation of Personal Data by DREISAM & DETECTIVE

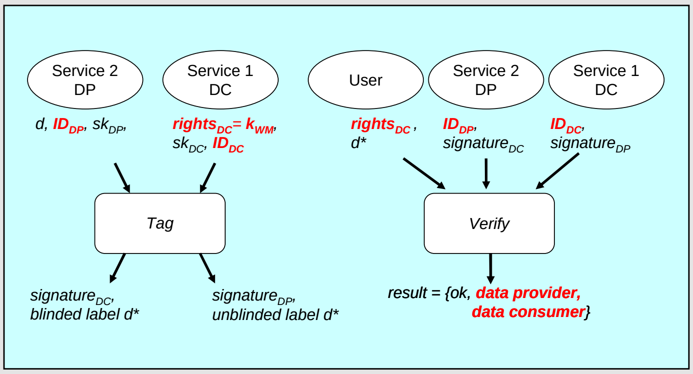
DREISAM: Non-linkable Delegation of Rights

- 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


User DP
CA
Service 1 DC
Service 2 DP (TTP)
A: Request for personal data
Pseudonyms
PKI
Commitments and ZKP
Issuance of Proxy Credential
4: Request ProxyCredential(rights), establish pseudonym
5: Show anonymous credential(rights, user, TTP)
6: Add Entry(TID, rights, pseudonym, credential) to delegation list
7: ProxyCredential(TID, rights, DC, CA)
8: ProxyCredential(TID, rights, DC, CA)
Issuance of anonymous credential
9: Show ProxyCredential(TID, rights, DC, CA), establish pseudonym
10: Check Delegation(Proxy Credential, rights), Log delegation
11: Return anonymous one-show credential(rights, DC, CA)
D: Access on personal data


Service 2 DP
Service 1 DC
User
Service 2 DP
Service 1 DC
d, ID_DP, sk_DP,
rights_DC = k_WM, sk_DC, ID_DC
rights_DC, d*
ID_DP, signature_DC
ID_DC, signature_DP
Tag
Verify
signature_DC, blinded label d*
signature_DP, unblinded label d*
result = {ok, data provider, data consumer}

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

NII Contact: Sven WOHLGEMUTH - JSPS Postdoctoral Fellow at the Digital Content and Media Sciences Research Division
TEL : 03-4212-2594 FAX : 03-3556-1916 (c/o Isao Echizen) Email : wohlgemuth@nii.ac.jp