RECOMMENDATIONS FOR THE EUROPEAN DIGITAL IDENTITY: ANALYZING PRIVACY PROTECTION MEASURES OF NOTIFIED EID SCHEMES

by Daniel Ostkamp, iHub, Radboud University

Disclaimer: work in progress

INTRODUCTION

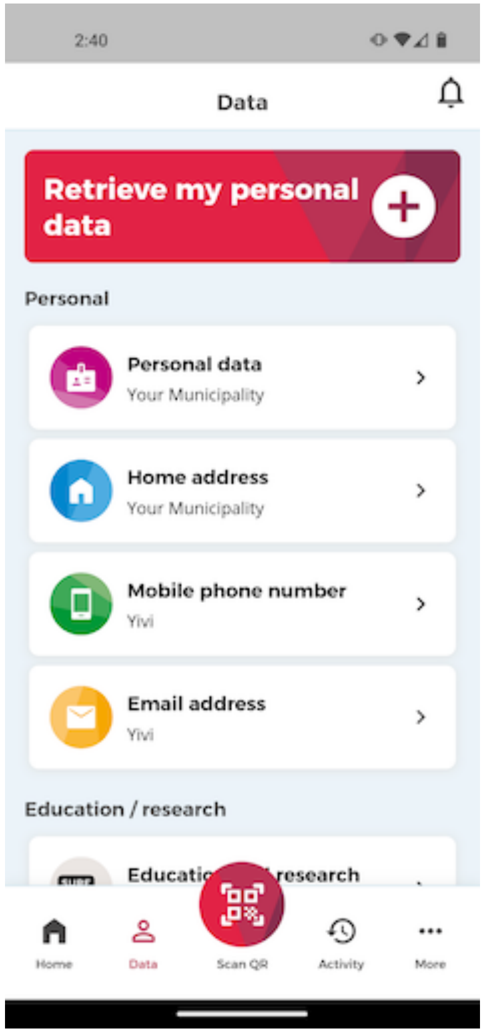
- Electronic IDentification (eID) often used to authenticate to public services.
- Via eIDAS 1.0 regulation, member states can register eID schemes within EU.
    - Goal: make it easy for citizens to authenticate across borders in a secure way.
- All schemes should be compliant with General Data Protection Regulation (GDPR).
    - Goal of GDPR: increase citizen's control and rights over their personal data.
    - Organizations need to implement "appropriate technical and organizational measures"

APPROACH

- First, gather information available online about schemes (GDPR Art. 12 asks for transparency)
- Second, analyze how schemes adhere to GDPR's privacy properties to identify technical measures
- Third, provide recommendations for European Digital Identity (EUDI) wallet providers to help achieve data protection by design and by default (GDPR Art. 25)

EUROPEAN DIGITAL IDENTITY WALLETS?

- Amend eIDAS 1.0 regulation
- Goal is to give citizens more control about their identity data and better data protection
- Have identity data stored within wallet app
- Yivi mobile app example:



2:40

Data

Retrieve my personal data

Personal

Personal data
Your Municipality

Home address
Your Municipality

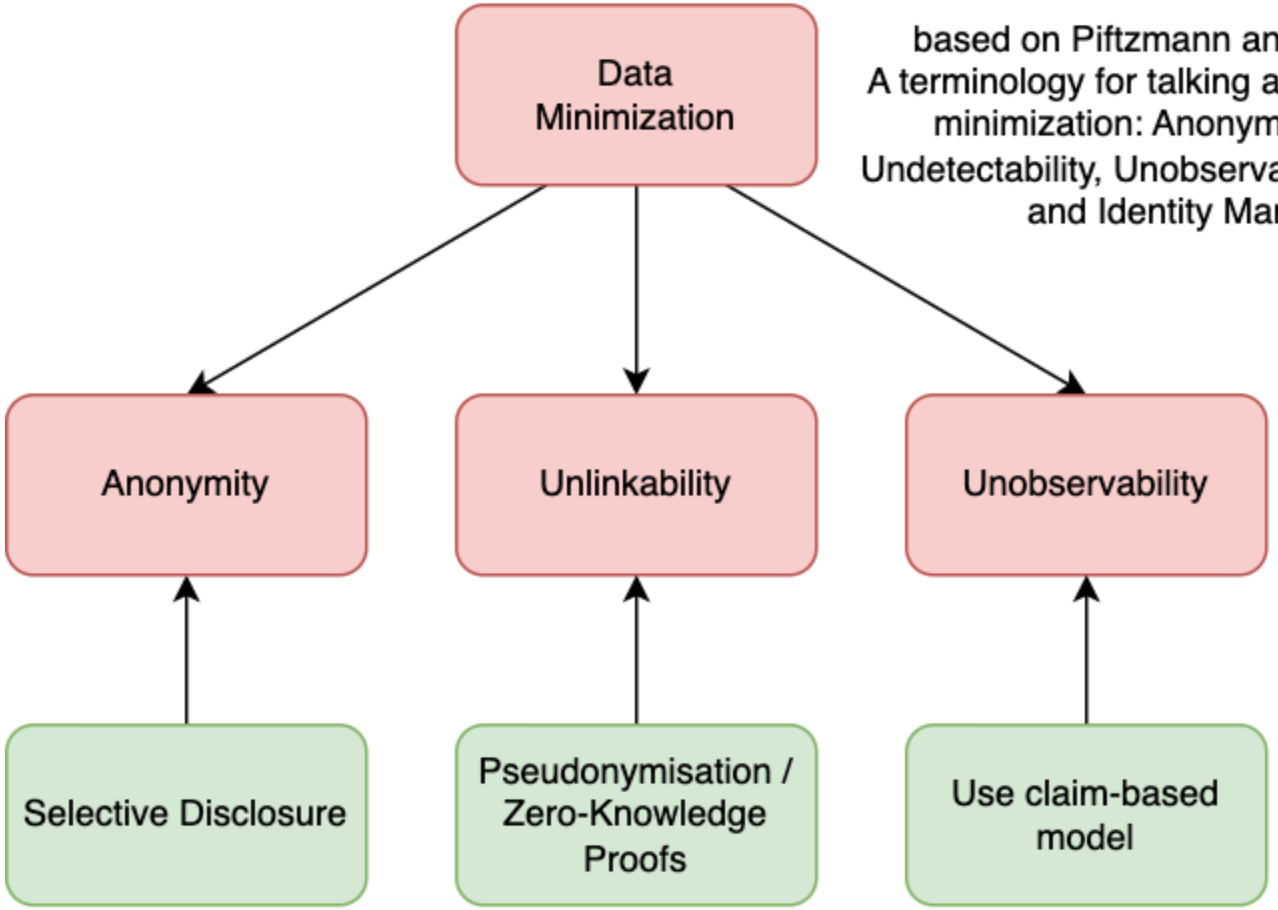
Mobile phone number
Yivi

Email address
Yivi

Education / research

Educatio research

PRIVACY PROPERTIES AND MEASURES



Data Minimization

Anonymity

Unlinkability

Unobservability

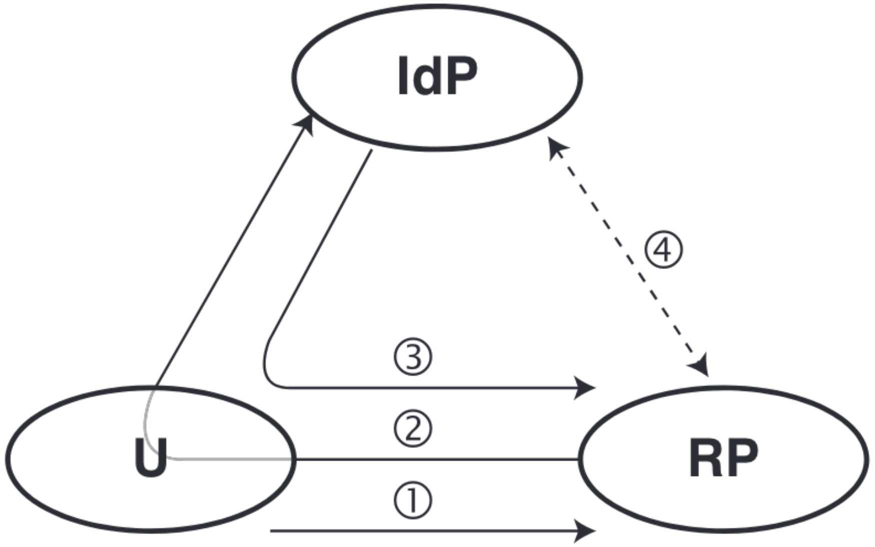
Selective Disclosure

Pseudonymisation / Zero-Knowledge Proofs

Use claim-based model

based on Piftzmann and Hansen (2011):
A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management

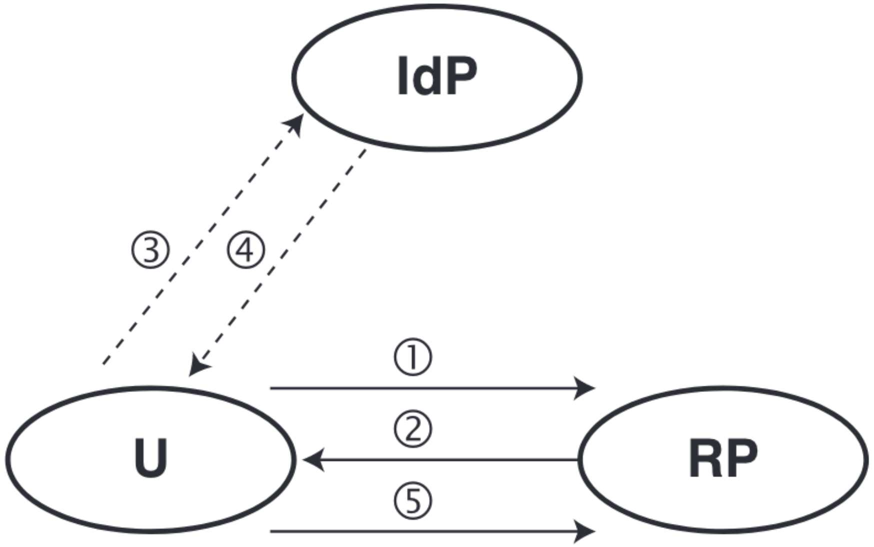
EID MANAGMENT SYSTEM MODELS



① request service
② authenticate at IdP
③ authentication result

optional step
④ *exchange additional info*

network-based



'cachable' steps
③ *authenticate*
④ *send claims*

① request service
② send policy
⑤ supply claims

claim-based

NOTIFIED EIDAS SCHEME AND CLAIM-BASED MODEL: GERMAN EID (NPA)

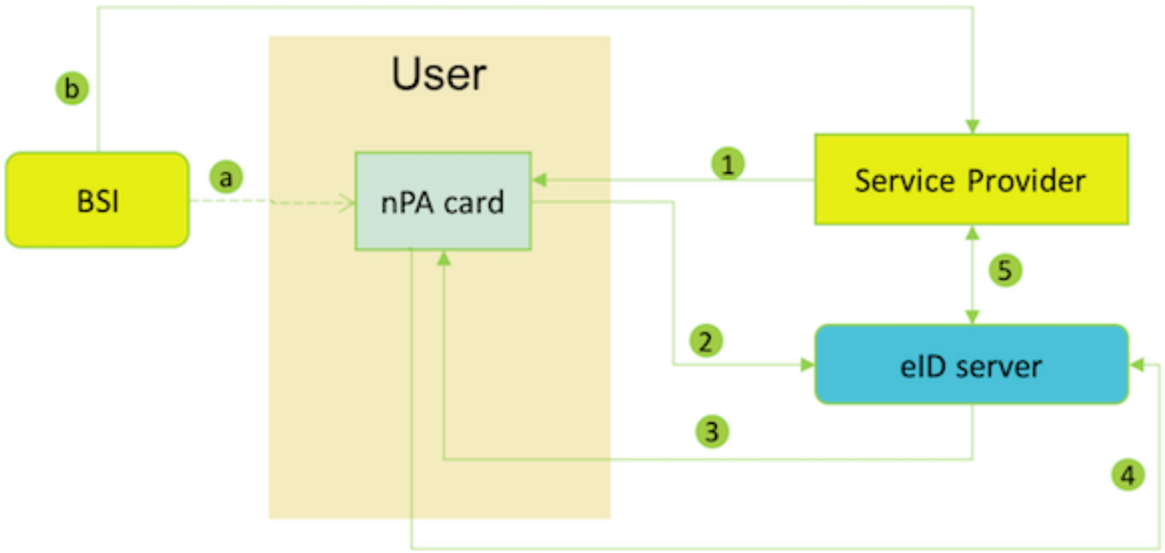


FIGURE 8.3: nPA actors and data flows

RECOMMENDATIONS FOR DATA PROTECTION BY DESIGN AND BY DEFAULT

- Be transparent to establish trust with citizens
    - Can increase adoption
- Conduct a Data Protection Impact Assessment (GDPR Art. 35)
- Focus on data minimization measures:
    - Selective disclosure (see nPA or Yivi)
    - Pseudonymization (see DigiD High)
    - Claim-based model (not mandatory in EUDI!)