Measures against over-asking in SSI and the Yivi ecosystem

Master thesis presentation, 13 October 2023
Job Doesburg
MEASURES AGAINST OVER-ASKING IN SSI

Agenda

1. Brief introduction to SSI (and Yivi)
2. Analysis of the over-asking problem
3. Some measures to reduce the problem
SELF-SOVEREIGN IDENTITY (SSI) / YIVI
MEASURES AGAINST OVER-ASKING IN SSI
FEDERATED IDM

Inloggen

(Identity Provider)
issuer

(Service Provider)
verifier

user

1

2

3

Sign in

Sign in with Google
MEASURES AGAINST OVER-ASKING IN SSI
YIVI ECOSYSTEM (PREVIOUSLY IRMA)
MEASURES AGAINST OVER-ASKING IN SSI
YIVI ECOSYSTEM (PREVIOUSLY IRMA)
OVER-ASKING
MEASURES AGAINST OVER-ASKING IN SSI

Problem

Webshop.nl asks you to disclose the following:

- Your first name
- Your last name
- Your postal address
- Your BSN

Cancel  Proceed
Problem

MEASURES AGAINST OVER-ASKING IN SSI

Your future employer asks you to disclose the following:

- Your first name
- Your last name
- Your diplomas
- Your medication list

Cancel  Proceed
Problem

Is clicking the “proceed” button actually true (freely given, informed) consent?

• Unawareness / ignorance of the user
• Power imbalance between verifier and user
How can we protect users against unacceptable disclosure requests?
“Requiring users to *know* which verifiers to trust is very similar to asking users to know which websites to trust, even when they have not visited them before. [...]”

Web browsers indicate if a secure TLS session has been established [...] by displaying a lock icon next to the web site’s URL. Something similar will be needed for SSI [...] to enable human users to determine if a verifier is trustworthy or not”

(Chadwick et al., 2023)
MEASURES AGAINST OVER-ASKING IN SSI

Problem

Is clicking the “proceed” button actually true (freely given, informed) consent?

• Unawareness / ignorance of the user
• Power imbalance between verifier and user

• Users actively need help protecting their own privacy!
  • Duty of care? For platform (Yivi)? Issuer? Government?
Why over-asking is a greater risk in SSI than in other forms of IdM:

- **Unsilousing of data** → more data that is more easily available
- **No gatekeepers** → no IdP can be held accountable
- **Loss of context-awareness** → no intuitive context association with specific IdP

- **Unfair expectations**: SSI is advertised as a privacy-friendly technology. People might expect that simply by using it, violating your own privacy is impossible.

- **Decentralized nature of SSI makes** over-asking intransparent and harder to detect
MEASURES AGAINST OVER-ASKING IN SSI

THE CURRENT YIVI ECOSYSTEM (AND THE GENERAL SSI LANDSCAPE)

• Few issuers, many verifiers
• Deliberate choice: everyone can be a verifier
• Being a verifier is easy (important for adoption)

• Yivi: “Back in charge of your digital data. All you. All yours”
• Users choose to whom they disclose their data (autonomy).
• Ideologically: full autonomy is a feature
  Pragmatically: some data might be too sensitive to be requestable by anyone (even with permission from the user)...
  → Don’t give a monkey a gun
MEASURES AGAINST OVER-ASKING IN SSI

BACKGROUND

• Use cases:
  • BSN
  • DNA medication passport (LUMC)
  • Biometric attributes
  • Other use cases... (possibly economic interests from the issuer!)

• Meanwhile, the EU Digital Identity Architecture and Reference Framework (outline):

  “In addition, the EUDI Wallet may: [...] restrict sharing certain sets of attributes with certain parties, or warn the user that the relying party may not be authorized to use/ask for these attributes.”

  → so, authorisation of relying parties will be a thing...
  ...while current SSI implementations ignore this
SOLUTIONS
MEASURES AGAINST OVER-ASKING IN SSI
RECALL: YIVI ECOSYSTEM (PREVIOUSLY IRMA)
**MEASURES AGAINST OVER-ASKING IN SSI**

**CHALLENGES**

**Challenges** for proof-requests:
1. Authentication
2. Authorisation

**Goals** for implementation:
- Technically feasible (easy to implement and maintain)
- Ease of use for verifiers (easy adoption)
- Maintaining SSI benefits (privacy, user autonomy)
- Minimal administrative workload, at the responsible parties

→ don’t introduce a dedicated PKI if it’s not necessary
• Attributes that can only be requested by an authorised party
• Easy to implement

• Yivi: authentication based on TLS hostnames (like already existing pretty verifiers)
  • Scheme links hostnames to requestor ID
  • No (extra) key management, TLS already required!

• Authorisation:
  • Via issuer-scheme (list authorised requestor IDs)
  • Via authorisation server (similar to revocation server)

⇒ For selected, (highly) sensitive attributes (issuer’s responsibility)
MEASURES AGAINST OVER-ASKING IN SSI

SOLUTION 1: PROTECTED ATTRIBUTES

Issuer scheme

Requestor scheme
Protected attributes are no general solution against over-asking.
- Consider a book-store asking for your email address.
- Context of a data request is essential!

→ Third-party judgement required, certifying disclosure requests.

General authority:
- Expensive & unrealistic on a global scale.

Open public self-registration (only authentication):
- Democratic bodies and interest groups can perform audits.
- Transparency → self-regulatory incentive.

Hybrid approach!

⇒ No perfect technical solution, but a sufficient countermeasure in practice.
MEASURES AGAINST OVER-ASKING IN SSI
SOLUTION 2: CERTIFIED DISCLOSURE REQUESTS

Requestor scheme

```json
[...
{
  "id": "pbdf-requests.someauthorisedparty",
  "name": {
    "en": "Example requestor",
    "nl": "Voorbeeld requestor"
  },
  "hostnames": [
    "authorised-requestor.example.com"
  ],
  "certified_requests": [  
    
    "disclose": [  
      ["pbdf.pddf.email.email"
      ],
    "reason": {
      "en": "To send you a newsletter",
      "nl": "Voor het versturen van een nieuwsbrief"
    }
    ],

    ]
  }

]...
```
MEASURES AGAINST OVER-ASKING IN SSI

CONCLUSION

- Protected attributes: *issuer’s responsibility*
- Certified disclosure requests: *third-party responsibility*
- Hybrid implementations are possible, systems can co-exist!

- User experience design is important, too!

- TLS-based authentication and scheme-based authorisation is easiest for Yivi and verifiers
  - Scalability might be problematic long-term
  - Federated schemes + *Just-In-Time*-scheme retrieval can reduce this problem
Measures against over-asking in SSI and the Yivi ecosystem

Master thesis presentation, 13 October 2023
Job Doesburg
ADDITIONAL SLIDES
MEASURES AGAINST OVER-ASKING IN SSI

USABILITY ASPECTS

- Wallet should display disclosure request context
  - Who receives the data?
  - Why do they need the data / for what reason are they authorised to receive this data?

- Permissive or strict wallets (warning or error)
  - Different kinds of warnings, should create awareness
  - Generally, permissive > strict

- Categorised credentials and verifiers
  - Sphere transgression will happen (and can be okay!), but users need to be made extra aware when it happens
MEASURES AGAINST OVER-ASKING IN SSI

FEDERATED SCHEME & JIT SCHEME-RETRIEVAL

• Including all verifiers in the central scheme is bad for scalability

• Wallet only needs to know (partial) verifier scheme upon communication with that verifier
  • Idem issuer/credential scheme
    → only send the partial scheme when it’s needed!

• Only send (signed!) partial schemes during disclosure/issuance session

• Scheme can be split up in hierarchical / federated schemes for governance