Service Provider Accreditation: Enabling and Enforcing Privacy-by-Design in Credential-based Authentication Systems

Stefan More
smore@tugraz.at
Graz University of Technology
and Secure Information Technology Center Austria (A-SIT)
Graz, Austria

Jakob Heher
jakob.heher@iaik.tugraz.at
Graz University of Technology
and Secure Information Technology Center Austria (A-SIT)
Graz, Austria

Edona Fasllija
edona.fasllija@iaik.tugraz.at
Graz University of Technology
and Secure Information Technology Center Austria (A-SIT)
Graz, Austria

Maximilian Mathie
mathie@student.tugraz.at
Graz University of Technology
Graz, Austria

Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES 2024)
https://doi.org/10.1145/3664476.3669934

Service Provider Accreditation:
Enabling and Enforcing Privacy-by-Design in Credential-based Authentication Systems

Stefan More, Jakob Heher,
Edona Fasllija, Maximilian Mathie

Graz University of Technology
and Secure Information Technology Center Austria (A-SIT)

Electronic Identity Systems

Focus:
User-centric (Credential-based)

Wallets

Credentials

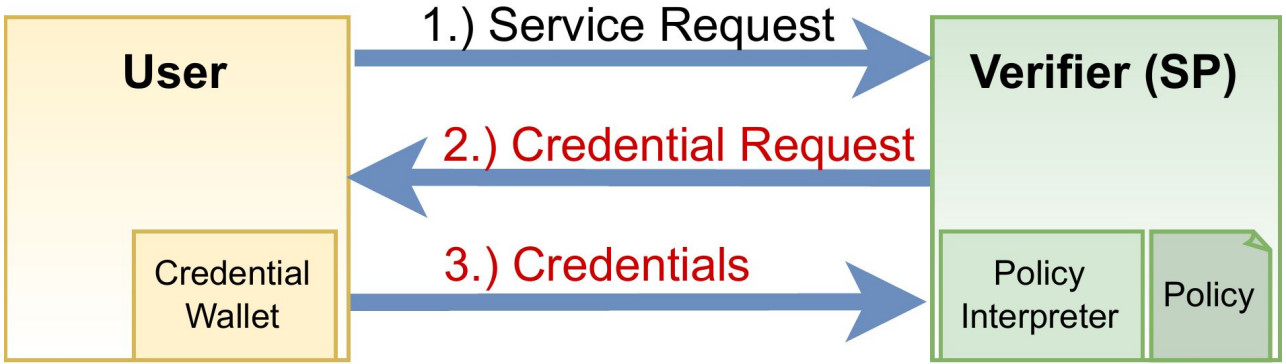
Green Pass

(and more)

[The EUDI Wallet's] vision is ambitious and requires functions way beyond what typical wallets do today. It also requires an infrastructure for trust management **to protect users from malicious** issuers, wallet providers or **relying parties**. Also, the security and privacy requirements are much higher than what has been implemented in the past, resistance against high attack potential in conjunction with **unlinkability and unobservability of transactions**, just to name a few.

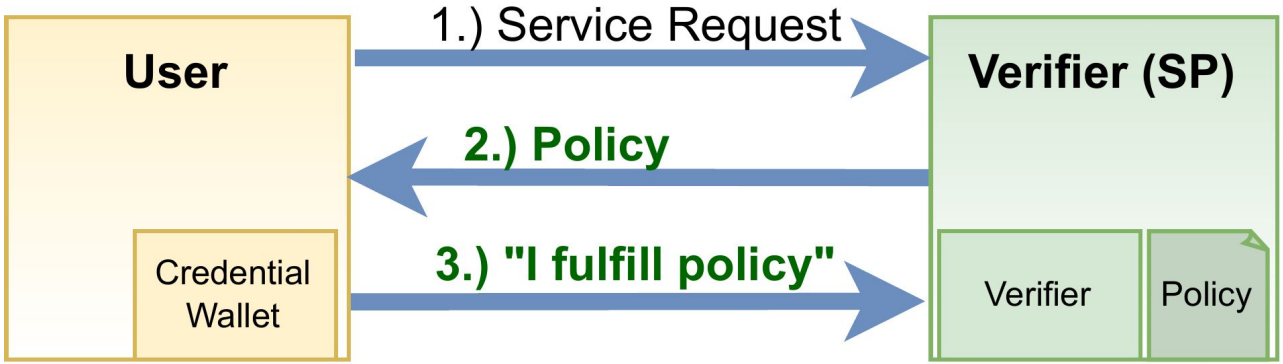
Abstract of Torsten Lodderstedt's EDId '24 Keynote

Wallet-based Authentication Flow



Service Provider = Verifier, Relying Party

Wallet-based Authentication Flow



Privacy Goals

Examples:

- Confidentiality, Data Minimization
- Unobservability, Unlinkability
- Anonymity and Pseudonymity

GDPR: Specific, explicit and legitimate **Purpose**

Challenges: Burden to decide is on the user

Problem: **SP (Verifier) Identity**
(Liability, Accountability …)
Legitimacy

Idea: **Accreditations**

Examples:
- Police service card (Dienstausweis)
- Doctor, hospital

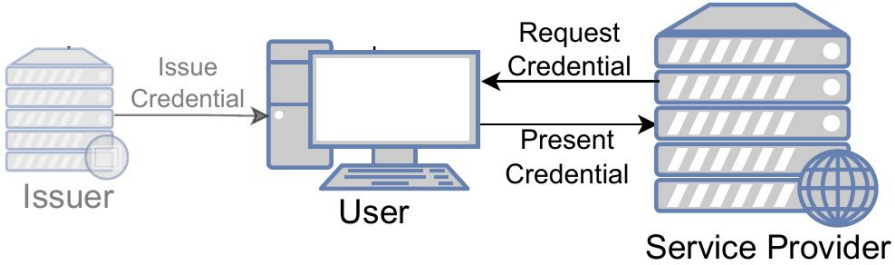
Problem: **Over-asking by SP**

Idea: **Enforceable Constraints**

Examples:
- Restrict to public-transport ticket
- Restrict to age-check

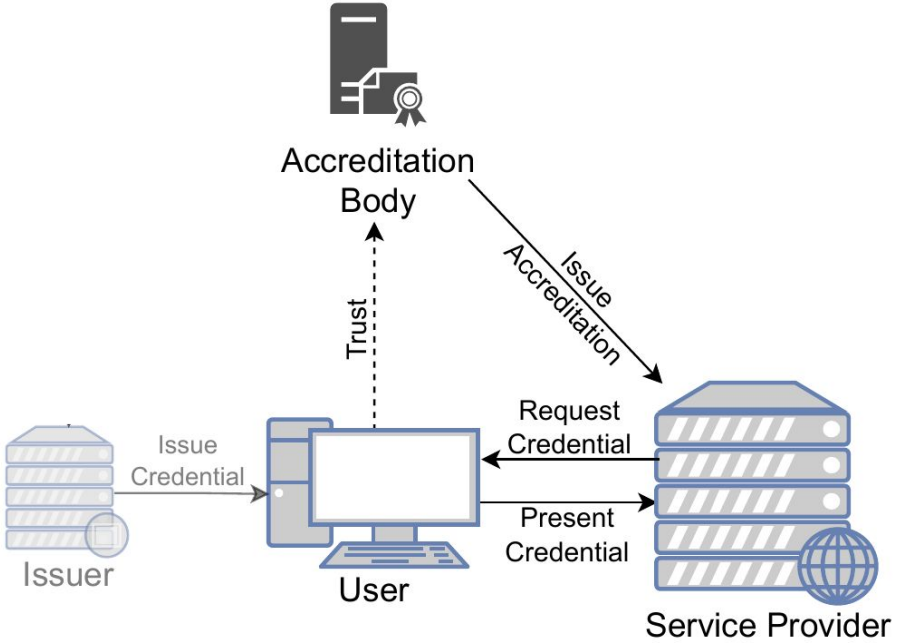
Service Provider Accreditation

Service Provider =
Verifier, Relying Party



Service Provider Accreditation

Service Provider =
Verifier, Relying Party



Types of Accreditation Constraints

Granularity:

Boolean
Ordinal
Advanced

Advanced Constraints:

- Credentials
- Attributes
- Predicates

Accreditation Constraints vs. Disclosure Policies

Accreditation Constraints:

- *(our working title)*
- Attached to *Accreditation* (SP Authorization)
- Rules about *what data* the SP is allowed to access

Disclosure Policies:

- eIDAS 2, Article 5a § 5 (e)
  but no details.
- Embedded in *Attestation* (User Credential)
- Rules about *which SP* is allowed to access the data
- Requirements in
  ARF (v1.4) §§ 6.6.3.3 & A.2.3.43

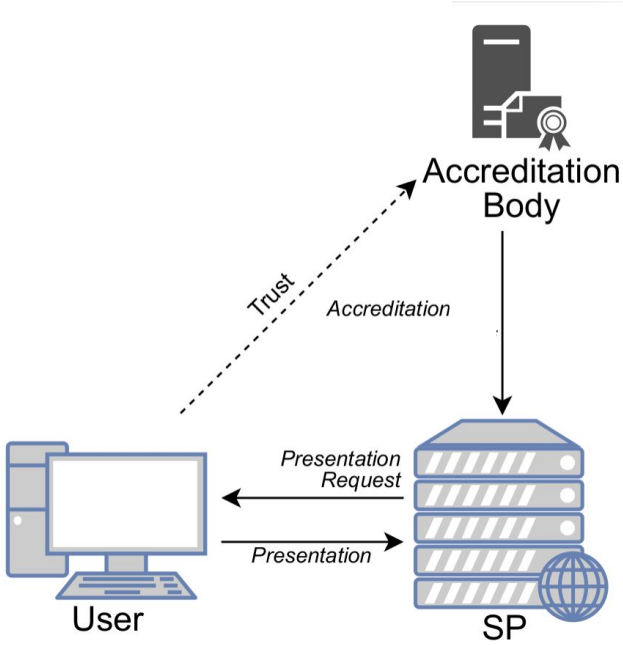
Further Challenge: Trust in the system

Problem: Over-asking by SP & **Misbehaving AB**

Idea: Let 3rd parties audit the Accreditation Body
Auditable Accreditation Registry

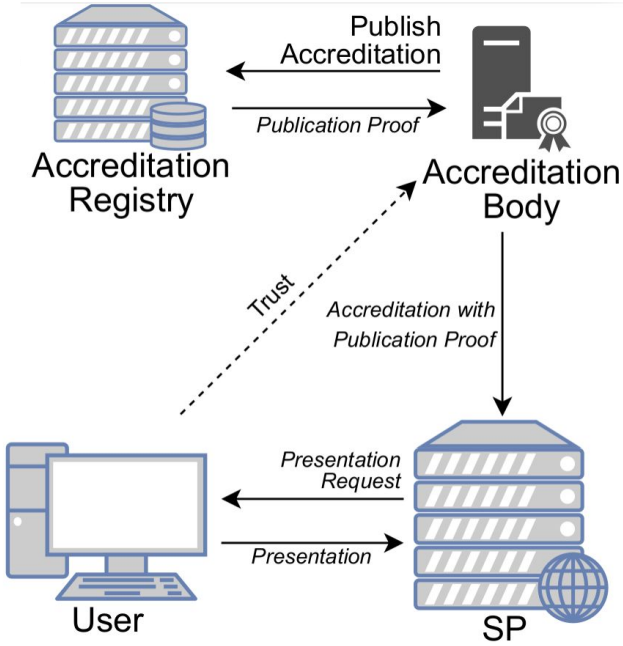
Related concept:
Data processing register

Auditable
Accreditation Registry

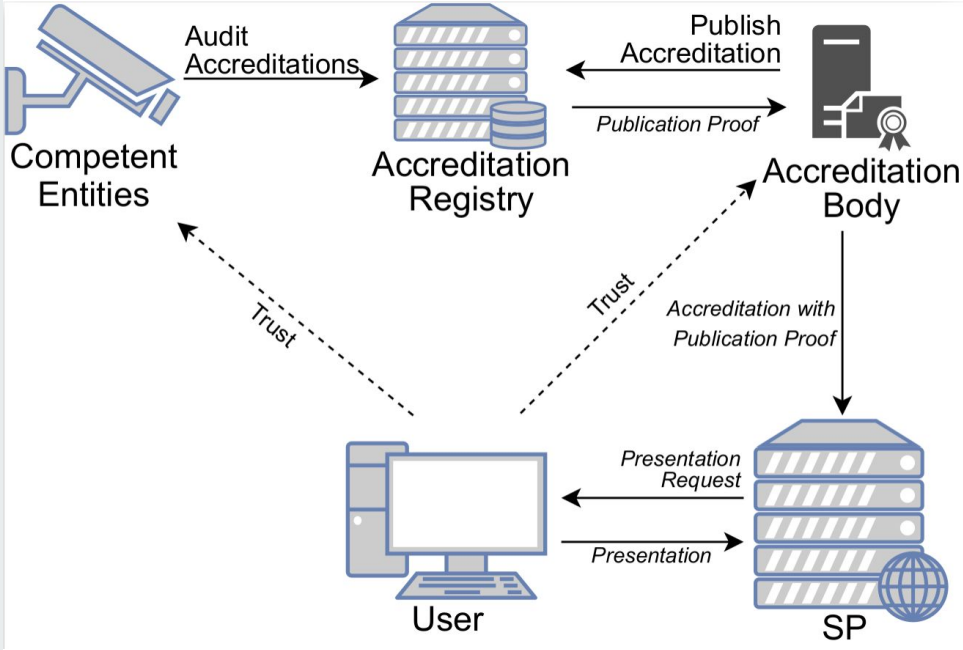


Auditable

Accreditation Registry



Auditable Accreditation Registry



eIDAS 2 Regulation: Inform or Enforce?

Article 5b

European Digital Identity Wallet-Relying Parties

1. Where a relying party intends to rely upon European Digital Identity Wallets for the provision of public or private services by means of digital interaction, the relying party shall register in the Member State where it is established.

2. The registration process shall be cost-effective and proportionate-to-risk. The relying party shall provide at least:

(a) the information necessary to authenticate to European Digital Identity Wallets, which as a minimum includes:

  (i) the Member State in which the relying party is established; and

  (ii) the name of the relying party and, where applicable, its registration number as stated in an official record together with identification data of that official record;

(b) the contact details of the relying party;

(c) the intended use of European Digital Identity Wallets, including an indication of the data to be requested by the relying party from users.

3. Relying parties shall not request users to provide any data other than that indicated pursuant to paragraph 2, point (c).

Auditable Accreditation Registry: Halfway there?

Article 5b

European Digital Identity Wallet-Relying Parties

1. Where a relying party intends to rely upon European Digital Identity Wallets for the provision of public or private services by means of digital interaction, the relying party shall register in the Member State where it is established.

2. The registration process shall be cost-effective and proportionate-to-risk. The relying party shall provide at least:

(a) the information necessary to authenticate to European Digital Identity Wallets, which as a minimum includes:

  (i) the Member State in which the relying party is established; and

  (ii) the name of the relying party and, where applicable, its registration number as stated in an official record together with identification data of that official record;

(b) the contact details of the relying party;

(c) the intended use of European Digital Identity Wallets, including an indication of the data to be requested by the relying party from users.

3. Relying parties shall not request users to provide any data other than that indicated pursuant to paragraph 2, point (c).

4. Paragraphs 1 and 2 shall be without prejudice to Union or national law that is applicable to the provision of specific services.

5. Member States shall make the information referred to in paragraph 2 publicly available online in electronically signed or sealed form suitable for automated processing.

Open Questions

- Standardization
  e.g., of SD/ZKP System?
- EC Signatures vs. *BBS/BBS#*?
- Credential/Attribute/Predicate Namespacing?
  [controlled vocabulary via catalogues]

- Enforce (strong privacy [Art. 5b § 3]) or Inform (user choice [Art. 5a § 5 (e)])?
- What if SP's legitimate requirements change [Art. 5b § 6]?
- Is SP's lists of constraints (required attributes) public [Art. 5b §. 2]?

eIDAS 2 Timeline?
(Implementing acts already until November 2024. Wallets until May 2026.)

Service Provider Accreditation:

Enabling and Enforcing Privacy-by-Design in Credential-based Authentication Systems

Stefan More, Jakob Heher,
Edona Fasllija, Maximilian Mathie

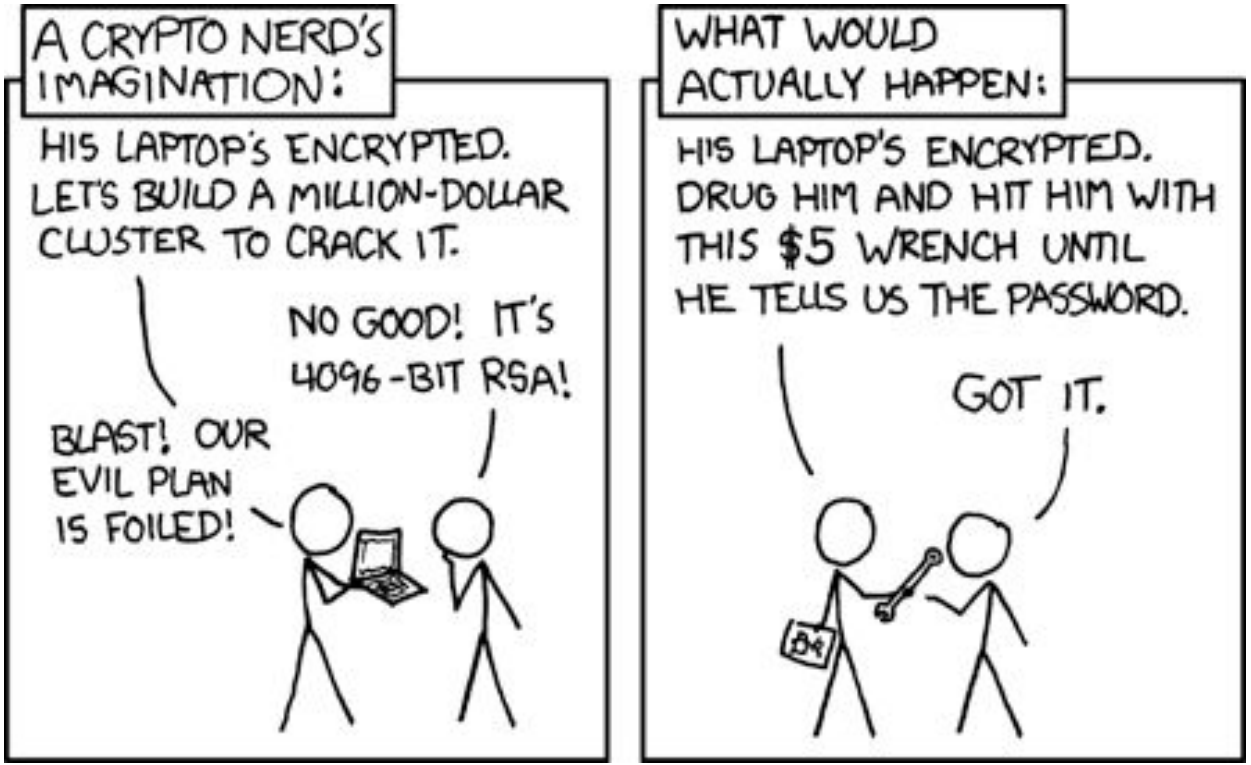
smore@tugraz.at

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020416 (ERATOSTHENES).

Backup Slides

(Wallet) Security

Or: Is (attested) sensitive data in the user or RP domain a good idea?



xkcd.com/538

Legal Requirements from eIDAS 2

SP Registration: A SP shall register in the Member State where it is established. SPs shall identify themselves to the user [8, Article 5b].

Purpose Registration: During registration, a SP shall provide indication of the data to be requested from users, and shall not request any other data than indicated [8, Article 5b].

Purpose Information: Wallets shall inform the user whether the SP has the permission to access a credential [8, Article 5a].

Auditability: The list of registered SPs and their indicated data processsing shall be public in a form suitable for automated processing [8, Article 5b].

Unlinkability: The technical framework shall ensure unlinkability [8, Article 5a].

Selective Disclosure: The technical framework shall ensure that selective disclosure of data is possible [8, Article 5a].

Unobservability: The technical framewark shall not allow Issuers or any other party to track, link or correlate user behavior [8, Article 5a].

Pseudonyms: The use of pseudonyms that are chosen and managed by the user shall not be prohibited [8, Article 5]. Wallets shall enable the user to generate pseudonyms and store them encrypted and locally [8, Article 5a]. SPs shall not refuse the use of pseudonyms, except where the identification of the user is required by law [8, Article 5b].

Privacy

Privacy (noun):

- from Latin *Privatus*: what is private
- *the claim of individuals [...] to determine for themselves when, how, and to what extent [any] information about them is communicated to others*

Privacy is a right!

Example: European Convention on Human Rights (Article 8):
Everyone has the right to respect for his private and family life, his home and his correspondence.

Privacy Preserving/Enhancing Technologies

Selective Sharing
of Credentials

Selective Sharing
Of Attributes
("Selective Disclosure")

Predicates on Attributes
("Zero-knowledge Proofs")

Multi-signatures, Accumulators, Multi-party computation, Homomorphic encryption, Private information retrieval, …

Stefan More

IAIK Secure Applications Group

Research Topics:

- Applied **Security**, Web Security
- Applied **Privacy**
- **Trust** and **Identity** Management