PETS 2026 POSTER DRAFT | EUDI WALLET PRIVACY

Privacy and Assurance Tensions in EUDI Wallet Presentation Flows

Anton Sokolov

Core Question

When an EUDI Wallet flow claims selective disclosure, pseudonymity, or unlinkability, what exactly is protected, against which actor, and what evidence could certification realistically inspect?

Motivation

The EUDI Wallet combines high-assurance identity, interoperability, and user-controlled disclosure. These goals are not automatically aligned.

A credential presentation can minimize disclosed attributes while still leaking correlatable metadata through verifier behavior, status checks, relying-party registration, wallet-unit binding, or repeated presentation identifiers.

The risk is that ecosystem participants treat "supports selective disclosure" or "supports ZKP" as a broad privacy guarantee.

Actors

- Holder / wallet user
- Wallet unit and wallet provider
- Issuer or attestation provider
- Verifier / relying party
- Relying-party registration authority
- Status and revocation infrastructure
- Conformity assessment body
- National or EU supervisory authority

Information Flow

Issuer verifies eligibility and issues credential > **Wallet stores credential, keys, status, lifecycle data**

Verifier requests attributes, predicates, or credential > **Wallet mediates consent and user intent**

Wallet produces presentation using profile/protocol > **Verifier checks authenticity, status, binding**

Privacy Properties To Separate

Selective Disclosure

- What attribute values or predicates are disclosed?
- Can hidden values be inferred from schema, issuer, status, or context?

Unlinkability

- Can two presentations be linked by the same verifier?
- Can presentations be linked across verifiers?
- Can issuer/status infrastructure observe presentations?

Pseudonymity

- Is the pseudonym pairwise, sector-specific, or global?
- Who derives or controls it?
- Can it be reset, rotated, or recovered?

Threat Scenarios

Verifier correlation A verifier asks for minimal attributes but stores timestamps, credential format details, wallet metadata, or stable identifiers.

Status correlation Online status checks reveal presentation events to issuers or status services.

Binding overreach Holder or wallet-unit binding creates a stable cross-context signal.

Consent overclaim The wallet lets a user withdraw consent after disclosure, but the relying party has already copied data.

Certification mismatch Wallet implementation certification is interpreted as covering the full relying-party ecosystem.

Assurance Matrix

Claim	Needs Evidence About	Boundary Risk
Selective disclosure	Protocol transcript, disclosed fields, UI request display	Inference from metadata
Unlinkability	Identifiers, status checks, verifier logs, pairwise behavior	Verifier or issuer correlation
User binding	User intent, authentication ceremony, key usage context	Stable binding signal
Consent evidence	Request, purpose, relying party, disclosed data, withdrawal event	Post-disclosure enforceability

Proposed Checklist

1. Disclosed data: attributes, predicates, identifiers, metadata.
2. Hidden data: what is not revealed to the verifier.
3. Linkability: same verifier, cross-verifier, issuer/status infrastructure.
4. Binding: subject binding, wallet-unit binding, device binding, user-presence binding.
5. Status checks: online/offline, freshness, correlation resistance.
6. Consent: request clarity, purpose display, evidence retained.
7. Recovery/lifecycle: device loss, migration, refresh, revocation.
8. Certification evidence: logs, test vectors, code paths, protocol proofs, audit artifacts.
9. Residual risks: risks outside the wallet certification boundary.

Contribution

This poster proposes a certification-aware privacy checklist for EUDI Wallet presentation flows.

The method separates protocol guarantees, wallet implementation properties, relying-party behavior, and ecosystem assumptions.

This helps avoid privacy overclaims and makes wallet privacy claims more testable.

Discussion Questions

- Should certification include relying-party behavior, or only wallet/provider behavior?
- What evidence is needed to certify unlinkability claims?
- Should status/revocation systems be part of the privacy threat model?
- How should wallets explain post-presentation consent limits?
- Can a trust mark express privacy properties without becoming misleading?

Next Work

- Apply the checklist to OpenID4VP and EUDI ARF presentation profiles.
- Compare ZKP-based and non-ZKP selective disclosure flows.
- Map claims to evidence that conformity assessment bodies can inspect.

Keywords: EUDI Wallet, privacy, selective disclosure, unlinkability, ZKP, assurance, certification.

Artifact: Draft poster prepared for PETS 2026 poster track.

Contact: Anton Sokolov