It Wasn’t Me, It Was You: Deniable Authentication for the European Digital Identity
Prof. Anja Lehmann, Karla Friedrichs, Cavit Özbay
Cybersecurity – Identity Management

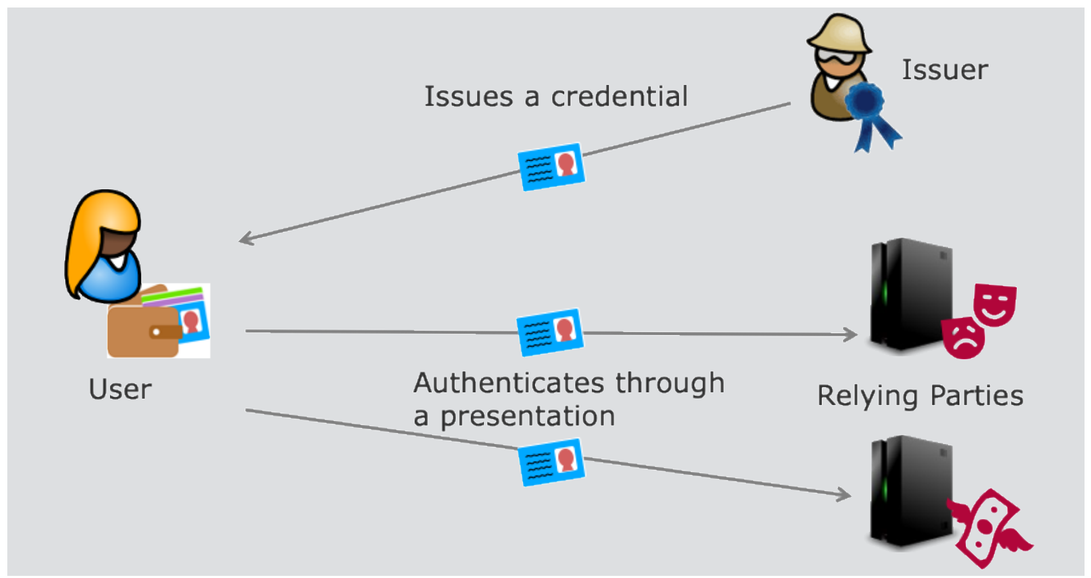
Hasso Plattner Institut
Digital Engineering · Universität Potsdam

It Wasn’t Me, It Was You: Deniable Authentication for the European Digital Identity

EU Digital Identity Wallet (EUDI)

The eIDAS 2.0 regulation requires every EU member state to provide a digital identity solution—the EU Digital Identity (EUDI) Wallet—by the end of 2026.

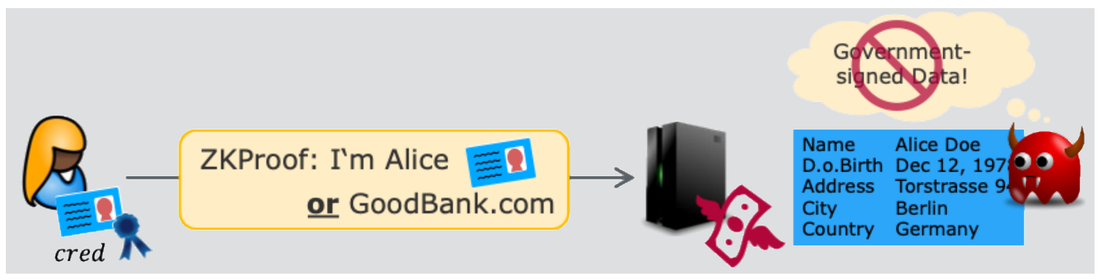
The EU decided to build the wallet from ECDSA-signed credentials, where a digital identity is an issuer’s signature on user attributes.



Critics reproach that this approach lacks an important privacy property: **plausible deniability**. When a user presents their digital identity, anyone can verify this presentation—and hence verifiers might be tempted to store and trade the authenticated data.

Deniable Authentication is Possible– Using Simple and Standard Techniques

Recent work shows that a standard zero-knowledge proof can add deniability to EUDI presentations. The idea is that the verifier holds its own key pair and that the user only reveals a part of the issuer’s signature. Then they prove, in zero knowledge, that they know either the rest of the issuer’s signature, or the verifier's secret key. Since the verifier knows its own secret key, it could have produced this proof itself—so the presentation convinces the intended verifier but is worthless as evidence to anyone else.



But: This solution (1) breaks down if a credential is presented more than once and (2) is purely theoretical for now.

Task 1: Explore Deniability Beyond the Single-Show Setting

As the presentation reveals one part of the issuer's signature, two presentations of the same credential expose an identical value. Deniability relies on the argument that the verifier could have fabricated the authentication transcript itself, sampling this value at random. But if two verifiers observe this same value, it is implausible that each produced it independently, by chance—the shared value is only explained by a genuine presentation of one underlying credential, and the user can no longer deny having authenticated.

The first task is, therefore, to develop a stronger security model and secure constructions in which credentials can be safely reused.

- **Formalize a multi-show notion of deniability**
- **Investigate constructions with multi-show deniability**

Task 2: Integrate Deniability into the EUDI Workflow and Data Formats

The EUDI system balances many requirements beyond deniability and follows the SD-JWT standard. We want to integrate the theoretical findings into this system—mapping the construction to the SD-JWT format and reconciling it with features such as session freshness and replay protection. Finally, we want to evaluate added communication and computation overhead of a proof-of-concept implementation to demonstrate real-world feasibility.

- **Map deniable presentations to the EUDI data formats and protocol flows**
- **Build and benchmark a proof-of-concept implementation**

Sneak Peak: Deniable ECDSA

Recall ECDSA signatures:

ECDSA.Sign$(sk, attr)$:
$k \xleftarrow{r} \mathbb{Z}_p^*$
$R \leftarrow G^k$
$r \leftarrow R.x$
$s \leftarrow k^{-1}(H(attr) + r \cdot sk)$
Return (r, s)

ECDSA.Vf$(pk, (r, s), attr)$: $R' \leftarrow \left(G^{H(attr)} + pk^r\right)^{s^{-1}}$
Return 1 if $R'.x = r$

Scan for details

To present an ECDSA signature deniably, we re-interpret the verification equation as a discrete logarithm relation between R' and $\left(G^{H(attr)} + pk^r\right)$. The user proves in zero-knowledge that it knows either s^{-1} or vsk: