

Salem Wollel

Authenticating and Authorizing the Caller: A Defense Mechanism Against Caller ID spoofing

Problem

- **Caller ID spoofing** presents a significant challenge in the context of phone communications.
- Attackers can manipulate caller ID information to impersonate a service provider.
- Call recipients currently lack effective methods to authenticate the identity of the caller.
- Beyond authentication, it is necessary to verify if the caller is authorized to use that phone number.
- Furthermore, a mechanism should exist to confirm that the call reaches the intended recipient.

European Digital Identity Wallet

- Based on eIDAS 2.0 regulation
- Cross-border electronic identification (e-ID)
- The future of strong authentication
- User Controlled Digital Identity – Personal Wallet
- Use Cases: Travel, driving license, online payments, SIM registration, sign contracts

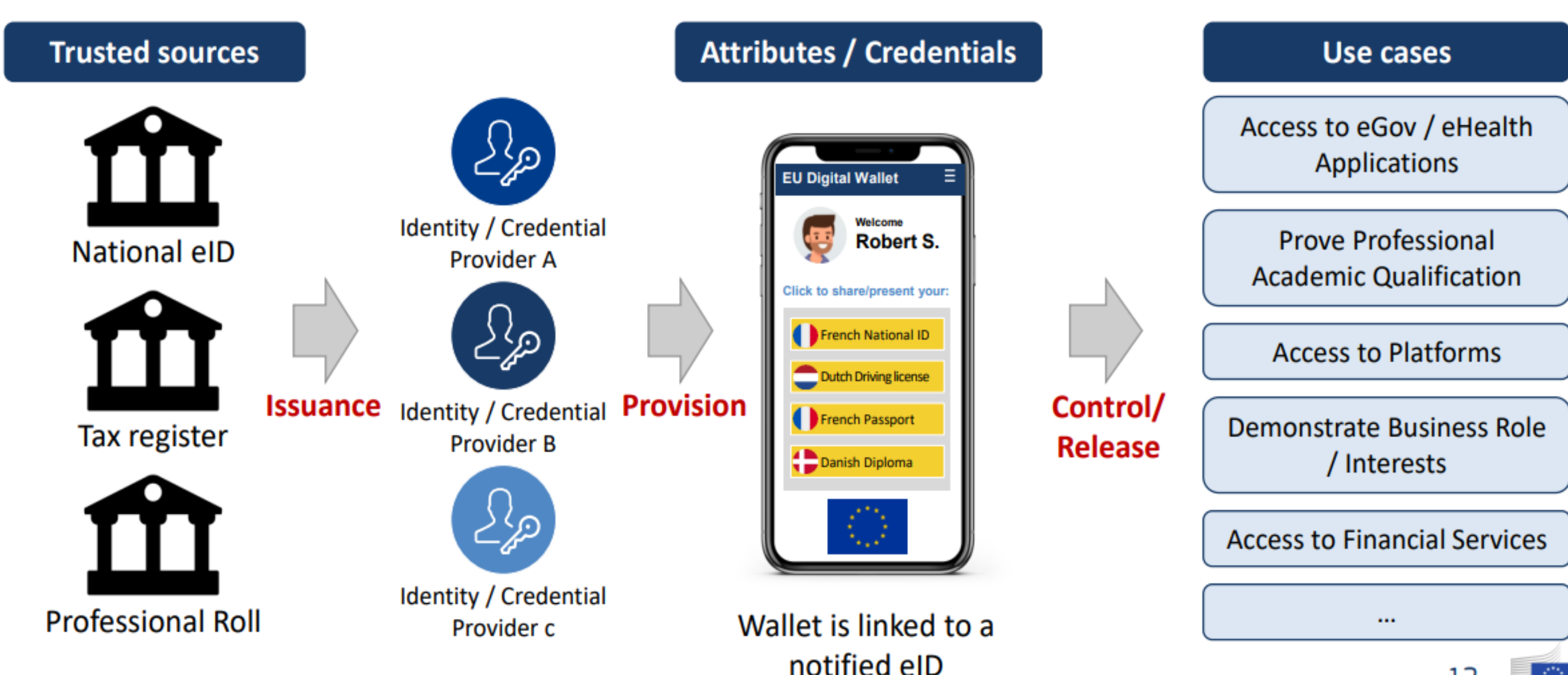


Figure 1: Overview of the EUDI Architecture

Proposed System Design

- A verifier caller application that authenticates the caller based on the credentials from the EUDI wallet
- Caller is authenticated **before** the call is forwarded

- Authorization of the calling personnel is verified for service provider calls.
- In sensitive scenarios, such as health care, it is crucial to make sure that the call reaches the intended recipient. For this reason, the caller can request for receiver authentication, after the call is established.

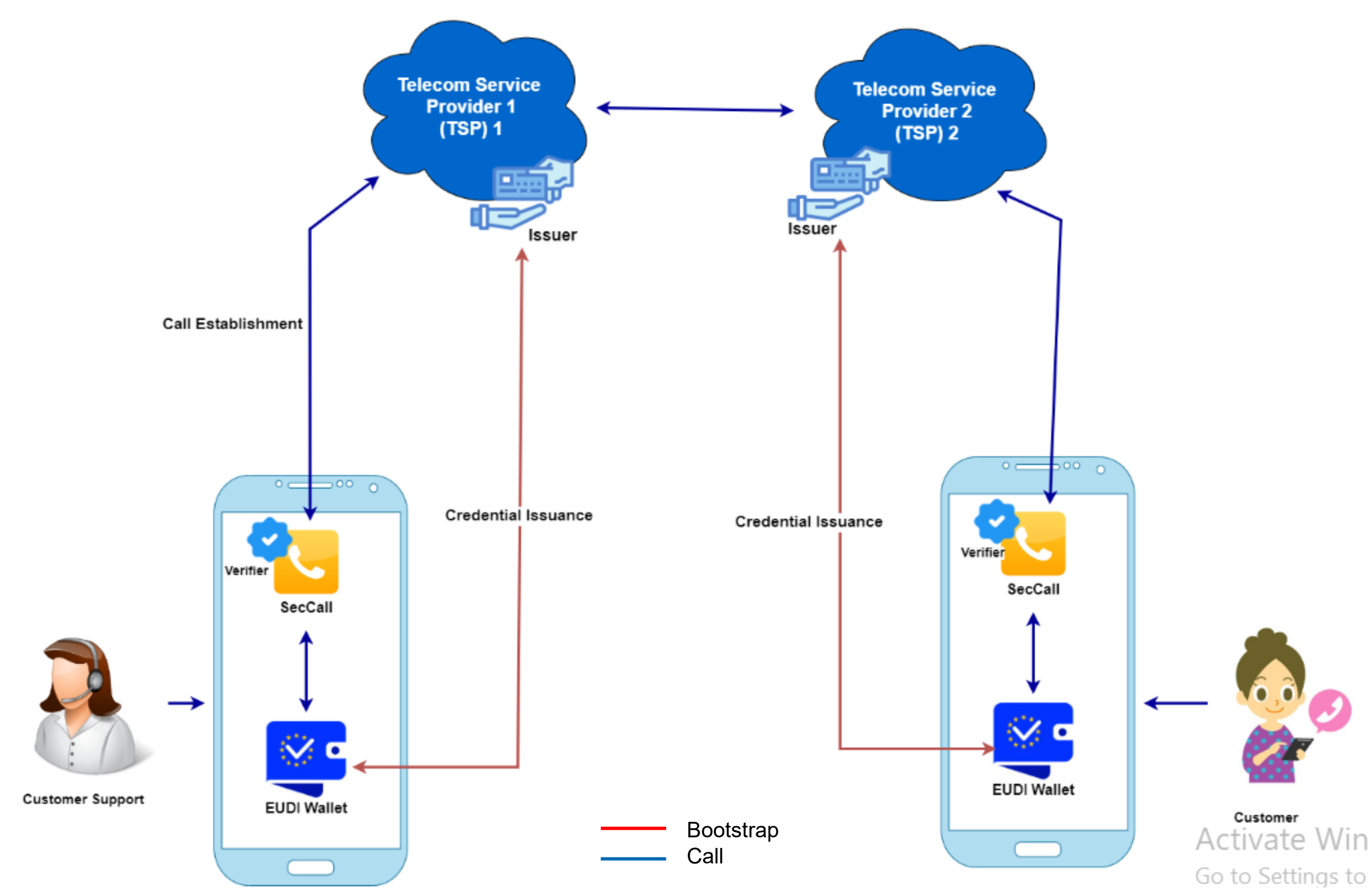


Figure 2: Proposed system design Architecture

Implementation (Planned)

- Implement a caller application that also serves as a verifier and integrate it to the EUDI wallet demo application