Real Time Economy

Legal person wallet anchoring in Finland

Draft flow description

Yrityksen digitalous | 17 Nov 2023 | Mikael Linden

Table of Contents

Version history

Version	Date	Editor	Description
0.1E	3 May 2023	Mikael Linden	First version for review within the project
0.2	6 Sep 2023	Mikael Linden	Aligned with the demo and screencast video
0.3	17 Nov 2023	Mikael Linden	Aligned terms

1 Introduction

1.1 Document goal

The goal of this document is to describe the current understanding of how an eIDAS 2.0 company[1] (legal person) wallet is anchored to the authentic source (Patent and Registration Office PRH's Business information system YTJ) in Finland.

The reader is supposed to be to some extent familiar with the key eIDAS concepts.

1.2 Document audience

The audience of this document is

- PRH and related public authorities in Finland, in their role as the PID/ODI attribute attestation issuer
- Potential wallet providers in Finland (and beyond), in their role as a party who needs to understand and support the retrieval of the PID/ODI attribute attestations to the wallets they host
- EUDI Wallet Consortium (EWC) Large Scale Pilot, whose WP3 and WP4 focus on PID/ODI issuing and retrieval to the company wallet

2 Description of attestations and actors

2.1 Assumed attribute attestations

Person Identification Data (PID) is the set of attributes to identify a legal or natural person. In EWC grant application, the PID for a legal person is called an **Organisational Digital Identity (ODI)**. It is assumed that the PID/ODI for a legal person consists of a name and a unique identifier, which in Finland is supposed to be the Business ID (Y-tunnus) issued by the Business Information System YTJ that Patent and Registration Office PRH manages.

Other organisational credentials are supposed to supplement PID/ODI by other relevant information on the company. Its contents are currently undefined but could cover, for instance, company status, legal form, address, date of registration and line of business. In Finland, that information is managed by PRH as well.

2.2 Description of actors

Business Information System YTJ, managed by Patent and Registration Office PRH, is the authentic source for company data in Finland.

Population registry, managed by Digital and Population Data Services Agency DVV, issues a Personal Identity Code (PIC, henkilötunnus) for each citizen and other person registered to the population registry.

Suomi.fi e-Identification service, managed by DVV, carries out strong (eIDAS

[1] The project's focus has been on company wallets, but it can be extended also to other registered legal persons, e.g. public sector entities.

substantial or high) authentication of a PIC holder and delivers the authenticated PIC to the relying party.

Suomi.fi e-Authorizations service, managed by DVV, receives (among other things) natural persons' roles in companies (e.g. CEO or a board member) from the Business Information System YTJ. Suomi.fi e-Authorizations service also manages permissions (e.g. to represent the organization in a particular transaction with public authorities) related to legal persons in its own database.

To enable company wallets, it is further assumed that

- PRH (or another designated public authority) has **a PID/ODI portal for wallet related interactions** (such as, issuing a PID/ODI to company wallet, revoking the PID/ODI in the company wallet and viewing the log of transactions done at PRH for the wallet of a particular company).
- PRH has its own **wallet for issuing PID/ODI**s to company wallets and the wallet is registered to a related trusted list of PID/ODI issuers (details are out of scope in this document). However, the decision if the wallet will be eventually managed by PRH or another public authority is pending.
- There are one or more (private or public) **wallet providers** that manage eIDAS compliant company (legal person) wallets for their customers.
- The wallet provider has a web based **control panel** for their hosted company wallets that authorised persons can access on behalf of the company. How the company wallets authenticate/authorise the persons using the wallet is up to each wallet provider to decide and out of scope for this document.
- The company wallet uses **standard protocols** for communicating with peer wallets (including the PRH wallet). In this document DIDComm/Aries is assumed, but using another protocol (such as, OID4VCI) wouldn't materially change the process.

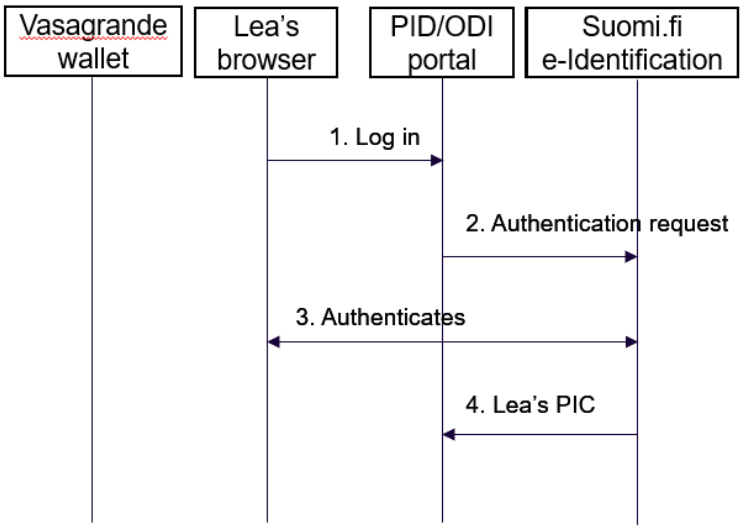
3 Steps to anchor a company wallet to the Finnish Business Information System

3.1 Preconditions

- Lea is a natural person, registered to the Population registry and has a PIC (henkilötunnus).
- Vasagrande Oy is a limited liability company, registered to Business Information System YTJ and has a Business ID (Y-tunnus).
- Lea has a permission (recorded by Suomi.fi e-Authorizations service) to represent Vasagrande Oy in issues related to management of Vasagrande Oy's company data in a wallet.
- Vasagrande Oy has acquired a company wallet from a wallet provider (how this happens is out of scope). Lea has access to the Vasagrande wallet's management console provided by the wallet provider.

3.2 Step 1. Authenticate Lea

Description	Natural person proves their identity to the PID/ODI portal
Actors	Lea PID/ODI portal Suomi.fi e-Identification
Precondition	PID/ODI portal is properly integrated to Suomi.fi e-Identification service. Lea is registered to the Population registry and possesses means for strong authentication (eIDAS substantial or high)
Outcome	PID/ODI portal knows Lea's authenticated PIC

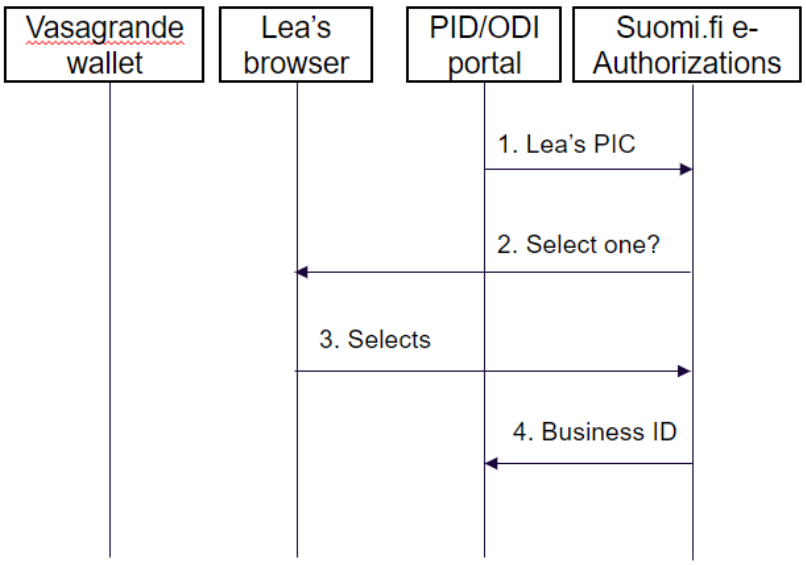


Sequence:

1. Lea browses to PID/ODI portal and clicks "Manage your company wallet's PID/ODI attribute attestations"
2. The portal redirects Lea to Suomi.fi e-Identification service (SAML 2.0 authentication request)
3. Lea uses her strong authentication means to authenticate at Suomi.fi e-Identification service (how this is done is not relevant here)
4. Suomi.fi e-Identification returns Lea's authenticated PIC to PID/ODI portal (SAML authentication response/attribute statement)

3.3 Step 2. Verify Lea's permission to represent Vasagrande Oy

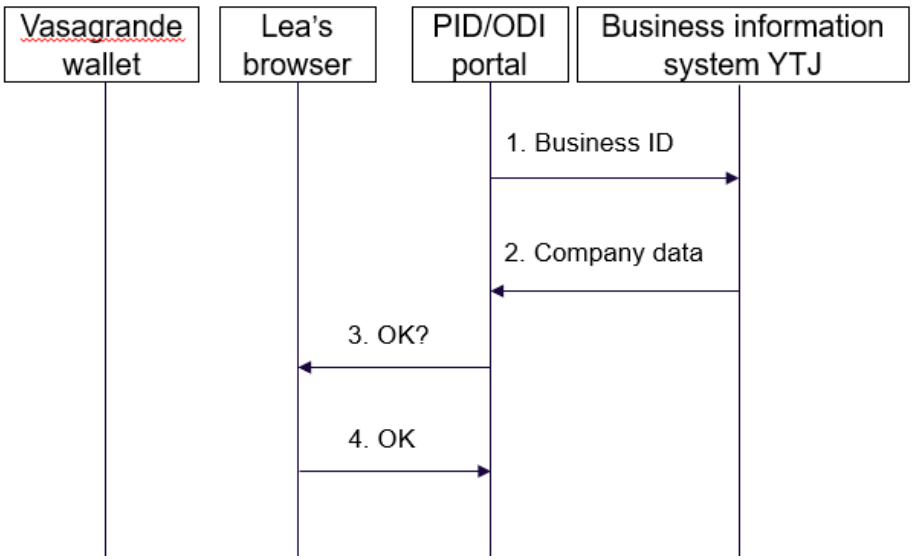
Description	PID/ODI portal makes sure that Lea (identified by her authenticated PIC) has the permission to represent Vasagrande Oy in issues related to management of Vasagrande Oy's PID/ODI attestations in a wallet.
Actors	Lea PID/ODI portal Suomi.fi e-Authorizations
Precondition	PID/ODI portal is properly integrated to Suomi.fi e-Authorizations service. Vasagrande Oy has used Suomi.fi e-Authorizations to grant Lea a permission to represent Vasagrande Oy in issues related to management of Vasagrande Oy's PID/ODI attestations in a wallet. PID/ODI portal has Lea's authenticated PIC (step 1).
Outcome	PID/ODI portal has learned that Lea, identified by her authenticated PIC, has a permission to represent Vasagrande Oy in issues related to management of Vasagrande Oy's PID/ODI attestations in a wallet.



1. PID/ODI portal sends Lea's authenticated PIC to Suomi.fi e-Authorizations's endpoint and queries which company Lea has a permission to represent in issues related to management of PID/ODI attestations in a wallet.
2. Suomi.fi e-Authorizations tells Lea that she is now requested to act in her capacity to represent a legal person in issues related to management of PID/ODI attestations in a wallet. If Lea has no permission to represent any company, an error message is displayed and the flow terminated. If Lea has a permission to represent multiple companies, she is asked to pick up one in the list.
3. Lea selects that she wants to act on behalf of Vasagrande Oy.
4. Suomi.fi e-Authorizations service returns to PID/ODI portal the Business ID of the company Lea has selected to represent.

3.4 Step 3. Collect company details from the Business Information System YTJ

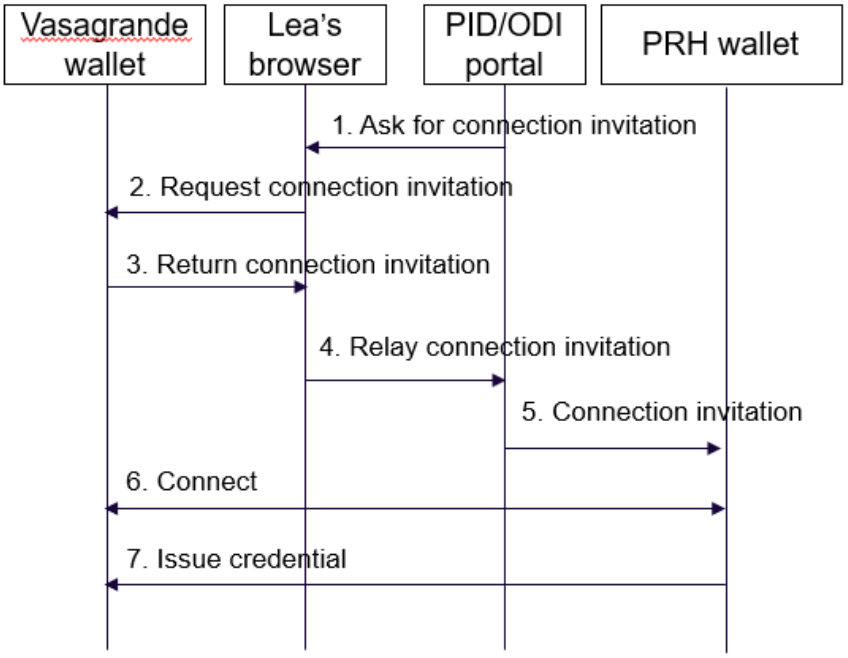
Description	PID/ODI portal collects Vasagrande Oy's information from the Business Information System YTJ.
Actors	Lea PID/ODI portal PRH's Business Information System YTJ
Precondition	PID/ODI portal has learned Lea has a permission to represent Vasagrande Oy in management of its wallet's PID/ODI attestations (Step 2).
Outcome	PID/ODI portal has all the necessary information for minting a PID/ODI attribute attestation for Vasagrande.



1. PID/ODI portal queries the Business Information System YTJ for Vasagrande Oy's data. This can be done for instance using PRH's public API: https://avoindata.prh.fi/bis/v1/<Business-id>
2. PRH's API returns the data required for minting Vasagrande's PID/ODI attribute attestations.
3. PID/ODI portal displays the collected data to Lea and asks for confirmation.
4. Lea confirms issuing the data to Vasagrande's wallet as a PID/ODI attestation.

3.5 Step 4. PRH wallet issues PID/ODI to Vasagrande's company wallet

Description	PRH wallet issues PID/ODI attribute attestations for Vasagrande Oy and let's Lea to accept them to Vasagrande's wallet. This section assumes the use of DIDComm/Aries for wallet communications (also other protocols are possible).
Actors	Lea Vasagrande Oy wallet (hosted by a wallet provider) PID/ODI portal PRH wallet
Precondition	PID/ODI portal has learned Lea is permitted to request the download of Vasagrande's PID/ODI attestations to Vasagrande's wallet (Step 2). The data is collected for issuing the PID/ODI (Step 3).
Outcome	PID/ODI is issued and written to Vasagrande's company wallet. The wallet now qualifies to EUDI wallet and Vasagrande can start using it.



1. PID/ODI portal asks Lea for an invitation that PRH wallet can use to connect to Vasagrande's wallet.
2. Lea logs in to Vasagrande wallet's management console and clicks "requests a connection invitation".
3. Vasagrande's wallet displays the connection invitation string.
4. Lea copies the connection invitation string and pastes it to PID/ODI portal.
5. PID/ODI portal relays the connection invitation and Vasagrande's company information to PRH wallet and requests it to connect and issue PID/ODI credentials to Vasagrande's wallet.[2]
6. PRH wallet establishes a connection to Vasagrande's wallet.
7. PRH wallet issues the PID/ODI credentials for Vasagrande Oy.

4 Other possible flows

Steps 1-2 can be utilised for offering also other services to Lea, such as

- Offer Lea a possibility to request revocation of Vasagrande Oy's wallet's PID/ODI
- View PRH logs and ODI/PID status to learn what PID/ODI credentials PRH has issued for Vasagrande Oy and what are their statuses.

5 Discussion

PID/ODI issuer. The document assumes the Patent and Registration Office PRH has its own wallet for issuing PID/ODI attribute attestations. However, it is also possible that the wallet (or related functionality for issuing (Q)EAA) is provided by some other public or private organisation. Due to the requirements on information security and related audits, it may be effective to centralise the technical capability to issue (Q)EAAs.

PID/ODI portal owner. The PID/ODI portal can but does not need to be owned and managed by the Patent and Registration Office PRH. The design enables the state government to introduce a centralised portal (potentially an extension of the www.suomi.fi portal) where legal persons can request and download attribute attestations to their wallets from different public authorities, such as PRH, tax authorities, legal register center etc. Being able to find all public sector attribute attestations in a single place can be desirable from a customer point of view.

Clear separation of responsibilities. The architecture clearly separates the responsibilities of PRH (as PID/ODI issuer) and the company wallet provider (who host the wallet for its customer). There are no direct integrations between the company wallet provider and the PID/ODI portal or PRH wallet. PID/ODI is requested from PRH wallet as any attribute attestation.

Real Time Economy

www.yrityksendigitalous.fi

Funded by the European Union – NextGenerationEU