

The background of the slide is a high-angle aerial photograph of a European city, likely Zurich, Switzerland. The city is built on a hillside overlooking a large body of water (Lake Zurich). In the foreground, there's a modern bridge spanning the lake. The city features a mix of traditional and modern architecture, with many buildings having red roofs. In the far distance, the Alps are visible under a clear blue sky.

Participation Meeting

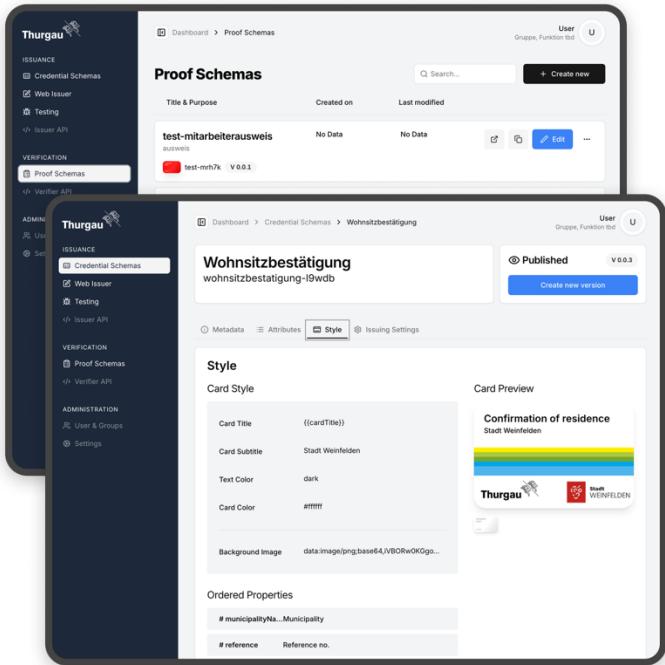
HEIDI Goes Public Beta

08.05.2025

ubique 

What is HEIDI?

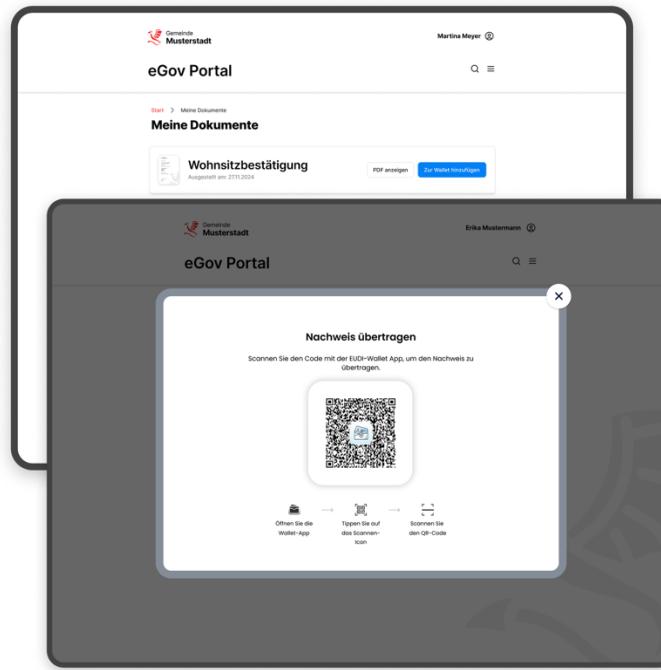
BACKOFFICE



Cockpit

Issuer & Verifier Services

ISSUANCE + VERIFICATION



Web Components / API
Integration in Systeme

HOLDER



Heidi Wallet

Open Source Wallet/SDK

HEIDI Goes Public Beta



HEIDI goes

Swiss Profile / Public Beta

HEIDI Wallet

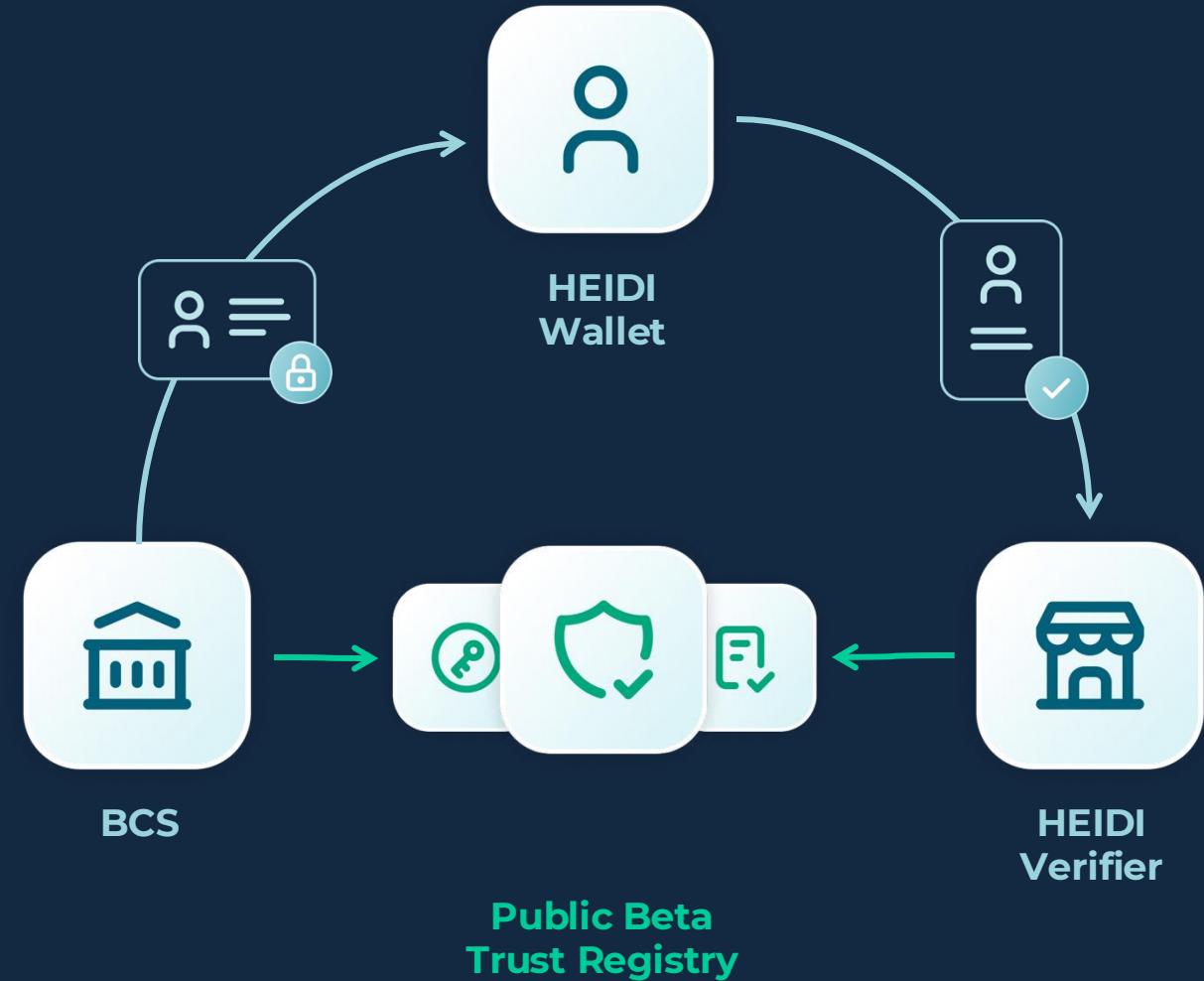
- ✓ Receives Beta-ID
- ✓ Connected to Trust Registry

HEIDI Issuer

- ✓ Issues VCs according to the «Swiss Profile»
- ✓ Onboarded on to Trust Registry

HEIDI Verifier

- ✓ Can verify Beta-IDs



[Back to the homepage](#)

Request a Beta-ID

Request a Beta-ID from a template

[Request the issuing of a Beta-ID](#)

Request a custom Beta-ID

 Female Male

Given name*
Marco Elio

Surname*
Prumaz

Date of birth*
19.06.1988

Place of birth*
Vallorbe

Place of origin
Echallens VD

Nationality*
CH, FR

OASI number*
756.6199.0539.28

[Upload a picture](#)[Picture of Helvetia](#)[Picture of Marco](#)

16:27 M 87%

← ✖

Beta ID
Prumaz Marco Elio



INFO

METADATA

Given name(s)
Marco Elio

Surname
Prumaz

Face image


Sex
1

Date of birth
19.06.1988

Born in
1988

Over the age of 16

Over the age of 18

[Back to the homepage](#)

Minimum age of 18 years

- The Beta-ID data is authentic
- This Beta-ID has not been revoked
- This Beta-ID is valid

Check minimum age of 18 years
true

Credential Type
betaid-sdjwt

16:28 M

87%



Information Request

Today, 16:27

REQUESTED BY

 swiyu Beta Credential Service (BCS)
 Verified Verifier
Swiss Trust-Framework

DOMAIN
bcs.admin.ch

 Valid Certificate

SHARED INFORMATION

 Beta ID
Prumaz Marco Elio
 > Vct
betaid-sdjwt
 > Age_over_18
true

HEIDI goes

Swiss Profile

	Swiss Profile	HEIDI
Identifiers	W3C Decentralized Identifiers did:tdw/did:webvh	✓
Status Mechanisms	Token Status List (Draft 3)	✓
Trust Protocol	Swiss Trust Protocol version 0.1	✓
Communication Protocol	OID4VCI – draft 13 (2024) OID4VP – draft 20 (2024)	✓ ✓
Payload Encryption	JWE	✓
VC-Format & Signature Scheme	SD-JWT VC – draft 4 SD-JWT draft 10 ECDSA P-256	(✓) ✓ ✓
Device Binding Scheme	Hardware-based Software-based	✓ ✓
VC appearance	Overlay Capture Architecture (OCA)	(✓)

Learnings

- **Tooling/Process**

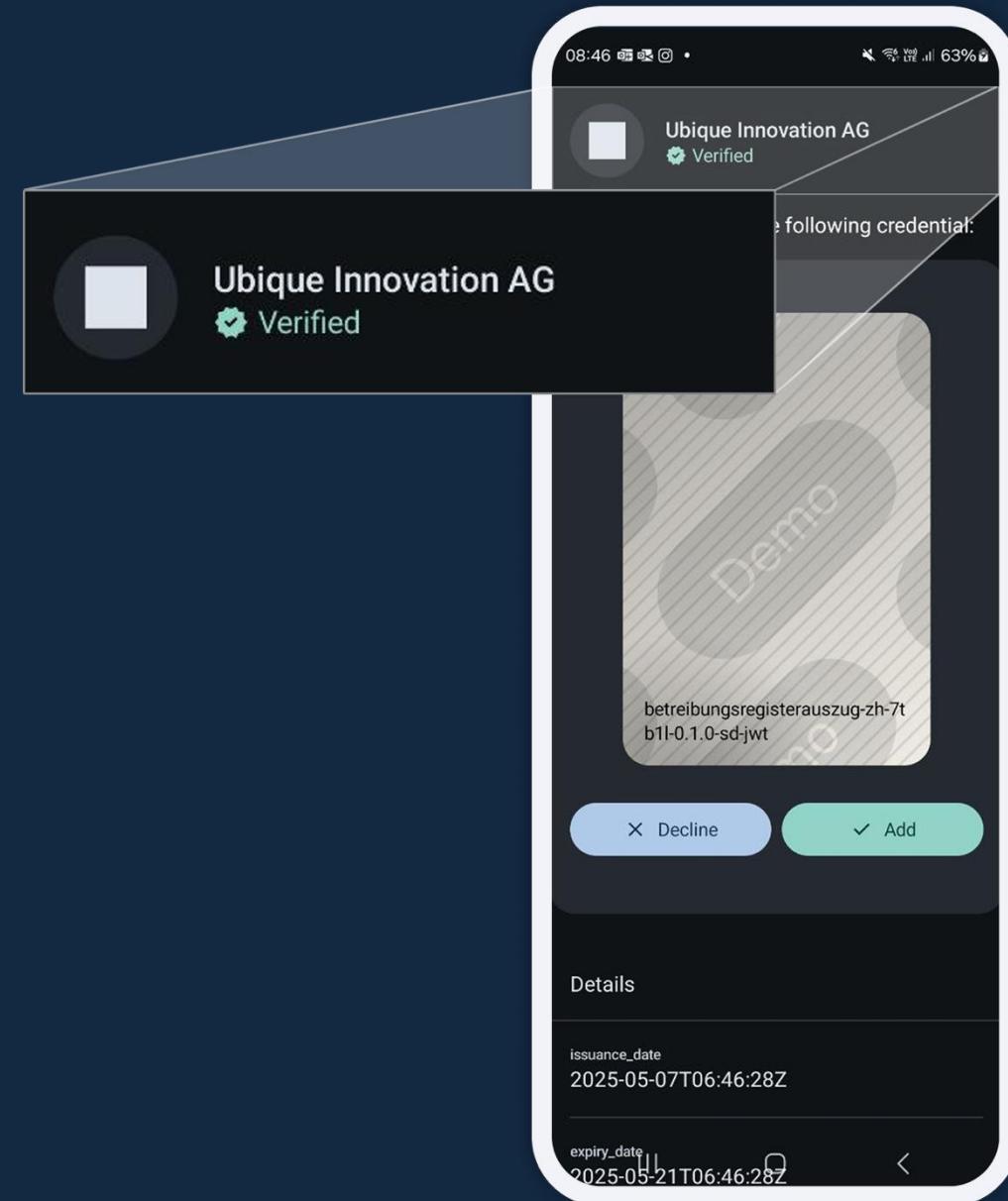
DID-Toolbox: useful

Cookbook: helpful

Eintrag in Trust Registry: fast

Wishlist

- API specification as Swagger
- Support for X.509 and P12 certificates



Learnings

- **Protocols are not yet final**

Swiyu

- OID4VCI Draft 13 (2024)
- OID4VP Draft 20 (2024)

Aktuell

- OID4VCI Draft 15 (2025)
- OID4VP Draft 28 (2025)

The screenshot shows the first page of the "OpenID for Verifiable Presentations - draft 28" specification. At the top, it displays the workgroup as "OpenID Digital Credentials Protocols", published on "24 April 2025", and authored by O. Terbu, T. Lodderstedt, K. Yasuda, and T. Looker, all from SPRIND. Below this is the title "OpenID for Verifiable Presentations - draft 28". A section titled "Abstract" follows, stating that the specification defines a protocol for requesting and presenting Credentials. The "1. Introduction" section explains that the specification builds on OAuth 2.0 [RFC6749] to provide a simple, secure, and developer-friendly layer for Credential presentation. It mentions W3C Verifiable Credentials Data Model [VC_DATA], ISO mdoc [ISO.18013-5], and IETF SD-JWT VC [I-D.ietf-oauth-sd-jwt-vc]. The text also notes that OAuth 2.0 [RFC6749] is used as a base protocol for its simplicity and security. It highlights how the specification can be combined with [SIOPv2] for OpenID Connect features like self-issued ID tokens. Additionally, it describes how to use OID4VP in conjunction with the Digital Credentials API (DC API) [DC-API]. The "1.1. Requirements Notation and Conventions" section is also visible at the bottom.

Workgroup: OpenID Digital Credentials Protocols
Published: 24 April 2025
Authors: O. Terbu T. Lodderstedt K. Yasuda T. Looker
SPRIND SPRIND Mattr

OpenID for Verifiable Presentations - draft 28

Abstract
This specification defines a protocol for requesting and presenting Credentials.

1. Introduction
This specification defines a mechanism on top of OAuth 2.0 [RFC6749] for requesting and delivering Presentations of Credentials. Credentials and Presentations can be of any format, including, but not limited to W3C Verifiable Credentials Data Model [VC_DATA], ISO mdoc [ISO.18013-5], and IETF SD-JWT VC [I-D.ietf-oauth-sd-jwt-vc].
OAuth 2.0 [RFC6749] is used as a base protocol as it provides the required rails to build a simple, secure, and developer-friendly Credential presentation layer on top of it. Moreover, implementers can, in a single interface, support Credential presentation and the issuance of Access Tokens for access to APIs based on Credentials in the Wallet. OpenID Connect [OpenID.Core] deployments can also extend their implementations using this specification with the ability to transport Credential Presentations.
This specification can also be combined with [SIOPv2], if implementers require OpenID Connect features, such as the issuance of Self-Issued ID Tokens [SIOPv2]. Additionally, it defines how to use OID4VP in conjunction with the Digital Credentials API (DC API) [DC-API].

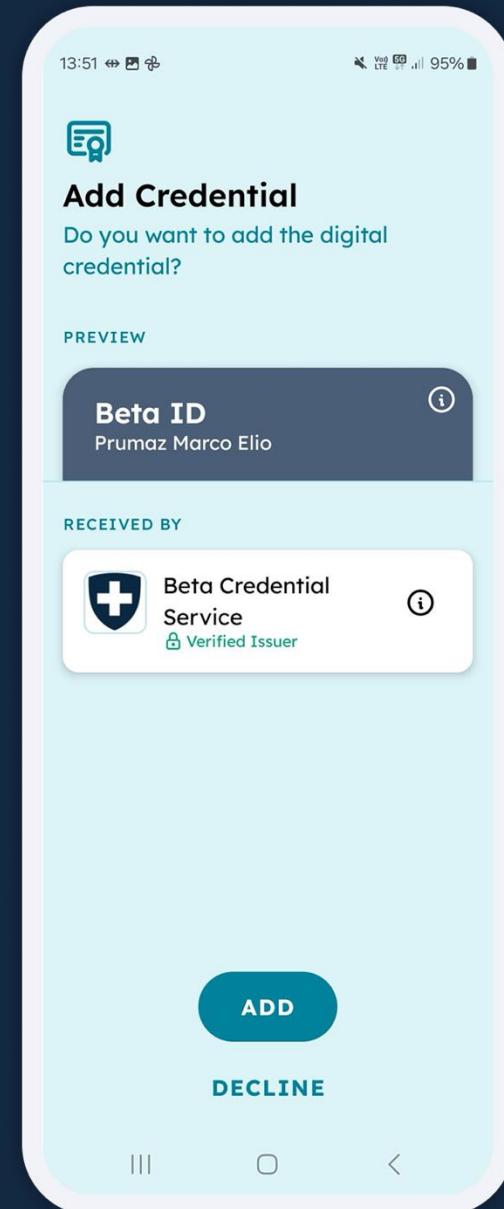
[OpenID.Core], in that they allow a Credential Issuer to assert End-User claims. A Verifiable Credential follows a pre-defined schema (the Credential type) and MAY be bound to a certain holder, e.g., through Cryptographic Holder Binding. Verifiable Credentials can be securely presented for the End-User to the RP, without involvement of the Credential Issuer.
Access to this API is authorized using OAuth 2.0 [RFC6749], i.e., the Wallet uses OAuth 2.0 to obtain authorization to receive Verifiable Credentials. This way the issuance process can benefit from the proven security, simplicity, and flexibility of OAuth 2.0 and existing OAuth 2.0 deployments and OpenID Connect OPs (see [OpenID.Core]) can be extended to become Credential Issuers.

1.1. Requirements Notation and Conventions

Learnings

- **Issuer Authentication only after issuance**

DID of issuer not available in metadata of issuer but only in SD-JWT VC payload.

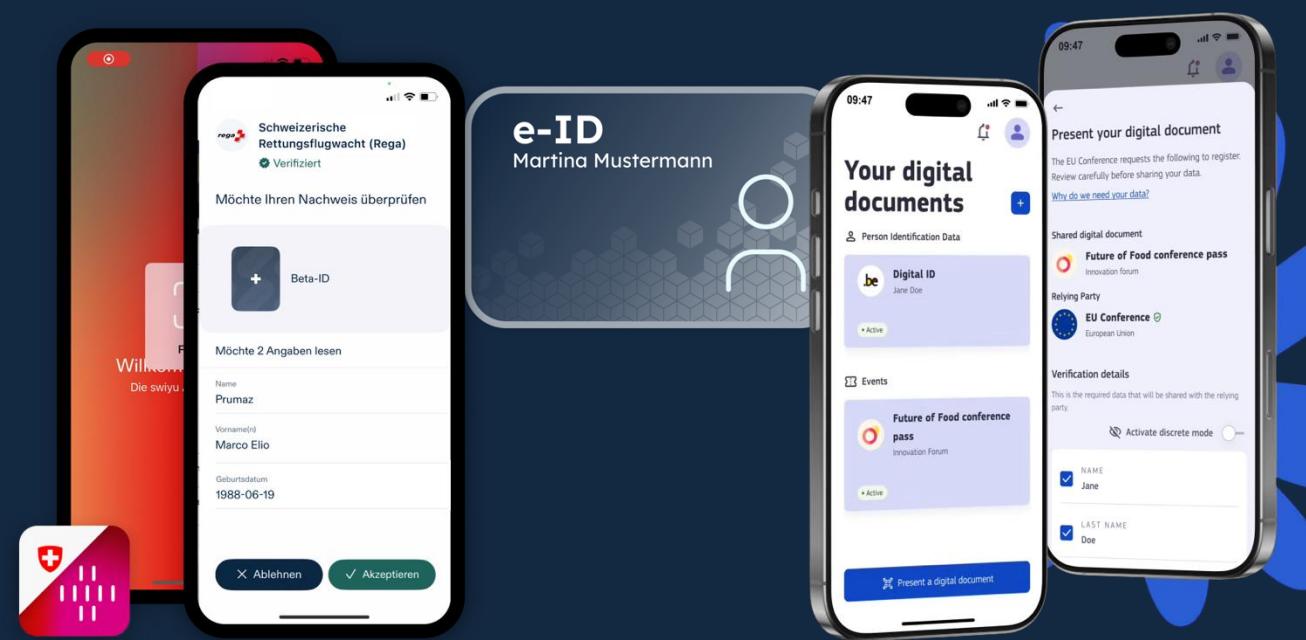


Public Beta

Learnings

- **Supporting multiple trust-frameworks not easy**

Swiss Profile
EUDI / HAIP



Interoperability EUDI



Protocols

Same Standards



Trust-Framework

Incompatible
Different



Schema

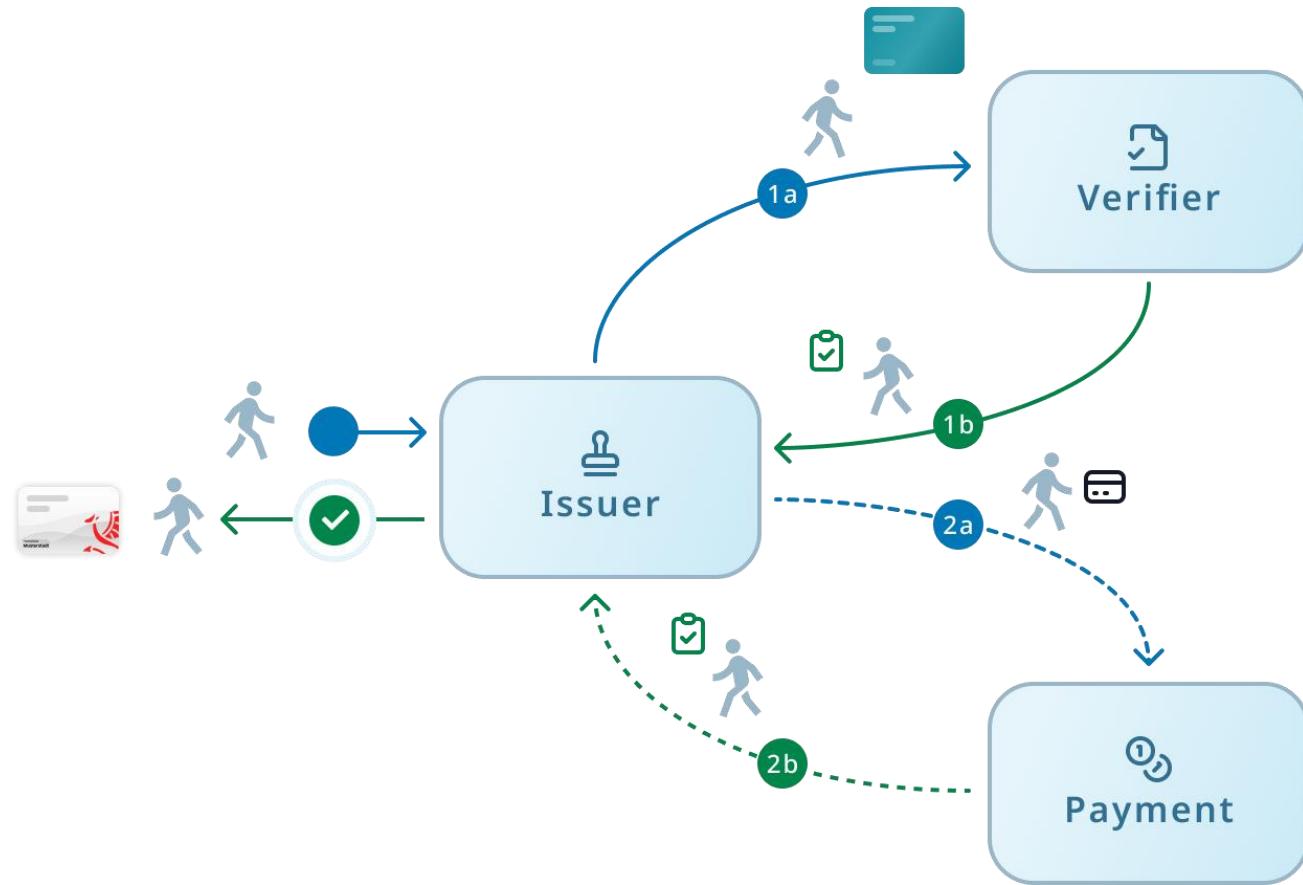
need harmonisation/
standardisation

DVS4U

Case “Extract from the debt enforcement register”

Presentation During Issuance

Beta ID → Extract from the debt enforcement register



Beta-ID prüfen

Beta-ID prüfen

fake-betaid	
<input type="text"/> birth_date	Date of Birth
<input type="text"/> family_name	String
<input type="text"/> given_name	String

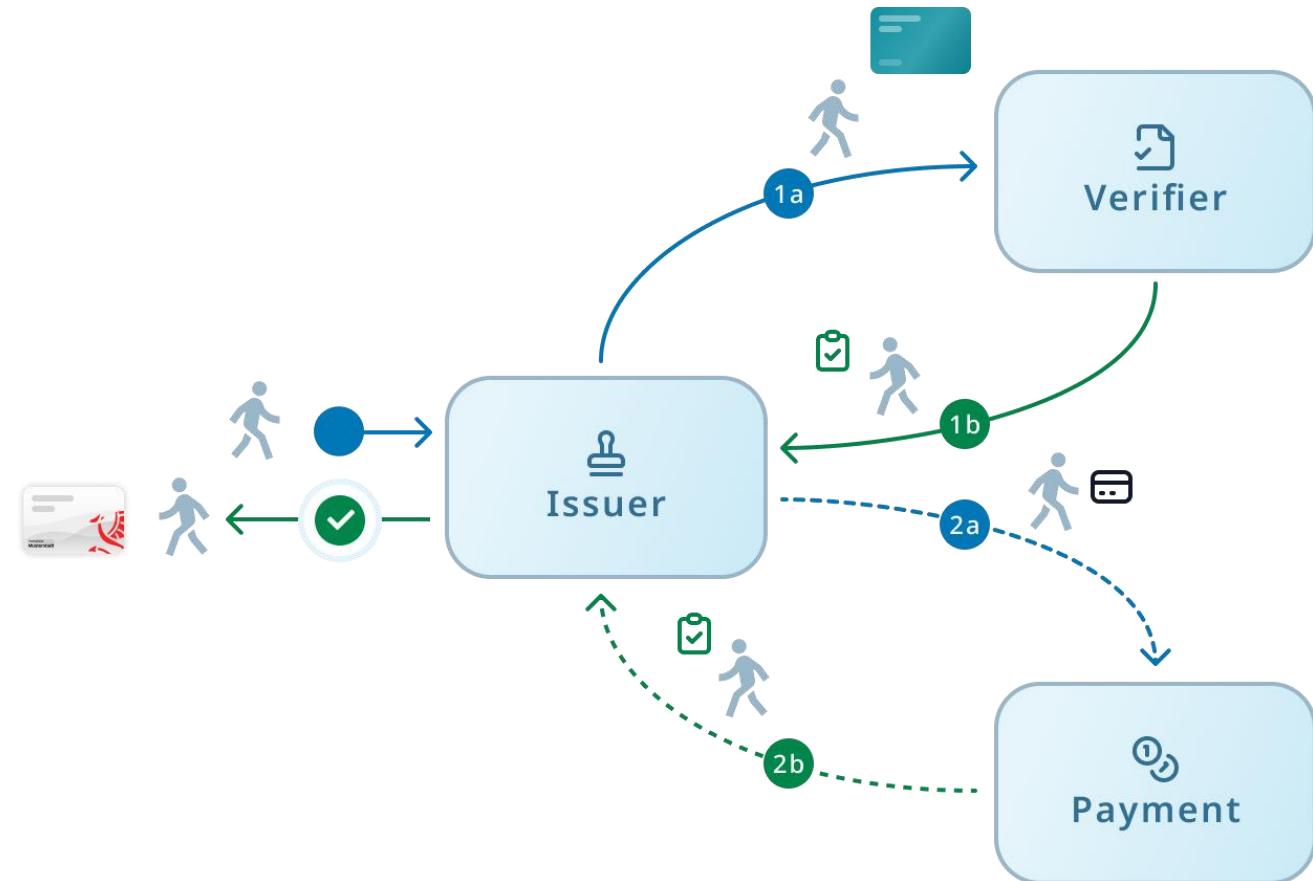
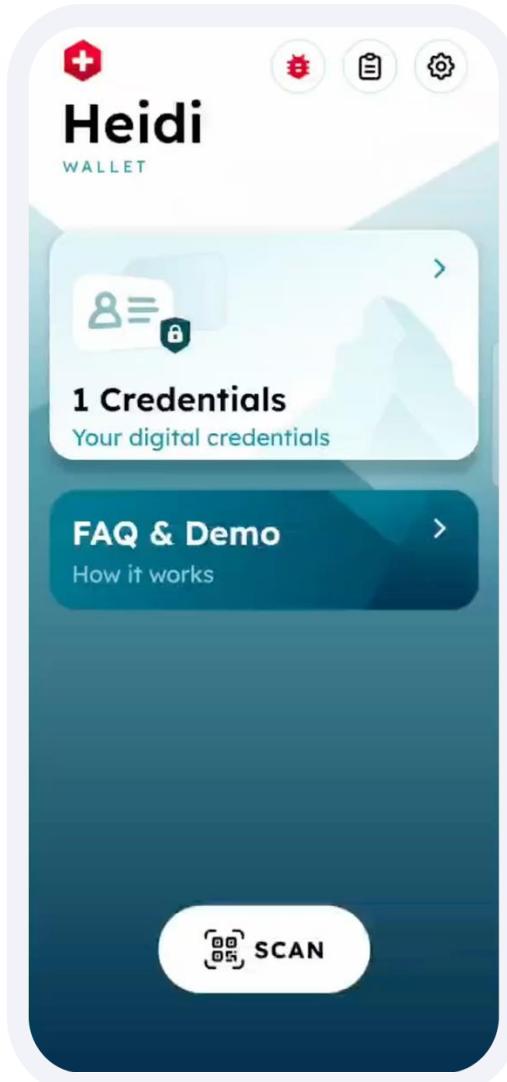
Betreibungsregisterauszug ZH

• Adresse	Musterstrasse 3	String
• Anhang	Musteranhang	String
• Behörde	Musterbehörde	String
• Bemerkung	Musterbemerkung	String
• Datum	Static Value	Datetime
• Einträge	1	String
• Geb	Static Value	Date of Birth
• Name	Static Value	String
• Nr.	1	Number
• Ref.	1	Number
• Vorname	Static Value	String



Presentation During Issuance

Beta ID → Extract from the debt enforcement register



What else...

- **Mehr Cases (DVS, ZVV, Thurgau,...)**
 - Member-Card
 - Tickets
 - Proof of education
 - ...
- **Zero-Knowledge-Proof** with Device Binding!
- **SPRIN-D: EUDI-Wallet**
- **Qualified Electronic Signatures (QES)**
- **Digital Credentials API**





HEIDI WALLET

The uncomplicated wallet app.

Your digital IDs and proofs, your data
sovereignty.

DOWNLOAD NOW!



Demo showcases

Test the Heidi Wallet and the advantages of
digital proofs.



www.heidi-universe.ch