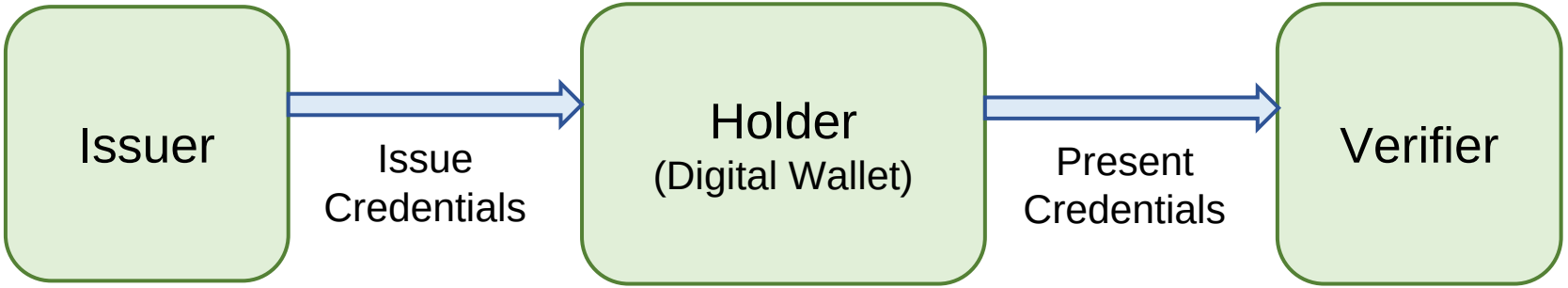
OpenID 4 Verifiable Credentials in the context of eIDAS

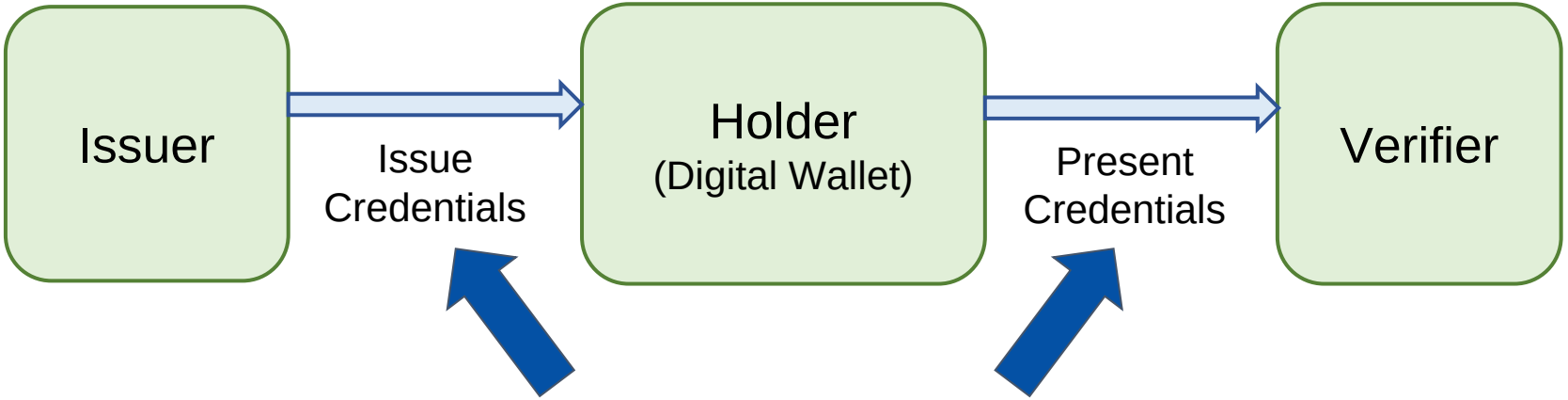
Dr. Torsten Lodderstedt, yes.com/OpenID Foundation

A Paradigm Shift: Issuer-Holder-Verifier Model



- eIDAS v2 embraces the concept of wallets and verifiable credentials (electronic attribute attestations & person identification data)
- This enables
  - decoupling of issuance from presentation (enhanced privacy)
  - multi-use of the credentials and offline use
  - combination of multiple credentials in single presentation

Challenge: Credential Exchange

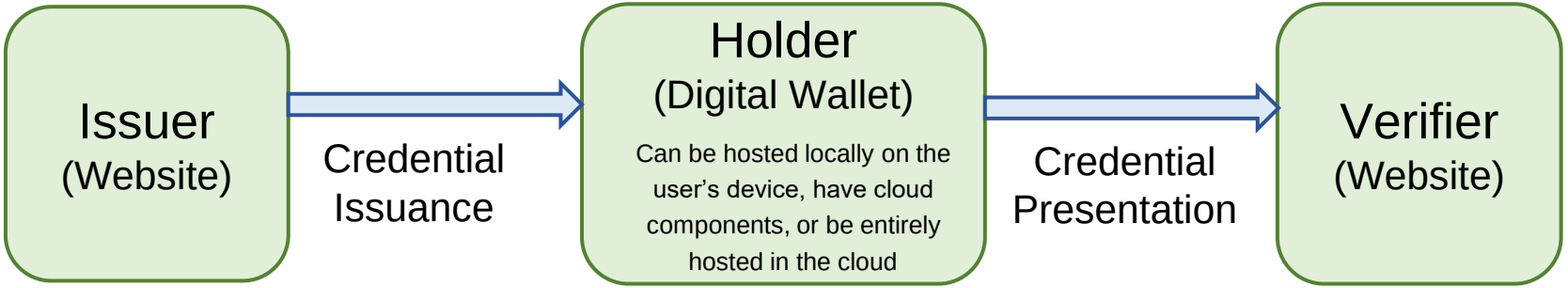


- Secure and Interoperable Issuance and Presentation of Verifiable Credentials (PID, (Q)EAA) …
- …for a variety of credential formats (see credential format survey)

OpenID for Verifiable Credentials

The next generation of OpenID

OpenID for Verifiable Credentials specifications

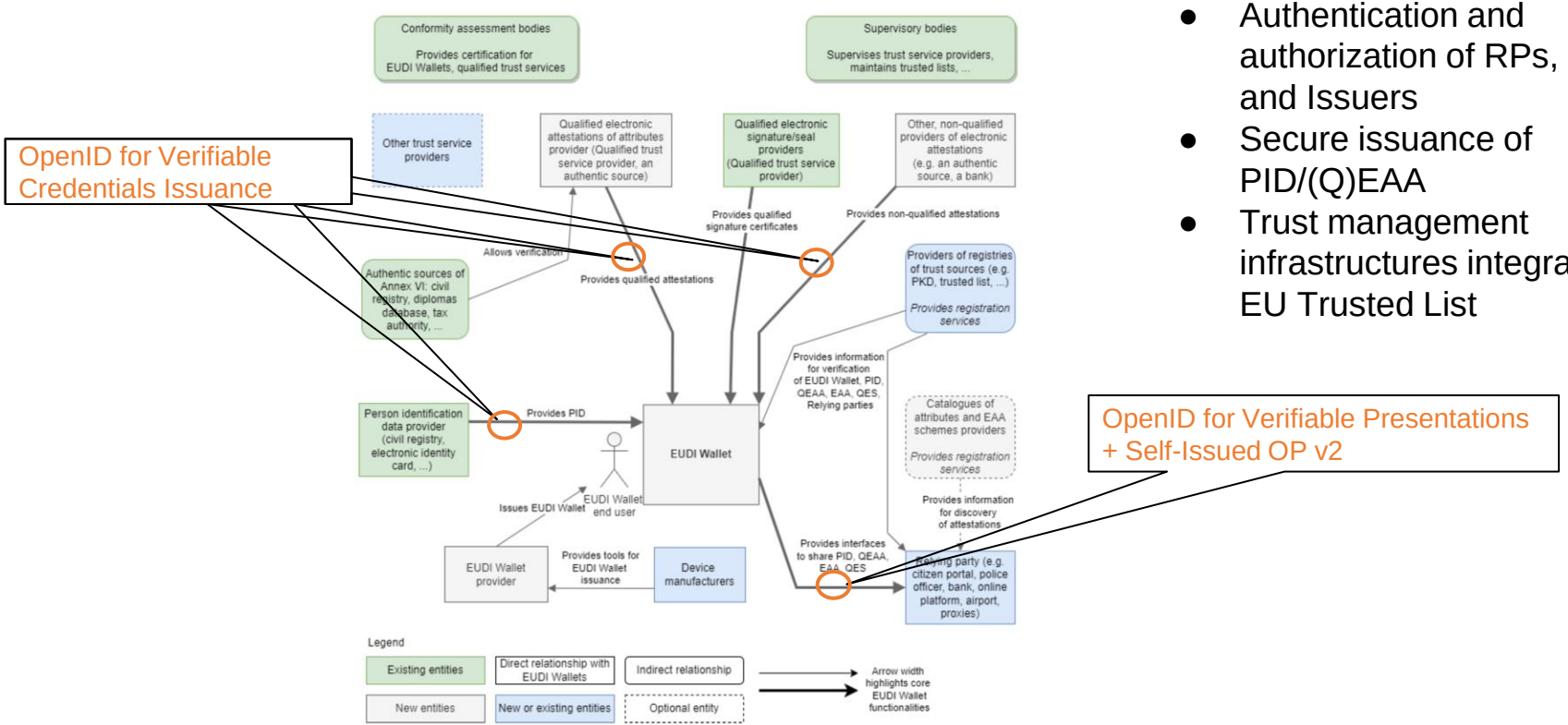


1 **OpenID for Verifiable Credential Issuance**
(Issuance of verifiable credentials)

2 **OpenID for Verifiable Presentations**
(Presentation of verifiable credentials)

3 **Self-Issued OP v2**
(authentication with user controlled identifiers)

The ARF and OpenID 4 VCs



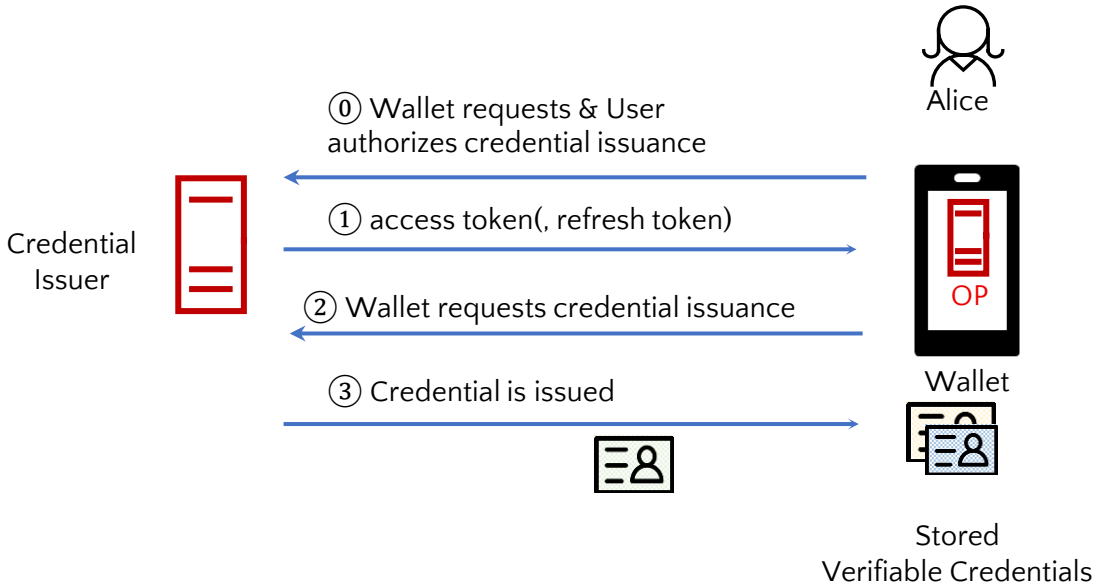
ARF significantly influenced design of OpenID 4 VCs:

- Authentication and authorization of RPs, Wallets, and Issuers
- Secure issuance of PID/(Q)EAA
- Trust management infrastructures integration, like EU Trusted List

source; https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline

OpenID for Verifiable Credential Issuance

Credential issuance via simple OAuth-authorized API



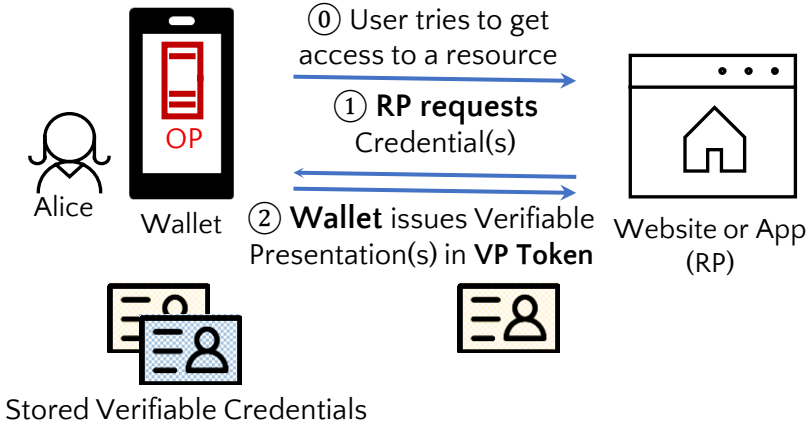
OpenID4VCs allows variety of choices in the VC tech stack

Component	Implementer's choices when using OpenID4VP
Format of VCs/PID/(Q)EAA	**Any format** (W3C VCs, ISO mDL, SD-JWT, AnonCreds, …)
Method to obtain Public Keys	**Any DID method, raw keys, or X.509 certs**
Cryptography	**Any cryptosuite** (EdDSA, ES256K, etc.)
Revocation	**Any mechanism** (Status List 2021, etc.)
Trust Management	**Any mechanism for managing trusted** Issuers, Wallets and Relying Parties (EU Trusted List, OpenID Connect Federation, TRAIN, …)

VCs/PID/(Q)EAA issuance using OpenID4VCI

- Simple & Secure OAuth protected API
  - Can be built & operated on top of existing OAuth libraries/deployments
  - Simple way for existing AS/IDPs to become PID/(Q)EAA issuers
  - Leverages OAuth security mechanisms
- Customizable for different credential formats, proof of possession and attestation methods
- Hardware-backed key material for cryptographic binding of attribute attestations (leveraging HSMs, SEs, TEEs)
- Same device and cross device scenarios
- Mutual authentication of wallet and issuer
- Note: referenced by draft ISO 23220-3 electronic ID standards

OpenID for Verifiable Presentations



- RP can request credentials by format*, type and select claims for selective disclosure, e.g
  - **format**: “ldp_vc”
    type: “IDCredential”
    claims: “given_name” & “last_name”
  - **format**: “mso_mdoc”
    doctype: “org.iso.18013.5.1.mDL”
    claims: “driving_privileges”
- Verifiable Presentations* are returned in the so-called VP Token (one or more)

VC/PID/(Q)EAA presentation using OpenID4VPs & SIOP v2

- Simple & secure protocol based on OAuth 2.0
- Uniform protocol across different credential formats
- Same device & cross device scenarios, offline
- Privacy preserving mutual authentication of RP and wallet
- Pseudonymous authentication of End-User to RPs through SIOP v2
- Works well with OAuth for authorization of API-based payments (e.g. PSD2) and remote signature creation (e.g. CSC)
- Note: referenced by ISO/IEC 18013-7 and 23220-4 Mobile Driving Licences related draft standards as data release method

Why use OpenID for Verifiable Credentials for eIDAS?

- **Native protocols** for wallet-based applications - leveraging promises and unique trust model of Verifiable Credentials
- **Simple & Secure** - leverages OpenID Connect/OAuth Deployment Experience and proven Security
- **Uniform & interoperable** across credential formats
- **Adoption** underway, e.g.
  - Projects in the EU (Finnish ID, EBSI/ESSIF, Secure Digital Identities Showcase)
  - Incorporated into major participant's products (e.g. Microsoft, Ping Identity, walt.id)
  - Considered by other standards bodies, e.g. ISO, ETSi, W3C (JFF plugfest)
  - Considered in Global Assured Identity Network (GAIN)
- **Backed** by Experienced, Agile, and Approachable Community

OpenID 4 Verifiable Presentations

https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

Self-Issued OP v2

https://openid.net/specs/openid-connect-self-issued-v2-1_0.html

OpenID 4 Verifiable Credential Issuance

https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

Q&A

Whitepaper
“OpenID for Verifiable Credentials”

- target audience: decision-makers, architects and implementers interested in the concepts, use-cases and architecture when verifiable credentials are used.
- goal: inform and educate the readers about this work to assist in the decision-making process.
- where: http://openid.net/wordpress-content/uploads/2022/05/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials_FINAL_2022-05-12.pdf
- Blog Post: https://openid.net/2022/05/12/openid-for-verifiable-credentials-whitepaper/

Verifiable Credentials around you

As Promised at WWDC-21, Apple Reveals the First States Adopting Driver's Licenses and State ID's in Apple Wallet

In June Patently Apple posted a report titled "Apple's iOS 15 is bringing a new Dimension to Apple Wallet that relates to Digital ID such as Driver Licenses and more." Apple Wallet and Apple Pay VP Jennifer Bailey introduced a new Digital ID feature coming to iOS 15 this fall that's a part of a much larger Apple project. Below is a video snippet from her keynote segment talking about bringing

Use Case 1: mobile Driving Licence

How to store vaccine information on your Samsung phone

Plan on going to some events before the end of the summer? This could help.

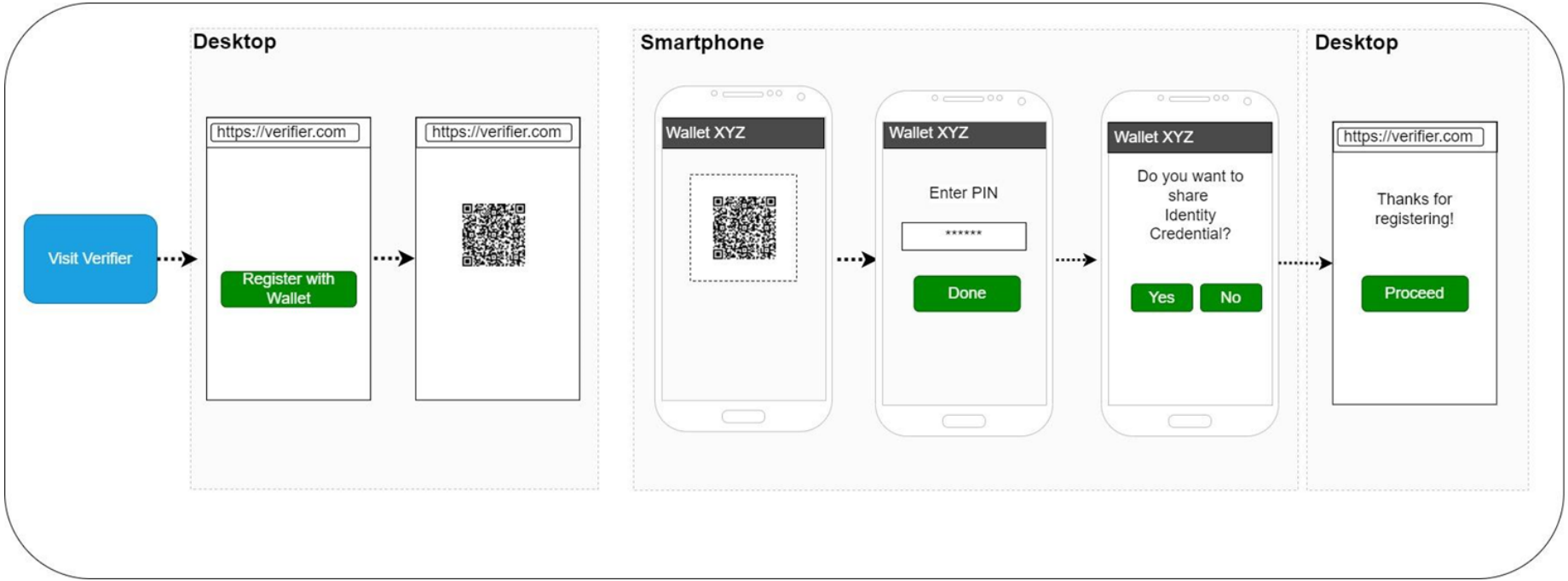
by Alex Gatewood August 19, 2021

Use Case 2: Vaccination QR Code

OpenID for Verifiable Presentations (OpenID4VPs)

Same Device Presentation

Cross Device Presentation



OpenID 4 VPs Request (OAuth 2.0 + Presentation Exchange 2.0)

```
GET /authorize?
   response_type=vp_token
   &client_id=https%3A%2F%2Fclient.example.org%2Fcb
   &redirect_uri=https%3A%2F%2Fclient.example.org%2Fcb
   &presentation_definition=...
   &nonce=n-0S6_WzA2Mj HTTP/1.1
 Host: wallet.example.com
```

presentation_definition

```
{
   "id": "example_ldp_vc",
   "input_descriptors": [
       {
           "id": "id_card_credential",
           "format": {
               "ldp_vc": {
                   "proof_type": [
                       "Ed25519Signature2018"
                   ]
               }
           },
           "constraints": {
               "fields": [
                   {
                       "path": [
                           "$.type"
                       ],
                       "filter": {
                           "type": "array",
                           "contains": {
                               "const": "IDCredential"
                           }
                       }
                   }
               ]
           }
```

OpenID 4 VPs Response

```
HTTP/1.1 302 Found
  Location: https://client.example.org/cb#
    presentation_submission=...
    &vp_token=...
```

presentation_submission

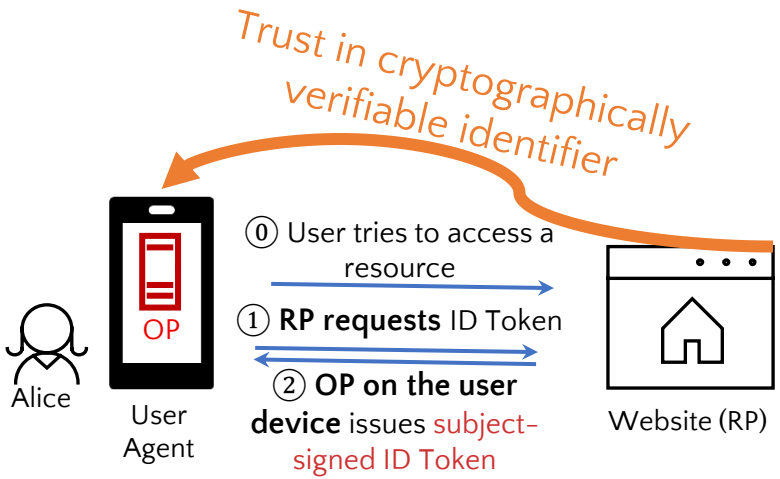

```
{
   "definition_id": "example_ldp_vc",
   "id": "example_ldp_vc_presentation_submission",
   "descriptor_map": [
       {
           "id": "id_credential",
           "path": "$",
           "format": "ldp_vp",
           "path_nested": {
               "format": "ldp_vc",
               "path": "$.verifiableCredential[0]"
           }
       }
   ]
}
```


vp_token


```
{
   "@context": [
       "https://www.w3.org/2018/credentials/v1"
   ],
   "type": [
       "VerifiablePresentation"
   ],
   "verifiableCredential": [
       {
           "@context": [
               "https://www.w3.org/2018/credentials/v1",
               "https://www.w3.org/2018/credentials/examples/v1"
           ],
           "id": "https://example.com/credentials/1872",
           "type": [
               "VerifiableCredential",
               "IDCredential"
           ],
           "issuer": {
               "id": "did:example:issuer"
           },
           "issuanceDate": "2010-01-01T19:23:24Z",
           "credentialSubject": {
               "given_name": "Max",
               "family_name": "Mustermann",
               "birthdate": "1998-01-11",
               "address": {
                   "street_address": "Sandanger 25",
                   "locality": "Musterstadt",
                   "postal_code": "123456",
```

Self-Issued OP (SIOP v2)

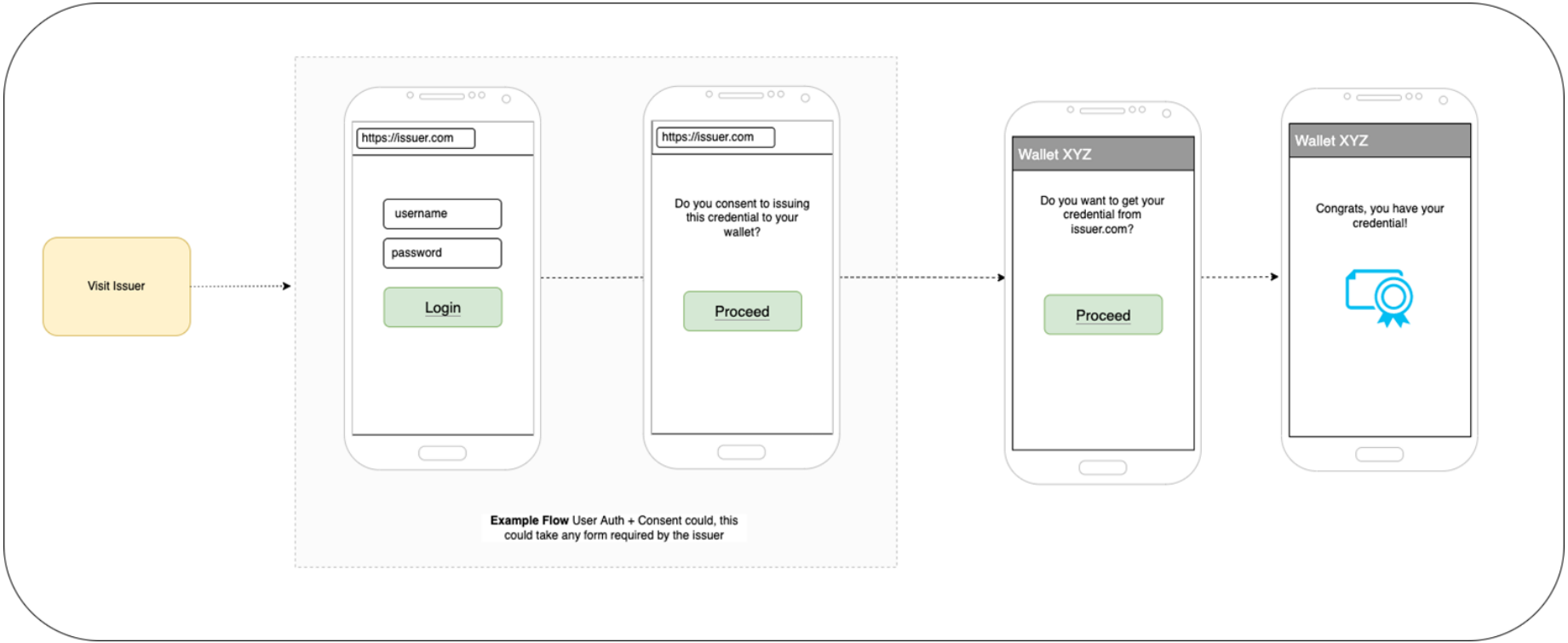
Self-Issued OP v2



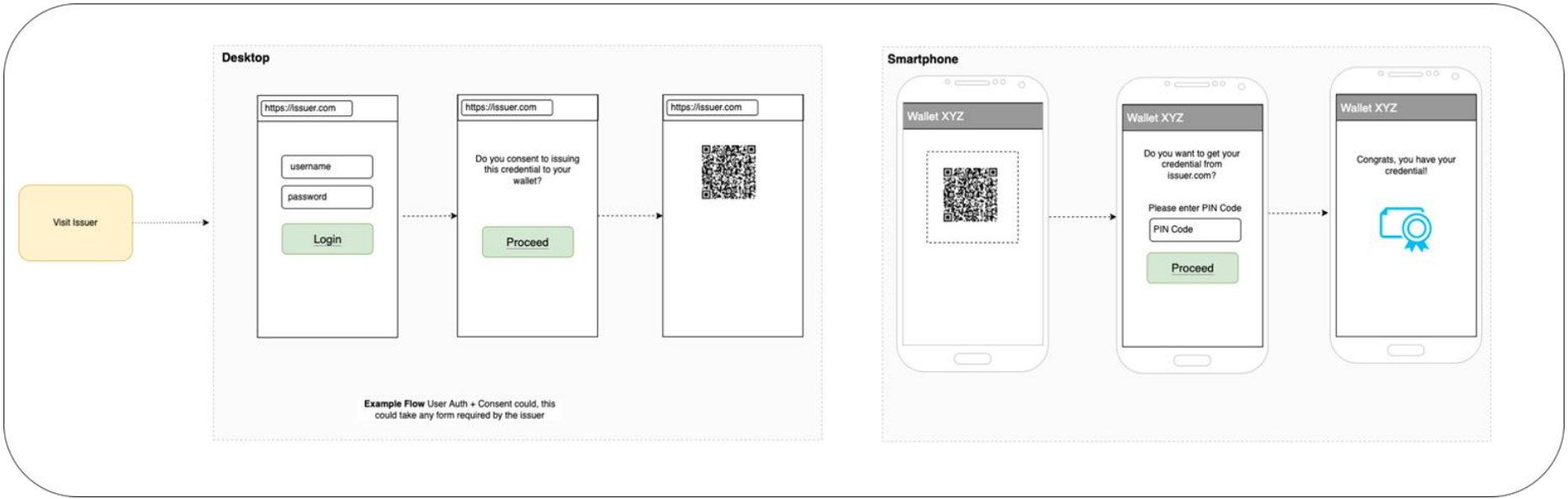
- ID Tokens are signed with user-controlled key material (pseudonymous authentication with pairwise subject identifiers)
- Identifiers are user controlled and do not depend on a third-party identity provider
- Can be used in combination with OpenID4VPs, when the use case requires end-user authentication, i.e. the features of OpenID Connect, such as issuance of ID Tokens.

OpenID for Verifiable Credential Issuance (OpenID4VCI)

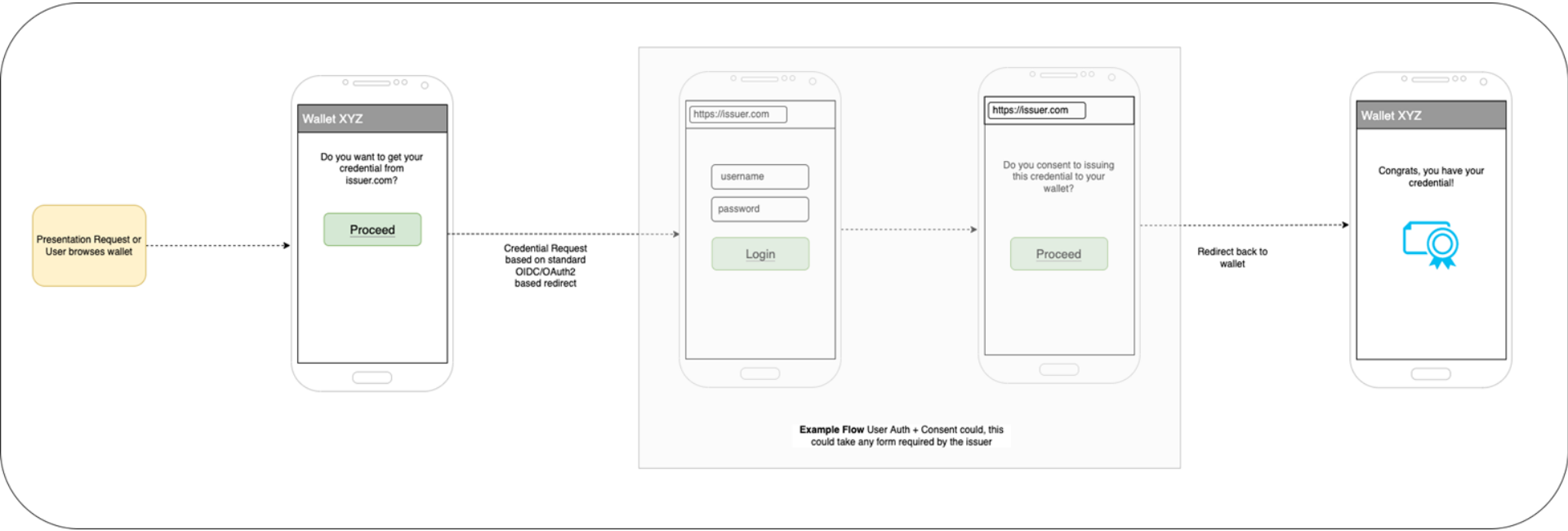
Issuer Initiates Process (same device)



Issuer Initiates Process (cross device)



Wallet Initiates Process (e.g. during presentation)



Design Principles

- Issuance via OAuth-protected Credential Endpoint
- Two authorization flows:
  - Code flow (others OAuth 2.0 grant types possible): authorization for one or more credentials at the Authorization Endpoint once the wallet is invoked
  - Pre-authorized code flow (new grant type): authorization for one or more credentials prior to the Wallet being invoked.
- Supports different methods for the Wallet to prove possession of key material used to bind credential

Example: Authorization Request

```
HTTP/1.1 302 Found
Location: https://server.example.com/authorize?

  response_type=code
  &client_id=s6BhdRkqt3
  &code_challenge=E9Melhoa2OwvFrEMTJguCHaoeK1t8URWbuGJSstw-cM
  &code_challenge_method=S256
  &scope=https://example.org/idcard
  &redirect_uri=https://client.example.org/cb
```

Example: Credential Issuance

Request

```
POST /credential HTTP/1.1

Host: server.example.com

Content-Type: application/x-www-form-urlencoded

Authorization: BEARER czZCaGRSa3F0MzpnWDFmQmF0M2JW


type=https://example.org/idcard

format=ldp_vc

did=did:key:z6MkqUDiu3MHxAmuMQ8jjkLiUu1mscLT8E9R5CKdbtr7gwR8

proof=%7B%22type%22:%22jwt%22…0aW9EkL1nOzM%22%7D
```

Response

```
HTTP/1.1 200 OK
  Content-Type: application/json
  Cache-Control: no-store
  Pragma: no-cache


{
   "format": "ldp_vc",
   "credential" : "eyJjcmVkZW50a...d0MifQ=="
}
```

Example: Issued Credential


```
{
    ...
    "issuer": "did:key:z6MkgF2pvVNEFXCksupWKrdPhL6ubecis3AWbWVsr9bNAbwC",
    "type": [
        "VerifiableCredential"
    ],
    "credentialSchema": {
        "id": "https://example.org/idcard",
    },
    "credentialSubject": {
        "placeOfBirth": {
            "country": "DE",
            "locality": "Berlin"
        },
```

Status

- First Implementer’s Drafts of OpenID4VPs and SIOP v2 approved
- Latest Changes and Work in Progress
  - further simplified specs (based on OAuth, scopes as aliases, added examples for JWT, LDP, AnonCreds, ISO mDL)
  - Documented design patterns for issuance with high security requirements
  - Adding presentation via BLE
  - Adding batch issuance & server metadata
  - Working on overall security analysis
- Targeting further implementers drafts for whole spec family by end of 2022

Planned and ongoing implementations

- The European Blockchain Services Infrastructure (EBSI)
- Finnish ID
- Microsoft
- Mattr
- IDunion
- walt.id & yes.com & BCDiploma (eSSIF-Lab)
- Talao.io
- Workday
- Ping Identity
- Trinsic/Dentity (incl. Auth0 plugin)
- Convergence.Tech
- Sphereon
- Gimly
- CAS Software AG

Specifications

1. Implement the specifications to unlock your use cases and provide us feedback (mailing list)
   - https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
   - https://openid.net/specs/openid-connect-self-issued-v2-1_0.html
   - https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
2. Read the whitepaper and stay up to date with the recent developments

Request Example (ISO mDL)

presentation_submission


```
{
   "id": "mDL-sample-req",
   "input_descriptors": [
       {
           "id": "mDL",
           "format": {
               "mdl_iso_cbor": {
                   "alg": [
                       "EdDSA",
                       "ES256"
                   ]
               },
               "constraints": {
                   "limit_disclosure": "required",
                   "fields": [
                       {
                           "path": [
                               "$.mdoc.doctype"
                           ],
                           "filter": {
                               "type": "string",
                               "const": "org.iso.18013.5.1.mDL"
                           }
                       },
                       {
                           "path": [
                               "$.mdoc.namespace"
                           ],
                           "filter": {
                               "type": "string",
                               "const": "org.iso.18013.5.1"
```

Response Example (ISO mDL)

presentation_submission

```
{
   "definition_id": "mDL-sample-req",
   "id": "mDL-sample-res",
   "descriptor_map": [
       {
           "id": "mDL",
           "format": "mdl_iso_cbor",
           "path": "$"
       }
   ]
}
```

vp_token

```
{
   "status": 0,
   "version": "1.0",
   "documents": [
       {
           "docType": "org.iso.18013.5.1.mDL",
           "deviceSigned": {
               "deviceAuth": {
                   "deviceMac": [
                       << {1: 5} >>,
                       {},
                       null, h'A574C64F18902BFE18B742F17C581218F88EA279AA96D0F5888123843461A3B6'
                   ]
               },
               "nameSpaces": 24(h'A0')
           },
           "issuerSigned": {
               "issuerAuth": [
                 << {1: -7} >>,
                   {
                       33:
h'30820215308201BCA003020102021404AD06A30C1A6DC6E93BE0E2E8F78DCAFA7907C2300A06082A8648CE3D040302
3025A45312E302C060355040A0C25465053204D6F62696C69747920616E64205472616E73706F7274206F66205A65746
030C1349414341205A65746573436F6E666964656E73301E170D3231303932393033333034355A170D3232313130333
806035504030C114453205A65746573436F6E666964656E7331253023060355040A0C1C5A65746F7069612043697479
66666963310B3009060355040613025A453059301306072A8648CE3D020106082A8648CE3D030107034200047C5545E9
3257C28D541C1CD0D604FC9D1E352CCC38ADEF5F7902D44B7A6FC1F99F06EEDF7B0018FD9DA716AEC2F1FFAC173356C7
041830168014BBA2A53201700D3C97542EF42889556D15B7AC4630150603551D250101FF040B3009060728818C5D0501
4CE5FD758A8E88563E625CF056BFE9F692F4296FD300E0603551D0F0101FF040403020780300A06082A8648CE3D0403
13FFEC5679F3B8CDDB51EAA4B95B0CBB1786B09405E2000E9C46618C02202C1F778AD252285ED05D9B55469F1CB78D77
8317C'
                   },
                   <<
                     24(<<
                         {
                           "docType": "org.iso.18013.5.1.mDL",
                           "version": "1.0",
                           "validityInfo": {
```

Request Example (AnonCreds)

presentation_submission


```
{
  "id": "example_vc_ac_sd",
  "input_descriptors": [
     {
        "id": "id_credential",
        "format": {
           "ac_vc": {
              "proof_type": [
                 "CLSignature2019"
              ]
           }
        },
        "constraints": {
           "limit_disclosure": "required",
           "fields": [
              {
                 "path": [
                    "$.schema_id"
                 ],
                 "filter": {
                    "type": "string",
                    "const": "did:indy:idu:test:3QowxFtwciWceMFr7WbwnM:2:BasicScheme:0\\.1"
                 }
              },
              {
                 "path": [
                    "$.values.first_name"
                 ]
              },
              {
```

Response Example (AnonCreds)

presentation_submission

```
{
   "definition_id": "example_vc_ac_sd",
   "id": "example_vc_ac_sd_presentation_submission",
   "descriptor_map": [
       {
           "id": "id_credential",
           "path": "$",
           "format": "ac_vp",
           "path_nested": {
               "path":
"$.requested_proof.revealed_attr_groups.id_credential",
               "format": "ac_vc"
           }
       }
   ]
}
```

vp_token

```
{
   "proof": {...},
   "requested_proof": {
       "revealed_attrs": {},
       "revealed_attr_groups": {
           "id_credential": {
               "sub_proof_index": 0,
               "values": {
                   "last_name": {
                       "raw": "Wonderland",
                       "encoded": "167908493…94017654562035"
                   },
                   "first_name": {
                       "raw": "Alice",
                       "encoded": "270346400…99344178781507"
                   }
               }
           }
       },
       …
   },
   "identifiers": [
       {
           "schema_id": "3QowxFtwciWceMFr7WbwnM:2:BasicScheme:0.1",
           "cred_def_id": "CsiDLAiFkQb9N4NDJKUagd:3:CL:4687:awesome_c
           "rev_reg_id": null,
           "timestamp": null
       }
   ]
}
```

IDunion Prototype

- Implemented within IDunion project
- Team: Sebastian Bickerle, Paul Wenzel, Fabian Hauck, & Dr. Daniel Fett
- Use Case: Login to NextCloud using Verifiable Credentials
- Based on
  - Existing NextCloud OpenID Connect Plugin
  - Lissi Wallet
  - Hyperledger Indy & Indy SDK & AnonCreds

IDunion

Supported by:

Federal Ministry
for Economic Affairs
and Climate Action

on the basis of a decision
by the German Bundestag

Architecture