GAIN Activity Report

Exploring Technical Feasibility for Inter-Ecosystem Interoperability

TDI 2024 on April 9th, 2024

Takahiko Kawasaki
Co-Founder of Authlete, Inc.

AUTHLETE

GAIN

Global Assured Identity Network

GAIN (Global Assured Identity Network) is a project to build a high-trust digital identity network over the Internet.

GAIN DIGITAL TRUST, the white paper of the project, was co-authored by over 150 professionals in related fields and published on September 13, 2021.

GAIN PoC Community Group was formed to research GAIN's technical feasibility.

https://gainforum.org/GAINWhitePaper.pdf

AUTHLETE

Current Ecosystem Architecture

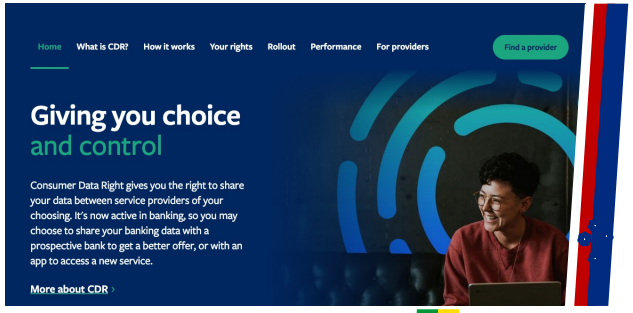
Current Ecosystem Architecture (1/4)

The open banking movement in the United Kingdom has spread to countries around the world.

Each country has built their ecosystems where multiple services and multiple applications connect with each other.

The services and applications have implemented authorization servers and OAuth clients respectively. Their technical details are defined in standards related to OAuth 2.0 and OpenID Connect.

United Kingdom Open Banking



Australia CDR

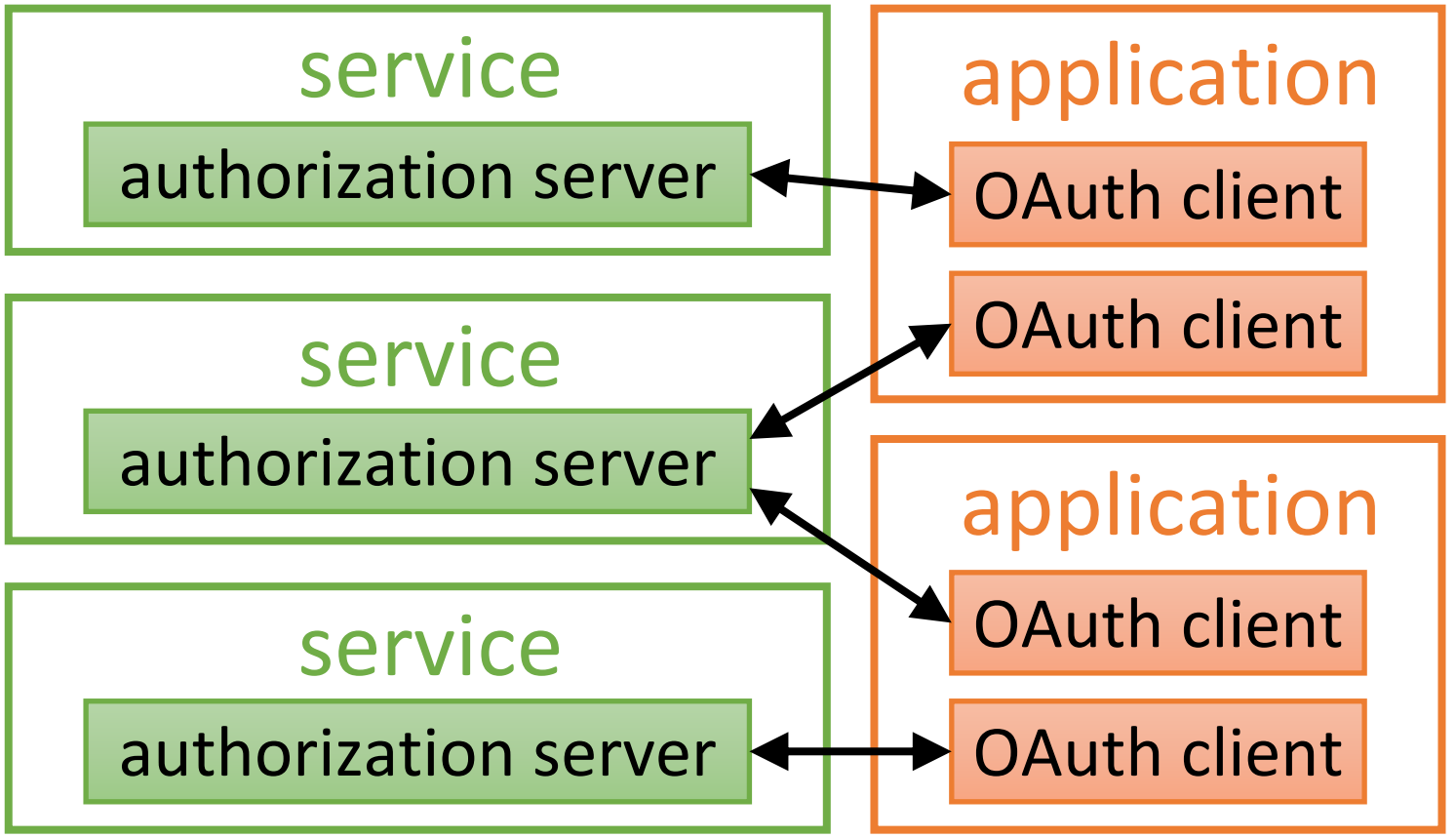
Brazil Open Finance

Saudi Arabia Open Banking

Current Ecosystem Architecture (2/4)

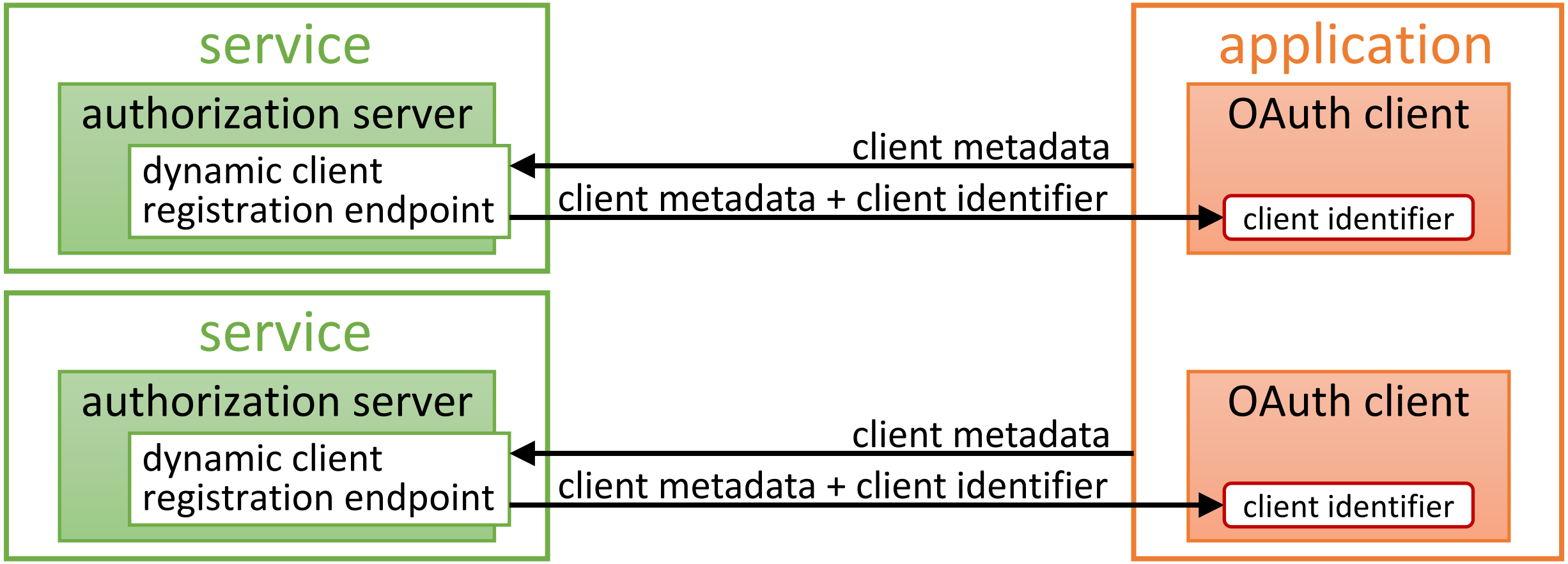
In a typical implementation, an OAuth client belongs to one authorization server at a time. An authorization server and an OAuth client that do not have such a relationship cannot communicate with each other.

Therefore, if an application wants to communicate with multiple services, the application has to establish a relationship with each service's authorization server one by one.



Current Ecosystem Architecture (3/4)

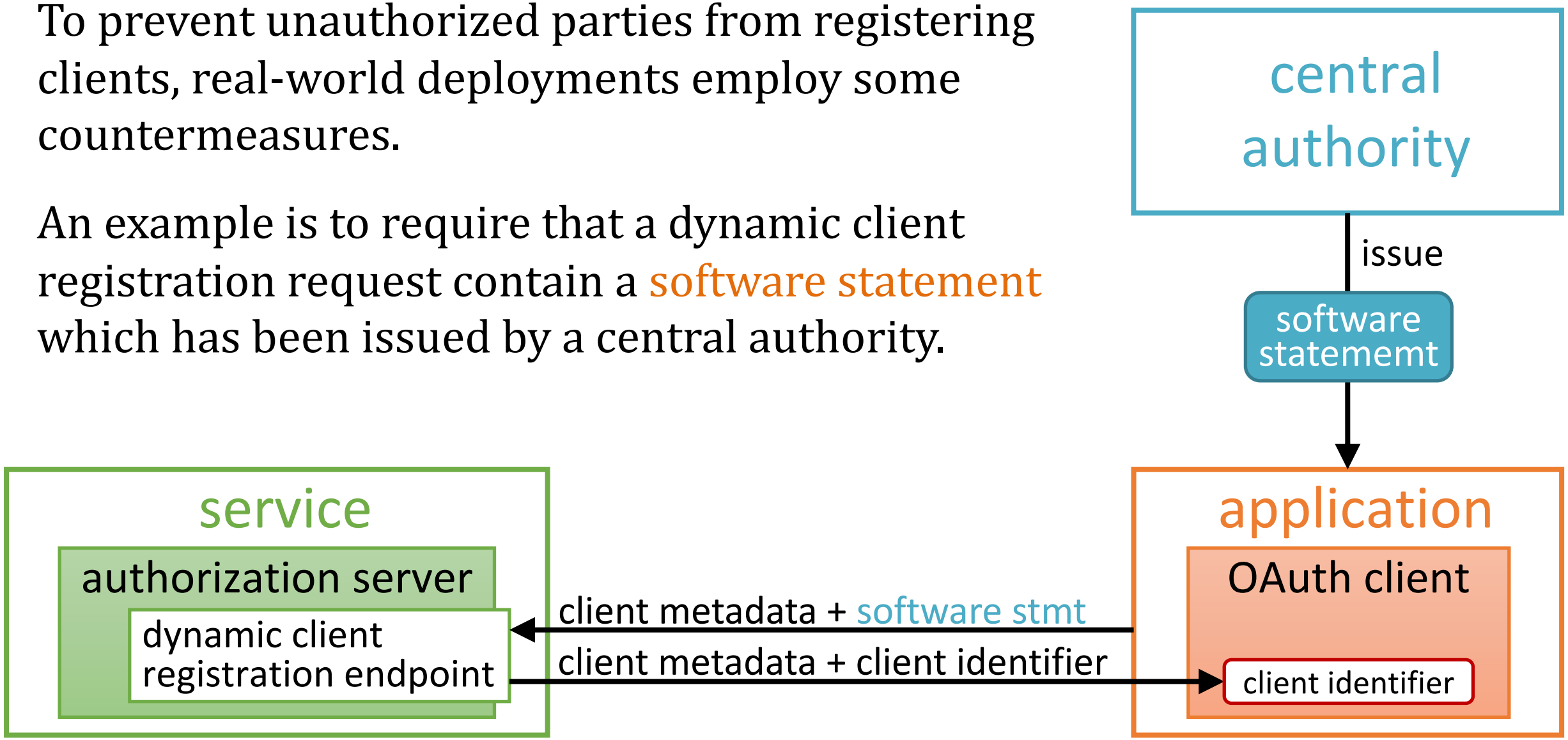
To establish the relationship, an application registers itself to each authorization server by using the mechanism called dynamic client registration.

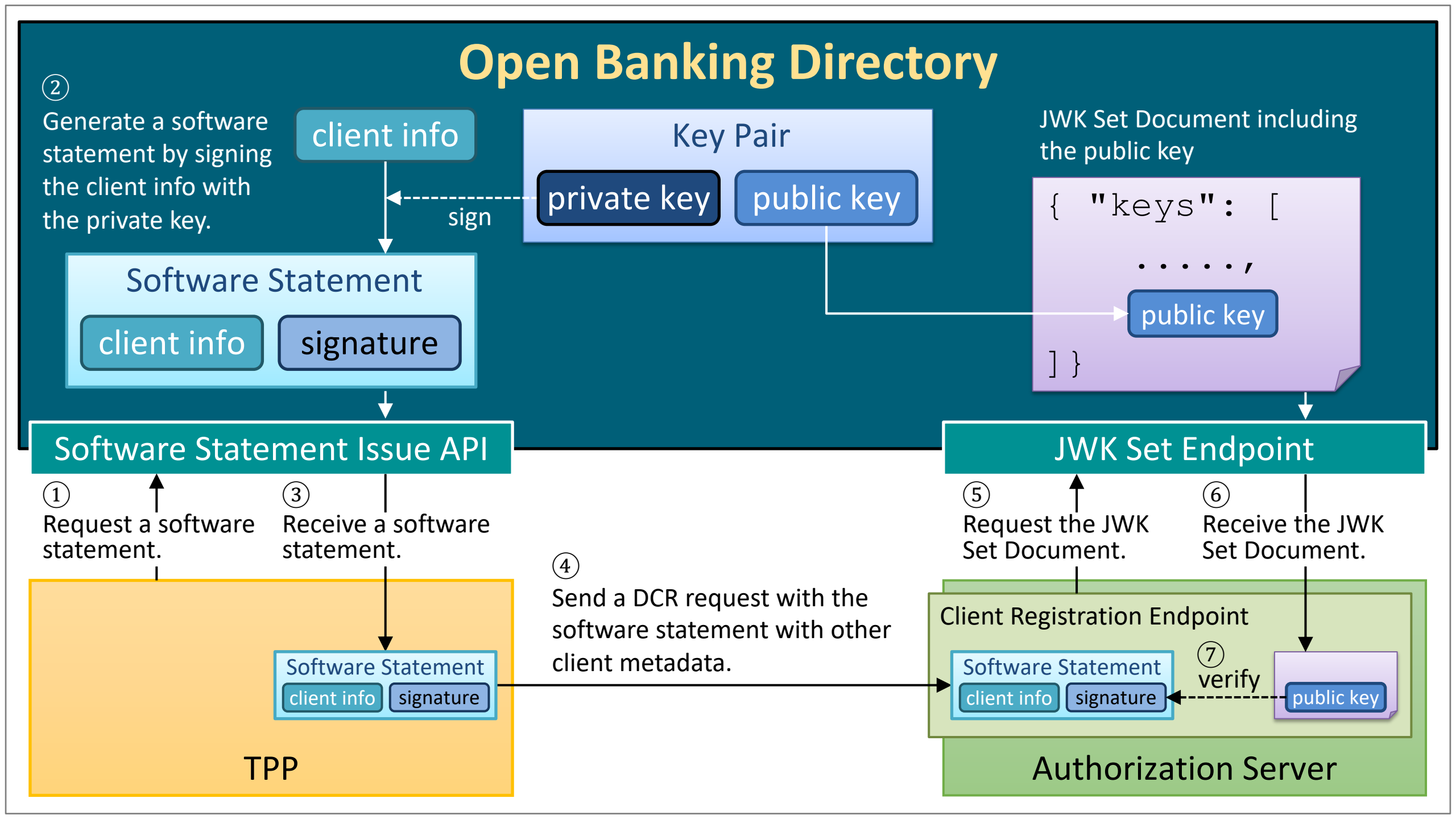


Current Ecosystem Architecture (4/4)

To prevent unauthorized parties from registering clients, real-world deployments employ some countermeasures.

An example is to require that a dynamic client registration request contain a software statement which has been issued by a central authority.




Open Banking Directory
②
Generate a software statement by signing the client info with the private key.
client info
sign
Key Pair
private key
public key
JWK Set Document including the public key
{ "keys": [
.....,
public key
]}
Software Statement
client info
signature
Software Statement Issue API
JWK Set Endpoint
①
Request a software statement.
③
Receive a software statement.
④
Send a DCR request with the software statement with other client metadata.
⑤
Request the JWK Set Document.
⑥
Receive the JWK Set Document.
Software Statement
client info
signature
TPP
Client Registration Endpoint
Software Statement
client info
signature
⑦
verify
public key
Authorization Server

AUTHLETE

Design Considerations

Design Considerations

Decentralized Trust

Trust between applications and services in different ecosystems should be able to be established without needing a single central authority.

Globally-Unique Client Identifiers

An application should be able to use the same client identifier across different services.

KYC

It should be ensured that user claims (such as family name and date of birth) have been obtained through KYC processes.

AUTHLETE

Adopted Standard Specifications

Adopted Standard Specifications

GAIN POC Phase 1 – Done 🎉

- OpenID Federation 1.0
- OpenID Connect for Identity Assurance 1.0 (OIDC4IDA)

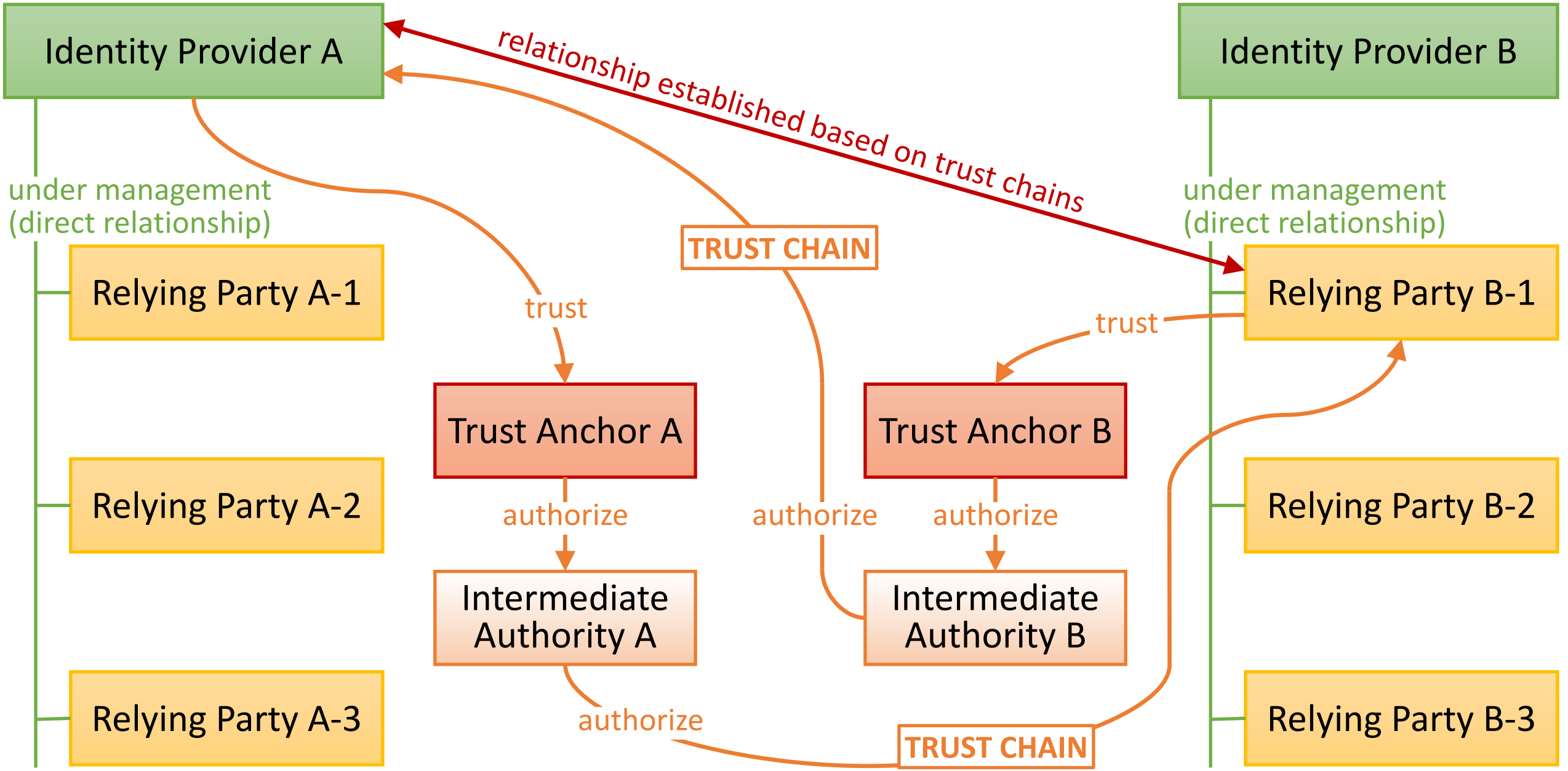
Independent implementations in Italy🇮🇹, Germany🇩🇪 and Japan🇯🇵 could communicate with each other using OpenID Federation 1.0.

GAIN POC Phase 2 – Ongoing (almost done)

- OpenID for Verifiable Credential Issuance (OID4VCI)
- SD-JWT-based Verifiable Credentials (SD-JWT VC)

In practice, this is an interoperability event of Digital Identity Wallet.

OpenID Federation 1.0



OpenID Connect for Identity Assurance 1.0 (OIDC4IDA)

OIDC4IDA defines a mechanism to transmit user claims that have been verified by official evidence such as passport and driver's license.

Information related to verified user claims is all put under the verified_claims claim embedded in ID tokens and/or userinfo responses.

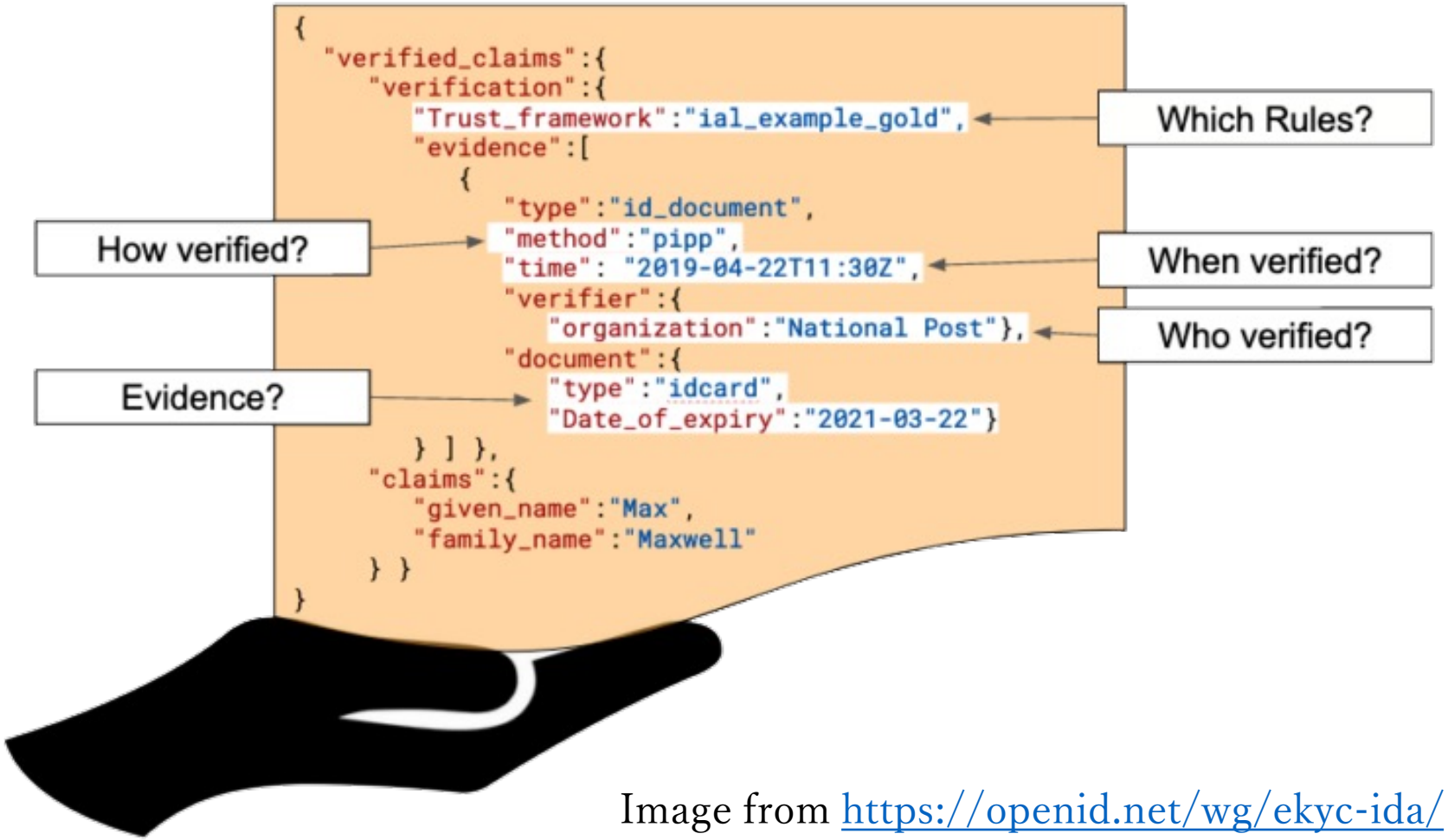
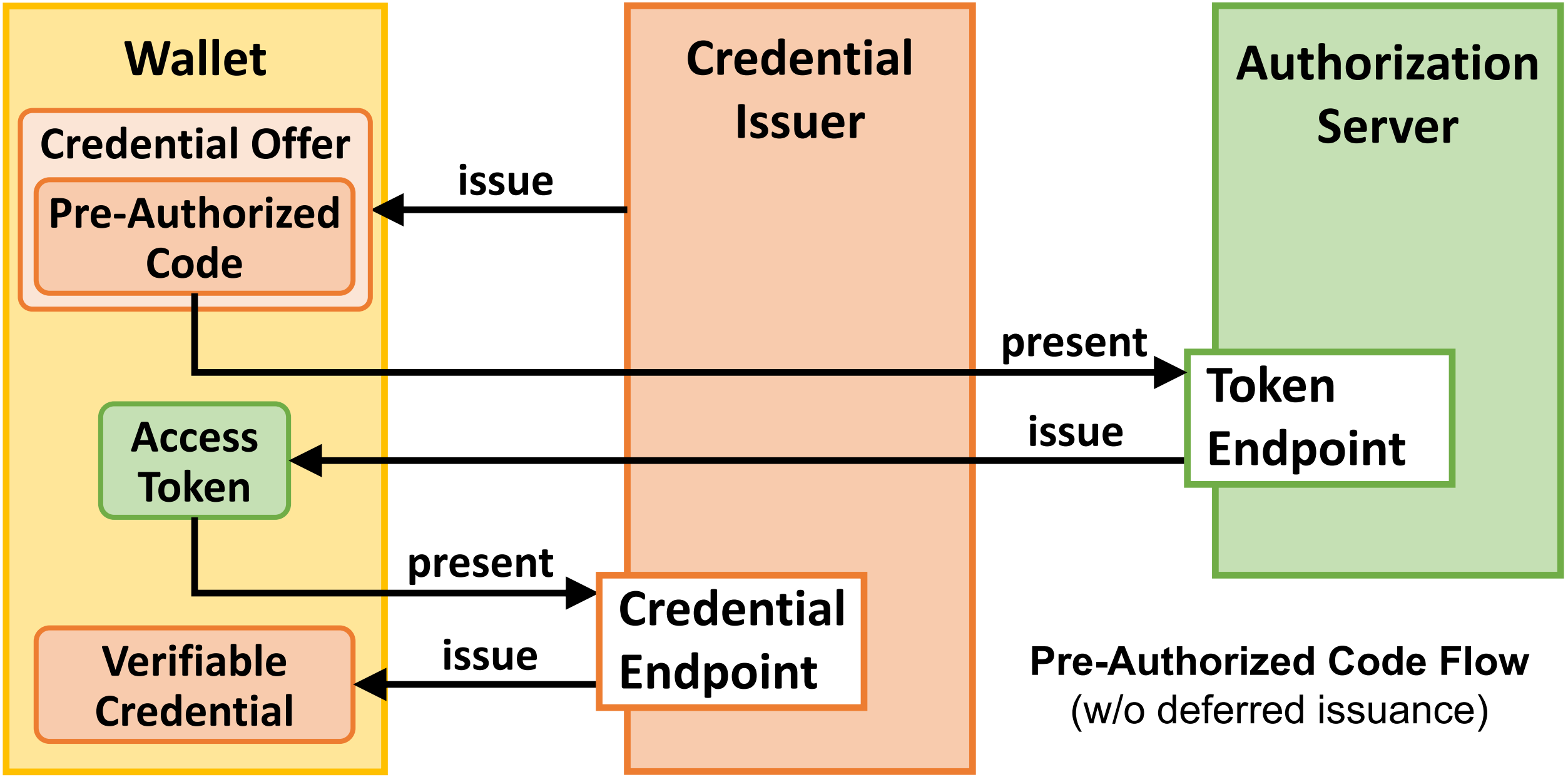


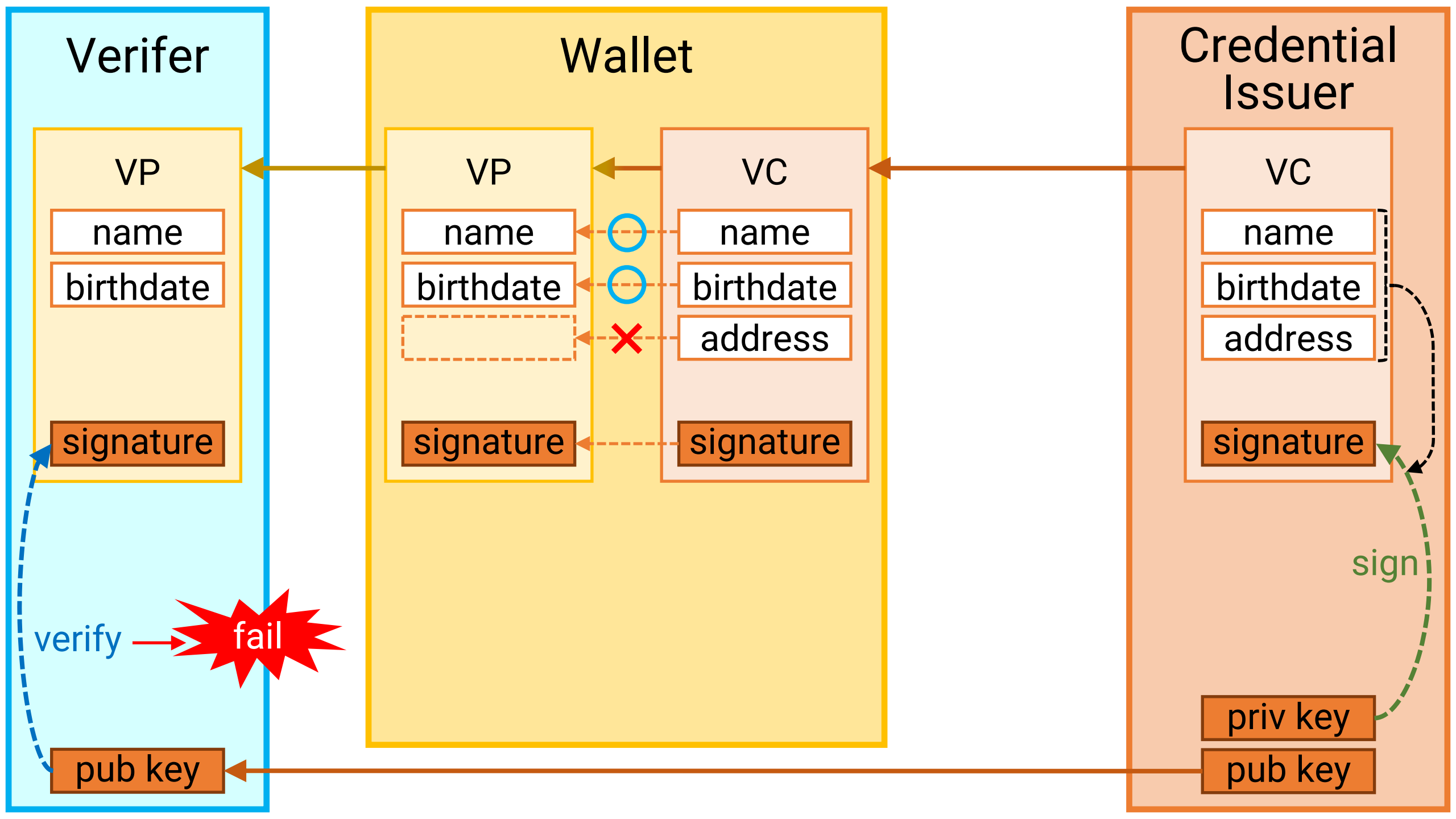
Image from https://openid.net/wg/ekyc-ida/

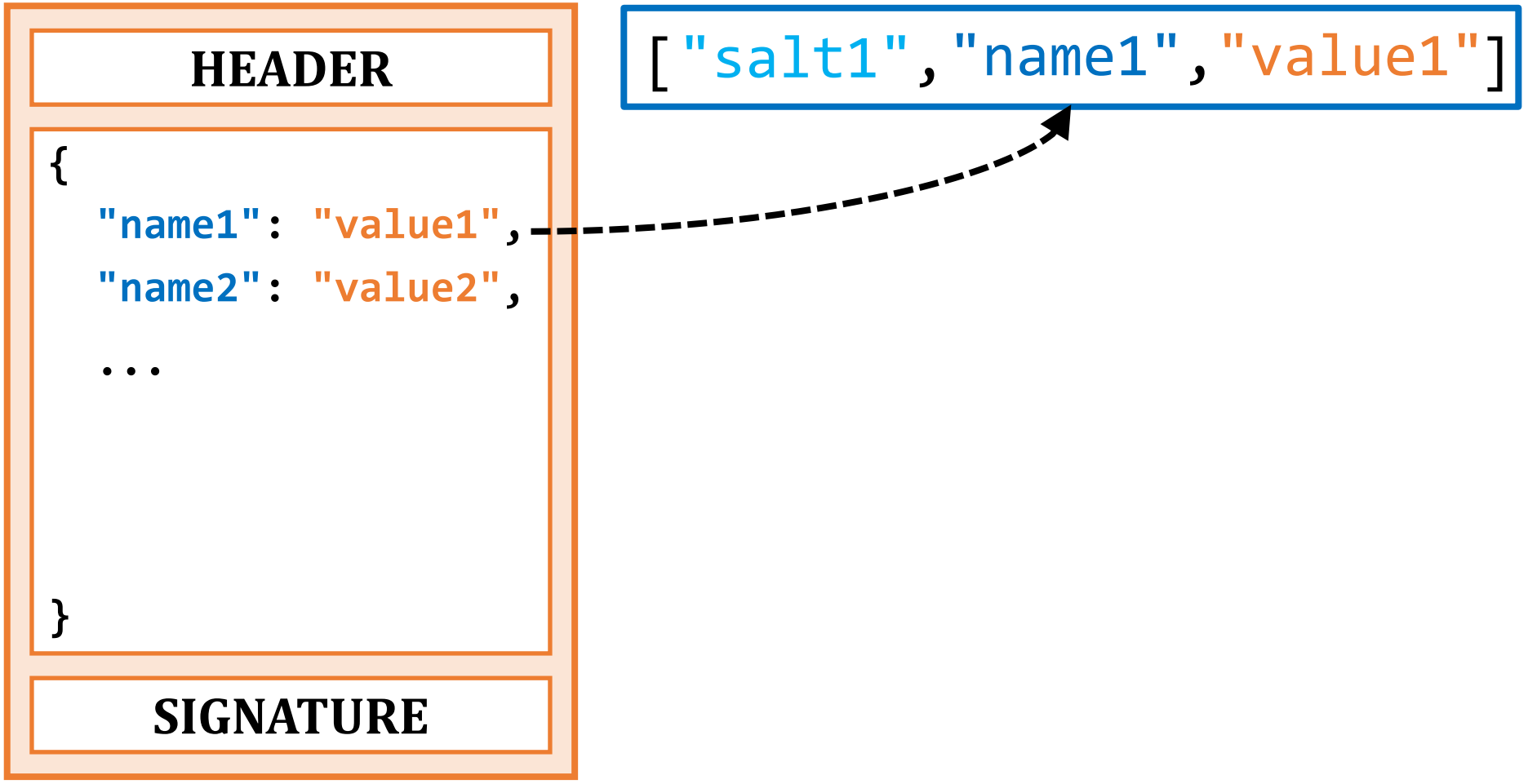
OpenID for Verifiable Credential Issuance (OID4VCI)

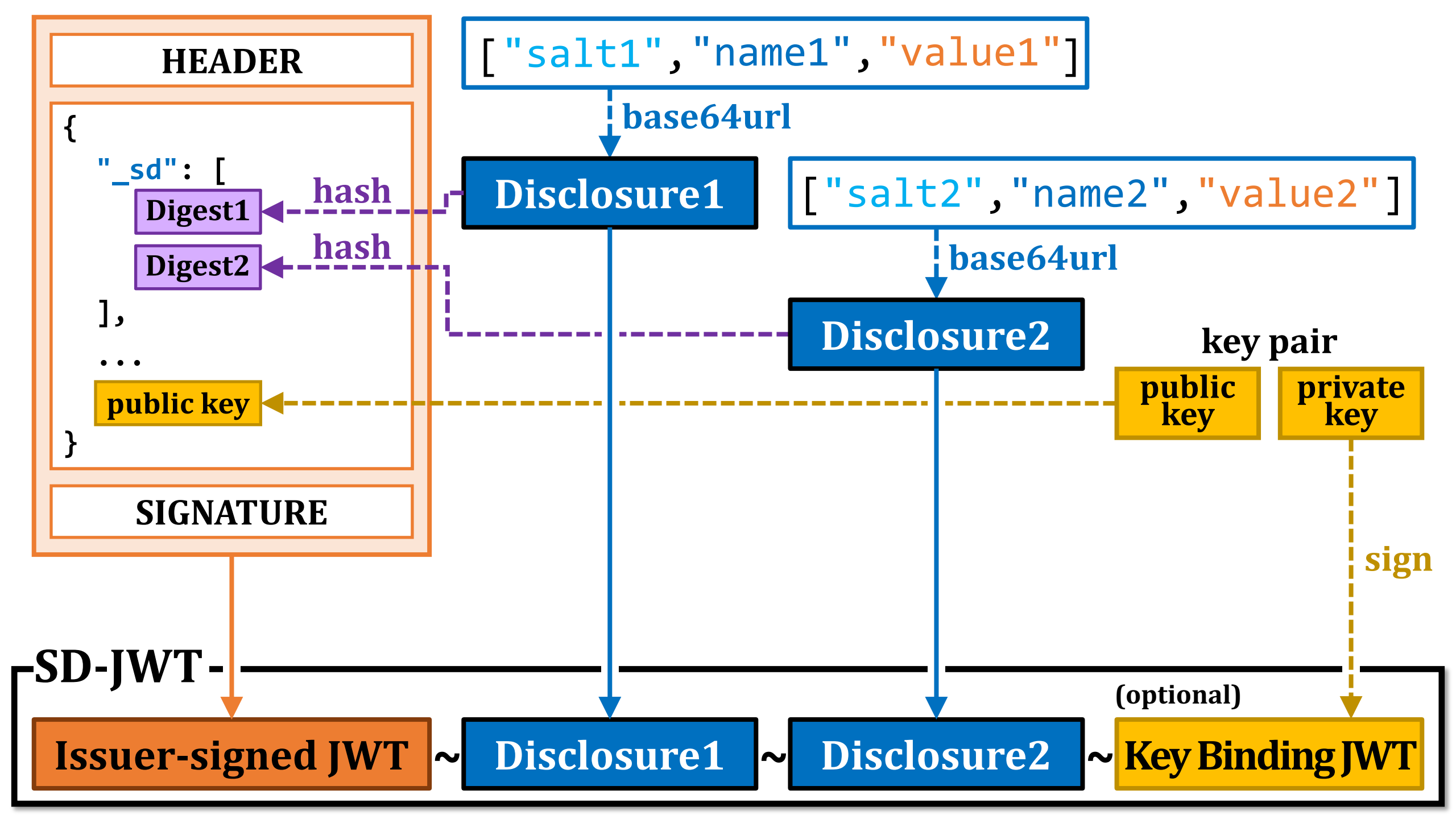


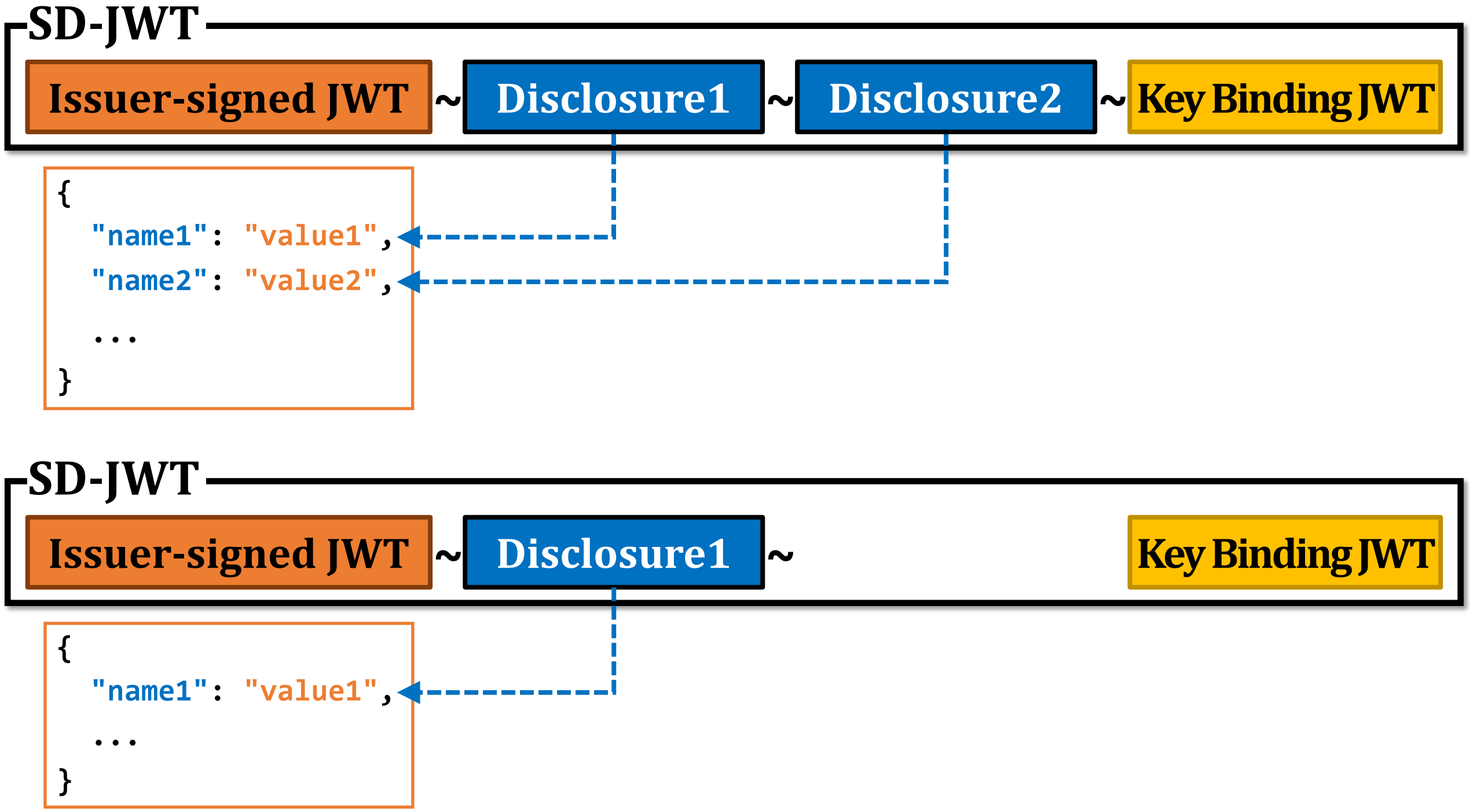
Pre-Authorized Code Flow
(w/o deferred issuance)


AUTHLETE
SD-JWT
Selective Disclosure for JWT


Verifer
Wallet
Credential Issuer
VP
name
birthdate
signature
VP
name
birthdate
signature
VC
name
birthdate
address
signature
VC
name
birthdate
address
signature
verify
fail
sign
pub key
priv key
pub key


HEADER
{
"name1": "value1",
"name2": "value2",
...
}
SIGNATURE
["salt1","name1","value1"]


HEADER
{
"_sd": [
Digest1
Digest2
],
...
public key
}
SIGNATURE
["salt1","name1","value1"]
base64url
Disclosure1
hash
hash
["salt2","name2","value2"]
base64url
Disclosure2
key pair
public key
private key
sign
SD-JWT
(optional)
Issuer-signed JWT
~
Disclosure1
~
Disclosure2
~
Key Binding JWT


SD-JWT
Issuer-signed JWT
~
Disclosure1
~
Disclosure2
~
Key Binding JWT
{
"name1": "value1",
"name2": "value2",
...
}
SD-JWT
Issuer-signed JWT
~
Disclosure1
~
Key Binding JWT
{
"name1": "value1",
...
}

Thank You

www.authlete.com
info@authlete.com
Palo Alto, Tokyo, Dubai

AUTHLETE