gaia-x

Gaia-X SUMMIT 2024

EMPOWERING GLOBAL DATA SPACES

SHAPING TOMORROW'S CLOUD INFRASTRUCTURE

Helsinki, Finland | 14 & 15 November

In partnership with gaia-x Hub Finland

Gaia-X 101: Technical Fundamentals about Gaia-X

09:50 – 10:20

Ewann Gavard

Technical Lead, Gaia-X

Summary

Technologies and standard used in Gaia-X

Gaia-X specifications & documents

Implementation

Renowned specifications

- Verifiable Credentials
- JSON-LD
- JsonWebSignature
- DID/DID Web
- SHACL

Verifiable Credentials W3C

gaia-x

- Shortened in VC
- Represents any form of credential, permit, license
- Used to represent companies, people, services, datacenter, …
- VCs are cryptographically signed by the issuer, allowing to check data tampering and issuer's legitimacy
- VCs are written using JSON-LD, allowing to intricate and bind credentials and claims
- Can be grouped in a Verifiable Presentation (VP)

JSON Linked Data

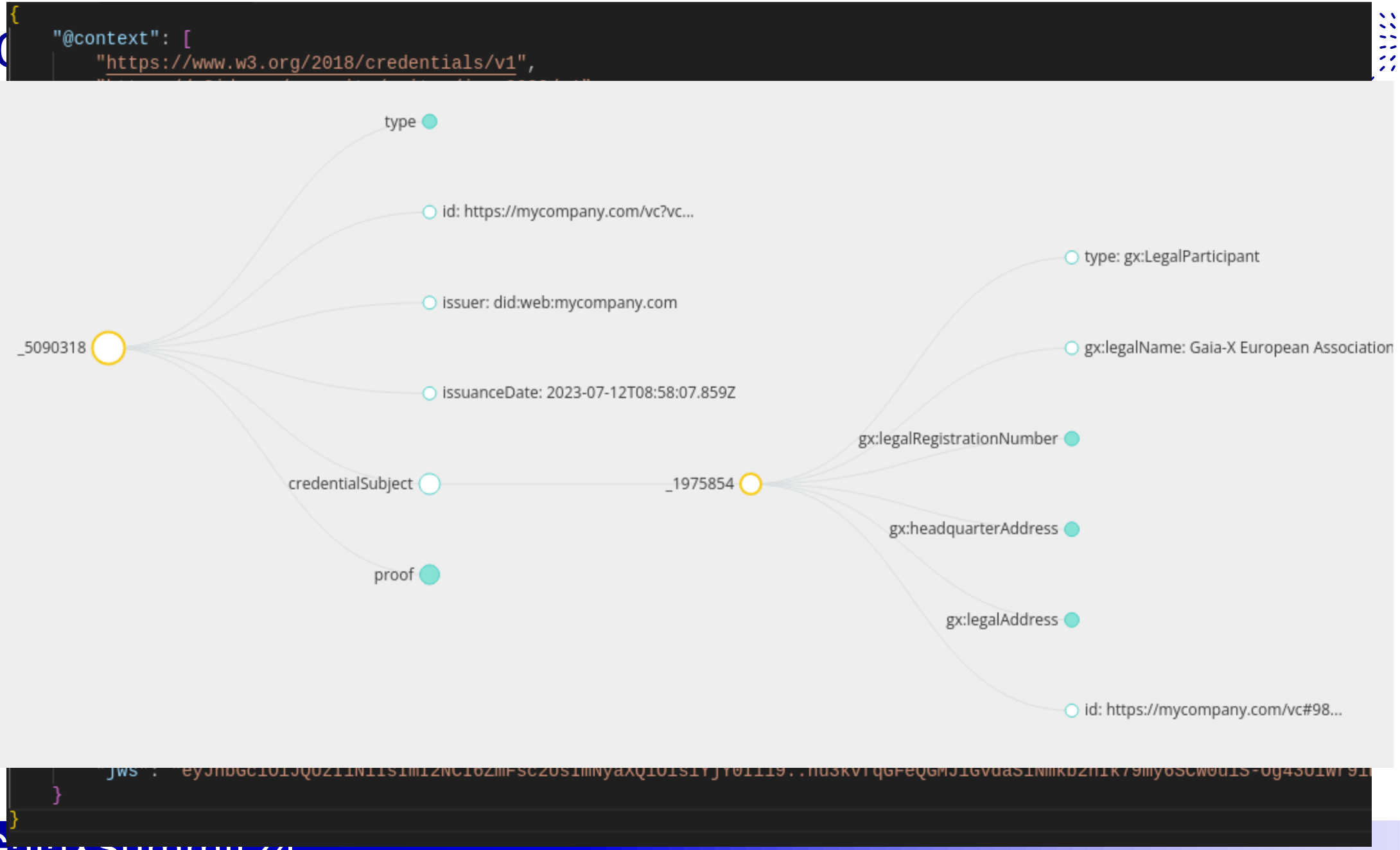
- Contexts
  - Same as XML contexts, allow to target attributes without name collisions
- Links
  - Each JSON-LD file is a graph, allowing to target other nodes, link other graphs
- Representation
  - JSON-LD is just one of many serialization for RDF

JSC

- C
- L
- R


```
{
    "@context": [
        "https://www.w3.org/2018/credentials/v1",
        "https://w3id.org/security/suites/jws-2020/v1",
        "https://registry.lab.gaia-x.eu/development/api/trusted-shape-registry/v1/shapes/jsonld/trustframework#"
    ],
    "type": [
        "VerifiableCredential"
    ],
    "id": "https://mycompany.com/vc?vcid=brown-horse",
    "issuer": "did:web:mycompany.com",
    "issuanceDate": "2023-07-12T08:58:07.859Z",
    "credentialSubject": {
        "type": "gx:LegalParticipant",
        "gx:legalName": "Gaia-X European Association for Data and Cloud AISBL",
        "gx:legalRegistrationNumber": {
            "id": "https://gaia-x.eu/legalRegistrationNumberVC.json"
        },
        "gx:headquarterAddress": {
            "gx:countrySubdivisionCode": "BE-BRU"
        },
        "gx:legalAddress": {
            "gx:countrySubdivisionCode": "BE-BRU"
        },
        "id": "https://mycompany.com/vc#9894e9b0a38aa105b50bb9f4e7d0975641273416e70f166f4bd9fd1b00dfe81d"
    },
    "proof": {
        "type": "JsonWebSignature2020",
        "created": "2023-07-12T08:58:08.438Z",
        "proofPurpose": "assertionMethod",
        "verificationMethod": "did:web:mycompany.com#JWK2020",
        "jws": "eyJhbGciOiJQUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..hu3kvfqGFeQGMJ1GvdaS1Nmkb2hIk79my6SCW0uiS-Og43UiWr9i
    }
}
```

JSO


"@context": [
"https://www.w3.org/2018/credentials/v1",
type
id: https://mycompany.com/vc?vc...
issuer: did:web:mycompany.com
issuanceDate: 2023-07-12T08:58:07.859Z
_5090318
credentialSubject
proof
_1975854
type: gx:LegalParticipant
gx:legalName: Gaia-X European Association
gx:legalRegistrationNumber
gx:headquarterAddress
gx:legalAddress
id: https://mycompany.com/vc#98...

JSO


```
{
    "@context": [
        "https://www.w3.org/2018/credentials/v1",
```

```
[
  {
    "https://www.w3.org/2018/credentials#credentialSubject": [
      {
        "https://registry.lab.gaia-x.eu/development/api/trusted-shape-registry/v1/shapes/jsonld/trustframework#headquarterAddress":
          {
            "https://registry.lab.gaia-x.eu/development/api/trusted-shape-registry/v1/shapes/jsonld/
trustframework#countrySubdivisionCode": [
              {
                "@value": "BE-BRU"
              }
            ]
          }
        ],
        "https://registry.lab.gaia-x.eu/development/api/trusted-shape-registry/v1/shapes/jsonld/trustframework#legalAddress": [
          {
            "https://registry.lab.gaia-x.eu/development/api/trusted-shape-registry/v1/shapes/jsonld/
trustframework#countrySubdivisionCode": [
              {
                "@value": "BE-BRU"
              }
            ]
          }
        ],
        "https://registry.lab.gaia-x.eu/development/api/trusted-shape-registry/v1/shapes/jsonld/trustframework#legalName": [
          {
            "@value": "Gaia-X European Association for Data and Cloud AISBL"
          }
        ],
        "https://registry.lab.gaia-x.eu/development/api/trusted-shape-registry/v1/shapes/jsonld/trustframework#legalRegistrationNur
[
          {
            "@id": "https://gaia-x.eu/legalRegistrationNumberVC.json"
          }
        ],
        "@id": "https://mycompany.com/vc#9894e9b0a38aa105b50bb9f4e7d09756412734l6e70f166f4bd9fd1b00dfe81d",
        "@type": [
          "https://registry.lab.gaia-x.eu/development/api/trusted-shape-registry/v1/shapes/jsonld/trustframework#LegalParticipant"
```

```
    }
}
```

JSC

```
{
    "@context": [
        "https://www.w3.org/2018/credentials/v1",
```

<https://mycompany.com/vc#9894e9b0a38aa105b50bb9f4e7d0975641273416e70f166f4bd9fd1b00dfe81d> <http://www.w3.org/1999/02/22-rdf-syntax-ns#type> <https://registry.lab.gaia-x.eu/development/api/trusted-shape-registry/v1/shapes/jsonld/trustframework#LegalParticipant> .
<https://mycompany.com/vc#9894e9b0a38aa105b50bb9f4e7d0975641273416e70f166f4bd9fd1b00dfe81d> <https://registry.lab.gaia-x.eu/development/api/trusted-shape-registry/v1/shapes/jsonld/trustframework#headquarterAddress> _:b2 .
<https://mycompany.com/vc#9894e9b0a38aa105b50bb9f4e7d0975641273416e70f166f4bd9fd1b00dfe81d> <https://registry.lab.gaia-x.eu/development/api/trusted-shape-registry/v1/shapes/jsonld/trustframework#legalAddress> _:b3 .
<https://mycompany.com/vc#9894e9b0a38aa105b50bb9f4e7d0975641273416e70f166f4bd9fd1b00dfe81d> <https://registry.lab.gaia-x.eu/development/api/trusted-shape-registry/v1/shapes/jsonld/trustframework#legalName> "Gaia-X European Association for Data and Cloud AISBL" .
<https://mycompany.com/vc#9894e9b0a38aa105b50bb9f4e7d0975641273416e70f166f4bd9fd1b00dfe81d> <https://registry.lab.gaia-x.eu/development/api/trusted-shape-registry/v1/shapes/jsonld/trustframework#legalRegistrationNumber> <https://gaia-x.eu/legalRegistrationNumberVC.json> .
<https://mycompany.com/vc?vcid=brown-horse> <http://www.w3.org/1999/02/22-rdf-syntax-ns#type> <https://www.w3.org/2018/credentials#VerifiableCredential> .
<https://mycompany.com/vc?vcid=brown-horse> <https://w3id.org/security#proof> _:b0 .
<https://mycompany.com/vc?vcid=brown-horse> <https://www.w3.org/2018/credentials#credentialSubject> <https://mycompany.com/vc#9894e9b0a38aa105b50bb9f4e7d0975641273416e70f166f4bd9fd1b00dfe81d> .
<https://mycompany.com/vc?vcid=brown-horse> <https://www.w3.org/2018/credentials#issuanceDate> "2023-07-12T08:58:07.859Z"^^<http://www.w3.org/2001/XMLSchema#dateTime> .
<https://mycompany.com/vc?vcid=brown-horse> <https://www.w3.org/2018/credentials#issuer> <did:web:mycompany.com> .
_:b1 <http://purl.org/dc/terms/created> "2023-07-12T08:58:08.438Z"^^<http://www.w3.org/2001/XMLSchema#dateTime> _:b0 .
_:b1 <http://www.w3.org/1999/02/22-rdf-syntax-ns#type> <https://w3id.org/security#JsonWebSignature2020> _:b0 .
_:b1 <https://w3id.org/security#jws> "eyJhbGciOiJQUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..hu3kvfqGFeQGMJ1GvdaS1Nmkb2hIk79my6SCW0ui
Og43UiWr9iHh96e7acYChLVopEF_Al2a0KAjT9BnkbfGlXCGgAAKYS5X22bV1EUX5B-NHJhmGRC5ScgCjfivU4yEzEdpoSrFiE4M0v-
NbMB7Q4qvWPPT4og0IRVyU4N5pBXWxn4pfc-__Rl_1k6us8Dhkl0yLgVFTQ562P1E7EorSHLZh73C2chV50YwYpH7DTmiLAaDlj5SC5X7ayWHa8LuPz3dRHl7Arj-
sdFyIjEockGeq9Mmzcc2N6QjTi2hYaA493lOSdoglhp3Aqz3A1fHbKkdRH662NAlERFFHDeg" _:b0 .
_:b1 <https://w3id.org/security#proofPurpose> <https://w3id.org/security#assertionMethod> _:b0 .
_:b1 <https://w3id.org/security#verificationMethod> <did:web:mycompany.com#JWK2020> _:b0 .
_:b2 <https://registry.lab.gaia-x.eu/development/api/trusted-shape-registry/v1/shapes/jsonld/trustframework#countrySubdivisionCode> "BE-BRU" .
_:b3 <https://registry.lab.gaia-x.eu/development/api/trusted-shape-registry/v1/shapes/jsonld/trustframework#countrySubdivisionCode> "BE-BRU" .

```
    }
}
```

DID: Decentralized Identifiers

Self-declared and self-hosted identity

Contains cryptographic material allowing to ensure trust

One specification used in Gaia-X at the moment : did:web

Examples:

did:web:compliance.lab.gaia-x.eu:v1 resolves to https://compliance.lab.gaia-x.eu/v1/did.json

did:web:bakeup.io resolves to https://bakeup.io/.well-known/did.json

DID: Decentralized I

Self-declared and self-

Contains cryptographi e trust

One specification usec id:web

Examples:

did:web:compliance.lab compliance.lab.gaia-x.eu/v1/did.json

did:web:bakeup.io resol own/did.json


```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/jws-2020/v1"
  ],
  "id": "did:web:bakeup.io",
  "verificationMethod": [
    {
      "id": "did:web:bakeup.io#JWK2020-RSA",
      "type": "JsonWebKey2020",
      "controller": "did:web:bakeup.io",
      "publicKeyJwk": {
        "kty": "RSA",
        "n": "...publicKey...",
        "e": "AQAB",
        "alg": "PS256",
        "x5u": "https://bakeup.io/.well-known/cert.crt"
      }
    }
  ],
  "assertionMethod": [
    "did:web:bakeup.io#JWK2020-RSA"
  ],
  "service": [{
    "id":"did:web:bakeup.io#participant",
    "type": "LinkedDomains",
    "serviceEndpoint": "https://bakeup.io/participant.json"
  },{
    "id":"did:web:bakeup.io#lrn",
    "type": "LinkedDomains",
    "serviceEndpoint": "https://bakeup.io/lrn.json"
  },{
    "id":"did:web:bakeup.io#tsandcs",
    "type": "LinkedDomains",
    "serviceEndpoint": "https://bakeup.io/tsandcs.json"
  },{
    "id":"did:web:bakeup.io#gx",
    "type": "LinkedDomains",
    "serviceEndpoint": "https://bakeup.io/gx.json"
  },{
    "id":"did:web:bakeup.io#service",
    "type": "LinkedDomains",
    "serviceEndpoint": "https://bakeup.io/service.json"
  }]
}
```

DID: Decentralized I

Self-declared and self-

Contains cryptographi trust

One specification usec id:web

Examples:

did:web:compliance.lab compliance.lab.gaia-x.eu/v1/did.json

did:web:bakeup.io resol own/did.json

DID: Decentralized Id

Self-declared and self-

Contains cryptographi trust

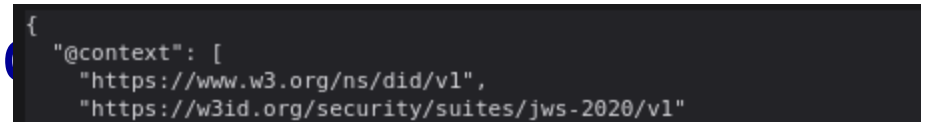
One specification used id:web

Examples:

did:web:compliance.lab compliance.lab.gaia-x.eu/v1/did.json

did:web:bakeup.io resol own/did.json

DID: Decentralized Id



Self-declared

Contains cry

One specific

@gaia-x/did-web-generator TS

1.0.1 • Public • Published a month ago

Readme | Code Beta | 2 Dependencies | 0 Dependents

Gaia-X AISBL DID Generator Library

This library allows you to generate a ready to use DID.

It uses your certificate to generate it, and thus relies on several x509/crypto libraries to work.

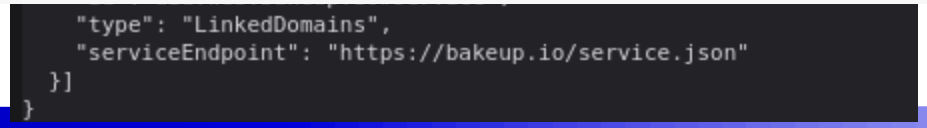
Usage

```
import {createDidDocument} from '@gaia-x/did-web-generator'
//...
function getDid(){
    return createDidDocument("https://mycompanydomain.com", "x509Certifica
}
```

Examples:

did:web:com .lab.gaia-x.eu/v1/did.js

did:web:bake n



SHACL W3C

gaia-x

Know as shapes in our ecosystem, and written in Turtle

Validates RDF structure of documents

Similar to XSD for XML

Not all constraints can be expressed in SHACL, some business rules need code to be implemented

SHACL

Know as shap e

Validates RDF

Similar to XSD

Not all constra business rules need code to

```
gx:LegalParticipantShape
    a sh:NodeShape ;
    sh:targetClass gx:LegalParticipant ;
    sh:property
        [
            sh:path gx:legalRegistrationNumber ;
            sh:node gx:legalRegistrationNumberShape ;
            sh:minCount 1 ;
        ],
        [
            sh:path gx:parentOrganization ;
            sh:node gx:LegalParticipantShape ;
        ],
        [
            sh:path gx:subOrganization ;
            sh:node gx:LegalParticipantShape ;
        ],
        [
            sh:path gx:headquarterAddress ;
            sh:minCount 1 ;
            sh:node gx:PostalAddressShape ;
        ],
        [
            sh:path gx:legalAddress ;
            sh:minCount 1 ;
            sh:node gx:PostalAddressShape ;
        ] .

gx:legalRegistrationNumberShape
    a sh:NodeShape ;
    sh:targetClass gx:legalRegistrationNumber ;
    sh:message "At least one of taxID, vatID, EUID, EORI or leiCode must be defined." ;
    sh:property
        [
            sh:path gx:taxID ;
            sh:datatype xsd:string ;
            sh:minLength 3 ;
        ] ;
    sh:property
        [
            sh:path gx:EUID ;
            sh:datatype xsd:string ;
            sh:minLength 3 ;
        ] ;
    sh:property
```

Gaia-X specifications

- Technical & Semantic interoperability
  - Identity & Credentials Access Management Document (ICAM)
  - Architecture Document (AD)
  - Data Exchange Document (DEX)
  - Gaia-X Ontology (Loire only)

- Legal & Organisational interoperability
  - For Tagus:
    - Trust Framework (TF, split between Compliance Document & Architecture Document)
    - Policy Rules & Labelling Document (PRLD)
  - For Loire:
    - Compliance Document (CD)

- Each document is available on docs.gaia-x.eu

Gaia-X

- Techn
  - Id
  - Ar
  - Da
  - Fo
- Legal
  - Fo
  - Fo
- Each

`ions`			Ecosystem as defined below

Example of T&C signed by the issuer

5.2 Legal person

For legal person the attributes are

Attribute	Cardinality	Trust Anchor	Comment
`registrationNumber`	1	registrationNumberIssuer	Country's registration number, which identifies one specific entity.
`headquartersAddress.countryCode`	1	State	Physical location of the headquarters in ISO 3166-2 alpha2, alpha-3 or numeric format.
`legalAddress.countryCode`	1	State	Physical location of legal registration in ISO 3166-2 alpha2, alpha-3 or numeric format.
`parentOrganization[]`	0..*	State	A list of direct `participant` that this entity is a subOrganization of, if any.
`subOrganization[]`	0..*	State	A list of direct `participant` with a legal mandate on this entity, e.g., as a subsidiary.

#GaiaX

Gaia-X

- Techn
  - Id
  - Ar
  - Da
  - Fo
- Legal
  - Fo
  - Fo
- Each

#Gaia

Criterion P1.1.1: The Provider shall offer the ability to establish a legally binding act. This legally binding act shall be documented.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: Using the Gaia-X Ontology, the declaration shall contain either a resolvable identifier pointing to the legally binding act offered by the Provider or a contact form to request more information.

Permissible Standards:

- SecNumCloud: 19.1
- BSI C5: BC-01, OIS-03
- CISPE (GDPR, Infrastructure & IaaS): 4.2
- EU Cloud CoC (GDPR, XaaS): 5.1.A, 5.1.B
- CSA CCM: STA-09
- SWIPO IaaS: FR1, FR2

Example Standards:N/A

Note

The Provider needs to ensure a process that guarantees that a legally binding act is in place before delivering any form of service.

aia-X

Gaia-X

- Techn
  - Id
  - Ar
  - Da
  - Fo
- Legal
  - Fo
  - Fo
- Each

#Gaia

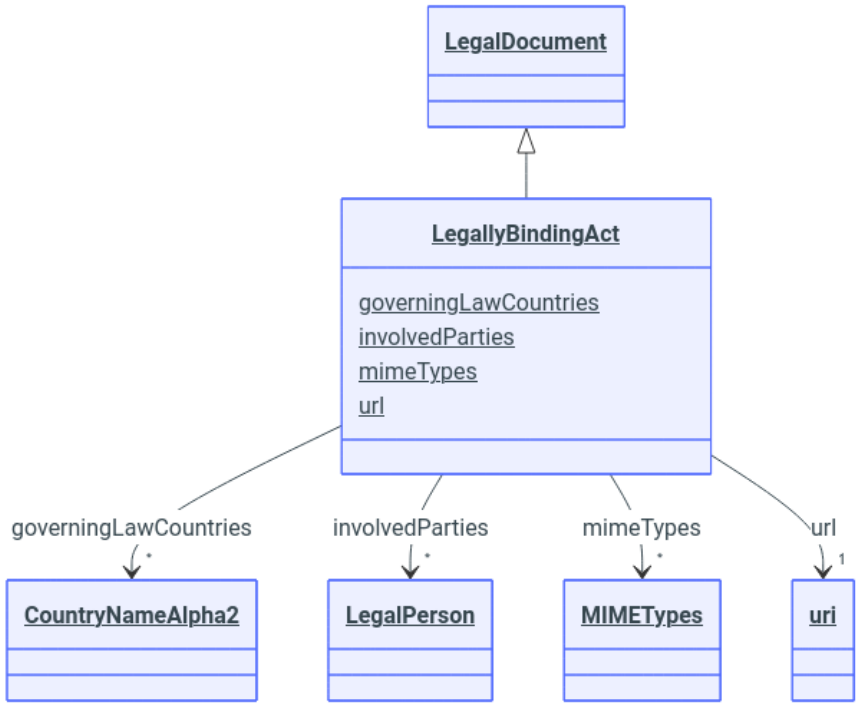
Criterion P1.1.1: The Provider shall offer the ability to establish a legally binding act. This legally

b

LegallyBindingAct

Legal document describing the legally binding act.

URI: gx:LegallyBindingAct



Inheritance

- LegalDocument
  - **LegallyBindingAct**

aia-X

IETF Signature

- Embedded proof for Tagus (IETF JWS)
- JWT-VC Enveloping proof for Loire (IETF JWT & VC-JOSE-COSE)

- Easier to manage, no need to canonize to check the signature
- Info about issuer, key are in the headers (iss, kid)

Gaia-X specifications in a slide (Tagus)

- Identity and Credentials Access Management 22.10
  - Everything is described using VerifiableCredentials in JSON-LD
  - On production, participant must use an EV-SSL or eIDAS certificate to sign their credentials
- Trust Framework 22.10
  - Each issuer has to provide signed terms and conditions (TL;DR be nice)
  - Participant has to provide a Legal Registration Number issued by an accredited notary
- Architecture Document 22.10
  - Few providers are accredited Gaia-X compliance issuers, more to come.
  - Having your credentials validated by the engine will result in a Gaia-X compliance VerifiableCredential
- Policy and Rules Labelling Document 22.11
  - Confirming adhesion to all criteria gives Label Level 1. No other levels specified/implemented

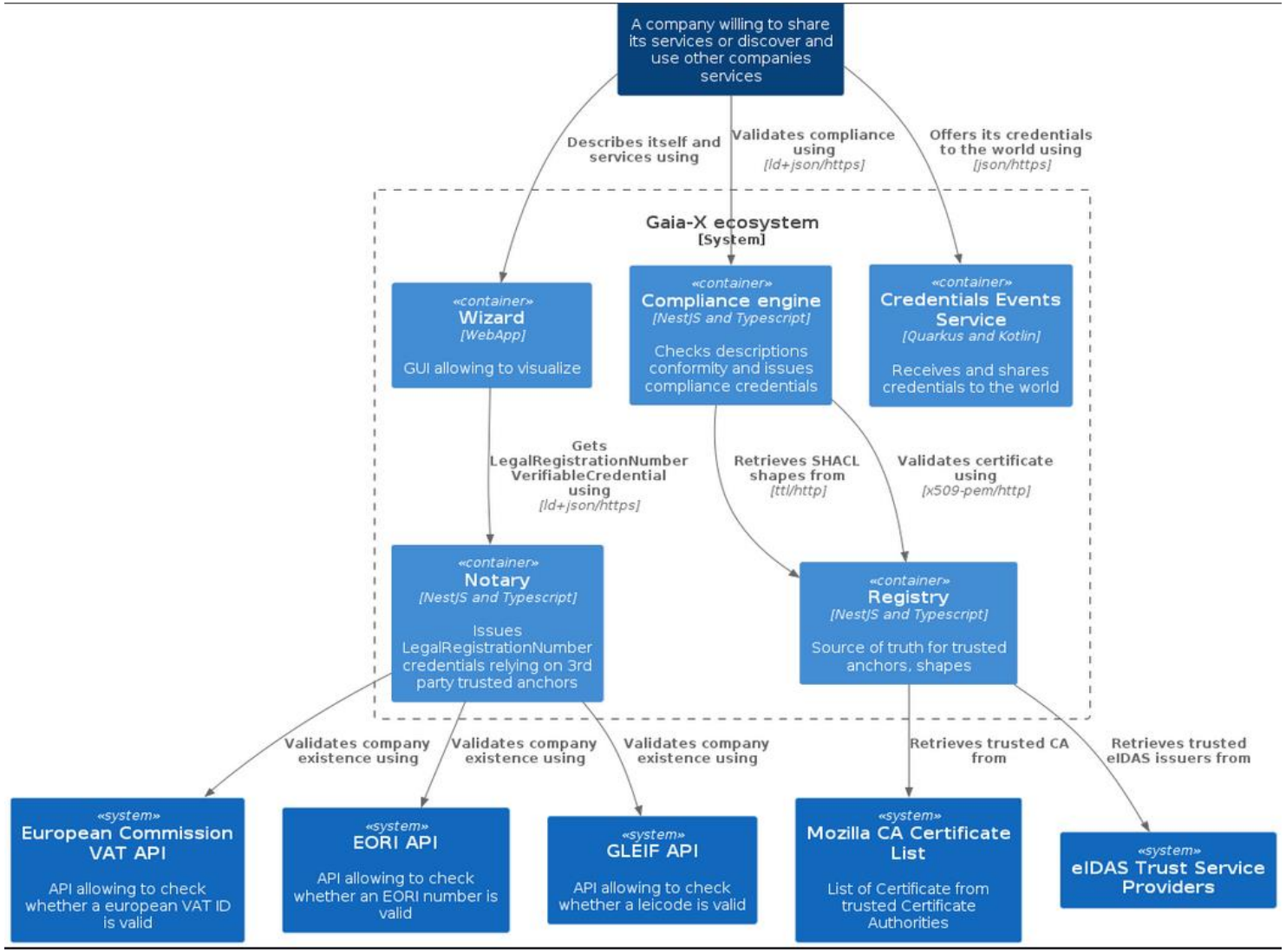
Gaia-X specifications in a slide (Loire)

- Identity and Credentials Access Management 24.11
  - Everything is described using VerifiableCredentials in JSON-LD
  - A new default format for Verifiable Credential signature has been introduced (enveloped signature): VC-JWT
  - Optional support for OID4VCI/OID4VP is described
  - Solutions for delegation of rights/definition of the scope of Trust Anchors

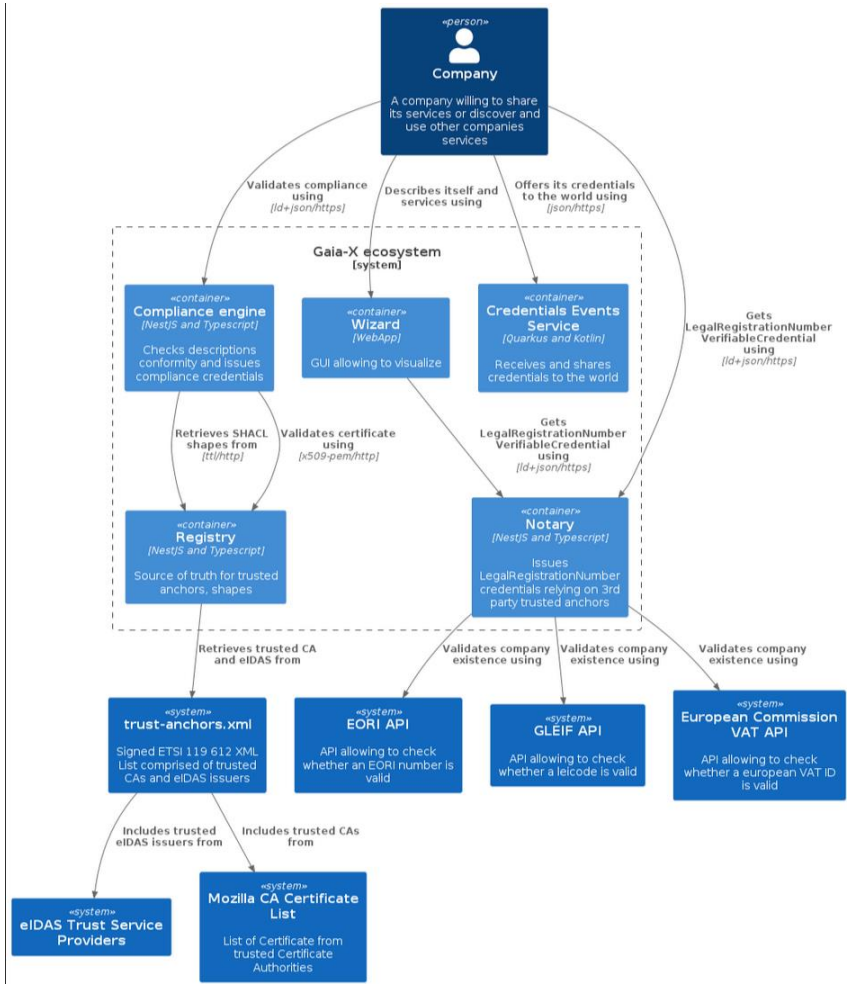
- Compliance Document 24.06
  - Establishes Compliance criteria for Cloud Services, with 4 different levels (Standard Compliance, Label L1, Label L2, Label L3)
  - Refers to the ontology for practical description of each class (Declaration)
  - Criteria for CABs approval (Certification)
  - Initial list of accredited CABs with reference to the identified permissible standards (Certification)

- Architecture Document 24.04
  - Few providers are accredited Gaia-X compliance issuers, more to come.
  - Having your credentials validated by the engine will result in a Gaia-X compliance VerifiableCredential
  - Representation of the Gaia-X Trust Framework process flow and roles, including CABs supporting Labels L2, L3
  - Updated decription of the section on "Policies" /reference to the ODRL profile
  - Protocols, Standards and APIs for mandatory components operated by GXDCHs)
  - Inclusion of the CES in the list of mandatory components and specifications update

Software architecture



Software Architecture v2



Implementation by the lab

- 3 main components:
  - Registry
  - Notary
  - Compliance
- Loire adds the Credential-Events-Service to publish Gaia-X Compliance credentials

- Libraries & tooling
  - DID generation, Signature (Tagus), Wizard (Tagus), Generator (Loire)

Details about v2 implementation

- 14:00 – 15:00 Tech theatre

Thank you!

Ewann Gavard

Navigating the Loire release

14:00 – 15:00

Ewann Gavard, Technical Lead, Gaia-X

Christoph Strnadl, Chief Technology Officer, Gaia-X

Pierre Gronlier, Chief Innovation Officer, Gaia-X

Navigating the Loire release

Christoph Strnadl - Pierre Gronlier - Ewann Gavard

Chief Technology Officer – Chief Innovation Officer - Technical Lead

Gaia-X Association for Data and Cloud AISBL

Summary

- Overview of the specifications
- Technical changes
- Discussion

What is in the Loire release ?

- Second production-ready implementation of the Gaia-X Trust Framework
  - Implements Compliance Document 24.06, Architecture Document 24.04, Identity Credentials & Access Management 24.07

- Several steps forward compared to Tagus
  - Proper validation of the Compliance Document criteria for declaration
  - Alignment with the Gaia-X Ontology

Compliance Document

- Policy and Rules Committee
- Translate EU Values, policies, directives into understandable and verifiable criteria
- Based on renowned permissible standards (SecNumCloud, BSI C5, GPDR)
- 4 levels defined, from Standard Compliance to Label level 3

Compliance Document translation

Criterion P1.1.2: The Provider shall have an option for each legally binding act to be governed by EU/EEA/Member State law.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: Using the Gaia-X Ontology, the declaration shall contain the list of ISO 3166-2 codes indicating the EU/EEA/Member States whose law may be applied as governing law for the legally binding act.

Permissible Standards:

- SecNumCloud: 19.1.c
- CISPE (GDPR, Infrastructure & IaaS): 4.2
- EU Cloud CoC (GDPR, XaaS): 5.1.A, 5.1.B, 5.1.C, 5.1.F, 5.4.F

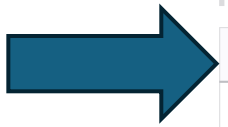
Example Standards:

- BSI C5: BC-01
- CSA CCM: STA-09
- SWIPO IaaS: FR1, FR2

Compliance Document translation

Criterion P1.1.2: The Provider shall have an option for each legally binding act to be governed by EU/EEA/Member State law.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration



Criterion P1.1.2

> The Provider shall have an option for each legally binding act to be governed by EU/EEA/Member State law.

Standard Compliance	Label L1	Label L2	Label L3
declaration	declaration	declaration	declaration
implemented	**implemented**	**implemented**	**implemented**

View in Compliance Document

Checks that the `ServiceOffering` has at least one `LegallyBindingAct` in its `legalDocuments` that is governed by an EAA country referenced in its `governingLawCountries`.

Implemented by ServiceOfferingLegallyBindingActsHaveGoverningLawCountry

Declaration: Using the Gaia-X Ontology, the declaration shall contain the list of ISO 3166-2 codes indicating the EU/EEA/Member States whose law may be applied as governing law for the legally binding act.

Permissible Standards:

- SecNumCloud: 19.1.c
- CISPE (GDPR, Infrastructure & IaaS): 4.2
- EU Cloud CoC (GDPR, XaaS): 5.1.A, 5.1.B, 5.1.C, 5.1.F, 5.4.F

Example Standards:

- BSI C5: BC-01
- CSA CCM: STA-09
- SWIPO IaaS: FR1, FR2

Compliance Document translation

Criterion P1.1.2: The Provider shall have an option for each legally binding act to be governed by EU/EEA/Member State law.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: Using the Gaia-X Ontology, the declaration shall contain the list of ISO 3166-2 codes indicating the EU/EEA/Member States whose law may be applied as governing law for the legally binding act.

Permissible Standards:

- SecNumCloud: 19.1.c
- CISPE (GDPR, Infrastructure & IaaS): 4.2
- EU Cloud CoC (GDPR, XaaS): 5.1.A, 5.1.B, 5.1.C, 5.1.F, 5.4.F

Example Standards:

- BSI C5: BC-01
- CSA CCM: STA-09
- SWIPO IaaS: FR1, FR2

Criterion P1.1.2

> The Provider shall have an option for each legally binding act to be governed by EU/EEA/Member State law.

Standard Compliance	Label L1	Label L2	Label L3
declaration	declaration	declaration	declaration
implemented	**implemented**	**implemented**	**implemented**

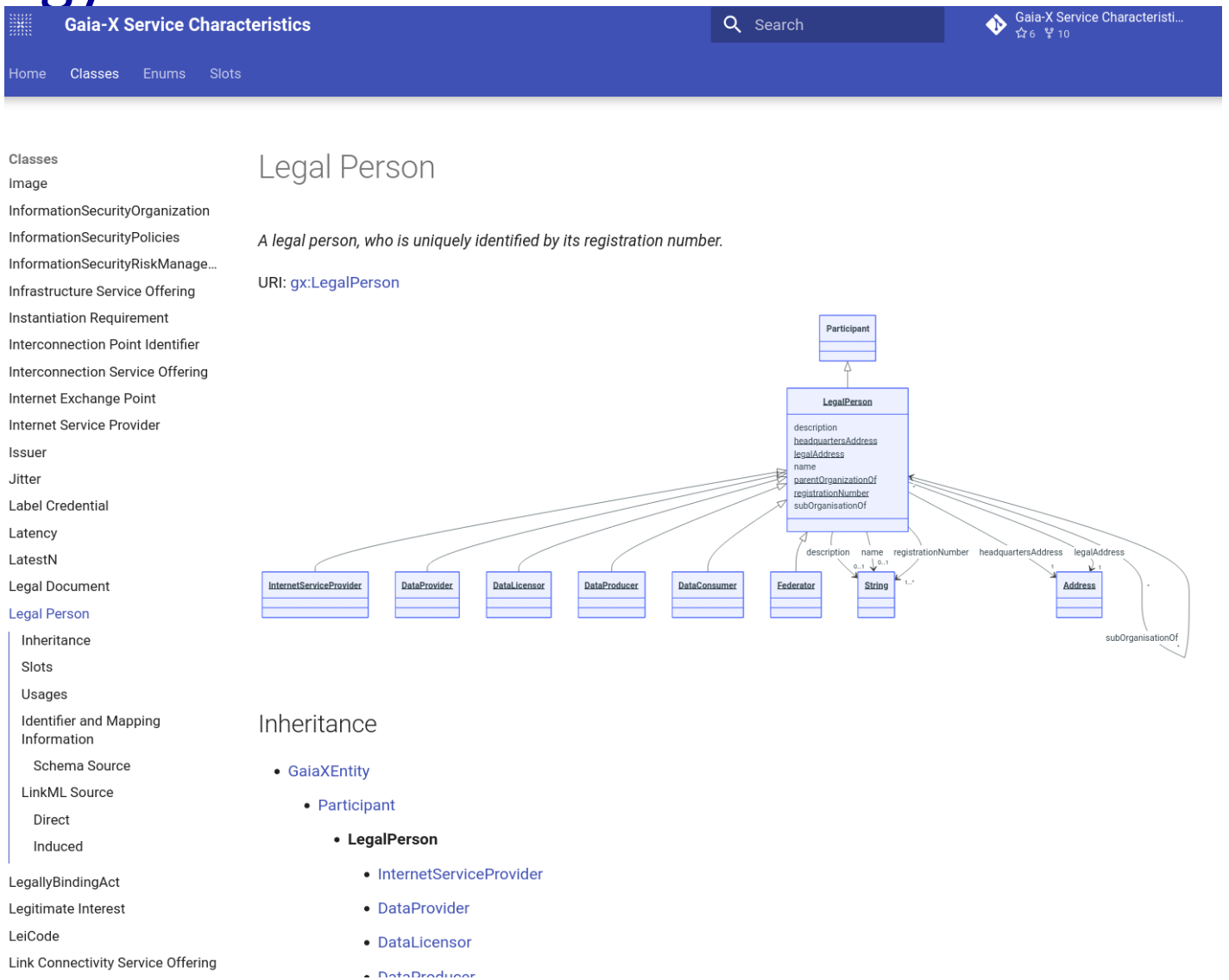
View in Compliance Document

Checks that the `ServiceOffering` has at least one `LegallyBindingAct` in its `legalDocuments` that is governed by an EAA country [illegible]ced in its `governingLawCountries`.

Implemented by ServiceOfferingLegallyBindingActsHaveGoverningLawCountry

```
verifyLegalDocuments(vpUUID: string, contextVersion: string, results: ServiceOfferingLegalDocuments[]): FilterValidationResult {
  this.logger.debug(`Checking that service offerings have legally binding acts that can be governed by EEA for VPUUID ${vpUUID}...`)

  const errorMessages: string[] = []
  let isP115Valid = true
  let isP112Valid = true
  for (const result of results) {
    const legallyBindingActs: LegalDocument[] = result.legalDocuments.filter(
      legalDocument => legalDocument.type === `w3id.org/gaia-x/${contextVersion}#LegallyBindingAct`
    )

    for (const legallyBindingAct of legallyBindingActs) {
      if (!legallyBindingAct.governingLawCountries.length) {
        this.logger.error(
          `P1.1.5 - Service offering ${result.serviceOfferingId} does not have a governing law country for legally binding act ${legallyBi
        )
        errorMessages.push(
          `P1.1.5 - Service offering ${result.serviceOfferingId} does not have a governing law country for legally binding act ${legallyBi
        )
        isP115Valid = false
      } else if (!legallyBindingAct.governingLawCountries.some(governingLawCountry => EEA_COUNTRY_NAME_ALPHA2.includes(governingLawCountry
        this.logger.error(
          `P1.1.2 - Service offering ${result.serviceOfferingId} with legally binding act ${legallyBindingAct.url} must have at least one
        )
        errorMessages.push(
```

Gaia-X Ontology



Identity & Credentials Access Management (ICAM)

- Switch to Verifiable Credentials Data Model 2.0
- Switch to enveloped proof (JOSE) and VC-JWT
- Enable OpenID4VCi/OpenID4VP proof of concept for credentials exchange

Technical changes

- VCDM 2.0
- VC-JWT
- Ontology

Verifiable Credentials Data Model 2.0

- Loire uses the latest VC Data Model

- Main changes:
  - IANA media types are now defined application/vc & application/vp
  - Credentials can be validFrom and validUntil to limit their validity in time
  - Better explanation for VC status and default type to BitstringStatusListEntry allowing validation like OCSP for certificates
  - Added name and description fields !!

Signature mechanism

- Tagus was using embedded proofs
  - Process was tedious and prone to errors to check validity (canonization URDNA 2015 -> SHA-256 hash (body & proof fields) -> concatenate -> sign with b64 encode false -> append the signature to the proof
  - Two serializations were co-living due to a mistake in the original implementation by the lab

Signature mechanism

- Loire uses enveloped proof aka JSON Web Token
  - Broadly used for authentication
  - Vast support in all languages
  - No more cumbersome serialization to try to match the signature
  - Information about holder are in the headers. Can perform eviction before even checking the credential signature
  - Presentations are signed by the holder too !

Sign

- Loi
  -
  -
  -
  -

Encoded PASTE A TOKEN HERE

```
eyJraWQiOiJkaWQ6d2ViOmV4YW1wbGUuY29tI0p
XSy0yMDIwIiwgImlzcyI6ImRpZDp3ZWI6ZXhhbX
BsZS5jb20iLCJhbGciOiJFUzI1NiJ9
.eyJAY29udGV4dCI6WyJodHRwczovL3d3dy53My
5vcmcvbnMvY3JlZGVudGlhbHMvdjIiLCJodHRwc
zovL3d3dy53My5vcmcvbnMvY3JlZGVudGlhbHMv
ZXhhbXBsZXMvdjIiXSwiaWQiOiJodHRwOi8vdW5
pdmVyc2l0eS5leGFtcGxlL2NyZWRlbnRpYWxzLz
E4NzIiLCJ0eXBlIjpbIlZlcmlmaWFibGVDcmVkZ
W50aWFsIiwiRXhhbXBsZUFsdW1uaUNyZWRlbnRp
YWwiXSwiaXNzdWVyIjoiaHR0cHM6Ly91bml2ZXJ
zaXR5LmV4YW1wbGUvaXNzdWVycy81NjUwNDkiLC
J2YWxpZEZyb20iOiIyMDEwLTAxLTAxVDE5OjIzO
jI0WiIsImNyZWRlbnRpYWxTY2hlbWEiOnsiaWQi
OiJodHRwczovL2V4YW1wbGUub3JnL2V4YW1wbGV
zL2RlZ3JlZS5qc29uIiwidHlwZSI6Ikpzb25TY2
hlbWEifSwiY3JlZGVudGlhbFN1YmplY3QiOnsia
WQiOiJkaWQ6ZXhhbXBsZToxMjMiLCJkZWdyZWUi
OnsidHlwZSI6IkJhY2hlbG9yRGVncmVlIiwibmF
tZSI6IkJhY2hlbG9yIG9mIFNjaWVuY2UgYW5kIE
FydHMifX19
.vLtI6zKqEquVX-2RPhGyvHzQ9xdKOdFGRoFaEn
G-UhQMGG7OGPi0WAoKPrj8OiT-
LDcLMAUNKPncwPc8B-lqKg
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "kid": "did:web:example.com#JWK-2020",
  "iss": "did:web:example.com",
  "alg": "ES256"
}
```

PAYLOAD: DATA

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "id": "http://university.example/credentials/1872",
  "type": [
    "VerifiableCredential",
    "ExampleAlumniCredential"
  ],
  "issuer": "https://university.example/
issuers/565049",
  "validFrom": "2010-01-01T19:23:24Z",
  "credentialSchema": {
    "id": "https://example.org/examples/degree.json",
    "type": "JsonSchema"
  },
  "credentialSubject": {
    "id": "did:example:123",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  }
}
```

a-x

even

#Gai

Sign

- Loi
  -
  -
  -
  -

even

Encoded PASTE A TOKEN HERE


```
eyJraWQiOiJkaWQ6d2ViOmV4YW1wbGUuY29tI0p
XSy0yMDIwIiwgImlzcyI6ImRpZDp3ZWI6ZXhhbX
BsZS5jb20iLCJhbGciOiJFUzI1NiJ9
.eyJAY29udGV4dCI6WyJodHRwczovL3d3dy53My
5vcmcvbnMvY3JlZGVudGlhbHMvdjIiLCJodHRwc
zovL3d3dy53My5vcmcvbnMvY3JlZGVudGlhbHMv
ZXhhbXBsZXMvdjIiXSwidHlwZSI6IlZlcmlmaWF
ibGVQcmVzZW50YXRpb24iLCJ2ZXJpZmlhYmxlQ3
JlZGVudGlhbCI6W3siQGNvbnRleHQiOiJodHRwc
zovL3d3dy53My5vcmcvbnMvY3JlZGVudGlhbHMv
djIiLCJpZCI6ImRhdGE6YXBwbGljYXRpb24vdmM
rand0LGV5SnJhV1FpT2lKRmVFaHJRazFYT1dadF
ltdDJWakkyTm0xU2NIVlFNbk5WV1Y5T1gwVlhTV
TR4YkdGd1ZYcFBPSEp2SWl3aVlXeG5Jam9pUlZN
ek9EUWlmUS5leUpBWTI5dWRHVjRkQ0k2V3lKb2R
IUndjem92TDNkM2R5NTNNeTV2Y21jdmJuTXZZM0
psWkdWdWRHbGhiSE12ZGpJaUxDSm9kSFJ3Y3pvd
kwzZDNkeTUzTXk1dmNtY3Zibk12WTNKbFpHVnVk
R2xoYkhNdlpYaGhiWEJzWlhNdmRqSWlYU3dpYVd
RaU9pSm9kSFJ3T2k4dmRXNXBkbVZ5YzJsMGVTNW
xlR0Z0Y0d4bEwyTnlaV1JsYm5ScFlXeHpMekU0T
npJaUxDSjBlWEJsSWpwYklsWmxjbWxtYVdGaWJH
VkRjbVZrWlc1MGFXRnNJaXdpUlhoaGJYQnNaVUZ
zZFcxdWFVTnlaV1JsYm5ScFlXd2lYU3dpYVhOem
```


Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE


```
{
  "kid": "did:web:example.com#JWK-2020",
  "iss": "did:web:example.com",
  "alg": "ES256"
}
```


PAYLOAD: DATA


```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://www.w3.org/ns/credentials/examples/v2"
  ],
  "type": "VerifiablePresentation",
  "verifiableCredential": [
    {
      "@context": "https://www.w3.org/ns/credentials/
v2",
      "id": "data:application/
vc+jwt,eyJraWQiOiJFeEhrQk1XOWZtYmt2VjI2Nm1ScHVQMnNVWV9O
X0VXSU4xbGFwVXpPOHJvIiwiYWxnIjoiRVMzODQifQ.eyJAY29udGV4
dCI6WyJodHRwczovL3d3dy53My5vcmcvbnMvY3JlZGVudGlhbHMvdjI
iLCJodHRwczovL3d3dy53My5vcmcvbnMvY3JlZGVudGlhbHMvZXhhbX
BsZXMvdjIiXSwiaWQiOiJodHRwOi8vdW5pdmVyc2l0eS5leGFtcGxlL
2NyZWRlbnRpYWxzLzE4NzIiLCJ0eXBlIjpbIlZlcmlmaWFibGVDcmVk
ZW50aWFsIiwiRXhhbXBsZUFsdW1uaUNyZWRlbnRpYWwiXSwiaXNzdWV
yIjoiaHR0cHM6Ly91bml2ZXJzaXR5LmV4YW1wbGUvaXNzdWVycy81Nj
UwNDkiLCJ2YWxpZEZyb20iOiIyMDEwLTAxLTAxVDE5OjIzOjI0WiIsI
mNyZWRlbnRpYWxTY2hlbWEiOnsiaWQiOiJodHRwczovL2V4YW1wbGUu
b3JnL2V4YW1wbGVzL2RlZ3JlZS5qc29uIiwidHlwZSI6Ikpzb25TY2h
lbWEifSwiY3JlZGVudGlhbFN1YmplY3QiOnsiaWQiOiJkaWQ6ZXhhbX
BsZToxMjMiLCJkZWdyZWUiOnsidHlwZSI6IkJhY2hlbG9yRGVncmVlI
iwibmFtZSI6IkJhY2hlbG9yIG9mIFNjaWVuY2UgYW5kIEFydHMifX19
.d2k4O3FytQJf83kLh-
```


#Gai

IPFS as backend storage

- The Gaia-X registry is a SPOF
  - We want to provide trusted anchors, shapes, schemas on a more distributed network
  - => IPFS
- The AISBL is still the trust anchor for the files, and publishes them
- Relies on a “TRAIN”-like anchoring of the IPFS CIDs

IPFS as backend storage

IPFS as back

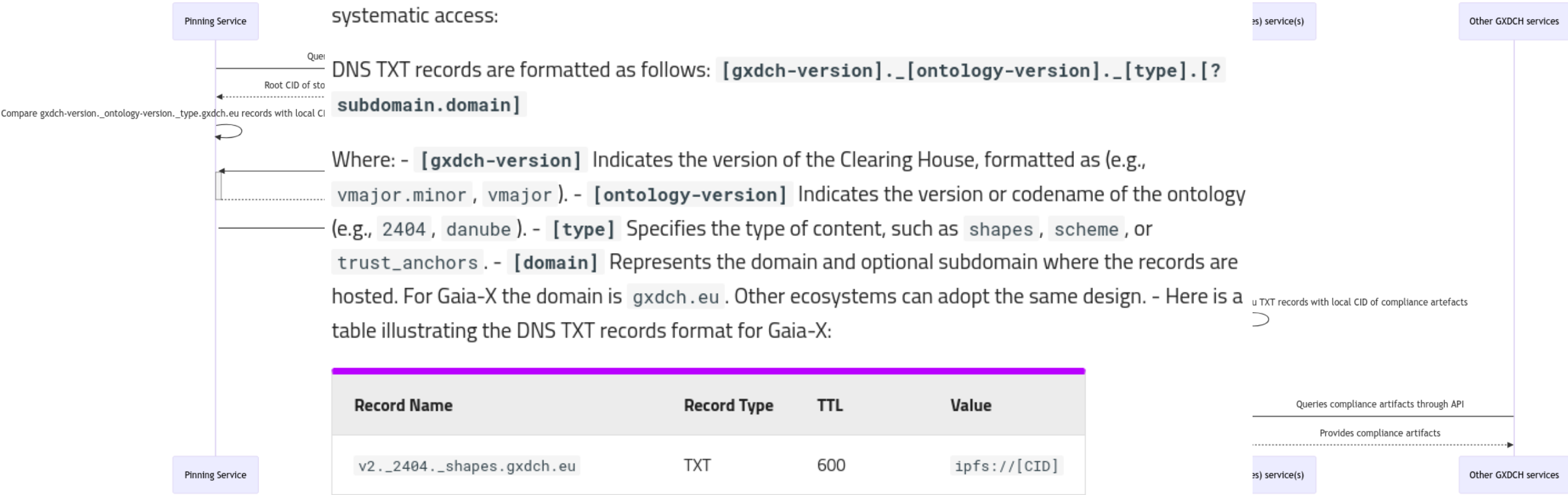
6.1.1 DNS TXT Records and Naming Convention

To facilitate the discovery and accessibility of the stored data, the Gaia-X Registry utilizes DNS TXT records. These records are used to advertise the current URIs (in the case of the Gaia-X ecosystem, they are ipfs:// links which include CIDs) associated with the latest versions of the stored documents. The structure of these DNS TXT records follows a specific naming convention to ensure easy and systematic access:

DNS TXT records are formatted as follows: `[gxdch-version]._[ontology-version]._[type].[?subdomain.domain]`

Where: - `[gxdch-version]` Indicates the version of the Clearing House, formatted as (e.g., `vmajor.minor`, `vmajor`). - `[ontology-version]` Indicates the version or codename of the ontology (e.g., `2404`, `danube`). - `[type]` Specifies the type of content, such as `shapes`, `scheme`, or `trust_anchors`. - `[domain]` Represents the domain and optional subdomain where the records are hosted. For Gaia-X the domain is `gxdch.eu`. Other ecosystems can adopt the same design. - Here is a table illustrating the DNS TXT records format for Gaia-X:

Record Name	Record Type	TTL	Value
`v2._2404._shapes.gxdch.eu`	TXT	600	`ipfs://[CID]`
`v2._2404._scheme.gxdch.eu`	TXT	600	`ipfs://[CID]`
`v2._2404._trust_anchors.gxdch.eu`	TXT	600	`ipfs://[CID]`
`v2._2404.gxdch.eu`	TXT	600	`ipfs://[CID]`



#GaiaXSumm

Other changes

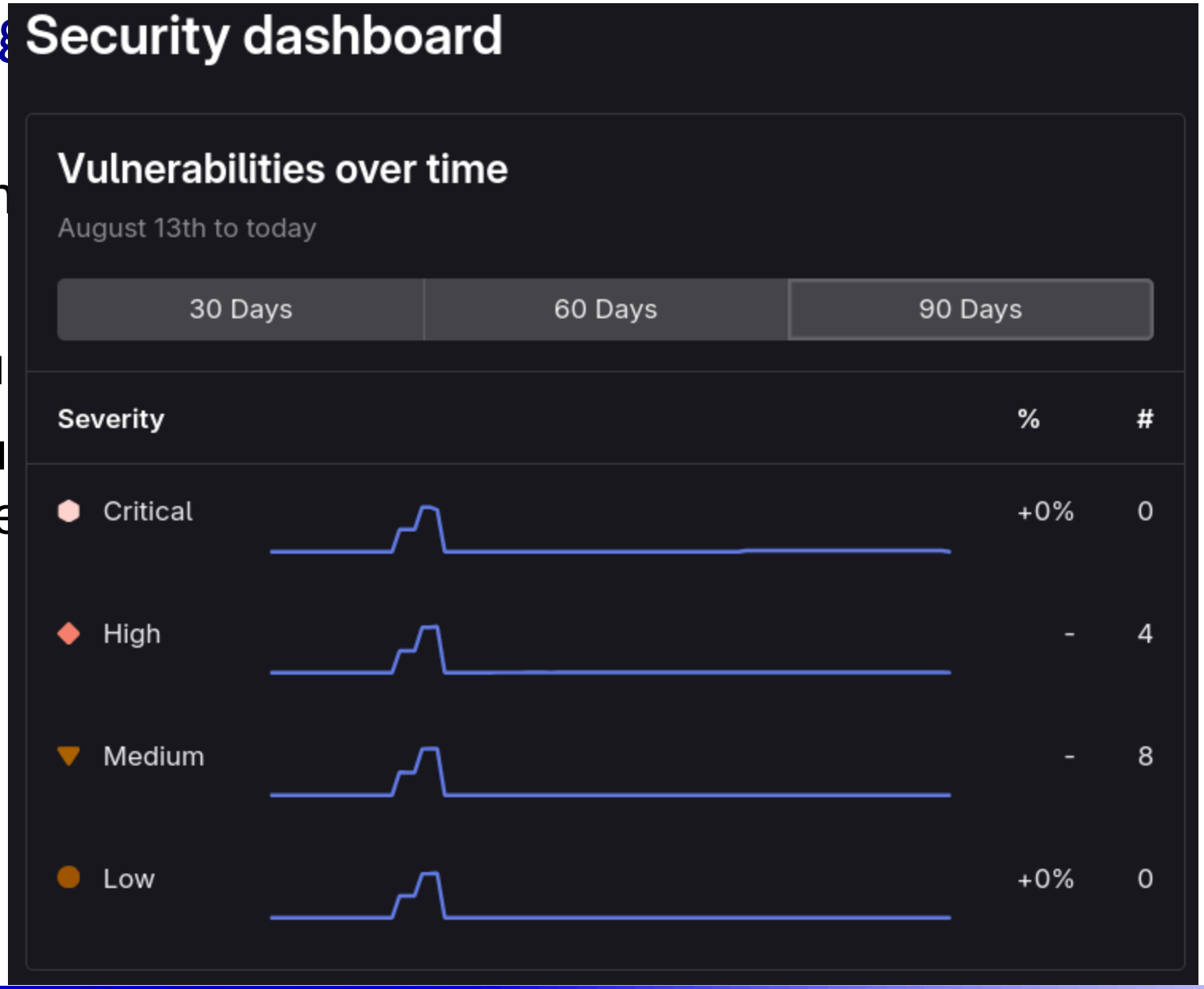
- All components bumped to NestJS latest version
- Support of Elliptic Curve keys (using Jose)
- Lot of security fixes integrated (and monitoring enabled)
- Prometheus support in the compliance engine (waiting for feedback to enable in registry/notary)

Other chang

- All compon
- Support of
- Lot of secu
- Prometheu

enable in re

feedback to



Gaia-X Academy

- Free courses
- More courses for members (log-in using the Members Platform)
- Course summarizing this presentation already online !

Open discussion

Thank you!

Christoph Strnadl - Pierre Gronlier - Ewann Gavard

Securely Sharing Credentials with OID4VC

Vincent Kelleher

Software Engineer

Gaia-X Lab Team

Nienke Broeksema @ Unsplash

SUMMARY

1. What is OID4VC ?
2. Roles & Interactions
3. Issuing Credentials
4. Presenting Credentials
5. Dynamic Credential Requests
6. What’s To Expect ?

WHAT IS OID4VC ?

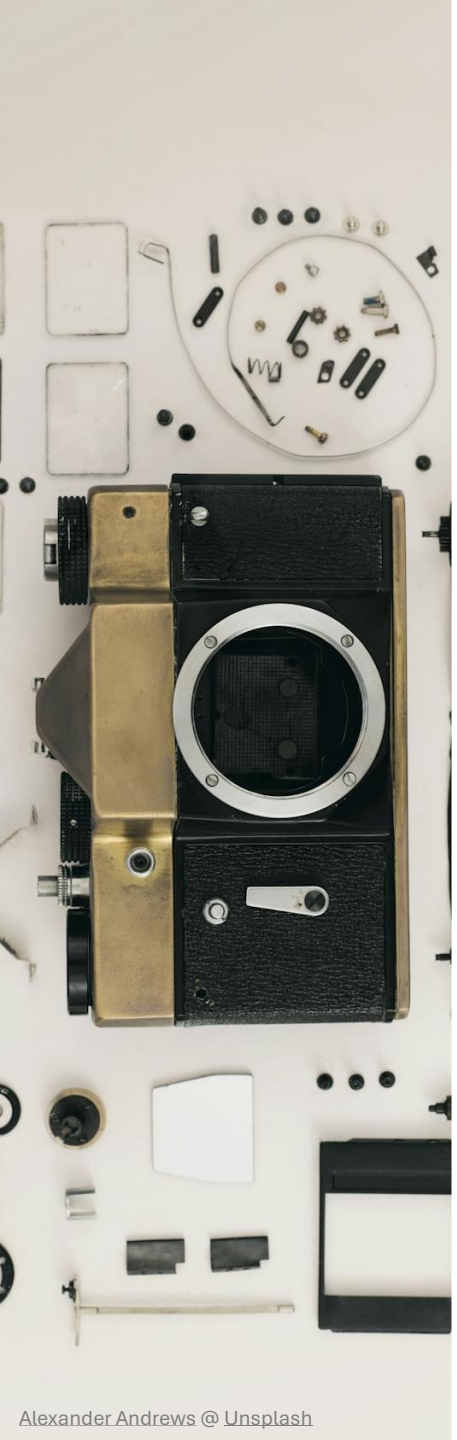
- OpenID for Verifiable Credentials is an umbrella specification
- Extension of OAuth 2.0 (authorization) & OpenID (authentication)
- Written by the OpenID Foundation
- Used to share credentials through a cryptographically secure transport

WHAT IS OID4VC ?

- OAuth 2.0 is an authorization protocol with multiple extensions
- OpenID Connect is an authentication protocol built on top of OAuth 2.0
- OID4VC, like OAuth 2.0, can have defined Profiles

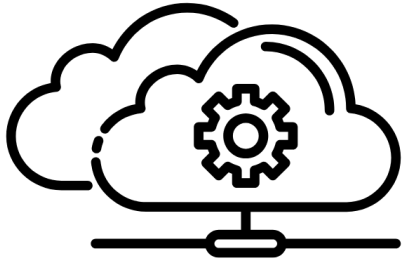
WHAT IS OID4VC ?

- OpenID for Verifiable Credentials has two main specifications
  - OpenID for Verifiable Credential Issuance
  - OpenID for Verifiable Presentations
- Both specifications support machine-to-human and machine-to-machine interactions

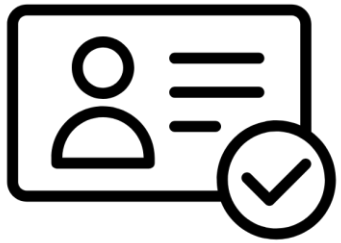


Alexander Andrews @ Unsplash

ROLES & INTERACTIONS

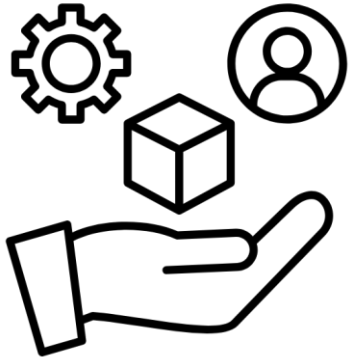


Client

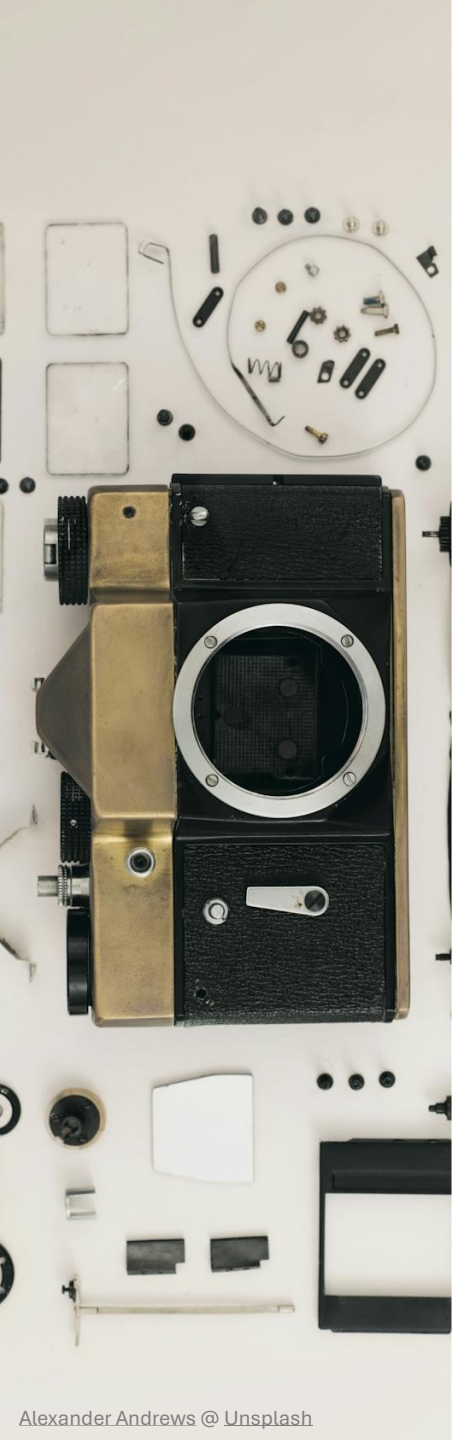


Authorization Server

Resource Owner

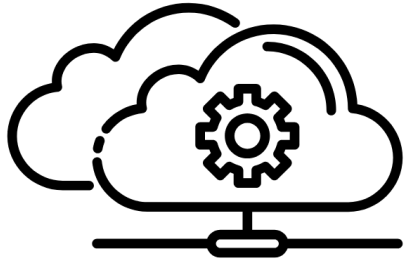


Resource Server



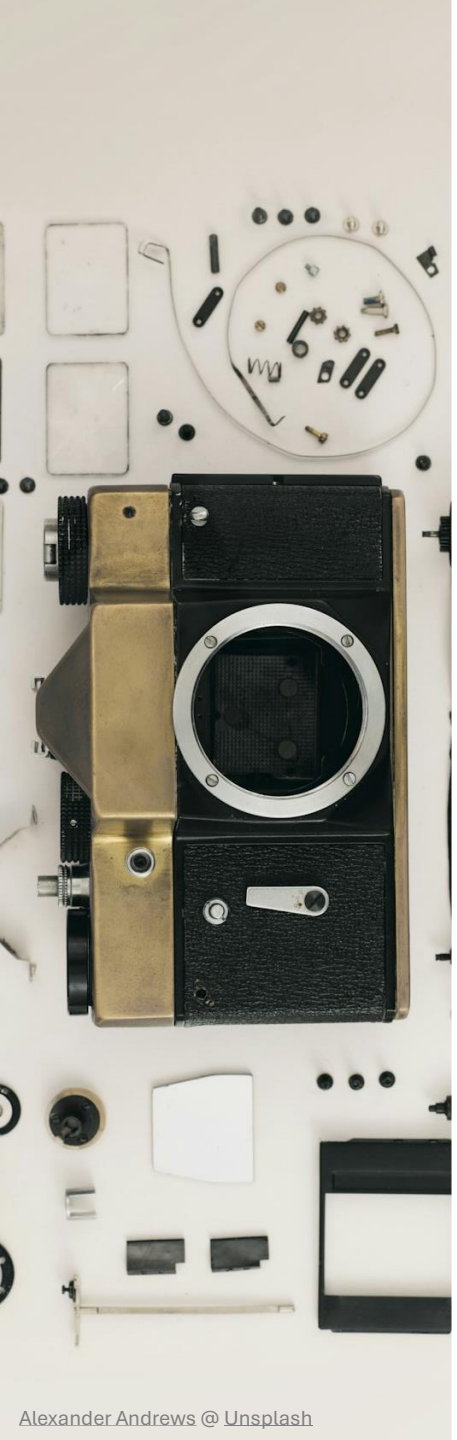
Alexander Andrews @ Unsplash

ROLES & INTERACTIONS



Client

- Initiates the authorization flow
- Party requesting the resource
- Interacts with all other roles
- Can be an application, a server or any other device/service

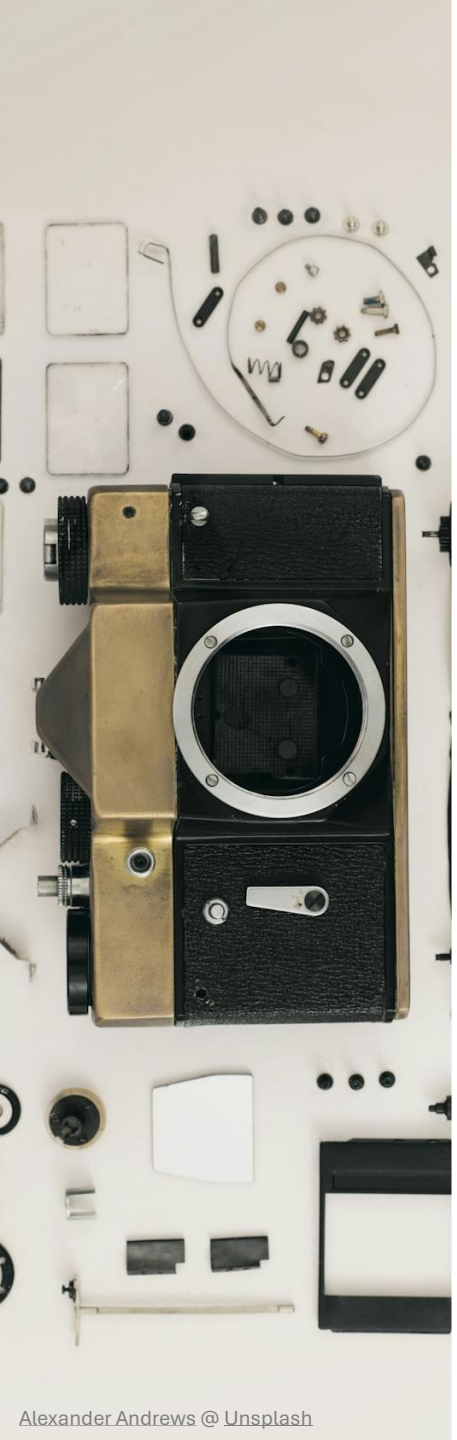


Alexander Andrews @ Unsplash

ROLES & INTERACTIONS

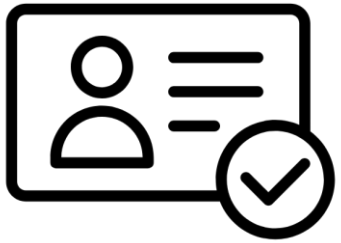
Resource Owner

- Owner of the protected resource the client wants access to
- Capable of granting access to the protected resource
- Can be a natural person (end-user), a legal person, a server, etc.



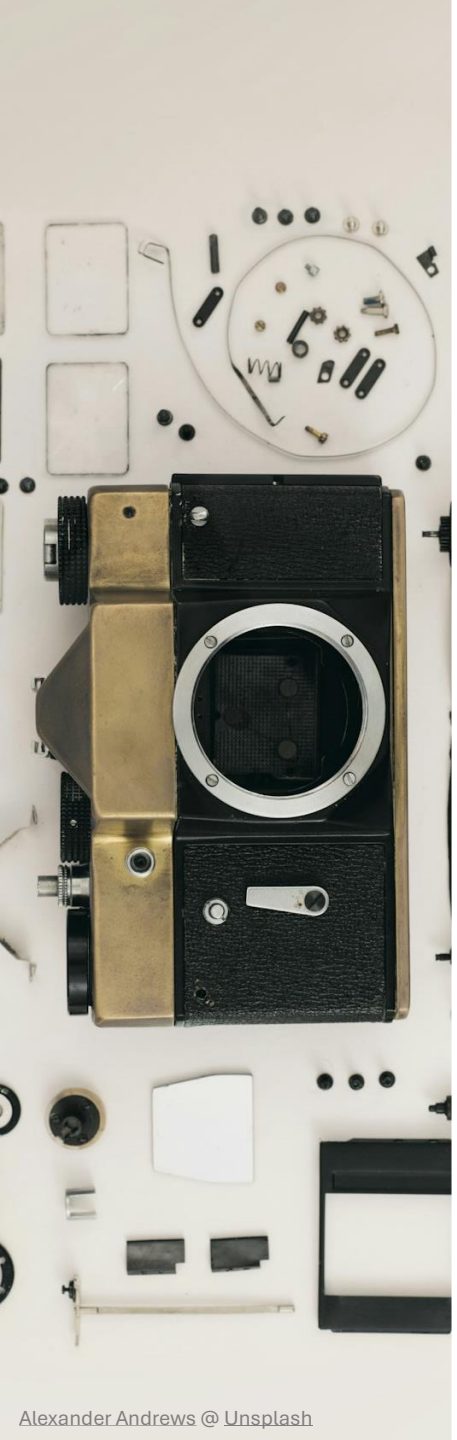
Alexander Andrews @ Unsplash

ROLES & INTERACTIONS



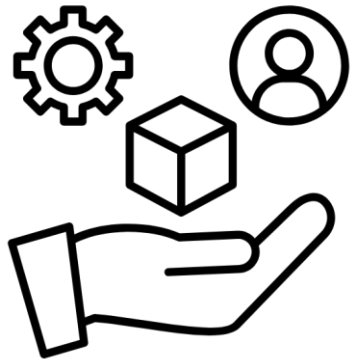
Authorization Server

- Grants the client access to the resource server
- Authenticates the resource owner
- Issues access tokens to the client



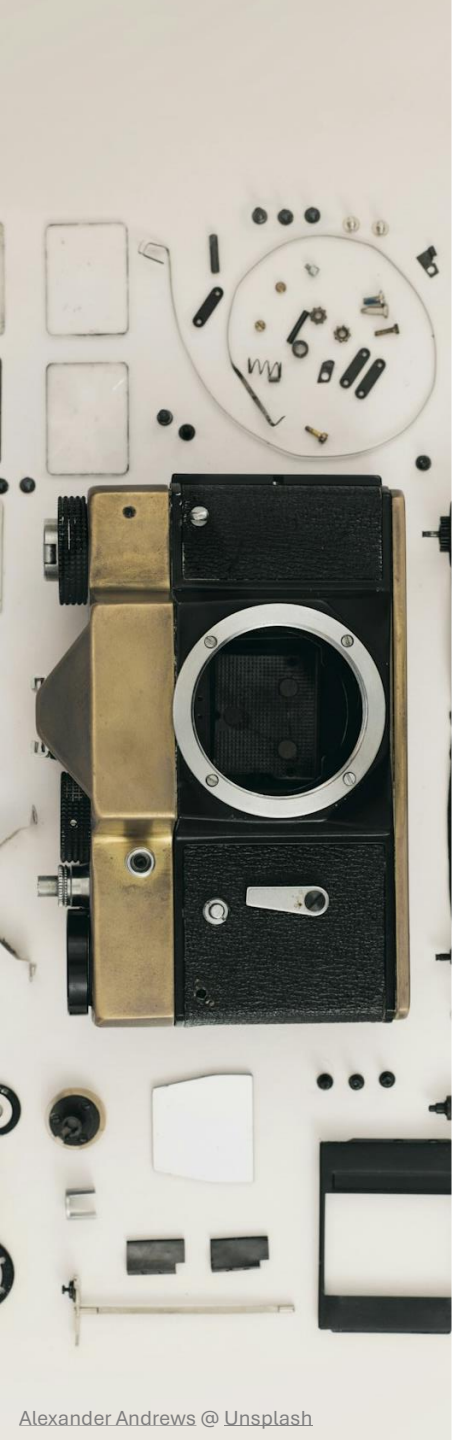
Alexander Andrews @ Unsplash

ROLES & INTERACTIONS



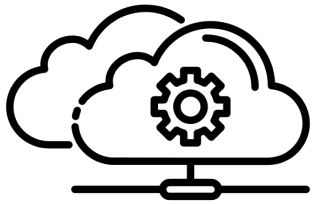
Resource Server

- Service hosting the resource owner’s protected resource
- Capable of delivering the protected resource
- Requires an access token to allow resource requests



Alexander Andrews @ Unsplash

ROLES & INTERACTIONS



Client

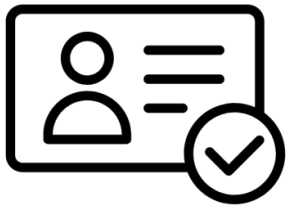
Authorization Request

Authorization Grant

Resource Owner

Authorization Grant

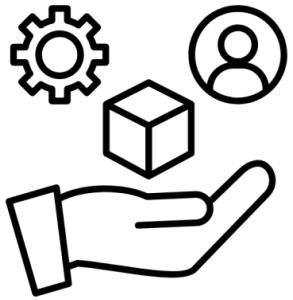
Access Token



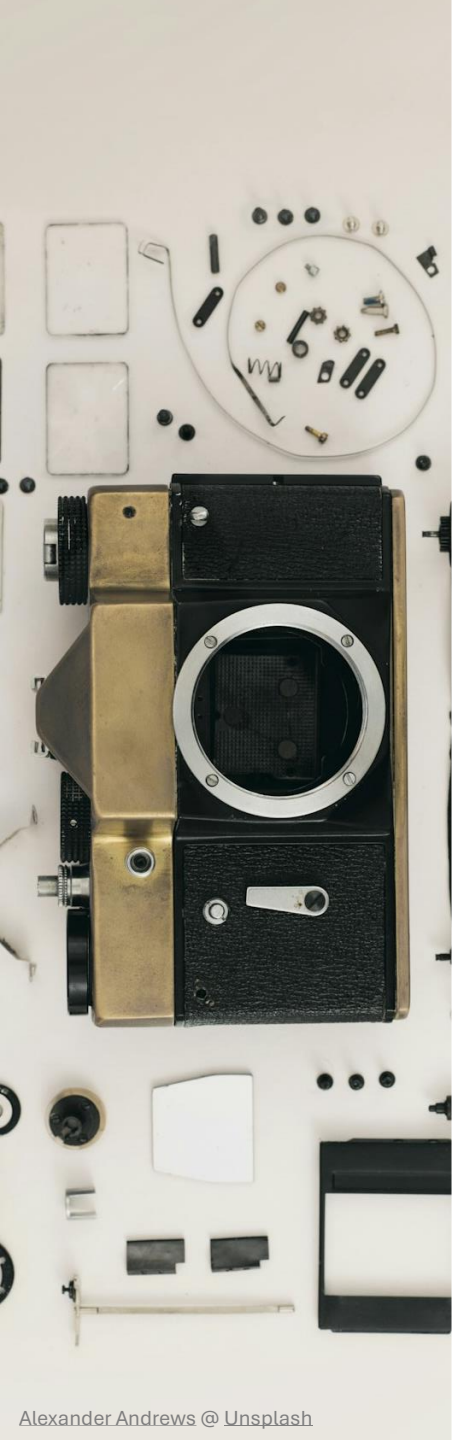
Authorization Server

Access Token

Protected Resource

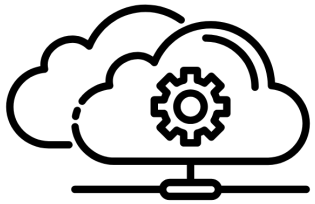


Resource Server



Alexander Andrews @ Unsplash

ROLES & INTERACTIONS



My App

Authorization Request

Authorization Grant

John Doe

Authorization Grant

Access Token

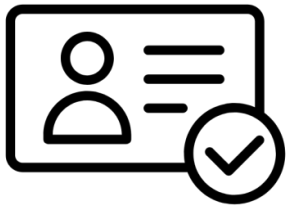


Photo Gallery Auth

Access Token

Holiday Album

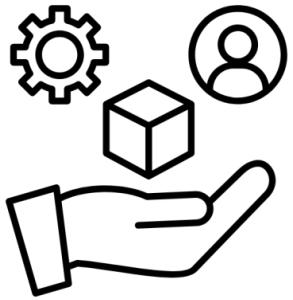
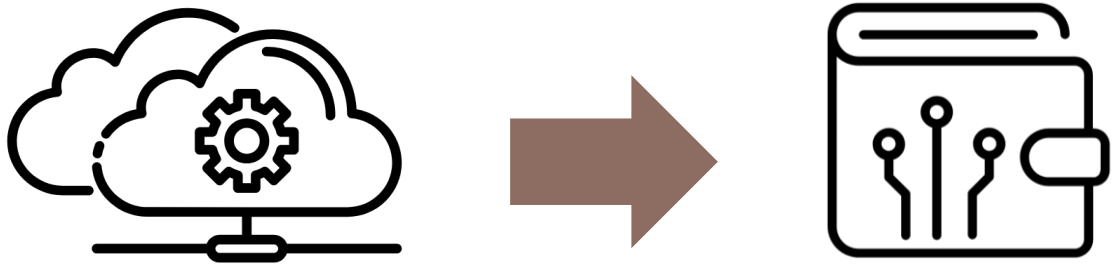


Photo Gallery

ISSUING CREDENTIALS

- Credential issuance is done with OpenID for Verifiable Credential Issuance (OID4VCI)
- Cryptographically binds a verifiable credential to a holder
- Imagine did:web as the username and private key as the password
- Two flows exist :
  - Authorization code flow
  - Pre-authorized code flow
- For example, OID4VCI is perfectly suited for the Gaia-X Notary's legal person credential issuance process

ISSUING CREDENTIALS

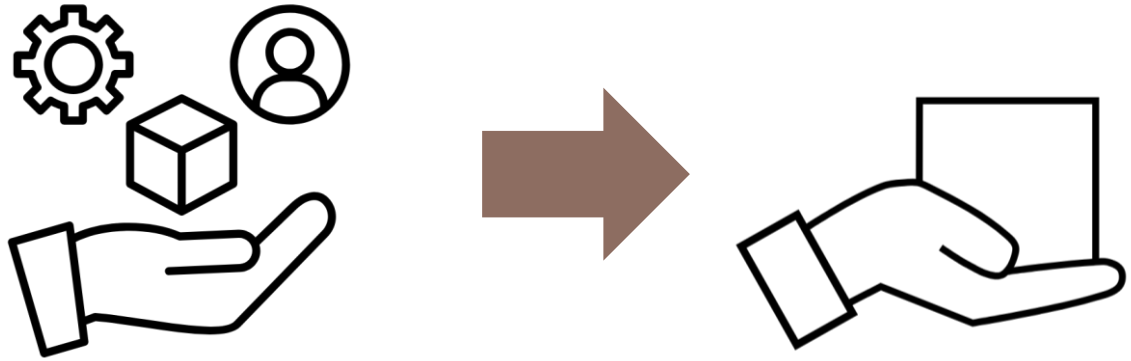


Client

Wallet

- Wallets interact with issuers to collect credentials
- Credentials are stored but not modified
  - Issuer remains the same
  - Credentials are later presented as they were received

ISSUING CREDENTIALS



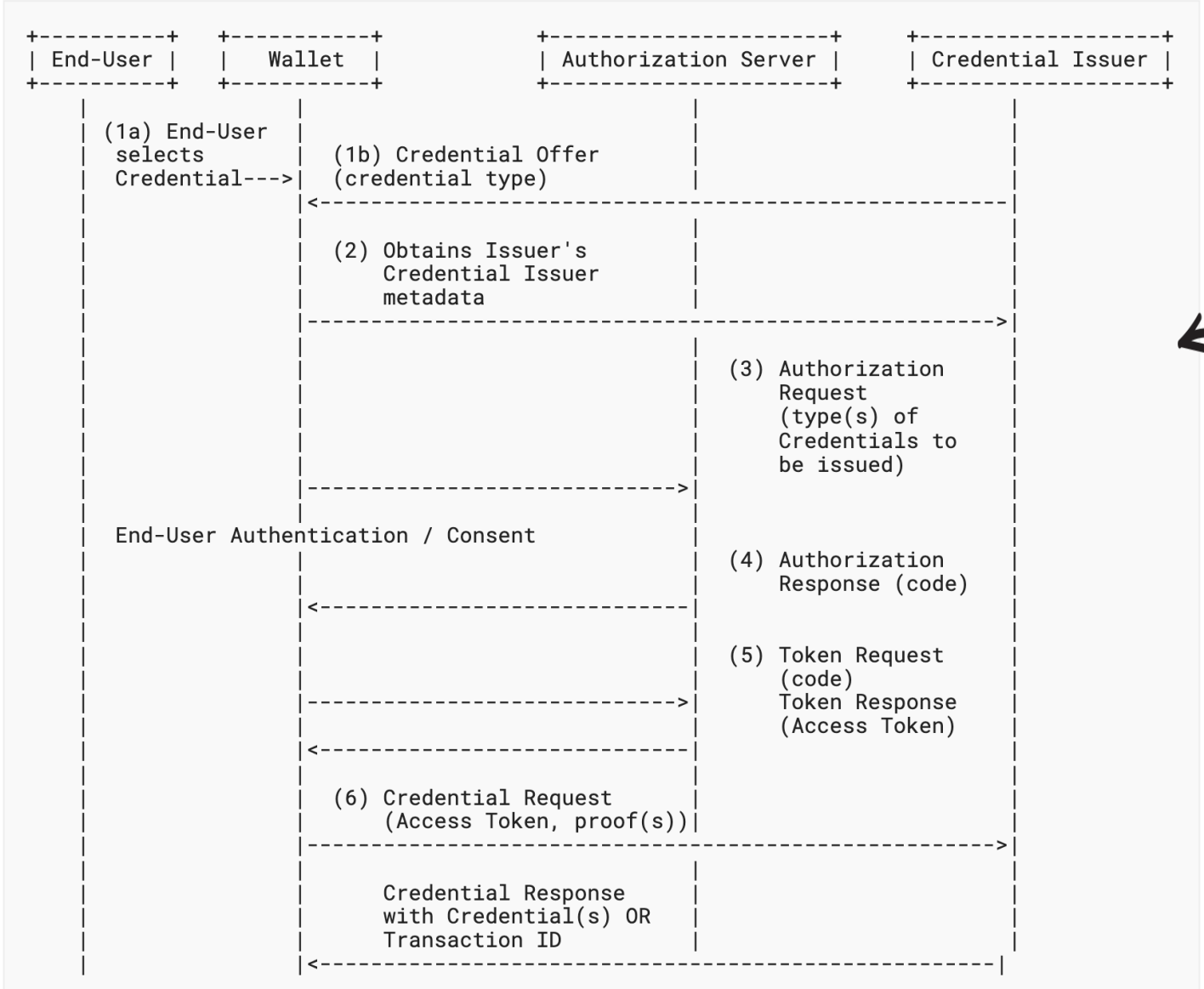
Resource Server

Issuer

- Issuers produce verifiable credentials
- Credentials are signed by the issuer’s private key
- Issuers are resource servers but can also be authorization servers

CardMapr.nl @ Unsplash

ISSUING CREDENTIALS



Authorization code flow

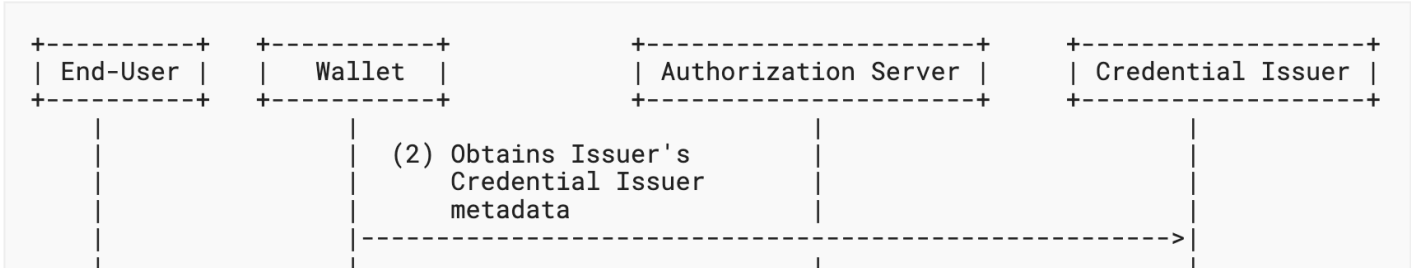
CardMapr.nl @ Unsplash

ISSUING CREDENTIALS


```
{
  "credential_issuer": "https://issuer.gaia-x.eu",
  "credential_configuration_ids": [
    "GaiaXVatID",
    "GaiaXComplianceCredential"
  ],
  "grants": {
    "authorization_code": {}
  }
}
```

Credential offer

ISSUING CREDENTIALS




```
{
  "credential_issuer": "https://issuer.gaia-x.eu",
  "credential_endpoint": "https://issuer.gaia-x.eu/credential",
  "display": {
    "name": "Gaia-X AISBL",
    "logo": "https://gaia-x.eu/wp-content/uploads/2022/05/Gaia-X_Logo_svg_resized_h.svg"
  },
  "credential_configuration_ids": [
    "GaiaXVatID",
    "GaiaXComplianceCredential"
  ]
  // ...
}
```

Issuer metadata

ISSUING CREDENTIALS

CardMapr.nl @ Unsplash

```
+----------+   +-----------+            +----------------------+     +--------------------+
| End-User |   |   Wallet  |            | Authorization Server |     | Credential Issuer |
+----------+   +-----------+            +----------------------+     +--------------------+
     |               |                                |                          |
     |               |                                |  (3) Authorization       |
     |               |                                |      Request             |
     |               |                                |      (type(s) of         |
     |               |                                |      Credentials to      |
     |               |                                |      be issued)          |
     |               |------------------------------->|                          |
```

Authorization request

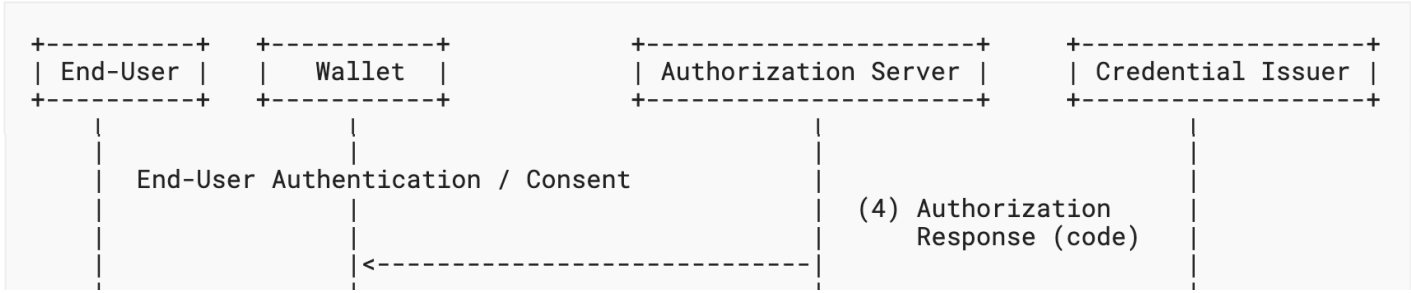
```
{
  "client_id": "did:web:wallet.gaia-x.eu",
  "request":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwi
aWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c"
}
```

kid: did:web:wallet.gaia-x.eu#OID4VC

```
{
  "client_id": "did:web:wallet.gaia-x.eu",
  "redirect_uri": "https://wallet.gaia-x.eu/authorization-redirect",
  "wallet_issuer": "https://wallet.gaia-x.eu",
  "response_type": "code",
  "authorization_details": {
    "type": "openid_credential",
    "credential_configuration_id": "GaiaXVatID"
  },
  "state": "V1StGXR8_Z5jdHi6B-myT"
}
```

CardMapr.nl @ Unsplash

ISSUING CREDENTIALS

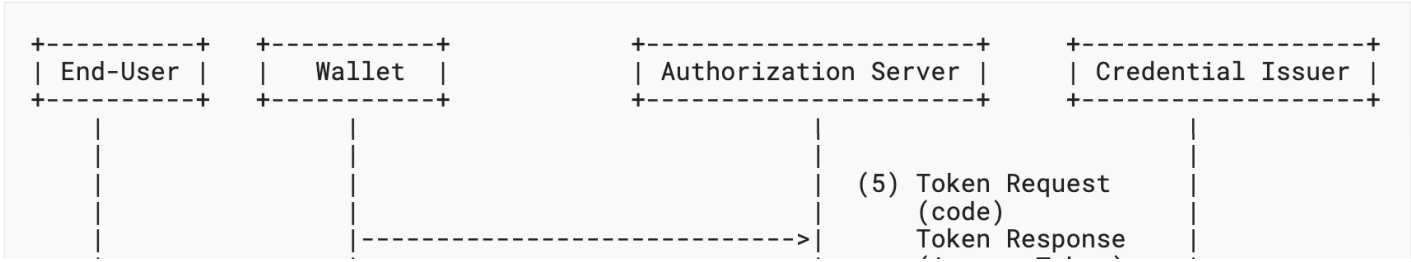



```
1 HTTP/1.1 302 Found
2 Location: https://wallet.gaia-x.eu/authorization-redirect
3     code=SplxlOBeZQQYbYS6WxSbIA
4     &state=V1StGXR8_Z5jdHi6B-myT
```

Authorization response

CardMapr.nl @ Unsplash

ISSUING CREDENTIALS




```
{
  "client_id": "did:web:wallet.gaia-x.eu",
  "grant_type": "authorization_code",
  "code": "SplxlOBeZQQYbYS6WxSbIA",
  "redirect_uri": "https://wallet.gaia-x.eu/authorization-redirect",
  "authorization_details": [
    {
      "type": "openid_credential",
      "credential_configuration_id": "GaiaXVatID"
    }
  ]
}
```

Token request

CardMapr.nl @ Unsplash

ISSUING CREDENTIALS


```
{
  "access_token":
"eyJhbGciOiJIUzIlNiIsInR5cCI6IkpXVCJ9.eyJzdWIi0iIxMjMONTY30DkwIiwiYWNjZXNzVG9rZW4i0iJCcmFh
YWFoIiwiaWFOIjoxNTE2MR15MDIyfQ.sV001Wd-OuRHwPjPeeF6gS6OITP7nL8ZA9y6DJWZY8",
  "token_type": "bearer",
  "expires_in": 600,
  "c_nonce": "tZignsnFbp",
  "c_nonce_expires_in": 600,
  "authorization_details": [
    {
      "type": "openid_credential",
      "credential_configuration_id": "GaiaXVatID",
      "credential_identifiers": ["GaiaXVatID"]
    }
  ]
}
```


Token response

ISSUING CREDENTIALS

```
+----------+   +-----------+           +----------------------+     +--------------------+
| End-User |   |   Wallet  |           | Authorization Server |     | Credential Issuer |
+----------+   +-----------+           +----------------------+     +--------------------+
     |               |                                 |                        |
     |               |  (6) Credential Request         |                        |
     |               |      (Access Token, proof(s))|                        |
     |               |-------------------------------------------------------->|
     |               |                                 |                        |
```

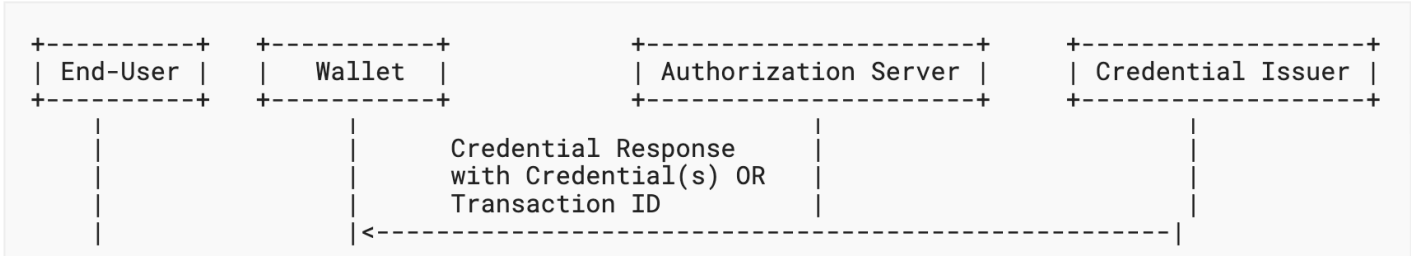
```
// HTTP Headers
// Authorization: Bearer
eyJhbGciOiJIUzIlNiIsInR5cCI6IkpXVCJ9.eyJzdWIi0iIxMjMONTY30DkwIiwiYWNjZXNzVG9rZW4i0iJCcmFh
YWFoIiwiaWFOIjoxNTE2MR15MDIyfQ.sV001Wd-OuRHwPjPeeF6gS6OITP7nL8ZA9y6DJWZY8

{
  "credential_identifier": "GaiaXVatID",
  "proof": {
    "proof_type": "jwt",
    "jwt":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJub25jZSI6InRaaWduc25GYnAifQ.QexzEqve_hgaM1w1nReOu
i5tPp88ebQIkoUgsTzMwHs"
  }
}
```

Credential request

```
{
  "nonce": "tZignsnFbp"
}
```

kid: did:web:wallet.gaia-x.eu#OID4VC

ISSUING CREDENTIALS

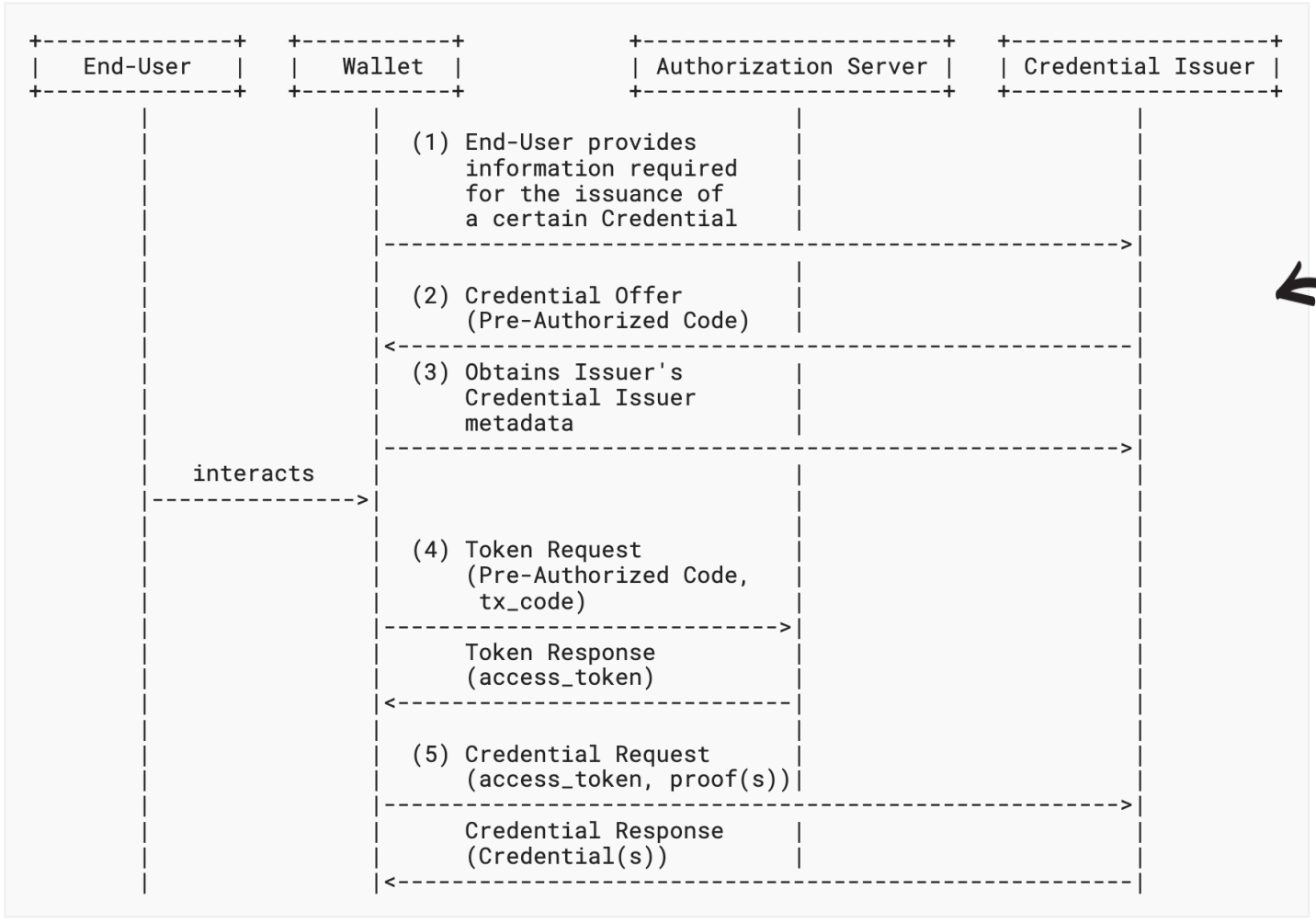



```
{
  "credentials": [
"eyJhbGciOiJFUzI1NiIsInR5cCI6InZjK2p3dCIsImN0eSI6InZjIiwia2lkIjoiZGlkOndlYjpsb2NhbGhvc3QlM
0EzMDAwOmlzc3VlciNPSUQ0VkMifQ.eyJAY29udGV4dCI6WyJodHRwczovL3d3dy53My5vcmcvbnMvY3JlZGVudGlh
bHMvdjIiLCJodHRwczovL3czaWQub3JnL2dhaWEteC9kZXZlbG9wbWVudCMiXSwidHlwZSI6WyJWZXJpZmlhYmxlQ3
JlZGVudGlhbCIsImd4OlZhdElEIl0sImlkIjoiaHR0cHM6Ly9leGFtcGxlLm9yZy92YXQtaWQiLCJuYW1lIjoiVkFU
IElEIiwiZGVzY3JpcHRpb24iOiJWYWx1ZSBBZGRlZCBUYXggSWRlbnRpZmllciIsImlzc3VlciI6ImRpZDp3ZWI6bG
9jYWxob3N0JTNBMzAwMDppc3N1ZXIiLCJ2YWxpZEZyb20iOiIyMDI0LTEwLTI5VDE0OjM0OjAyLjU1MSswMTowMCIs
InZhbGlkVW50aWwiOiIyMDI1LTAxLTI5VDE0OjM0OjAyLjU1MSswMTowMCIsImNyZWRlbnRpYWxTdWJqZWN0Ijp7Im
lkIjoiaHR0cHM6Ly9leGFtcGxlLm9yZy92YXQtaWQjY3MiLCJneDp2YXRJRCI6IkZSMTIzNDU2Nzg5IiwiZ3g6Y291
bnRyeUNvZGUiOiJGUiJ9LCJldmlkZW5jZSI6eyJneDpldmlkZW5jZU9mIjoiVkFUX0lEIiwiZ3g6ZXZpZGVuY2VVUk
wiOiJodHRwOi8vZWMuZXVyb3BhLmV1L3RheGF0aW9uX2N1c3RvbXMvdmllcy9zZXJ2aWNlcy9jaGVja1ZhdFNlcnZp
Y2UiLCJneDpleGVjdXRpb25EYXRlIjoiMjAyNC0xMC0yOVQxNDozNDowMi41NTErMDE6MDAifSwiaWF0IjoxNzMwMj
A4ODQyLCJpc3MiOiJodHRwczovL2xvY2FsaG9zdDozMDAwL2lzc3VlciIsImF1ZCI6ImRpZDp3ZWI6bG9jYWxob3N0
JTNBMzAwMDp3YWxsZXQiLCJleHAiOjE3NjE3NjY0NDJ9.S_7xabmGZBKYLzzQNruhbca66Le7feZwDiDGh8_8GIqn_
3CuTHE1VDo281EAPa1fHLDGYQM_3wiVRSx64PTFxw"
  ],
  "c_nonce": "fGFF7UkhLa",
  "c_nonce_expires_in": 86400
}
```


Credential response

CardMapr.nl @ Unsplash

ISSUING CREDENTIALS



Pre-authorized code flow

CardMapr.nl @ Unsplash

ISSUING CREDENTIALS


```
1 {
2   "credential_issuer": "https://issuer.gaia-x.eu",
3   "credential_configuration_ids": [
4     "GaiaXVatID",
5     "GaiaXComplianceCredential"
6   ],
7   "grants": {
8     "urn:ietf:params:oauth:grant-type:pre-authorized_code": {
9       "pre-authorized_code": "abcdef123456789",
10      "tx_code": {
11        "length": 4,
12        "input_mode": "numeric",
13        "description": "Please provide the one-time code that was sent via e-mail"
14      }
15    }
16  }
17 }
```

Credential offer

ISSUING CREDENTIALS

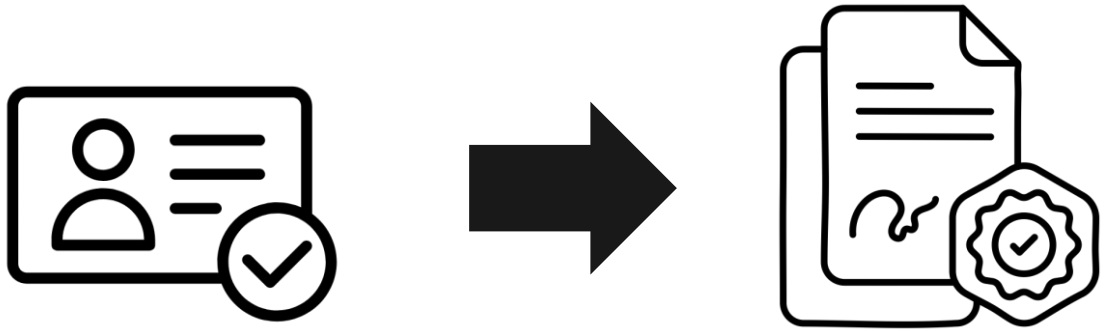
In a nutshell, OID4VCI proposes :

- A new credential offer endpoint
- A new `/.well-known/openid-credential-issuer` metadata endpoint
- A new credential endpoint
- Credential offers that can be sent through a QRCode for cross-device flows or via HTTP
- Support for VC-JWT, ISO mDL and IETF SD-JWT VC by default
- Support of multiple credential issuance and deferred issuance

PRESENTING CREDENTIALS

- Credential presentation is done through OpenID for Verifiable Presentations (OID4VP)
- Only the authorization request/response part of OAuth 2.0 is used
- Verifiable Credentials are presented as Verifiable Presentations
- Can be used with Self-Issued OpenID Providers v2 (SIOPv2)
- For example, OID4VP can be used to present Gaia-X credentials to a verifier

PRESENTING CREDENTIALS



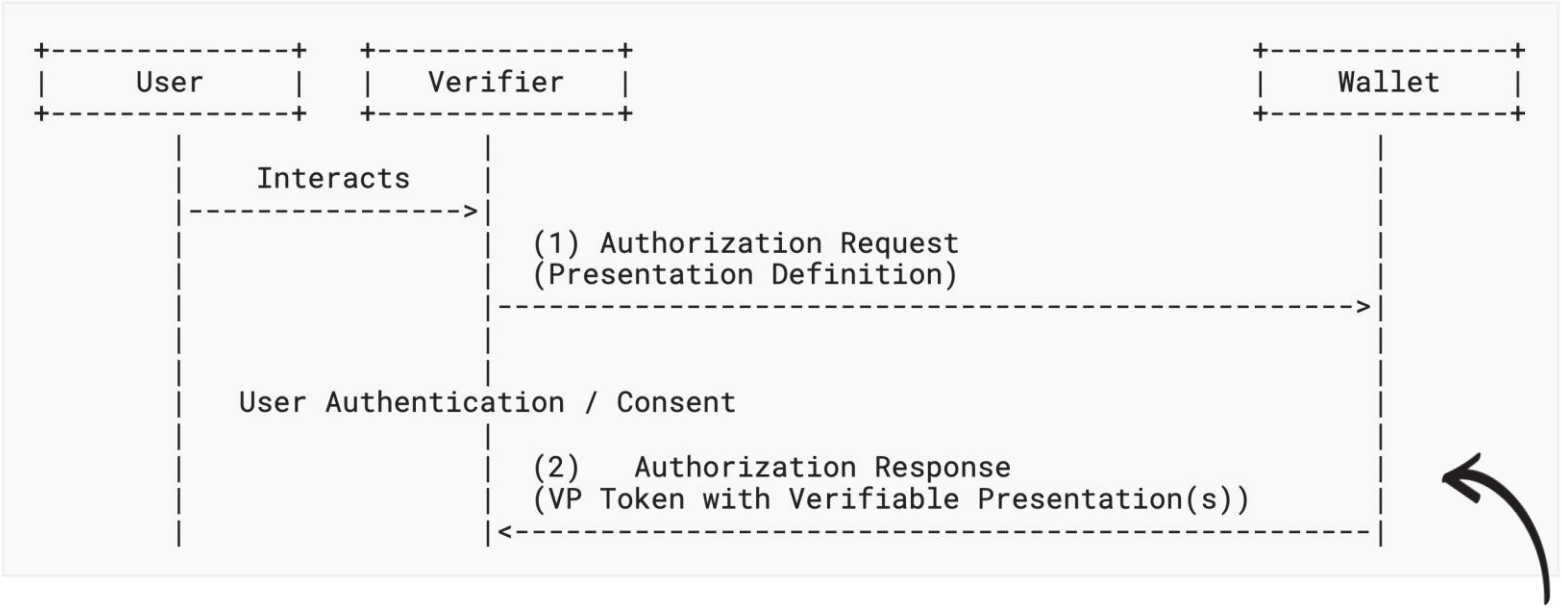
Authorization Server

Verifier

- Verifiers request credentials
- They are in charge of verifying that
  - Verifiable presentations containing credentials are valid
  - Verifiable credentials within the VPs are valid

Kelly Sikkema @ Unsplash

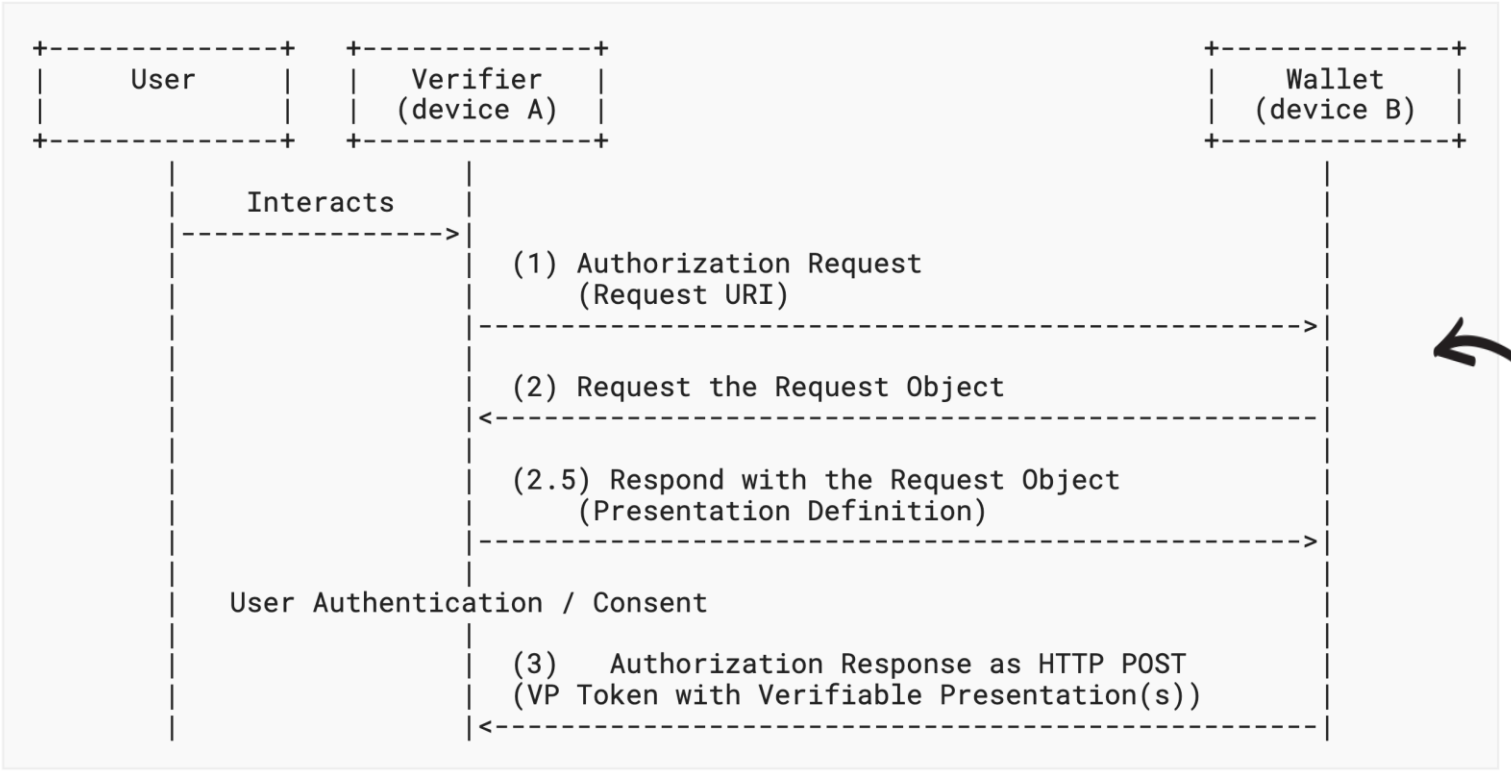
PRESENTING CREDENTIALS



Same device flow

Kelly Sikkema @ Unsplash

PRESENTING CREDENTIALS



Cross-device flow

PRESENTING CREDENTIALS

- OID4VP uses DIF's Presentation Exchange 2.0.0 which is transport and format agnostic
- Presentation definitions are used by the verifier to query credentials from the wallet
- Presentation submissions locate where the requested credentials are in the wallet's response

Kelly Sikkema @ Unsplash

PRESENTING CREDENTIALS

```
{
  "presentation_definition": {
    "id": "GaiaXVatIdPresentationDefinition",
    "input_descriptors": [
      {
        "id": "GaiaXVatId",
        "name": "Gaia-X Vat ID Registration Number",
        "purpose": "Identify a legal person",
        "constraints": {
          "fields": [
            {
              "path": [
                "$.type"
              ],
              "filter": {
                "type": "string",
                "pattern": "gx:VatID"
              }
            }
          ]
        }
      }
    ]
  }
}
```

Presentation definition

Kelly Sikkema @ Unsplash

PRESENTING CREDENTIALS

```
{
  "presentation_submission": {
    "id": "a30e3b91-fb77-4d22-95fa-871689c322e2",
    "definition_id": "GaiaXVatIdPresentationDefinition",
    "descriptor_map": [
      {
        "id": "GaiaXVatId",
        "format": "jwt_vc",
        "path": "$.verifiableCredential[0]"
      }
    ]
  }
}
```

Presentation submission

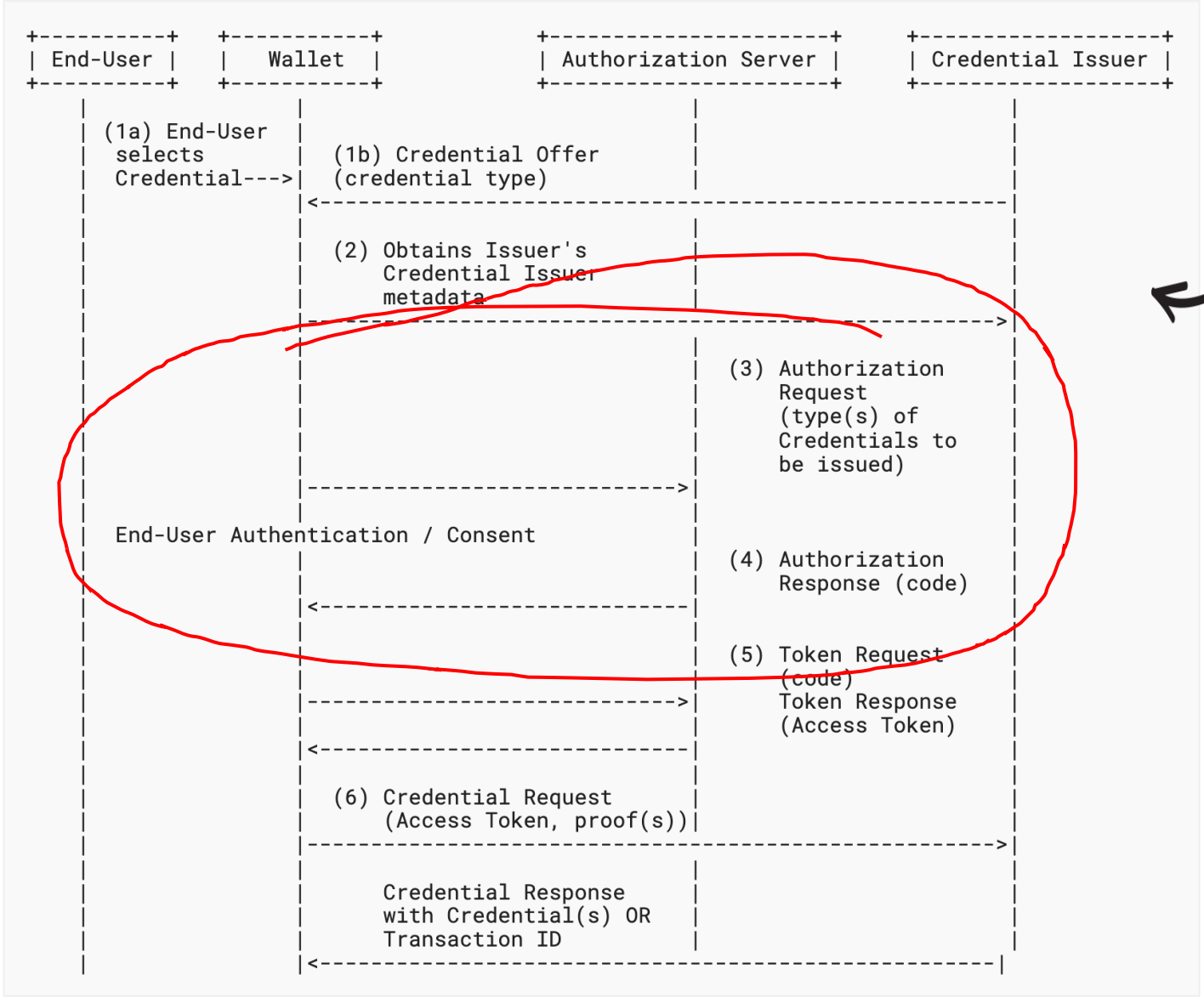
DYNAMIC CREDENTIAL REQUESTS

PiggyBank @ Unsplash

- Sometimes, credentials are required to issue another credential
- OID4VCI describes Dynamic Credential Requests
- Quick switch between OID4VCI and OID4VP
- Only works for Authorization Code Flows
- Still in discussion, not clearly specified
- For example, this can be used when requesting a Gaia-X compliance credential or for securing data transfers between participants

PiggyBank @ Unsplash

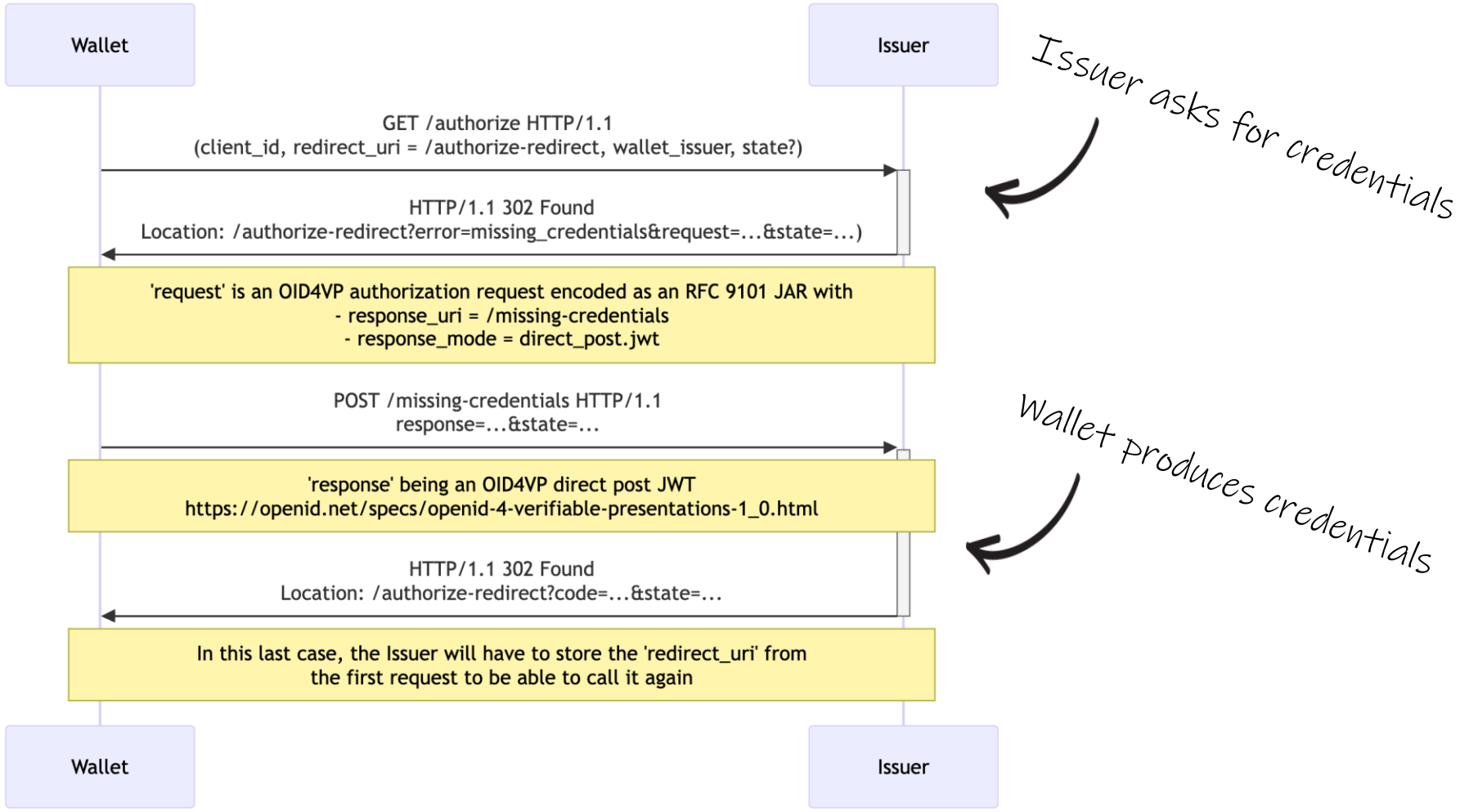
DYNAMIC CREDENTIAL REQUESTS



Authorization code flow

DYNAMIC CREDENTIAL REQUESTS

PiggyBank @ Unsplash



WHAT'S TO EXPECT ?

- At the moment, many natural person use cases are promoted (human-to-machine)
- But enterprise use cases exist too (machine-to-machine)

Drew Beamer @ Unsplash

WHAT'S TO EXPECT ?

- Wallets aren't only smartphone applications anymore
- Wallets are hosted by corporations as services to become Cloud Wallets
- Corporations give power of attorney to key employees through enterprise wallets
- Faster processes including credential issuance

Drew Beamer @ Unsplash

WHAT'S TO EXPECT ?

- Different ecosystems and actors define OID4VC Profiles
- Issuers, wallets and verifiers from different ecosystems use a universal secure protocol
- Decentralization is standard practice through DIDs
- New features and improved security through OAuth 2.0 extensions
- Any OAuth 2.0 improvement can be ported to OID4VC

Drew Beamer @ Unsplash

BONUS : PROOF OF CONCEPT

OID4VC Proof of concept

https://gitlab.com/gaia-x/gaia-x-community/openid-for-verifiable-credentials/

Thank you!

Vincent Kelleher
vincent.kelleher@gaia-x.eu