W3C Verifiable Credentials for ATLAS

Morocco Smart Port Challenge
Draft version Jan 2021
(Work in progress)

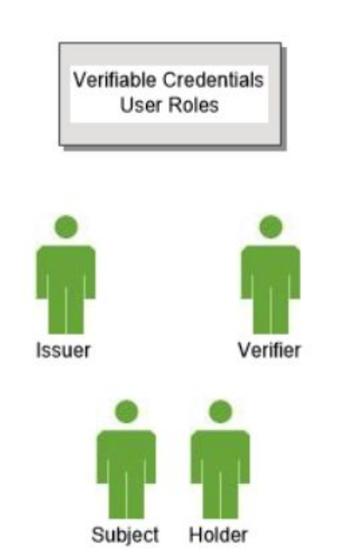
José Manuel Cantera
IOTA Foundation

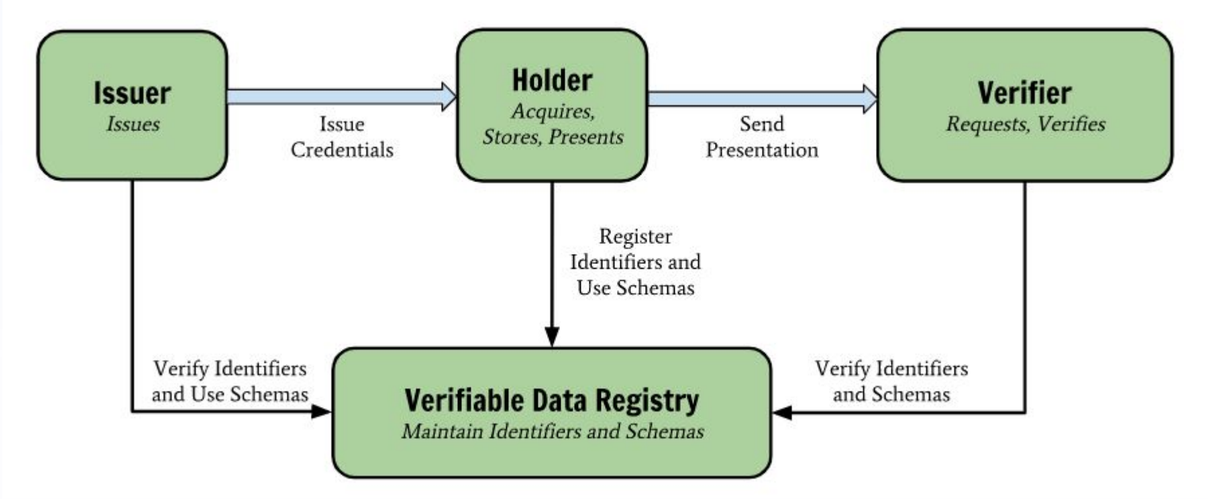
W3C Verifiable Credentials Standard

- **What is a Verifiable Credential?**
  - A *machine-readable* document intended to express credentials in a way that is cryptographically secure, privacy respecting, and *machine-verifiable*.
- W3C VCs defines a **Data Model (encoded as JSON-LD 1.1)** for credentials
  - Ready for contemporary trade digitalization. Already recommended by the *World Economic Forum*.
  - Terms with well-defined semantics that can accommodate existing international trade standards. Prevent semantic ambiguity.
  - Extensible, Customizable, Multi-purpose (could also be used for *phytosanitary*, etc.)
  - Developer-friendly (*it is just JSON*) → Easy to integrate with existing platforms and toolchains
  - Internationalization off-the-shelf
  - Enables **Linked Data** (compliant with the Web Architecture and already used by millions of websites to publish machine-readable data)

IOTA

W3C Verifiable Credentials Roles

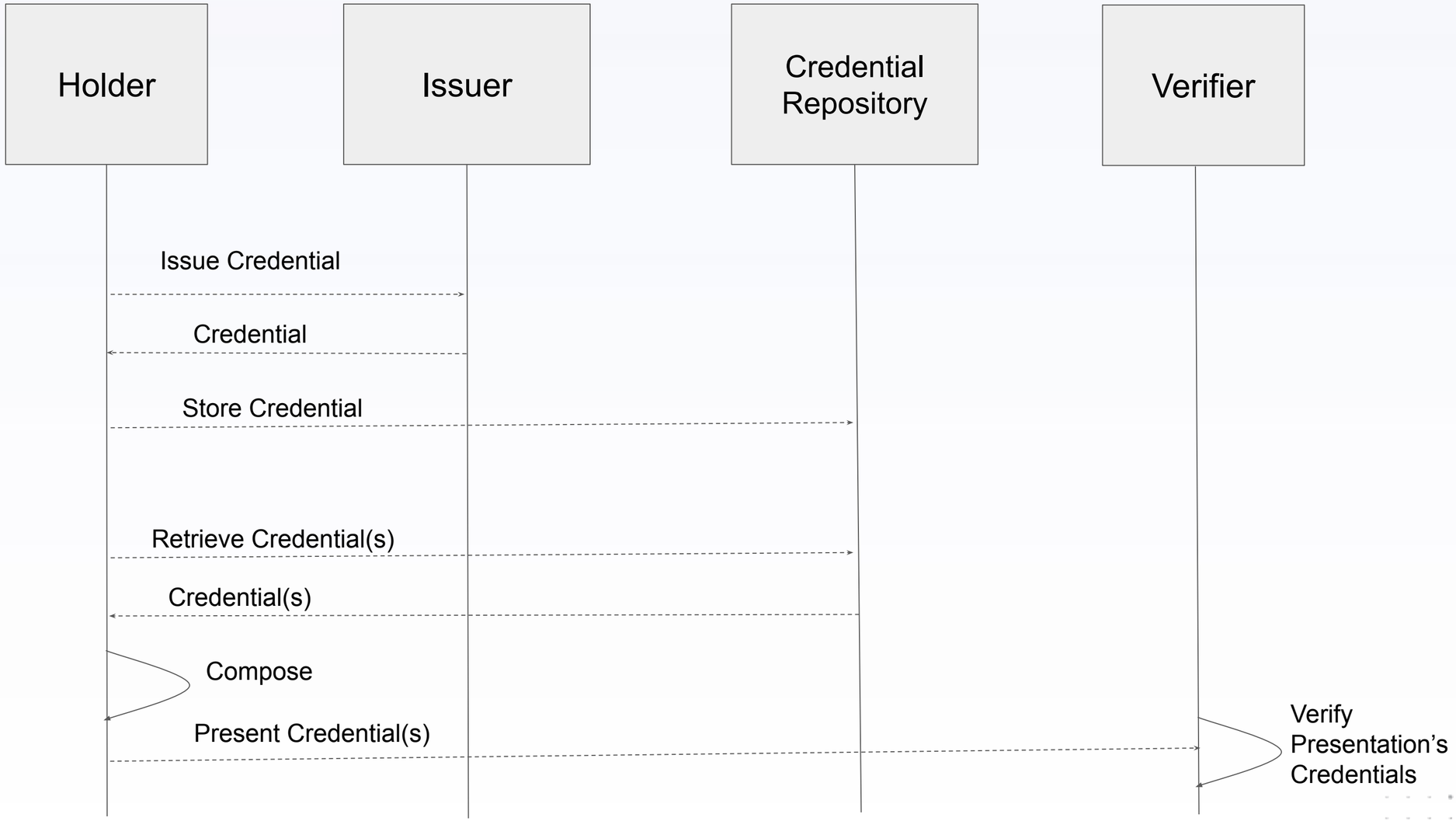




Source: W3C

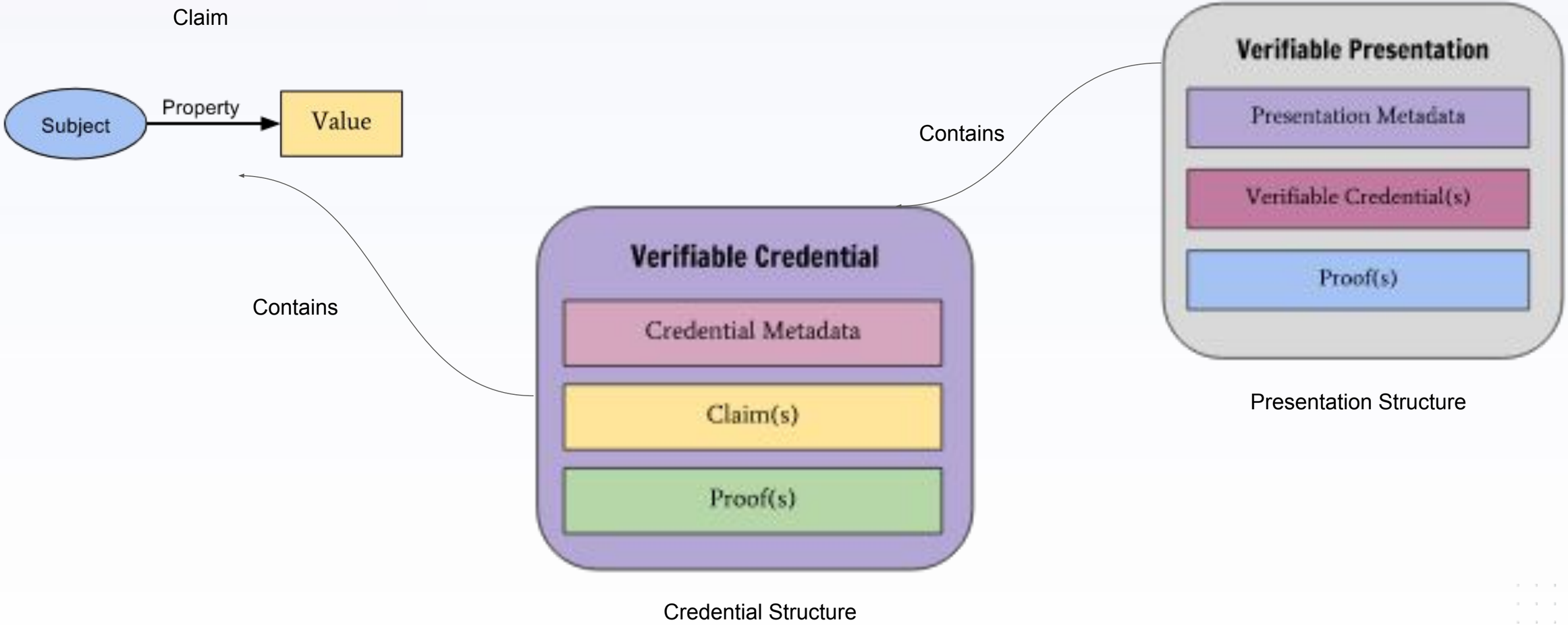
IOTA

W3C VCs .- The most simple Data Flow



IOTA

W3C Verifiable Credentials Data Model



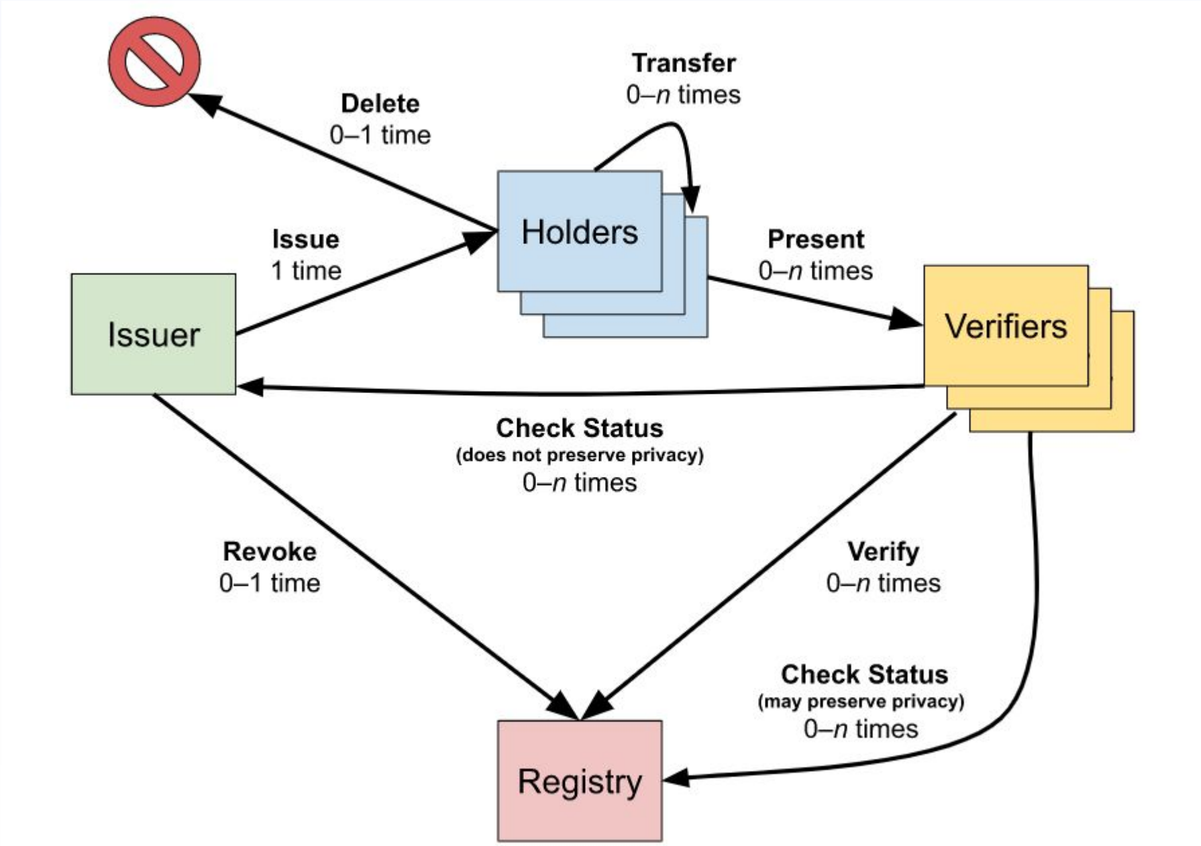
Presentation Structure

Credential Structure

Source: W3C

IOTA

W3C VC Roles and Lifecycle



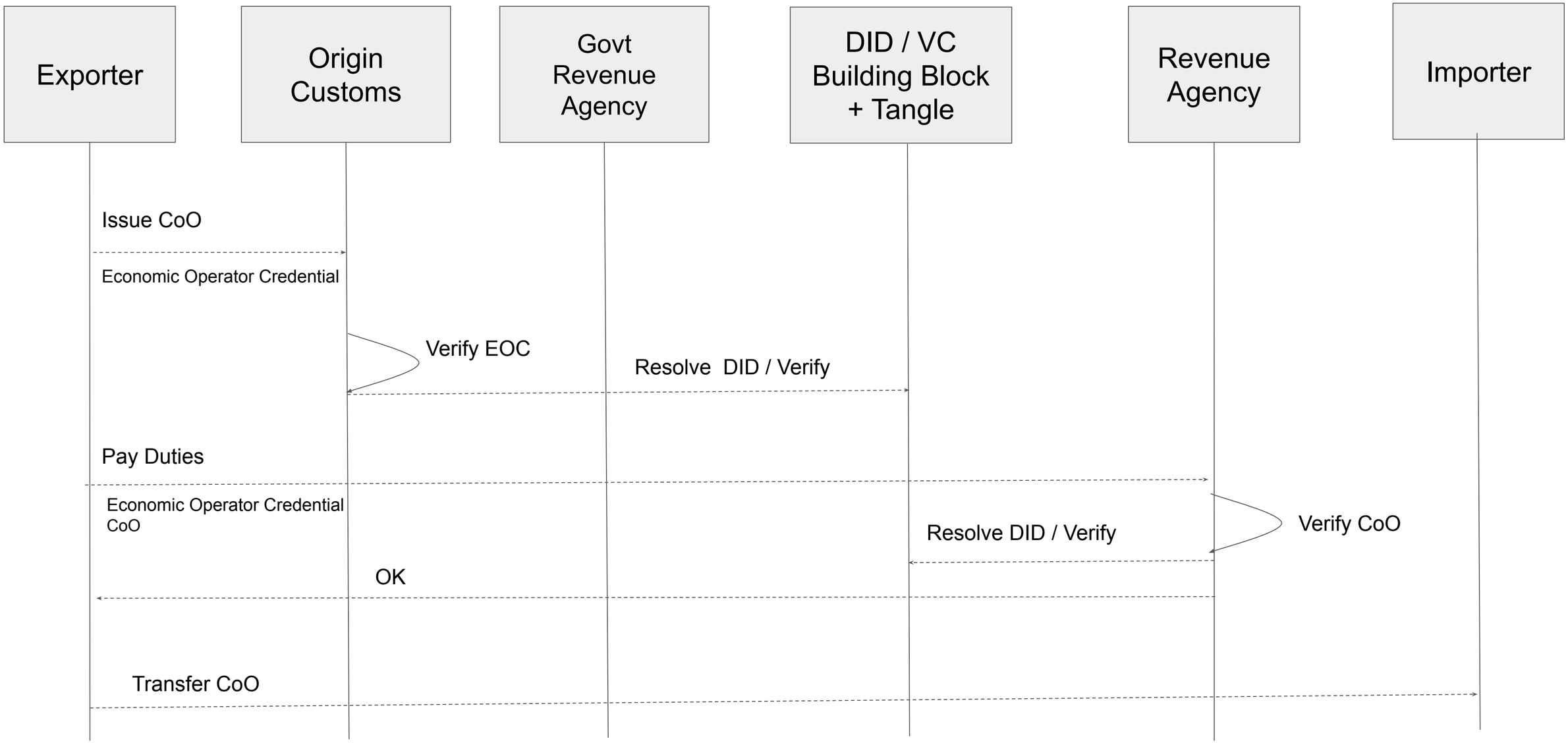
Source: W3C

IOTA

Simplified Generic Flow for a CoO (I/II)

- Entities/actors can play different roles (*issuer, holder, verifier*) at different moments in time
  - Commercial Registration Agency, Revenue Agency, Exporter, Freight Forwarder, Origin Customs, Importer, Destination Customs, ...
- The **Commercial Registration Agency** issues an Economic Operator Credential (EOC) to the Exporter. The Exporter stores the Credential.
- The **Exporter** presents the Economic Operator Credential plus possibly other credentials (or documents) to Origin Customs and asks for a Certificate of Origin (CoO)
- **Origin Customs** verifies the EOC and issues a CoO to the Exporter
- The **Exporter** presents the CoO (as a credential) to the Revenue Agency to pay custom duties
- The **Revenue Agency** verifies the CoO
- The **Exporter** *transfers* the CoO credential to the Importer. How?
- The **Importer** presents the CoO at the Destination Customs
- The **Destination Customs** verifies the CoO
- .....

Simplified Generic Flow for a CoO (II/II)



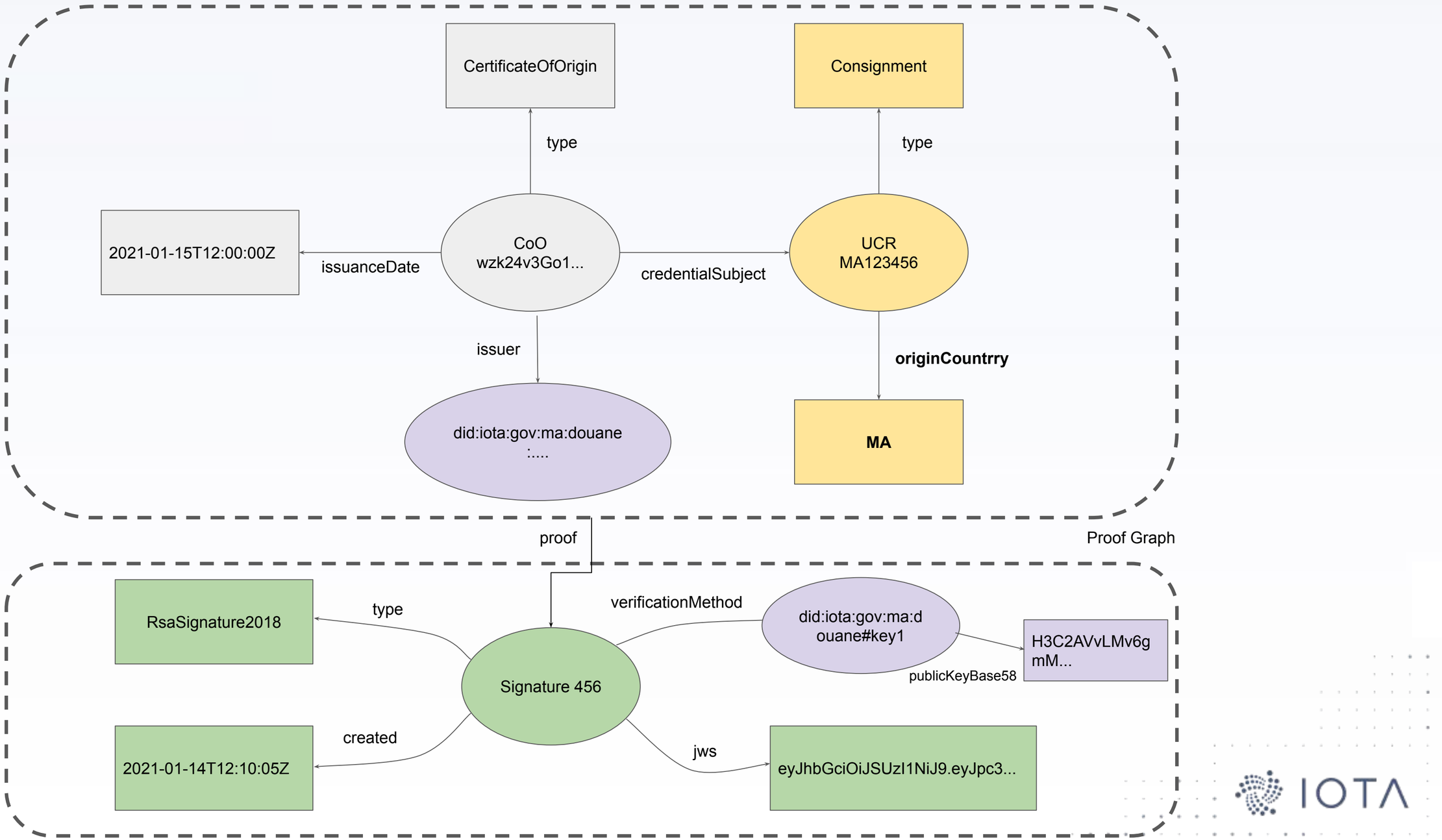
Case Study

Certificate of Origin as a W3C Verifiable Credential

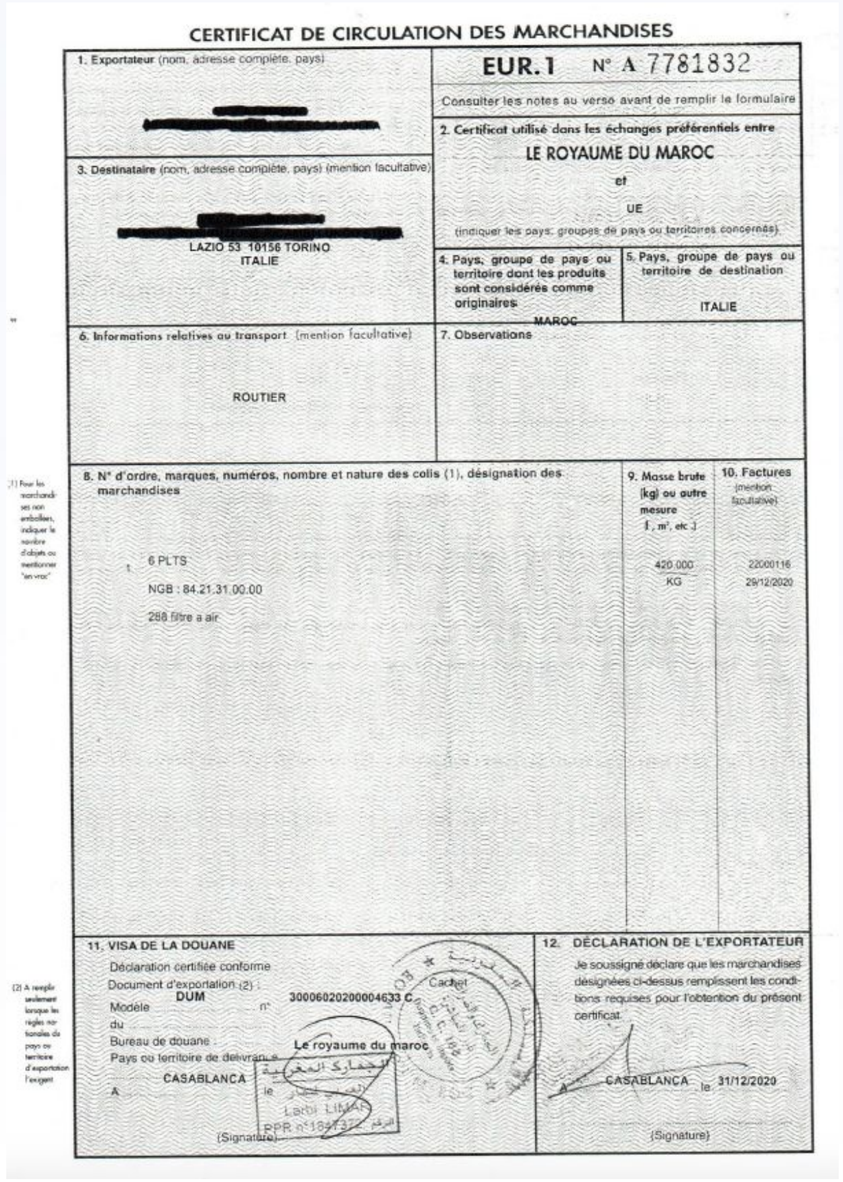
- Use Case: An exporter from Morocco wants to export oranges and mandarins to Spain
  - Exporter wants to enjoy the reduced duties according to the preferential trade agreement between the EU and Morocco
  - A new consignment is prepared containing:
    - 300 kilos of oranges
    - 100 kilos of mandarins
  - The means of transportation of the consignment will be *sea shipping*
- **Next Step:** How the CoO as a W3C Verifiable Credential would look like?

IOTA

CoO as a VC (Linked Data Graph)



From a paper-based CoO to JSON-LD-based VC



CERTIFICAT DE CIRCULATION DES MARCHANDISES

1. Exportateur (nom, adresse complète, pays)

[redacted]

EUR.1 N° A 7781832

Consulter les notes au verso avant de remplir le formulaire

2. Certificat utilisé dans les échanges préférentiels entre

LE ROYAUME DU MAROC

et

UE

(indiquer les pays, groupes de pays ou territoires concernés)

3. Destinataire (nom, adresse complète, pays) (mention facultative)

[redacted]

LAZIO 53 10156 TORINO
ITALIE

4. Pays, groupe de pays ou territoire dont les produits sont considérés comme originaires

MAROC

5. Pays, groupe de pays ou territoire de destination

ITALIE

6. Informations relatives au transport (mention facultative)

ROUTIER

7. Observations

8. N° d'ordre, marques, numéros, nombre et nature des colis (1), désignation des marchandises

9. Masse brute (kg) ou autre mesure (l, m³, etc.)

10. Factures (mention facultative)

1 6 PLTS
NGB : 84.21.31.00.00
288 filtre a air

420.000 KG

22000116 29/12/2020

(1) Pour les marchandises non emballées, indiquer le nombre d'objets ou mentionner "en vrac"

11. VISA DE LA DOUANE

Déclaration certifiée conforme
Document d'exportation (2)
Modèle DUM n° 300060202000046 33 C
du
Bureau de douane
Pays ou territoire de délivrance
A CASABLANCA le

Le royaume du maroc

Cachet

(Signature)

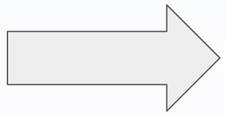
12. DÉCLARATION DE L'EXPORTATEUR

Je soussigné déclare que les marchandises désignées ci-dessus remplissent les conditions requises pour l'obtention du présent certificat.

A CASABLANCA le 31/12/2020

(Signature)

(2) A remplir seulement lorsque les règles régionales du pays ou territoire d'exportation l'exigent




```
{
    "@context": [
        "https://www.w3.org/2018/credentials/v1",
        "https://schema.org",
        "https://w3id.org/atlas/coo/v1"
    ],
    "credentialSchema": {
        "id": "https://schema.atlas.io/certificate-of-origin.json",
        "type": "JsonSchemaValidator2018"
    },

    "id": "https://www.douane.gov.ma/credential/coo/wzk24v3Go1dDMabh",
    "type": ["VerifiableCredential", "CertificateOfOrigin"],

    "issuer": "did:iota:gov:ma:douane:7LnJCtcxGtRPAXz125xv7RGLcOPLkHRS",

    "holder": "did:iota:com:exporter:ma:BxxW4q37dlN6ZqUKIFr9MRxAVNIK7Mqf",

    "credentialStatus": {
        "type": "CertificateOfOriginStatus",
        "id": "https://w3id.org/atlas/coo/v1#validStatus"
    },

    "validFrom":  "2021-01-12T12:00:00Z",
    "validUntil": "2021-01-19T12:00:00Z",

    "credentialSubject": {
        "id": "https://www.douane.gov.ma/ucr/MA1234567893123456789",
        "type": "Consignment",
        "ucr": "MA1234567893123456789",
        "commercialInvoice": {
            "type": "Invoice",
            "invoiceNumber": "A-56789",
            "invoiceDate": "2021-01-09"
        },
        "countryOfOrigin": {
            "type": "Country",
            "name": "MA"
        },
        "importingCountry": {
            "type": "Country",
            "name": "ES"
        },
        "consignor": {
            "id": "did:iota:com:exporter:ma:BxxW4q37dlN6ZqUKIFr9MRxAVNIK7Mqf",
            "type": "Organization"
        },
        "consignee": {
            "id": "did:iota:com:importer:es:Ai1vC5DdKyE6f8V6EJOgxZkcNKfQK3bd",
            "type": "Organization"
        },
        "items": [
            {
                "type": "Product",
                "hsCode": "1080510",
                "description": "Oranges",
                "weight": "100"
            },
            {
                "type": "Product",
                "hsCode": "1080520",
                "description": "Mandarines",
                "weight": "50"
            }
        ]
    },

    "document": {
        "type": "DataDownload",
        "contentUrl": "https://ipfs.atlas.io/0HUc4uyO56MXUja6dWGo5dP7fudbtV1PjMkFiXgJcIH64EQUcFtA8Y4DzhVUFtvg",
        "encodingFormat": "application/pdf"
    },

    "proof": {
        "type": "RsaSignature2018",
        "created": "2021-01-12T11:22:54Z",
        "proofPurpose": "assertion",
        "jws":
"eyJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ.eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ",
        "verificationMethod": "did:iota:gov:ma:douane:7LnJCtcxGtRPAXz125xv7RGLcOPLkHRS#keys-1"
    }
}
```

Anatomy of a CoO as a W3C Verifiable Credential (I of III)


```
{
    "@context": [
        "https://www.w3.org/2018/credentials/v1",
        "https://schema.org",
        "https://w3id.org/atlas/coo/v1"
    ],

    "id": "https://id.douane.gov.ma/credential/coo/wzk24v3Go1dDMabh",

    "type": ["VerifiableCredential", "CertificateOfOrigin"],

    "issuer": "did:iota:gov:ma:douane:7LnJCtcxGtRPAXz125xv7RGLcOPLkHRS",

    "holder": {
        "id": did:iota:com:exporter:ma:BxxW4q37dlN6ZqUKIFr9MRxAVNIK7Mqf",
        "type": "Organization"
    },

    "credentialStatus": {
        "type": "CertificateOfOriginStatus",
        "id": "https://w3id.org/atlas/coo/v1#validStatus"
    },
    "issuanceDate":   "2021-01-12T12:00:00Z",
    "expirationDate": "2021-01-19T12:00:00Z",
```


Which vocabularies are being used?

id of the Certificate of Origin (as a Digital Link)

This is a Certificate of Origin

DID of the Govt Agency

DID of the Exporter

CoO Status

validFrom

validUntil

IOTA

Anatomy of a CoO as a W3C Verifiable Credential (II of III)

```
"credentialSubject": {
        "type": "Consignment",
        "ucr": "MA1234567893123456789",

        "countryOfOrigin": {
            "type": "Country",
            "name": "MA"
        },
        "importingCountry": {
            "type": "Country",
            "name": "ES"
        },

        "consignor": {
            "id": "did:iota:com:exporter:ma:BxxW4q37dlN6ZqUKIFr9MRxAVNIK7Mqf",
            "type": "Organization"
        },
        "consignee": {
            "id": "did:iota:com:importer:es:Ai1vC5DdKyE6f8V6EJOgxZkcNKfQK3bd",
            "type": "Organization"
        },

        "items": [
            {
                "type": "Product",
                "hsCode": "1080510",
                "description": "Fruit, edible; oranges, fresh or dried",
                "weight": 300
            },
            {
                "type": "Product",
                "hsCode": "1080520",
                "description": "Fruit, edible; mandarins (including tangerines and satsumas), clementines...",
                "weight": 100
            }
        ]
    }
```

UCR as per WCO Recommendation

A GS1 Digital Link to the consignment's Digital Twin could also be provided

Origin Country as per ISO 3166

Other data could be encoded such as the invoice number, etc.

Exporter DID

Importer DID

UN Harmonized Commodity Description and Coding

Other information about the consignment could also be encoded (Vessel id, etc.)

IOTA

Anatomy of a CoO as a W3C Verifiable Credential (III of III)


```
  "proof": {
     "type": "RsaSignature2018",

     "created": "2021-01-12T11:22:54Z",

     "proofPurpose": "assertionMethod",

     "jws":
"eyJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ij
p0cnVlfQ.eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ",

     "verificationMethod": "did:iota:gov:ma:douane:7LnJCtcxGtRPAXz125xv7RGLcOPLkHRS#keys-1"
    }

}
<EOF>
```


Proof to verify the authenticity of the CoO

Signature as per JWS standard IETF RFC 7515

Points to the public key of the contained on the Govt Agency DID that allows to verify the CoO

IOTA

Next Steps

- Deep dive towards a **VC Vocabulary / Extensions** for Trade
- Deep dive towards a **Reference Architecture** for VCs applied to international trade
- Deep Dive towards **VC Protocols for Trade** (*Remember that the standard only defines the Data Model*).
  - Just HTTP + JWT to present a credential?
  - How credential transfer could be implemented?
- Deep dive towards **full implementation of VC in ATLAS**
  - IPFS → Credential Repository
  - Tangle → Verifiable Registry
  - Data Matrix to extract data from a VC
- Deep dive towards further specification / coding of the **DID/VC Building Block** for ATLAS
  - Issue VC, Expose VC, Verify VC, Anchor VC to Tangle, Revoke VC, … Generate PDF from VC, …

IOTA

Backup Slides

W3C DID Standard

- **What is a Decentralized ID (DID)?**
  - A new type of identifier that allows the participation of cross-border actors without relying on a centralized and foreign authority.
  - A DID is globally unique, resolvable with high availability, and cryptographically verifiable.
  - DIDs are resolved to DID documents which include cryptographic material, such as public keys, and service endpoints, for establishing secure communication channels.
  - Standardized by W3C. A DID is a **JSON-LD** document. Recommended by *World Economic Forum*
- All the participants in the ecosystem should have a DID
  - Government Agencies
  - Customs
  - Economic Operators
  - ...
- DIDs might be verified by a Government institution and recorded on a DLT for immutability

IOTA

Anatomy of a W3C DID Document. Ex. Govt Agency.

```
{
    "@context": [
        "https://www.w3.org/ns/did/v1",
    ],
    "id": "did:iota:gov:ma:douane:7LnJCtcxGtRPAXz125xv7RGLcOPLkHRS",

    "verificationMethod": {
      "id": "did:iota:gov:ma:douane:7LnJCtcxGtRPAXz125xv7RGLcOPLkHRS#key-1",
      "type": "RsaVerificationKey2018",
      "controller": "did:iota:gov:ma:douane:7LnJCtcxGtRPAXz125xv7RGLcOPLkHRS",
      "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV",
    },
    "services": [
      {
         "id": "did:iota:gov:ma:douane:7LnJCtcxGtRPAXz125xv7RGLcOPLkHRS#cooService",
         "type": "CertificateOfOriginIssueService",
         "serviceEndpoint": "https://www.douane.gov.ma/credential/coo/issue/"
      }
    ]
}
```

Which vocabularies are being used?

Resolvable DID URI

Cryptographic material for verification purposes

Who controls the DID

Service to obtain a new CoO

IOTA

The JSON-LD *@context*

- What is the JSON-LD ***@context***?
  - When two people communicate with one another, the conversation takes place in a shared environment, typically called "*the context of the conversation*".
  - It allows to use **shortcut terms**, like the first name of a mutual friend, to *communicate more quickly but without losing accuracy*.
- The JSON-LD *@context* allows two applications to use a **shared vocabulary** to communicate with one another more efficiently, but without losing accuracy.
  - The *@context* maps univocally terms to URIs (concepts) with well defined semantics
    - `"CertificateOfOrigin"` → `"https://w3id.org/atlas/v1/coo#CertificateOfOrigin"`
    - `"CertificatdOrigine"` → `"https://w3id.org/atlas/v1/coo#CertificateOfOrigin"`
  - The *@context* is just another JSON-LD document referenced by a JSON-LD document
- Multiple *@context* can be used at the same time: ex. *schema.org*, the *GS-1 Web Vocabulary*, https://www.gs1.org/gs1-web-vocabulary , a custom one for ATLAS, etc.

IOTA

JSON-LD and international trade

- One interesting feature of JSON-LD is that it enables seamless, off-the-shelf internationalization using the so-called *language map* feature. Example

```
"@context": {
    ...
    "description": { "@id": "https://schema.org/description", "@container": "@language" }
  }

"items": [
            {
                "type": "Product",
                "hsCode": "1080510",
                "description": {
                  "en": "Fruit, edible; oranges, fresh or dried",
                  "fr": "Fruits comestibles; oranges, fraîches ou séchées".
                  "es": "Frutas comestibles; naranjas, frescas o secas"
                },
                "weight": 300
            },
            {
                "type": "Product",
                "hsCode": "1080520",
                "description": {
                  "en": "Fruit, edible; mandarins (including tangerines and satsumas), clementines...",
                  "fr": "Fruits comestibles; mandarines (y compris mandarines et satsumas), clémentines ... ",
                  "es": "Frutas comestibles; mandarinas (incluyendo satsumas), clementinas..."
                },
                "weight": 100
            }
        ]
```

Descriptions in multiple languages
Ready to be consumed by different applications at different countries