edi3 Self-Sovereign Identity 1.0 Specification

## Status

Raw

## Glossary

Phrase | Definition

———— | ————-

This service depends on - TBA.

The TBA specification depends on this document. Note, TBA.

## Licence

All material published on edi3.org including all parts of this specification are the intellectual property of the UN as per the [UN/CEFACT IPR Policy](https://www.unece.org/fileadmin/DAM/cefact/cf_plenary/plenary12/ECE_TRADE_C_CEFACT_2010_20_Rev2E_UpdatedIPRpolicy.pdf).

This Specification is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 3 of the License, or (at your option) any later version. See http://www.gnu.org/licenses.

## Change Process

This document is governed by the [2/COSS](http://rfc.unprotocols.org/spec%3A2/COSS/) (COSS).

## Language

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119.

# Introduction

The concept of Self-Sovereign Identity is an intuitive and powerful approach to establishing trust on the web. While this new paradigm is not sector-specific, it is particularly relevant to international supply chains.

SSI comprises roughly of two complimentary technologies: Decentralized Identifiers and Verifiable Credentials.

## Decentralized Identifiers

Put very simply, a Decentral Identifier (DID) is a self-issued key which only the owner has access to. A DID can represent people and organizations, but also less tangible objects, event, etc. While not strictly necessary, DIDs are commonly kept on a dedicated identity blockchain.

The DID standard can be found here:
https://www.w3.org/TR/did-core/

## Verifiable Credentials

Trust is established by issuing Verifiable Credentials (VCs) amongst DIDs. This intuitively mirrors “the real world”: your passport proves citizenship, a diploma represents your academic achievements, and the driver license proves that you can drive a car.
VCs work the same way: - a credentials **issuer** makes a claim against the credential **holder**. - subsequently, the holder proves that claim to a credentials **verifier**.

In short, if the verifier knows and trusts the issuer, he can also trust the holder’s claims.

Technically, this is enabled by common asynchronous cryptography, linking VCs to DIDs.

The VC standard can be found here: https://www.w3.org/TR/vc-data-model/

# Structure of a Verifiable Credential

The following is piece by piece breakdown of a Verifiable Credential. As an example this takes the shape of a Bill Of Lading, generated from the methodology https://edi3.org/tools-and-methods/. Please note that this is just an illustrative example with fake data.

## Contexts

 "@context": [
 "https://www.w3.org/2018/credentials/v1",
 "https://unece.cefact.org/vocab/bsp",
 "https://dcsa.org/vocab"
 ],

The @context indicates where used semantics are defined.

The first defines the VC elements such as VerifiableCredential, issuer, proof and credentialsSubject.

The next is the UN/CEFACT B-S-P semantic model expressed for machine linkage. Exposing this vocabulary is among the main goals of the edi3 project (see https://edi3.org/specs/edi3-json-ld-ndr/develop/). At time of writing this is still work in progress.

Finally, since the Bill Of Lading is a key carrier-related document, it can be expected that DCSA.org will at one point express certain definitions, including BillOfLading.

## Identifier

 "id": "http://ebl.tradelens.com/6057611a-0122-40ec-a584-ac5c8c0a874f",

Being a JSON-LD document, the Bill Of Lading document needs an identifier. In this case the BOL is issued on TradeLens.

## Document Type

 "type": [
 "VerifiableCredential",
 "BillOfLading"
 ],

This defines that the document is a Verifiable Credential expressing a Bill Of Lading.

## Issuer

 "issuer": "did:v1.maersk:43ba3108-dbce-11ea-87d0-0242ac130003",

The issuing organization. In this case Maersk, represented by an example DID

## Validity Period

 "issuanceDate": "2020-06-22T06:25:10Z",
 "expirationDate": "2021-06-22T06:25:10Z",

The validity period of a VC can be limited, here limited to one year.

## Signature

 "proof": {
 "type": "RsaSignature2018",
 "created": "2020-04-17T18:03:18Z",
 "verificationMethod": "did:example:123#key-1",
 "nonce": "c0ae1c8e-c7e7-469f-b253-86e6a0e7387e",
 "signatureValue": "5TcawVLuoqRjCuu4jAmRqBcKoab2YVqxG8RXnQwvQBHNwP7RhPwXh"
 },

The issuer’s signature of the VC.

## Schema

 "credentialSchema": {
 "id": "https://dcsa.org/schemas/billOfLading.json",
 "type": "JsonSchemaValidator2018"
 },

JSON Schema of the credential. In this case defined by DCSA.

## Credential

 "credentialSubject": {
 "consignor": {
 "id": "did:sov:peachesww:ac8bd10a-dbce-11ea-87d0-0242ac130003",
 "name": "Peaches Worldwide",
 "printedParty": "PEACHES WW",
 "partyRef": "12700219780"
 },
 "consignee": {
 "id": "did:v1:tradingco:4bdc45e2-dbce-11ea-87d0-0242ac854126",
 "name": "TRADING CO",
 "printedParty": "TRADING CO",
 "partyRef": "12700219780"
 },
 }

Everything which makes up the actual credential is included in the credentialSubject element. Its content is what is signed in proof and can be validated against the schema defined in credentialSchema.

With this, the consignee and consignor - represented by DIDs on separate identity networks - can proof their role in relation to this Bill Of Lading. Specifically, Peaches Worldwide (did:sov:peachesww:ac8bd10a-dbce-11ea-87d0-0242ac130003) can prove that they are the consignor, and TRADING CO (did:v1:tradingco:4bdc45e2-dbce-11ea-87d0-0242ac854126) can prove to be the consignee. Both claims attested by Maersk (did:v1.maersk:43ba3108-dbce-11ea-87d0-0242ac130003), the issuer.

# Full Example

The following is the full example of the elements explained above:

{
 "@context": [
 "https://www.w3.org/2018/credentials/v1",
 "https://unece.cefact.org/vocab/bsp",
 "https://dcsa.org/vocab"
 ],
 "id": "http://ebl.tradelens.com/6057611a-0122-40ec-a584-ac5c8c0a874f",
 "type": [
 "VerifiableCredential",
 "BillOfLading"
 ],
 "issuer": "did:v1.maersk:43ba3108-dbce-11ea-87d0-0242ac130003",
 "issuanceDate": "2020-06-22T06:25:10Z",
 "expirationDate": "2021-06-22T06:25:10Z",
 "proof": {
 "type": "RsaSignature2018",
 "created": "2020-04-17T18:03:18Z",
 "verificationMethod": "did:example:123#key-1",
 "nonce": "c0ae1c8e-c7e7-469f-b253-86e6a0e7387e",
 "signatureValue": "5TcawVLuoqRjCuu4jAmRqBcKoab2YVqxG8RXnQwvQBHNwP7RhPwXh"
 },
 "credentialSchema": {
 "id": "https://dcsa.org/schemas/billOfLading.json",
 "type": "JsonSchemaValidator2018"
 },
 "credentialSubject": {
 "negotiable": false,
 "dateOfAcceptance": "2020-06-23T00:01:00Z",
 "eBL": true,
 "shippedOnBoardDate": "2020-06-25T00:01:00Z",
 "billOfLadingNumber": "330942870",
 "bookingNumber": [
 "910912872"
 ],
 "transportEquipmentQuantity": 1,
 "arrivalDate": "2020-07-17T00:01:00Z",
 "notifyParty": {
 "name": "TRADING CO",
 "printedParty": "TRADING CO",
 "partyRef": "6531477551"
 },
 "serviceMode": "SD/CY",
 "partBillIndicator": false,
 "carrier": {
 "carrierCode": "SAFM",
 "name": "Safmarine Espana (Valencia)"
 },
 "consignee": {
 "id": "did:v1:tradingco:4bdc45e2-dbce-11ea-87d0-0242ac854126",
 "name": "TRADING CO",
 "printedParty": "TRADING CO",
 "partyRef": "12700219780"
 },
 "consignmentItems": [
 {
 "sequence": 1,
 "information": "1 Container Said to Contain 21 PALLETS PEACH",
 "equipmentStuffing": [
 {
 "equipmentNumber": "MSEU0517390",
 "stuffedGrossVolume": {
 "value": 52.0,
 "unit": "cbm"
 },
 "stuffedGrossWeight": {
 "value": 18320.0,
 "unit": "kgs"
 },
 "stuffedTransportPackages": {
 "quantity": 21
 }
 }
 ],
 "grossWeight": {
 "value": 18320.0,
 "unit": "kgs"
 },
 "grossVolume": {
 "value": 52.0,
 "unit": "cbm"
 },
 "transportPackages": {
 "quantity": 21,
 "type": "PALLETS",
 "shippingMarks": [
 ""
 ]
 }
 }
 ],
 "consignor": {
 "id": "did:sov:peachesww:ac8bd10a-dbce-11ea-87d0-0242ac130003",
 "name": "Peaches Worldwide",
 "printedParty": "PEACHES WW",
 "partyRef": "12700219780"
 },
 "mainCarriageTransportMovement": {
 "identification": "026E",
 "usedTransportMeans": {
 "name": "SANTA CRUZ"
 }
 },
 "utilizedTransportEquipment": [
 {
 "equipmentNumber": "MNBU0517390",
 "printedEquipmentType": "40 REEF",
 "seals": [
 {
 "identifier": "ML-ES88221",
 "type": "Carrier Seal"
 }
 ]
 }
 ],
 "information": [
 {
 "type": "billOfLadingClause",
 "text": "This shipment is subject to compliance with UN, EU and US sanction laws."
 },
 {
 "type": "billOfLadingClause",
 "text": "SHIPPER'S LOAD, STOW, WEIGHT AND COUNT"
 },
 {
 "text": "https://terms.safmarine.com/carriage",
 "type": "termsAndConditions"
 }
 ],
 "placeOfIssue": {
 "name": "Valencia",
 "printedLocation": "Valencia"
 },
 "placeOfReceipt": {
 "name": "Valdivia",
 "printedLocation": "Valdivia"
 },
 "portOfDischarge": {
 "name": "Jebel Ali",
 "printedLocation": "Jebel Ali"
 },
 "portOfLoading": {
 "name": "Algeciras",
 "printedLocation": "Algeciras"
 },
 "originatorName": "Safmarine Espana (Valencia)",
 "originatorId": "SAFM",
 "issue": "2020-06-22T06:30:00Z",
 "originalIssued": 1,
 "references": [
 {
 "type": "contractNumber",
 "value": "321239005"
 }
 ]
 }
}