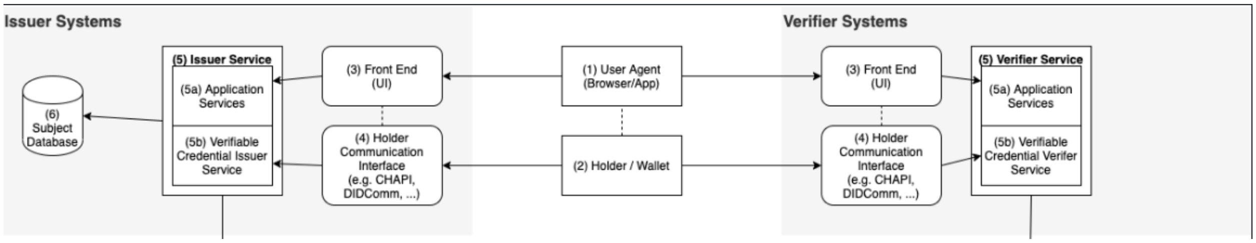
Rationale: (Juan Caballero, DIF/Spherity)

There have been some discussions lately both in the open repo of the VC-HTTP-API (primarily on PR 168, but see also issues 172, 174 and 136) and the private SVIP repo (issue 1). These discussions have been difficult to resolve on github because there is no previously agreed-upon Use Cases & Requirements ("UCR") for the VC-HTTP-API, and no clear consensus on whether external use cases are applicable and if so how. Many SVIP participants and CCG onlookers would like to get as quickly as possible from the current opaque impasse to a place where API design can be evaluated against an agreed-upon UCR.

To that end, I'd like to follow Markus' suggestions that 1.) the repo's architecture document be taken as a starting point for a UCR, and 2.) that three different APIs be treated as distinct.


Issuer Systems
(6) Subject Database
(5) Issuer Service
(5a) Application Services
(5b) Verifiable Credential Issuer Service
(3) Front End (UI)
(4) Holder Communication Interface (e.g. CHAPI, DIDComm, ...)
(1) User Agent (Browser/App)
(2) Holder / Wallet
Verifier Systems
(3) Front End (UI)
(4) Holder Communication Interface (e.g. CHAPI, DIDComm, ...)
(5) Verifier Service
(5a) Application Services
(5b) Verifiable Credential Verifer Service

The basic problem to be solved is that the components 1 & 2 in the current VC-HTTP-API are defined somewhat minimally, in a way that assumes data subjects will be the only holders and that only one holder exists in any given use case. The supply chain use-cases under development and alignment in the SVIP program all have some amount of "information brokerage," i.e. custodial or notary relationships between agents, where VCs need to be passed between holders or to verifiers on behalf of a data subject. In particular, the architecture of large-scale systems of brokerage where information would be verified or collated before being passed to CBP or other government agencies is particularly important in this regard. For obvious reasons, information about design proposals in this last use case are more difficult to speak to or publicize than other supply chain interactions where holder-to-holder APIs would be worth specifying in this project's general-purpose API definitions.

Issuance Flow and Scope

Issuing a Verifiable Credential to a Holder requires several logical steps. This section provides guidance on which steps are in scope for this API. **Steps in scope are marked bold**.

1. Determine if Holder or Client (and represented entities, like the user) are eligible for the Verifiable Credential. This is an Issuer Service Application and Client level operation.

2. Locate and establish a communication channel between the Issuer Service and the Holder. This is the operation of the Issuer-to-Holder Communication Interface.

3. Establish trust with the Holder or Client through implemented policies and governance frameworks. This is an Issuer Service Application or Governance level operation, but specifying a few common, uncontroversial options for the Holder and the Issuer-to-Holder Communication Interface may be necessary to lower barriers to participation and delegation for Enterprise prototyping and adoption.
    a. OAuth2 has been chosen as the first of these; addition of more in the coming months would be timely for clients working with enterprise partners in large-scale supply chain use cases (see issue 1 if you can on SVIP private repo).
4. Access internal data stores to build the set of claims/properties for the Subject to be encoded in the Verifiable Credential document. Currently this is Issuer Service Application and Issuer Subject Database operations, but may become in scope for the HTTP API Service.
5. Construct the Verifiable Credential Data Model representation in a compliant format. This is (currently) an Issuer Service Application operation - but may be supported by construction and templating APIs when defined.
6. **Validate that the Credential is constructed in accordance with the W3C Verifiable Credential Specification, then generate cryptographic proof for the Credential, and assemble the completed Verifiable Credential into a Verifiable Presentation per the W3C Verifiable Credential Specification for delivery to a Holder.**
    a. This is *currently* the operation of the Verifiable Credential Issuer HTTP API Service. Note that the Holder does not have to be the subject of the Verifiable Credential.
7. Communicate/deliver the final Verifiable Credential object to the Holder as a Verifiable Presentation.
    a. Currently scoped as an operation of the Issuer Application and Isser-to-Holder Communication Interface, but may become a function of the HTTP API Service.
8. Maintain an **auditable** lifecycle for the issued Verifiable Credential (optional).
    a. This is an operation of the Issuer HTTP API, but lifecycle decisions and policies are driven by the Issuer Service Application.

Holder Flow and Scope

Presenting a Verifiable Credential to a Verifer or to another Holder requires several logical steps. This section provides guidance on which steps are in scope for this API. **Steps in scope are marked bold**.

1. Determine if Second Holder or Verifier (and represented entities, like the user) would want a set of credentials. This is an Holder Service Application and Client level operation.

2. Locate and establish a communication channel between the Second Holder/Verifier's Service and the Holder. This is the operation of the Holder-to-Holder and/or Holder-to-Verifier Communication Interface {To be specified?}.

3. Establish trust with the Second Holder/Verifier through implemented policies and governance frameworks. This is an Holder Service Application or Governance level operation, but may be technically enabled by the Holder-to-Holder and/or Holder-to-Verifier Communication Interface .

4. Communicate/deliver proposal for Verifiable Presentations the Second Holder/Verifier. Currently scoped as an operation of the Holder Application and Holder-to-Holder and/or Holder-to-Verifier Communication Interface , but may become a function of the HTTP API Service.

    a. DIF Presentation Exchange and/or DIDComm credential definition protocols ***might*** be worth comparing to VP Request Spec (in partic Query by Example), specifically in terms of how a VP is proposed ***semantically***.

5. Negotiate equivalence or appropriate match between VCs on offer (and relationship between them) and VCs accepted/expected by Second Holder/Verifier.

    a. DIF Presentation Exchange and/or DIDComm credential definition protocols ***might*** be worth comparing to VP Request Spec (in partic Query by Example), specifically in terms of this negotiation.

6. Choose your own adventure:

    a. (PUSH version) Second Holder/Verifier returns an endpoint ready to receive a VP signed by the holder and one or more challenge/nonce(s).

        i. 7A: Construct a Verifiable Presentation in a compliant format. This is (currently) an Holder Service Application operation - but may be supported by construction and templating APIs when defined.

    b. (PULL version - EDV edition) Second Holder/Verifier returns approval (and possibly something else like a token or identifier? I'm unclear on the mechanics). Holder responds with capability/authZ and endpoint for storage (such as EDV or Resource Server).

    c. (PULL version - Centralized Storage edition) TKTKTK

7. Construct the Verifiable Credential Data Model representation in a compliant format. This is (currently) an Issuer Service Application operation - but may be supported by construction and templating APIs when defined.
    a. The use cases under discussion may justify specifying

Verifier Flow and Scope

Issuing a Verifiable Credential to a Holder requires several logical steps. This section provides guidance on which steps are in scope for this API. **Steps in scope are marked bold**.

1. TKTKTKTK

New Use Cases

TKTKTKTKTK

Andreas' rough idea for some use cases:
u can push a VP to another holder -> I give you my vaccination booklet
or you can pull it from me -> healthcare provider pulls the booklet from a known data store/resource server e.g. CDC

so i can notify you that VPs for you are available and in the response you can define how you want to get to them
1 tell me to send them to you (defined endpoint)
2 tell me to tell you where to get them from

Use Cases from Traceability Vocab UCR (relevant sections **in bold**)

Admittedly, these are more requirements than use cases in the sense of data journeys or flows, but we can expand on them or give more examples in a follow-up! [__juan]

The following use cases outline a number of key scenarios that readers might find useful in a variety of sectors, especially those that deal with cross border supply chain data interchange.

2.1 Steel and Metals

The global steel industry relies on cross-party communication of product and business information to successfully move materials from mines, to manufacturers, through customs, to end customers (such as automotive and construction companies). Today this information exists primarily in siloed paper documents. In the current format it is very difficult to make data comparisons across a small number of parties, let alone across millions of shipments over time. It can also be difficult to catch forged documents in the absence of digital signatures and clearly defined organization data attributes.

A shared vocabulary creates opportunities for steel trading partners to work from a common digital representation of trade information. Take the example of a mill report for a steel product. This document provides important information about the chemical make-up of steel materials, helping to ensure the desired specification and grade have been met. It also acts as evidence about the origins of steel materials. Unambiguous representation of mill report fields is critical for assessing appropriate duties, meeting customer requirements, and ultimately ensuring consumer safely.

By defining the schema for each field, importers can now answer questions like “How many pipes of specification XYZ did we purchase last year?” (i.e., ChemicalProperty). The mill report can also be linked to other trade documentation such as commercial invoices and bills of lading when those credentials are specified and defined. **Regulators can also ask questions across a large number of mill reports** to help catch transshipment issues, such as “How much steel product imported last month specified Vietnam as the country of origin?” (i.e., addressCountry).

Credentials of interest:

- Mill Test Report Certificate
- Commercial Invoice Certificate
- Bill of Lading Certificate

2.2 Food and Agriculture

Several use cases exist for common vocabulary in the food and agriculture space. Key priorities for this project revolve around items that are required for the safe and succesful importation of food to various countries.

The top level AgInspectionReport object has been created as a parent object that allows for the recording of the following inspections and audits, while giving flexibility to account for newly defined inspection types as needs change in the food and agricultre industry. This object can be sub-classed to allow for schema level validation of specific types of inspections and audits as required by the specifics of a given use case. Verifiable Credentials can be issued for this object or sub classes of this object to allow for **external verification by third parties** that are implementing the Verifiable Credentials specification

Farm GAP Inspection Report

Keep track of Good Agricultural Practices (GAP) audits and share results with a vendor

FSMA Inspection

Food Safety Modernization Act inspections and results for sharing with relevant parties, regulatory bodies and vendors.

Foreign Site Certificate of Inspection and/or Treatment

USDA APHIS PPQ FORM 203 that is required for pre-clearance of imported food and ag goods into the US

2.3 Oil and Gas

Oil and Gas value chains are large, convoluted and very dynamic, which in many cases makes tracing back the origin of the product hard and requires a lot of effort. At the same time the industry is subject to regulatory pressures which mandate the production of timely data that has been shown to be inconsistent in many cases.

A common traceability vocabulary enables creation of a common digital representation of oil and gas assets, opening the door to the true digitization of the industry and a variety of use cases. The most immediate application of this digitization would be for the purposes of border clearance and regulatory compliance. Today many importers are overpaying tarifs at the tune of 5 to 11ct per barrel because they are not able to provide evidence of the origin of the oil. By relying on having the asset history, origin, and composition recorded as Verifiable credentials we would be in the position to solve the current challenges and generate many other opportunities.

The asset-specific CrudeOil VC (and NaturalGas VC) object serves as a root object that stores the key attributes of the asset as well as origin and composition. In addition to the asset VC, we are planning to represent key events in the asset's lifecycle (inspection, transportation, transfer of ownership) as Verifiable Credentials.

2.4 E-Commerce

A common traceability vocabulary will allow complex supply chains that import goods to US-resident customers to register individual packages and pre-register products intended for sale to the US with US Customs. For the data needs of Customs to be met by highly heterogenous supply chains that might require much "internal confidentiality" (between supply chain actors), a highly sharded data model is required, whereby many different actors can each submit data points separately that get combined at time of customs processing.

Without strong identification of legal entities (i.e., legally defined and registered supply chain actors) and of products, and without high levels of semantic flexibility, the shards can be quite hard to combine usefully. Linking the registration of individual packages together with the pre-registration of commercial products and actors is the key value-add of this system, but could also be a burdensome request on importers, retailers, and freight forwarders. To minimize this burden, we are aligning wherever possible with the ontology work of GS1 (GTINs and vLEIs), and with shipping and tracking semantics already adopted today by international logistics consortia. We distinguish between the VCs that are issued in relation to a specific package and the contextual information that needs to be queried to validate package information, as well as to make valuable assessments, inferences, and **data quality remediation** on Customs pre-entry data.