Demonstrating the Verifiable Organizations Network (VON)

Introduction **2**

The Conceptual VON Model **3**

The Verifiable Claims Model **4**

The Demo Big Picture **5**

The Demo Component List 5

The Value of TheOrgBook Service **8**

The Presentation **9**

Prerequisites 9

Part 1: The Problem 9

Part 2: Demonstrating TheOrgBook 9

Verifiable Organizations Record Page 10

Part 3: Using TheOrgBook to get Verified Data 10

Part 4: Bootstrapping the Verifiable Organizations Network 11

VON Interaction Scenarios 12

Interaction Diagram: Bulk Load with VON-Loader 12

Interaction Diagram: Enrollment via Verifiable Claim from TheOrgBook - BC 13

Interaction Diagram: Publish a Claim to TheOrgBook Following Enrollment 14

Terminology **15**

Introduction

NOTE: This document is from October, 2017, prior to the creation of the components of VON. For the most part, the vision outlined here has been accomplished - and more.

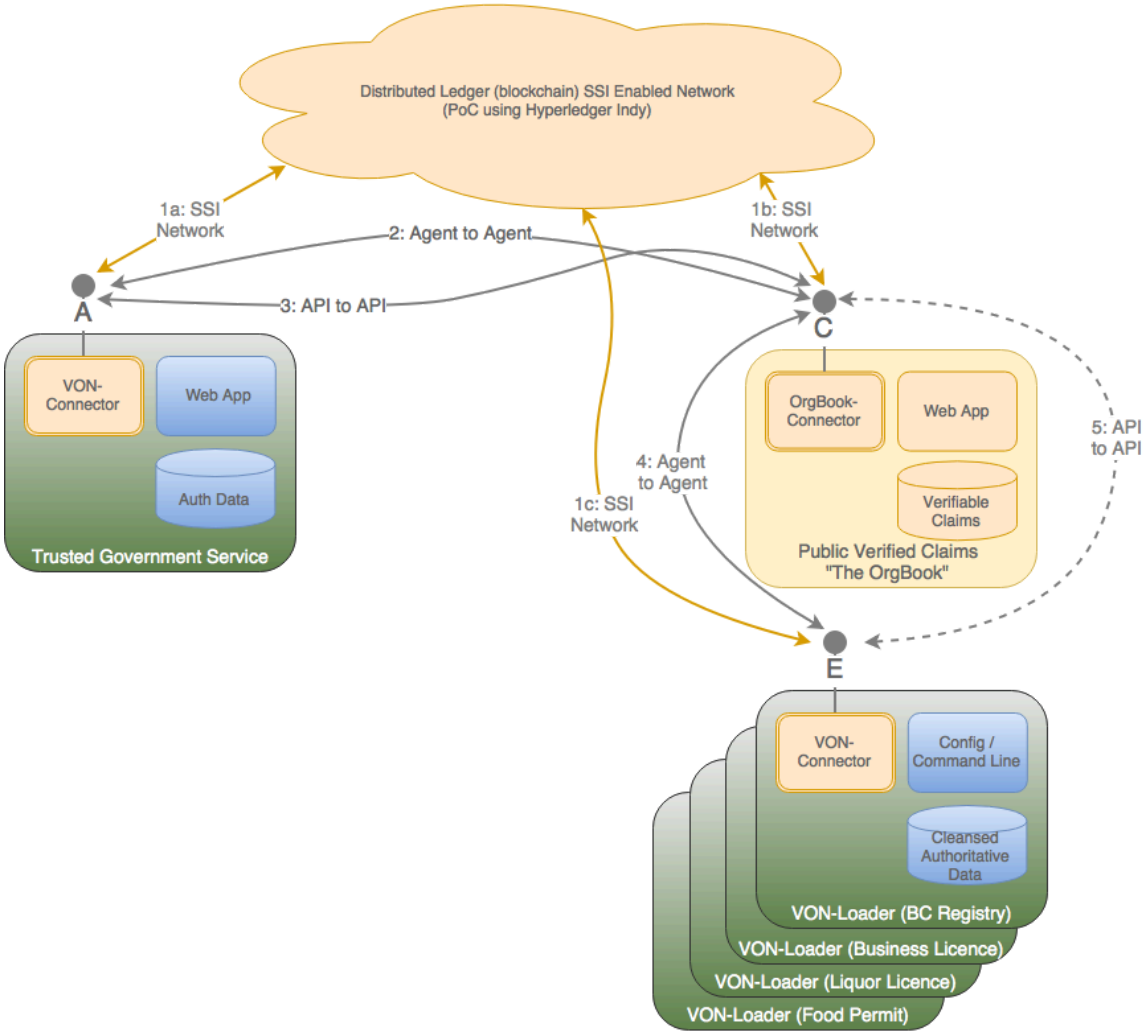
This document describes the demonstration we are planning for the Verifiable Organizations Network (VON) deliverable.

This work and our first demonstration effort is about the discovery, design and development a suite of digital capabilities which moves us closer to enabling a trusted digital ecosystem for BC businesses. The goal of ecosystem is to empower businesses with a trusted digital identity issued by their local government and with which they can conduct their affairs globally. Thus, in our case, the Province of British Columbia aims to locally enable and globally connect its businesses via the digital economy.

In order to achieve this goal, we need to create a new trusted digital network which is globally connected, interoperable, secure, and easy to join. The key elements upon which the VON is constructed are described in the Terminology section at the end of this document.

This document assumes the reader has reviewed the key elements in the Terminology section and has a background in the VON project, including Verifiable Organizations, Verifiable Claims, Self-Sovereign Identity (SSI), the Hyperledger Indy Project, Sovrin, government services enrolment processes, and corporate registration.

The Conceptual VON Model



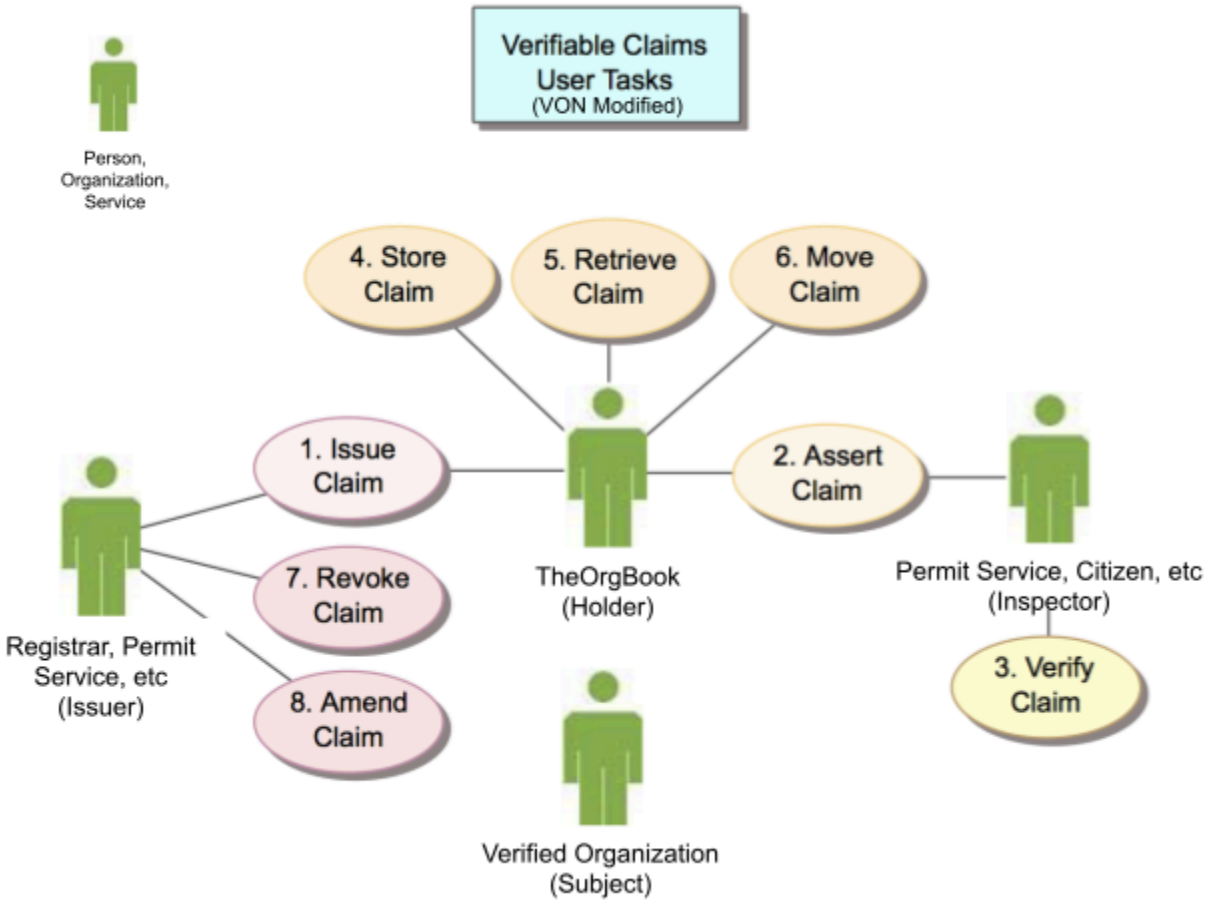
This model depicts the early conceptual model for bootstrapping a Verifiable Organizations Network from existing services each of which contain a list of businesses that have been granted a permission such as a permit, licence, registration and the like. The extended goal of this initial model is to inform organizations of the credentials available to them (digital forms of the permits, licenses, etc.), to encourage them to claim those credentials as part of their own digital identity and then to use them to drive a more secure and efficient digital economy.

As we evolve our understanding of an SSI-enabled ecosystem, we will be able to know if the suggested connections (1 - 5) are required, what flows over them and what claims (data) is stored in what claim store.

The next section depicts the components described in the model above as they will be instantiated for a two jurisdiction, multi-service demo.

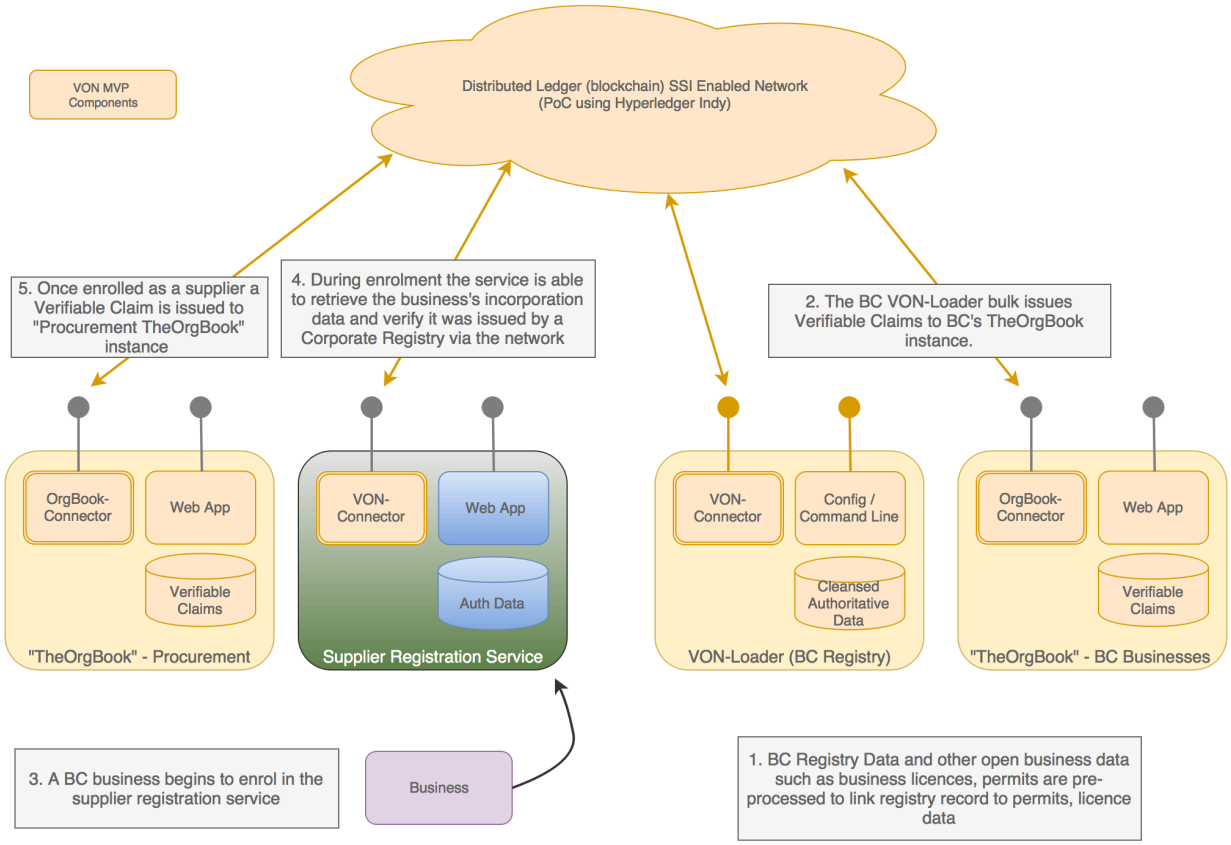
The Verifiable Claims Model

The Verifiable Claims Model depicts the key actors and tasks in a Verifiable Claims based decentralized identity ecosystem. We are exploring the application of this model to the Verifiable Organizations context. Please refer to the Terminology section for how we map this model to the concepts of the Verifiable Organizations Network.



The Demo Big Picture

The following is a picture of what we are building. We're providing the yellow-ish items, while we are assuming the things in the other colours already exist.



The Demo Component List

The following components will be built out to implement the Demo Big Picture.

- **Distributed Ledger**: A blockchain-based ledger supporting Self-Sovereign Identity (SSI) including the issuing of verifiable claims to holders and the verification of those claims by Verifiers. The Distributed Ledger supports the digital signature infrastructure (the identifier registry) of the claims so that the Verifiers can trust the information is indeed from the Issuer of the claim and has not been tampered with by the Holder or any other party. This is an example of the Issuer, Holder, Verifier model described in the Verifiable Claims data standard.
  We'll use Hyperledger Indy for the initial test implementation and could use the Sovrin Network (built on Hyperledger Indy) as we move toward production. Other SSI

compatible networks could be used as trust roots as they become available. Ideally these networks will make use of the interoperability capabilities being developed by the Decentralized Identity Foundation.

- **TheOrgBook**: Is a digital service which provides human and machine readable access to a collection of Verifiable Organizations Records. In our first scenario, these records will pertain to a legal entity incorporated by the BC Registry.

  TheOrgBook service is:
  - being created as an Open Source project.
  - a Self-Sovereign Identity enabled service (contains an agent which provides connectivity to the SSI network and to other agents in the ecosystem).
    - The test version is being developed using Hyperledger Indy as the trust root network.

  We will build TheOrgBook as an open source project providing a capability for digital credentials providers - particularly governments - who may wish to create a public repository of Verifiable Claims about "real world" entities in a defined domain. Examples of such domains are organizations, land parcels, or perhaps logical "entities" such as "procurements" which are comprised of a number of records that together form the logical entity. In the case of a procurement, the records would be Request for Proposal, questions and answers, bids, awards, contracts, invoices which all linked together to form a "procurement". (as described in the Open Contracting Standard) A "procurement" could be a set of linked Verifiable Claims.

  It is envisioned that TheOrgBook will facilitate the owner (or authorized representative) of a Verifiable Organizations in establishing their own Self-Sovereign Identity through the collection of public Verifiable Claims found in TheOrgBook. Each of these collections necessarily point to the services the newly minted Verifiable Organization had been issued (the list of public DIDs for the Issuers).

  In our demo, we plan to have the following instances of TheOrgBook:
  - **'TheOrgBook" - BC Businesses**: A repository of BC Verifiable Organizations. This repository will:
    - will contain an initial Verifiable Claim from the BC Registry which establishes the foundation for a Verifiable Organizations
    - store public Verifiable Claims linked to a Verifiable Organizations (e.g. permits, licences, contracts)
    - provide a UX and API for searching the set of Verifiable Organizations and their linked Verifiable Claims
      - include the ability to search the directory in a variety of ways, such as by Legal Name, type of claims held and location - e.g. "Find me the licensed establishments within 2k of Joe's Panama Pub".

        - provide a UX and API for display of a Verifiable Organizations Record page for each grouping of Verifiable Claims linked to the Verifiable Organizations foundational Verifiable Claim
        - provide the ability to cryptographically verify the claims contained in a Verifiable Organizations Record on demand via the UX or an API

    - **"TheOrgBook" - Procurement**: A repository of Government of Canada Procurement-related Verifiable Claims
        - will contain an initial Verifiable Claim from the Supplier Registration Information Service which establishes the foundation for a Verifiable Organizations in the Government of Canada procurement context
        - will link the initial Verifiable Claim for the supplier to a Verifiable Claim from a trusted source such as the BC Public Verifiable Claims Service (an incorporation Verifiable Claim issued by BC Registries)
        - store public Verifiable Claims linked to a Verifiable Organizations (e.g. contracts, awards)
        - provide a UX and API for searching the set of Verifiable Organizations and their linked Verifiable Claims
        - provide a UX and API for display of a Verifiable Organizations Record page for each grouping of Verifiable Claims linked to the Verifiable Organizations foundational Verifiable Claim
        - provide the ability to cryptographically verify the claims contained in a Verifiable Organizations Record on demand via the UX or an API

- **VON-Connector** is an Open Source project (to be created on github) providing a generic SSI-aware agent for a Government Service wanting to connect their digital service to the Verifiable Organizations Network (as defined here). This allows the Service to create secure peer to peer (agent to agent) connections with one or more instances of TheOrgBook, and other VON-connected digital services. Each digital service (Supplier Registry, BC Registries, etc.) can use it's own instance of VON-Connector to interact with instances of TheOrgBook to create/update Claims about organizations, and to request proofs about organizations from an instance of TheOrgBook. The VON-Connector will also enable service to service communications for the secure exchange of Verifiable Claims. In our demo, we plan to have several instances of the VON-Connector
    - **Supplier Registration:** To request proofs from the BC Public Verifiable Claims repository about a BC Verifiable Organizations and to push Claims to the PSPC Public Verified Procurement Claims repository.
    - **BC Registries and other BC permitting services**: To create claims to be pushed to the BC Public Verifiable Claims.

- **VON-Loader** is configuration or mode of the VON-Connector that helps a Government Service bootstrap it's use of an instance of TheOrgBook by providing a capability to bulk

load existing Claims. There may be a set of utilities to correlate claims to the foundational claims, and to use the bulk load capability of the VON-Connector agent to push those claims to the appropriate instance of TheOrgBook. Some legacy services may make use of this capability to bulk load claims on a schedule if it proves challenging to modify the service to issue claims via the real-time API mode.

The Value of TheOrgBook Service

What differentiates TheOrgBook from existing directory services with similar data about entities is that it includes a collection of public Verifiable Claims about the listed entities. The case we are describing in this document proposes entities as legally incorporated organizations, and registered suppliers to the government. However, as mentioned earlier in this document, it is conceivable that there could be multiple instances of the “TheOrgBook” even within a single jurisdiction if there is the concept of a “foundational” Verifiable Claim to which other Verifiable Claims (or just data) could be attached. Land Parcels seems to be a logical example of a potential foundational entity. The key idea is that there is value to the transparency and trust enabled by having Verifiable Claims pertaining to an entity made available and attested to by trusted issuers.

There are two important characteristics about TheOrgBook:

- TheOrgBook contains Verifiable Claims which can be verified. Verified means that the data they contain is what was originally issued (immutable - cannot be tampered with) and that the issuer of the claim can be confirmed and the claim can be checked for revocation. This capability is a result of the digital signatures that are applied to the claims using the HL-Indy capabilities. It is then up to the user of the Verifiable Claim to decide if they trust the Issuer. Since we’ll be accepting Verifiable Claims from Government Organizations, most users will trust the claim issuers, and therefore, the claims.
- A Government (or even a non-governmental) Service that needs to collect information about an Organization in order to do business with that organization can use TheOrgBook to get Verifiable Claims which they know is from a trusted source. They can use Hyperledger Indy software to automatically collect that information.

In the future, we expect to extend the functionality of TheOrgBook to allow the Verifiable Organizations to find their own Verifiable Claims to expedite the process of getting those claims issued from the services directly. At that point a VON Enabled Verifiable Organization would be in possession of their own set of Verifiable Claim pertaining to their organization which would enable them to use any other Self-Sovereign Identity-enabled services. We hope to use this single-user mode strategy to bootstrap a network effect which will encourage the use of Verifiable Claims across the economy.

The Presentation

Prerequisites

- The components deployed to accessible environments. We expect all of the components except the SRI application/agent to be running in the BC Government's OpenShift environment. The SRI application/agent will be running in the Dev or Test environment for the new SRI application.
- Pre-process records from various sources in the BC Government to match data with the BC Registries records. This ensures that the database will contain good data to demo - organizations with multiple claims.
- Load TheOrgBook/BC Instance with claims created from data from the BC Registries and several other public licensing/permitting sources, with the claims matched to common Verifiable Organizations.
- Load TheOrgBook/PSPC Instance with claims created from SRI data.

Part 1: The Problem

Discuss the problem that exists and the solutions we are proposing to eliminate that problem. Talk about Self-Sovereign Identity as it relates to both people and organizations. Talk about the particular challenges with Verifiable Organizations - the need for an ever changing cast of characters to act on behalf of the organization in a digital world. Talk about the need for the Organization to control that delegation of authority without having to visit every website in the world with which the Organization is doing business.

Talk about trust on the Internet and how it is achieved.

Part 2: Demonstrating TheOrgBook

Use the Web Interface for the TheOrgBook to demonstrate the discovery of and subsequent drilling into a Verifiable Organizations Record:

1. Query the database by Name
2. NTH: Navigate the database by searching by Claims Held By or Location matching that of a found record.
3. Drill into a Verifiable Organizations to see its summary page and list of Verifiable Claims (see below)
4. Drill into a Verifiable Claim to see the information collected about the Verifiable Organizations that has been provided by the Issuer.

5. NTH: Demonstrated and active verification of the Claim - e.g. something like this from the OpenBadge standard (click on the View button).
    a. Show graphic and CLI-esque view at same time?
6. FUTURE - onboard organization to assist it in gathering its claims.

Verifiable Organizations Record Page

Part 3: Using TheOrgBook to get Verified Data

An existing Government Service - in this case the Federal Government's Supplier Registration - is extended to allow a person enrolling an organization in the service to use a Verifiable Claim data from an instance of TheOrgBook. Once the service incorporates the Verifiable Claim into the rest of the collected data and the enrollment processes successfully completes, the Service creates and writes a new Verifiable Claim to an TheOrgBook instance.

1. Create an account on the Service Website as a new user representing an organization.

2. Enter some data such that the Service knows the organization is likely in a known instance of TheOrgBook and an identifier it can use to find the organization.
3. Request a Proof from TheOrgBook instance.
4. Receive back the information to fulfill the Proof - a claim about the organization being enrolled in the service.
5. Enroll the organization into the Service, including creating and pushing a Verifiable Claim into an instance of TheOrgBook.
6. Go to the instance of TheOrgBook and search for and find the newly created Verifiable Claim.

Part 4: Bootstrapping the Verifiable Organizations Network

While there are many uses for instances of TheOrgBook, the ultimate value of the VON wil be realized when organizations collect and use the Verifiable Claims about themselves to conduct digital business transactions. For example, when opening a bank account, rather than showing the paper associated with incorporating with BC Registries, the Bank can request Proof of BC Registries enrollment and the organization can supply directly the Verifiable Claim from BC Registries.

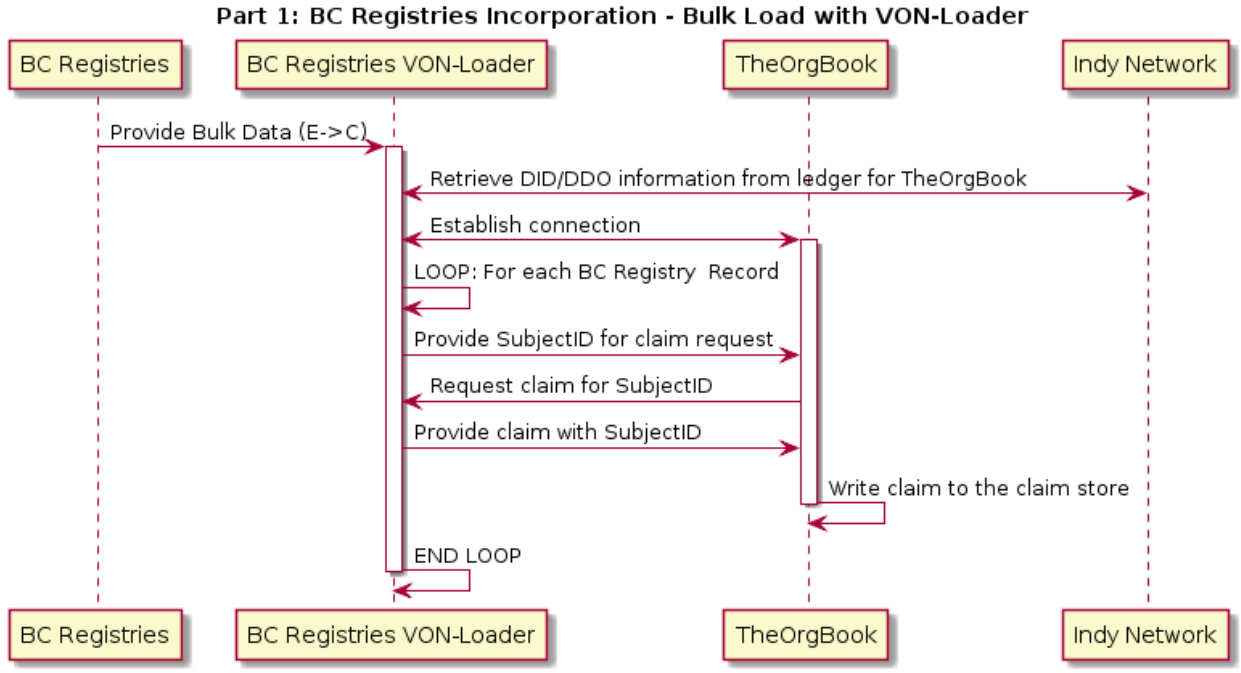
TheOrgBook can bootstrap this process by helping Organizations find what claims they have available, and directing the Organization to the issuing Service. From there, the Organization can provide the necessary digital proof of who they are, and receive back their own instance of a Verifiable Claim. As more business establish their Self-Sovereign Identity, more Services will become Self-Sovereign Identity-aware, and the virtuous cycle will repeat until online digital transactions become the norm. Or at least, that the plan. And when that happens, the problems described in Part 1 will be solved.

VON Interaction Scenarios

Interaction Diagram: Bulk Load with VON-Loader

Aside: You can use the PlantUML Gizmo google doc add on to edit these diagrams.

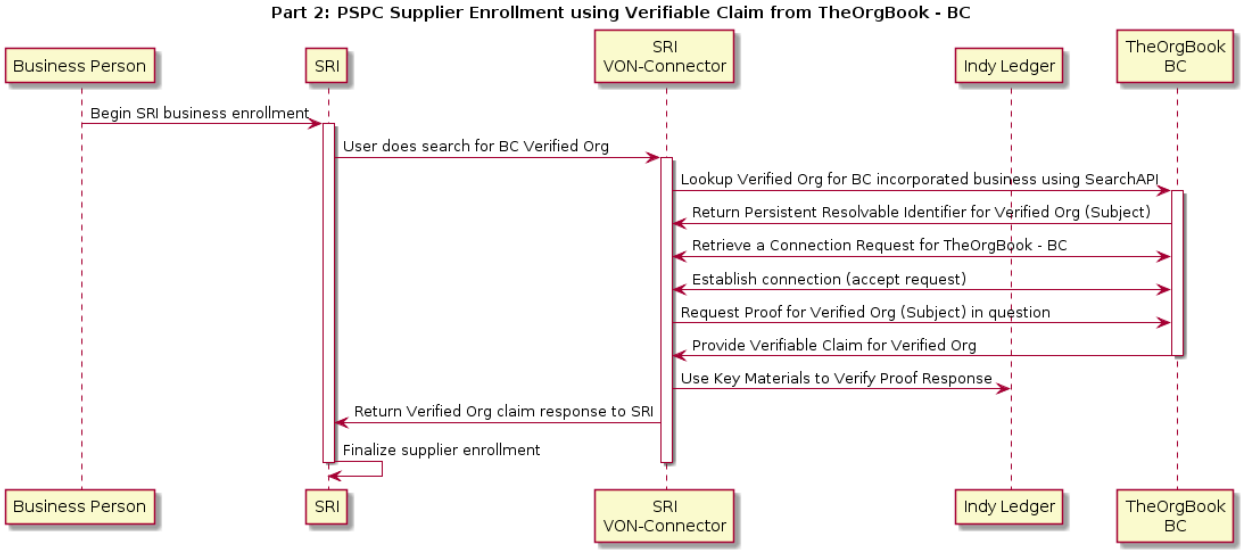
Bulk loading existing claims from the BC Registries to TheOrgBook (BC Instance). Iterate through the current registration and for each incorporated organization, notify TheOrgBook that a claim is available for the SubjectID (e.g. an incorporated organization), which triggers TheOrgBook to request the claim for that organization. Once TheOrgBook has the claim - write it to the Claim Store.



This process would be run (via Command Line, for now) for each of the BC Services for which we want to load claims into TheOrgBook. Note that the data from all the sources must be aligned with the foundational claim we are using for TheOrgBook - the one from BC Registries. For a production use of this system, the data cleansing and alignment effort will be a challenge.

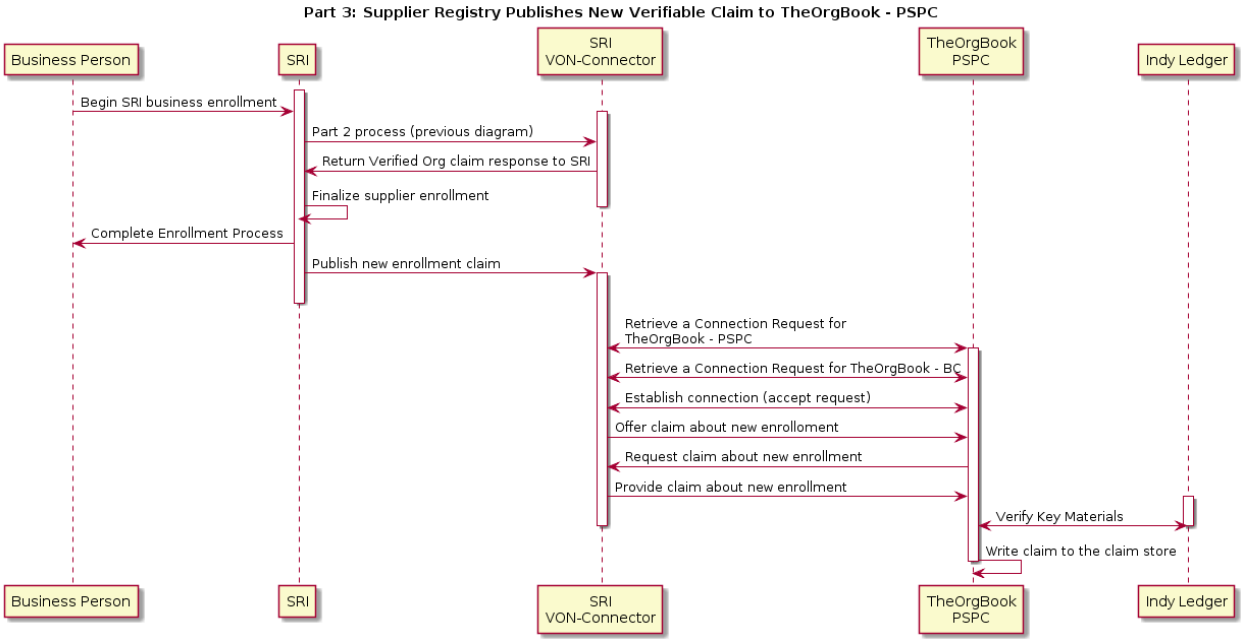
Interaction Diagram: Enrollment via Verifiable Claim from TheOrgBook - BC

A business person is interacting with the Supplier Registry (SRI) site to enroll their organization as a supplier. In doing that, information is needed about the organization that is available as a Verifiable Claim from BC Registries via TheOrgBook - BC. When that data is needed, and the user has identified the Organization sufficiently, send a Proof Request to TheOrgBook, which will use the Claims about the Organization to respond to the Proof Request. SRI will verify the claim, including checking for revocations, and if all is correct, use the claim to populate the data required for enrollment.



Interaction Diagram: Publish a Claim to TheOrgBook Following Enrollment

Following the previous enrollment interaction (summarized in this diagram), SRI makes the resulting Verifiable Claim available to TheOrgBook - PSPC, a repository of Federal Procurement-related organizations and claims. TheOrgBook - PSPC requests the claims, verifies the key materials and saves the claim.



This pattern would be used for many Services interacting with instances of TheOrgBook. For example, after the bulk loading of the existing claims held by the BC Registries, BC Registries would publish new claims to TheOrgBook - BC as new organizations are verified.

Likewise, the other BC Services that published to TheOrgBook - BC (e.g. from the Big Picture Drawing - Business License, Liquor License, etc.) would use both of the interaction diagrams here (2 and 3) to first use the BC Registries Verifiable Claim during the enrollment process, and then to publish new Verifiable Claims to TheOrgBook - BC.

NOTE: There are other interactions between the Services and TheOrgBook instances that we are anticipating, but are not covered here. Those include (at minimum) replacement of time-limited claims, revocations, and updates (which are likely - revocations and the issuance of a new claim). TheOrgBook could play a crucial additional role as Publish/Subscribe service for loosely coupled systems - notifying other systems when Claims information about organizations change.

Terminology

1. **Verifiable Claim**: A machine-readable statement made by an entity that is cryptographically authentic (non-repudiable). (Source: W3C Verifiable Claims Working Group Charter)

2. **Verifiable Organizations**: A Verifiable Organization (in TheOrgBook service's context) is a legal entity for which a Verifiable Claim has been issued by an authority empowered by law to create legal entities. (Reference: Pan Canadian Trust Framework: Verifiable Organizations Standard) An example of a legally empowered authority would be a federal or provincial corporate registrar. There may also be one or more further Verifiable Claims issued by authoritative services such as permits, licences, contracts, accreditations, etc.

   In terms of the Verifiable Claims model and in the context of TheOrgBook, a Verifiable Organizations is a "Subject".

3. **Verifiable Organizations Record**: A collection of Verifiable Claims about a single legal entity (Subject). The first and foundational Verifiable Claim MUST be issued by a service which is a part of the Verifiable Organizations Network and can issue Verifiable Organizations claims.

4. **Verifiable Organizations Network**: A trusted digital network which is globally connected, interoperable, secure, and easy to join. Active members of Verifiable Organizations Network include one or more "TheOrgBook" services and one or more digital services which are able to issue and/or request Verifiable Claims pertaining to Verifiable Organizations.

5. **TheOrgBook**: A digital service which provides human and machine readable access to a collection of Verifiable Organizations Records. In terms of the Verifiable Claims model, TheOrgBook is a "Holder", however it is a Holder of Verifiable Claims pertaining to Subjects other than itself.

   In our first scenario, a legal entity is an incorporated organization. There could be other types of legal entities which could be added to the Verifiable Organizations Network such as partnerships, societies/non-profits, sole-proprietorships, enacted legal entities such as municipalities, ministries, universities, crown corporations and the like.

   Organizations could be a "Verifiable Organizations" in a particular context … for example … within the tax realm if they have been issued a Business Number (in Canada) or within the Government of Canada procurement realm if they are a registered supplier. It

is up to each realm to determine what the necessary evidence is for it to consider an organization to be verified. One realm could certainly rely on another. For example, the supplier may need to be a legal entity of a certain type (corporation) and therefore need to have a Verifiable Claim attesting to such a fact.

TheOrgBook name references the beginnings of Facebook (originally “The Facebook”) which started as a simple directory of published information about and for students at Harvard. This “single-sided” strategy is a possible way to bootstrap a network effect as described in this presentation by Andreessen Horowitz.