# Company ID Proof of Concept Project Summary Report

**12.2.2021**

Contributing partners

VERO SKATT

vastuu group

---

With advisory partners from

# Executive Summary

Aim of this project was to find a way to issue a secure, digital company ID for an existing foreign company, so that it could be used in further conduct of company's business in Finland. Lack of this kind of digitally verifiable ID causes inefficiencies in many business transactions as companies' backgrounds and statuses are validated through manual work. In order to demonstrate operations using this digital identity, a method to issue credentials as a digital notary was designed. In this perspective the digital foundational company identity includes thereto linked, contextual credentials.

This report gathers together the key findings of a short proof-of-concept (PoC) project executed over second half of year 2020. Terminology used and elaborated is defined in Appendix A – Glossary. Documented PoC demonstrates and evaluates issuance of self-sovereign company identities and company wallets by a novel **Notary service** that is hosted outside of the official government-managed company ID registries. After receiving the basic (foundational) digital identity a company is then able to hold and use related **verifiable credentials** issued to their wallet to acquire other similar digital documents from other issuers (see Appendix B for details).

Selected use case was about **establishing digitally an existing foreign company onto Finland** as a locally recognized entity, equipped with digitally verifiable electronic company identifiers and other certifications required to demonstrate legal compliance against local employer regulation - in real-time. This compliance means proofs of having a registered presence (local business ID and VAT number; and, e.g., status of company's possible tax debt towards local tax authorities. Required employer registrations are left for the next phase of the project.

Project was arranged by Finnish Tax Administration and Vastuu Group and advisory comments from OP Bank as a Findy consortium member. Use-case innovation and legal evaluation included use of business and product management from the involved parties. Legal expertise was acquired from Finnish Tax Administration and via a parallel project's legal studies conducted over company data related regulation. Execution of the project's demo was handled mostly by Vastuu Group's and Finnish Tax Administration's software architects and experts over period of summer-autumn 2020.

**Table of Contents**

# Concept Overview

Digital business transactions ideally would require all parties of the transaction to be adequately identified and verified against local business compliance. We are introducing a **digital company ID and a company wallet** as a tool to use such ID as the acceleration mechanism to handle compliance requirements for existing legal entities about to enter Finland for business.

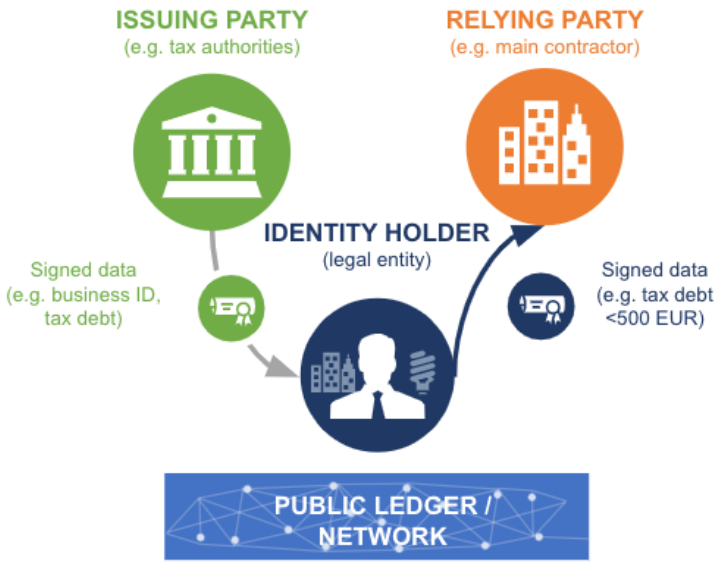


Figure 1 – Deploying self-sovereignty to company attributes and wallets

Any entity meeting the entry criteria for conducting business in Finland (local or foreign) are notarized through digital entry with a digital ID and other claims that let the **business onboarding and compliance related transactions** to be finalized and logged (in majority of cases) in real-time. This happens via a digital transaction instead of concurrent process that still means, e.g., queueing in person at Finnish Tax Administration's' or Company Registries' offices physically in Finland.

Natural persons authorized to act on behalf of legal entities are still the actors utilizing the digital notary service. After authentication and validation of their representation rights they manage the company IDs through a digital company wallet, that in this scenario is hosted by the same service that provides the digital notary function.

# Concept in Detail

## Current process

Legal persons and sole traders (later 'companies') don't have an anchored, public digital presence or identifier on the Internet, if you don't count a company's digital SSL certificate (usually representing the company's official web site) as one. Legal presence of a company in a particular target jurisdiction/region is acquired through a long, multi-step process that means at least applying for a local business ID and may include hiring a local representative to the company to act on its behalf.

To operate at that new state the legal person may have to apply for registration in local tax registry. This may be included in aforementioned process or be an additional one: Tax number for a company may be the same number as in trade register (Finnish TIN; in Finnish 'Y-tunnus'), nevertheless in some states all tax registrations may have their individual number to be used only for this particular tax type - e.g., in France tax registration number differs from trade registration numbers.

Foreign natural persons may act digitally on behalf of a company once their role and identity have been validated through proper authentication and may include a control of the person from the source state register or a certificate represented from source state indicating a status (a copy of passport or TIN). Currently, this may be a manual process using copies which cannot be verified at the point of registration but may be verified later if needed and if this source register is (from practical perspective) available. Note that this is often not possible automatically due to missing formal links or other connections between target and source country registries.

There does not exist a general concept that an organization would have a 'digital twin' on the Internet, with verifiable information about the organization, its legal representatives and permissions & certifications available for other businesses and digital transactions. At best, the required company information is held in various digital registers in data format defined only by that single register, and e.g., representative data can be checked from these via the relying parties, but it may be ambiguous and unreliable when or if the data has been properly updated.

Good example of a trusted register holder and service provider is Vastuu Group and its partner ecosystem where all member companies' (licensees, partners) data is collected and managed centrally by the organizing body and offered out as PDF records and/or as machine-readable data served through an API to the ecosystem members. Verification and validation of company information is done periodically to guarantee up-to-date data, after validating first time at time of onboarding, done usually in manual fashion using digital interfaces to official source registries and

databases where this is possible. Example of such is the current Vastuu Group's Reliable Partner (Luotettava Kumppani)[1] service, where data acquisition and enrollment may include up to 15, more or less manual, steps.

## Proposed new process

An approach named self-sovereign identity (SSI) has become a proposition as next-stage evolution of identity management, typically covering authentication and handling of identity and other personal data in case of *natural persons* (humans). SSI is a tool for entities to hold and represent data about themselves in different contexts, using cryptographic information in form of verifiable credentials (VCs). That is, cryptographic containers backed (issued at a given time) by digital issuers, but only used by the entities themselves through their sovereignly held 'identity wallets' when they interact with relying parties. Issuers are responsible for issuing credentials against their policy and taking care of credential revocation and information necessary to allow verifiers to conduct revocation checks.

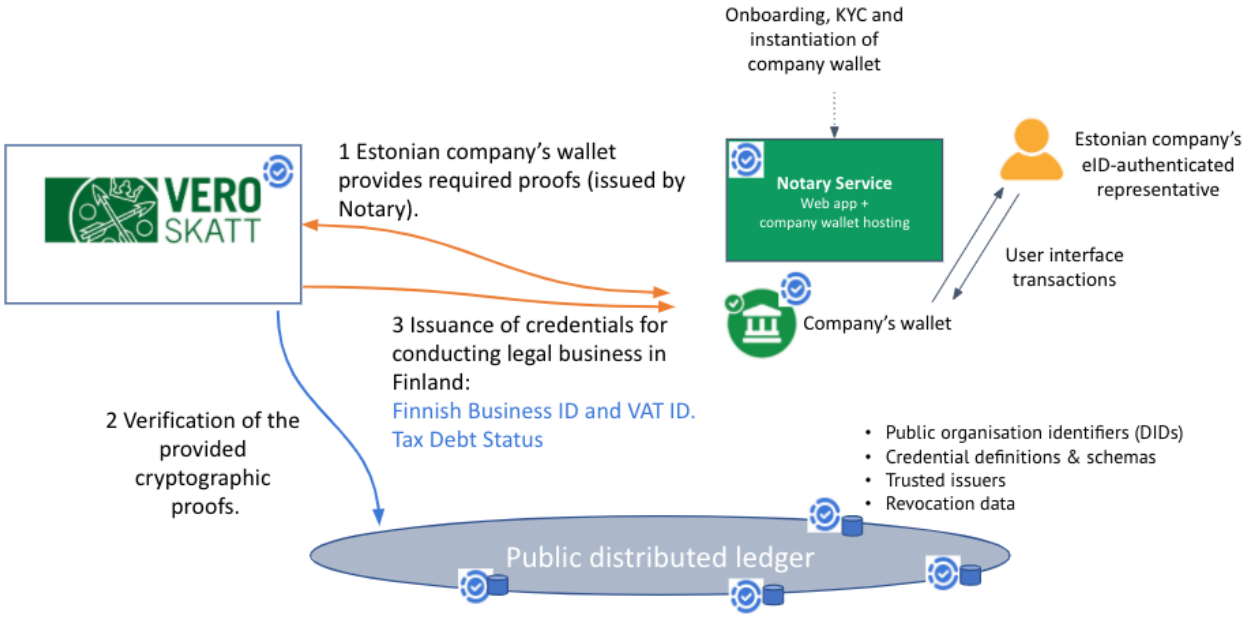


Figure 2 – simplified overview of the actors and new process tested.

The technologies and frameworks harnessed to implement the new process were:

- A developer package implementing a cloud agency for hosting organization agents and company wallets + enabling Hyperledger Aries -compatible peer-to-peer communications between Issuers, Verifiers and a Holder
- Sovrin Staging Network (an available global test network) for storing the credential definitions and schemas in a stable Hyperledger Indy network

[1] https://www.vastuugroup.fi/fi-en/our-services/reliable-partner

- An API sandbox from Finnish Tax Administration providing their data in JSON format which is converted to Hyperledger Indy compatible verifiable credentials within the API-to-agent integration component of the issuer

Technical, detailed overview document of the architecture & design is available upon request.

Through this process, different legal entities - or communities on their way to become associated as a formal legal entity one day - are equipped to hold their digital, verifiable data through similar setup, i.e., possess a company wallet with VCs issued to the company, the legal entity. Generalizing, one single organization wallet structure may cover all necessary entity types (NGOs, foundations, associations, sole traders) not restricting registration only to trade registration).

The pre-existing company data and verification process (KYC) required against acquiring an identity credential is derived by the use case and organization type at hand. This project used as KYC prototype the process which parties already have agreed and authorized between Finnish Tax Administration and Vastuu Group (both have real-time connections to neighboring states company registries for fact and representative rights validation).

Hosting the company IDs and wallets happens herein by a novel Notary service, which acts as a new service element between company registries in different countries and the business organization. Notary authenticates the company's legal representative/s, offers a wallet-as-a-service hosted in the cloud and helps the foreign company to get the initial verifiable data onto their wallet (conducts the agreed KYC process). This data can later be used with Tax Authorities and compliance certifying services like Reliable Partner to acquire more credentials over time.

Note that the company's anchor identifiers in different countries' company registries become formally (and cryptographically) linked through the use case, helping to recognize the legal links between company identifiers (here Business IDs) that have been issued to it in different countries.

# Use Cases

We implemented a three-phase case of onboarding a registered foreign company to hold a wallet and upon automatic request by Notary be registered as taxable person (issued with necessary tax authorities' verifiable credentials) to conduct taxable operations in Finland as a registered entity. Use case completes with issuance of a cryptographic version of company's Reliable Partner status report which relies on validation of all previously acquired credentials presented to the verifier as proofs.

To reach the end goal, digitally verifiable status as Reliable Partner, a company needs to hold and present proofs that they are indeed an existing company, have a valid local Finnish business ID, Finnish VAT-identifier and proof of tax debt status. Currently all this is collected step by step and often manually, from different foreign or national registries consuming resources and everybody's time, though some of the data is available conveniently through digital interfaces already. Furthermore, it may be unclear to parties requiring data when or if the data has been updated. For business transactions reliable real-time status is essential.

The three steps are:

## Step 1 - Offering a company wallet

- Vastuu Group's enrolment of foreign companies is extended to offer a digital wallet for accelerated and trusted entry to local markets.
- Company's representative is authenticated with eID, and checked for their rights to act on behalf of the entity
- Company enters through its representative agreeing to the terms of the service to use the Notary service, where the KYC system helps them to acquire first credentials issued by the service (operated by Vastuu Group). The entrant's digital wallet is instantiated at this point, and it is provided with a public identifier in used local public ledger / trust network.
- If the digital background checks about the company status succeed, a base compliance credential 'CompanyID' is issued to the wallet by the notary. This credential states the facts verified from the company's home country registries.

## Step 2 - Issuance of Finnish Business ID+VAT number, and tax debt status

- Wallet user is proposed to establish a connection with Finnish Tax Administration (a credential issuer, a role in context of used public distributed ledger) and to request the credentials available: previously non-existent Finnish business ID that links the origin ID to new local one, VAT number and status of company's tax debt situation. Use cases include such registrations which are handled by Finnish Tax Administration, such as registering a foreign company in Finland without established subsidiary (in Finnish: 'kiinteä toimipaikka' and 'ulkomainen yhteisö'). In these circumstances it is essential for the Finnish Tax Administration (as well as other notaries) that the link to the source register (use case includes this time Estonia's Äriregister) may be created automatically and in real time, instead of manual verification or a batch verification at a later date.

### Step 3 Reliable Partner membership (Vastuu Group)

- A credential is created based on the company's eligibility to a Reliable Partner status, issued against presenting the necessary credential-based proofs via the company's wallet (which have been acquired in earlier steps 1 and 2).
- Regarding the trust position and legal authority of the proposed set-up, the authority to issue a Reliable Partner certification is based on an (existing) bilateral agreement and a power of attorney given to Vastuu Group to fetch and publish the data needed to form the concurrent Reliable Partner report and status.
- URL link to the full Reliable Partner report in machine-readable format is attached to the credential (In the proof-of-concept, only the Reliable Partner membership status is shown, without specific interpretation information & URLs pointing to this information).

From the Finnish Tax Administration's point of view a successful completion of this process supports business operations of such companies which have been properly registered and have submitted tax returns in both states (use case Estonia – Finland).

## Use cases to be implemented later with the piloted system

### Unregistered association as a digital actor

Additional credential types were suggested and created at definition level for scenarios where authorized person/s of an *entity still in to-be-incorporated status* (in Finnish 'toimiminen perustettavan osakeyhtiön nimiin' or similar) or an informal group of people (say a hobbyist jazz group renting a training facility from a city) need to make binding digital transactions within the trust network.

Defined *Unregistered Association* credential is something the notary service would issue to a natural person/s that are acting on behalf of the entity being registered (see Appendix B) after the person enters the notary service with aforementioned goal (doesn't represent any officially registered entity). Power of available transactions within the trust network would be limited for such association's wallet holder, due to missing the formal entity registration status. Such credential could be used by its holder to conduct limited range of legally binding transactions with help of its Notary-hosted digital wallet, though it doesn't (yet) have a formal status of a legal person.

Acting as unregistered association would offer also a limited-powers mechanism for foreigners willing to set up a new company in Finland to familiarize with Finnish business services & compliance requirements remotely – initiate certain processes without a formal business ID and establishment decision already in place and registered in the Finnish Registration Office.

## Accident and liability insurance certificate

The full status of Reliable Partner includes statements about company insurance coverage for employee incidents at work and liability in case of incidents related to business relationships and conductance. Issuer/s for these are insurance companies operating in target jurisdiction or offering international coverage.

- A company needs to acquire proof of their active insurance and necessary details as a verifiable credential (one for each insurance type) through a transaction with Notary, that proxies as the issuer for the insurance companies.
- These are used as atomic proofs, e.g., to acquire an extended/updated version of the earlier issued Reliable Partner status credential.
- Proxying would be legally enabled through a power-of-attorney agreement between the insurance companies and the notary. Additionally, the parties would have to agree a governance agreement that declares their duties and positions in the trust network wherein the proxy function is present.

## Occupational healthcare certificate

Organizing occupational healthcare for employees becomes mandatory in Finland as you employ your first employee. Acquiring certificate of an active healthcare agreement with a provider is a natural case for a verifiable credential. Many providers are however small non-IT savvy companies spread wide across the nation. In this situation the Notary service is a natural trusted proxy which can include issuance of occupational healthcare certificates to their portfolio. Business case analysis for the case would suggest the healthcare providers could join the partner program and be ensured the notary issues the certificates against a small annual fee that would cover the work required in screening the certificate status from small providers.

## Employee Pension Insurance certificate

Employees and entrepreneurs (full-time owners with high-enough ownership of shares and enough paid income) of a company need to be insured for mandatory pension insurance ('TyEL' and 'YEL/MyEL' in Finland). Insurance companies could issue the existence of insurance and no-payments-due status, and if necessary (YEL), the per-person coverage limits as verifiable credentials. Companies already issue these in non-cryptographically verifiable form (PDFs) via their customer portals & email, so a transition to VCs would be a logical step forward.

## VAT related credential possibilities

VAT is a transaction-based tax. Therefore, credentials are needed to design from transactions because they may offer supporting data to confirm transaction's tax status. On the basic level credential confirms registration status, but in future it may be designed to support other kind of transaction types.

Taxable persons registered for VAT[2] have to charge VAT on sales and therefore may deduct it from their purchases (VAT due from invoices). From practical point of view the VAT registration may offer business advantages for a company and therefore the need to register for VAT should be carefully analysed when setting up a business in Finland.

Credentials relating to VAT could include following credentials:

- *VAT registration valid at the timestamp of request*, issued by a notary. This is a status-indicating verifiable credential of Boolean type (registration valid or not: true - valid/false - not registered).
- Additional attributes may apply either within the VAT registration credential or as separate credentials - registration valid since this date, existence of a tax warehouse agreement and registration for leasing of immovable properties. Also, tax free sale to consumers could benefit from credential-based verification procedure. At the moment procedure is based on manual work of all parties.
- International trade could benefit from basic verification procedures which could include other data than just VAT registration number and tax debt: e.g., *customs registration number* and *AEO/EORI status*.
- Proposed issuers of credentials include Finnish Tax Administration and Finnish Customs. Depending on the use case Notary node requests correct combination of credentials.
- More advanced credentials for the future could include several approaches. One smart contract -based approach could be *confirmation of exempt transaction*. This has been concepted and tested as a possible smart contract procedure within a Kela/TietoEvry smart money project[3]. Second approach could include VAT specific data shared by a legal person, confirmed and signed digitally by the Tax Administration.
- Other tax related registrations issued as verifiable credentials scheduled for next phases include *registration as an employer* (in Finnish 'työnantajarekisteri') and *registration for withholding tax* (in Finnish 'ennakkoperintärekisteröinti').

[2] On requesting registration for VAT in Finland

[3] https://medium.com/kelalab/experimenting-with-smart-money-f645512aeb8e

# What We Came Across - List of Questions, Ideas and Issues

The PoC and its analysis revealed points for concern and ideas for further development. These are collected under this section.

**Open question for further development: Presenting up-to-date VC?**
How to confirm for the verifier of the verifiable credential that presented data is still valid, and is properly and timely updated (that is, the holder is presenting most current version of such credential)? This becomes a question with registrations and other issuances that don't get revoked but are refreshed over some time.

With contemporary approach, there are two channels to retrieve validation data. First is to use direct access to issuer which often requires use license or registration. Second one is an approach where company itself takes manually an extract from its' tax data. The latter approach is not in any way confirmed data in the eyes of a third party. On a general level, the preferred method should be designed such, that the source of the data (issuer) confirms and shares the data from the original source and indicates the 'this is the latest available update' information as credential metadata – without introducing to the verifier a need to poll the issuer directly for actual credential verification.

**Interim solution:**
In this proof-of-concept use case all data is verified in real time from the source register before issuing it as a verifiable credential. A third party using the data verifies the credential's status from a distributed ledger. The used SDK to realize verifiable credentials and wallets supports a (so-far non-standard) method to ensure that the version of the credential presented for a relying party is the most recent version of the credential to guarantee all updates.

**Serving Companies or entities without a formal authoritative registry**
It is not possible for the Notary to ensure electronically its right to create and maintain the digital identity for an entity (company) unless there exists a registry for the entity type in question. Most entity types do have a registry and a TIN registered therein.

Company forms that do not currently have public registration entry:

- Unregistered associations
- Foreign organizations without a local Trade Register Extract

However, it is desirable that also such associations should be able to conduct limited-power transactions in the digital trust network, after they have been established with the '0-level' presence in it.

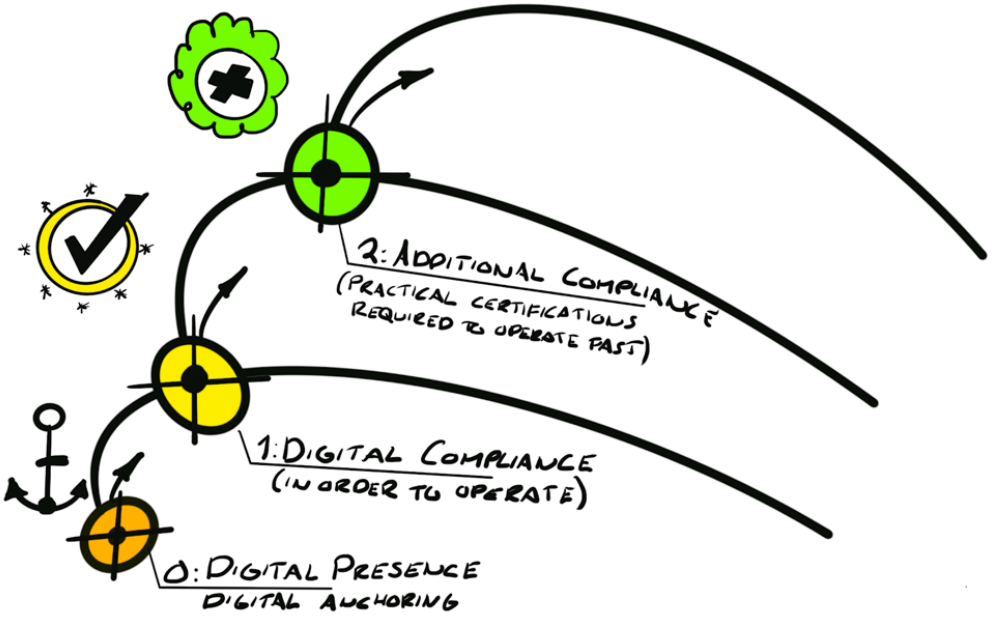


Figure 3 - Digital anchoring and presence would enable limited-power operations also to unregistered associations and foreigners aiming to set up business in target state.

**Suggested solution:**
An inviting digital business environment needs a solution for the limited-power actors as well – the unregistered association level should be experimented with large cities that typically have plenty of such partners. Also, foreign persons willing to establish a company in Finland could be offered playground on the same level, just to familiarize with Finnish digital business environment prior to making a decision to enter.

**Automatic exposure of linked business IDs**

The introduction of the company ID credential includes the technical detail that it automatically links (downwards) a new Finnish Tax Administration -issued business ID to

- existing business ID,
- interim digital ID of an unregistered association,
- ID issued under some other jurisdiction or state with traditional means (verified by the notary's KYC process), or
- ID that comes from company's earlier life cycle as a sole proprietor or to-be-incorporated-LLC.

This is a superior improvement, as oftentimes any confusion, misinterpretations, or illegalities and fraud linked to businesses are often linked to misuse or hiding of the links between company's different identities – such as parallel existence of a Business ID in another state, linking existence of a local Business ID in Finland to employer's automatic compliance with commonly agreed salary levels paid to its employees and such.

However, this trail - the separate credentials issued to an entity during its different lifecycles - don't solve automatically **how the authorities can stay up to date on the entirety of transactions conducted over the company's lifecycle**. This could be only implemented technically if ID linking can be implemented both upwards and downwards. Due to nondeterministic nature of ID issuance (in clear: A credential issued at lower level of compliance cannot include the company's verified future official business ID before it has been issued for real later) an audit-trail across IDs is currently rather complicated.

With this in mind, and acknowledging that some founding transactions would be possible also as an unregistered association, it becomes necessary to treat company IDs differently from natural person's identities and prefer **maximal transparency**: Instead of privacy-by-default-and-design, a company presenting its digital identity should be forced - by automation offered by verifiable credential/proof mechanism - to release all valid linked company identifiers (former and concurrent) to a relying party upon a holder-verifier transaction. This enforcement can be implemented through the verification policy of the credential (proof) verifiers.

This 'open hand' also would provide automated 'step-up' of entity's digital transaction powers without necessitating applying for those powers separately against the newly acquired formal company identity. Such automation and enforcement could be implemented specifically to company identifiers (layers 0 and 1 in Figure 3) as a special verifiable credential category.

Contextual, business specific credential exchanges (layer 2 credentials in Figure 3) could work differently as the business network would flexibly agree its best practices through a jointly shaped governance rulebook.

**Notary-specific identifier**

There may be a need to separate an even more simplistic root identifier that is issued for the company wallet at onboarding of the Notary Service. This would work as an internal registration of the customer instance (local identifier) but would also be necessary in case of any cross-wallet/Notary transitions: a company may have in future company wallets (hosted in several member states) due to reasons stemming from regulation or trust infrastructure differences - we would not be able to reach a Universal Notary across all providers e.g. within the EU. In this case it may be useful to be able to proof customership at a particular wallet provider, and also to link/chain the

multiple wallets. Functions with this kind of credential would be studied in the next steps of this project.

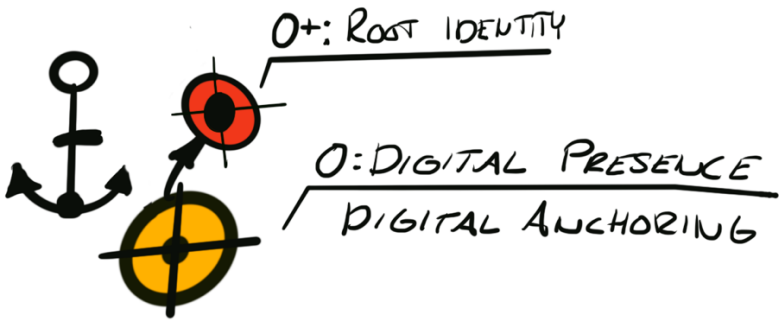


Figure 4 – Local root identity (identifier) of a Notary-anchored entity, which could also be utilized as a credential to proof wallet presence at this particular Notary.

## Business Value Assessment

What business benefits did we find in the concept compared to current practice?

- Notary as a public registry of compliant companies/associations offers a whole new spectrum of services built on top of verifiable data exchange.
- Overall cost of digital enablement could be offered at a very low annual fee assuming there are 4 to 6 -digit volumes of digital company users
- Identifier is equivalent to companies' current e-invoicing addresses (OVT-numbers) but this time for a solution that allows proving this in real-time transactions as a credential.
- Integration cost for relying parties and issuing parties can be kept reasonable and would be available against existence of a REST API & data product (i.e., credential/attribute set) definition baseline. This would make the issuer/verifier role adaptation a logical extension over the upcoming deployment of Tiedonhallintalaki[4] within public sector entities.
- If Finnish Tax Administration is connected in real time to other states through this network (like is doable with Estonia), the legal person's original identity in other member state is automatically linked (without manual procedure) to its registration in Finland. The client database at the Finnish Tax Administration is thereafter more precise and accurate, and it could benefit also the legal person acting in both states as the client.
- Parties to transactions would receive real-time status information concerning tax registrations and tax debt. Number of uncertain tax positions (the other party's registration not being valid) which are handled after the transactions can be avoided. Unregistered parties may be controlled in real time.

[4] https://www.finlex.fi/fi/laki/alkup/2019/20190906 (in Finnish and Swedish only)

# Legal Assessment

**Notary service's 'right to existence' based on current legislation**

Is it possible for the Finnish Tax Authorities, with regard to tax debt information, provide a (contractual or legal) delegation for the Notary service to *act on its behalf* (technically, and as a trusted party defined by primarily by bi-lateral authorization agreement or secondarily, by legislation) as an issuer of tax debt credential? Can this be achieved without changes to Finnish regulation (Julkisuuslaki[5] and other regulation governing tasks and duties of the Finnish Tax Administration) as it is written as of now?

**Authorizations**

When the data is public it is up to the parties to agree on the use of the data. In this POC we use only public data. In the course of this POC we created a system where this restricted data can be issued as credentials and therefore can be further shared and used. Nevertheless, currently only fraction of data is in a format which can be used digitally. Furthermore, the data in digital format may require a license or other fee because a private party as service provider has transformed the data into digital format from a traditional format.

If the data is not public and public authorities have this data, we lack technical tools, authorization management, legal base and semantic models for sharing. Therefore, the data cannot be issued and used in a digital format. Even though, taxpayer is allowed to see tax information and an authorized person is able to handle and see tax data, there is limited possibilities to take this data in another format than PDF. So therefore, the data cannot be used as a verifiable credential. Furthermore, the tax system OmaVero/MyTax) is designed for taxation and the purpose is not to issue and share further tax data. Therefore, currently not the taxpayer nor an authorized person can share tax data as credentials to third parties. If legislation allows for Tax Administration sharing of tax data to a party, like public funding, there may be APIs for sharing tax data. This requires always legislation and is created if need for API exists.

Currently authorizations are based on Suomi.fi services and these are used only for taxation purposes. Suomi.fi services do not include an authorization for a tax data lookup. And credential cannot be issued. Taxpayer and an authorized person (Suomi.fi authorized person) can retrieve basically PDFs.

**Legal person does not have a digital identity through legislation**

Currently we have separate solutions designed for limited and specified use cases. They are typically based on the situation where a person has the right to act in the name of a legal person. Procedure may use trade register's authorization details (in Finnish 'PRH nimenkirjoittajat') and bank identification (Finnish Trust Network FTN). Examples of solutions include Visma eSign and Suomi.fi services. To develop more advanced services and possibilities to represent a company would require a digital identity for a legal person.

Via using a digital identity a legal person may share to a third-party data routed from the source register (Estonian Business Register, Finnish Tax Administration and Finnish Trade Register PRH) up-to-date data in real time. When the legal person's data is public (annual review, registration details and tax debt), this allows development of automatic processes. In the use case, Vastuu Group

creates the reliable partner certificate (Luotettava Kumppani) automatically in real time when the legal person in question needs to provide this data to a public procurer or to a buyer of construction services.

**Digital signing prior to tax data delivery**

One historical way to develop a workable approach similar to verifiable credentials would be where Finnish Tax Administration 'eSigns' (using W3C compatible XML signing, 2013)[5] certain documents and so confirms that these documents are unaltered and are taken from the source. This 'eSign' would indicate to the third party that data has not been changed and is true at the point of 'eSign'. Verifiable credentials as a technology framework implement exactly the same, as the verification process ensures that a) non-repudiation b) rightful holder and c) integrity (tamper-proofness) of a VC can always be checked upon.

Sharing this information further to third parties belongs to the taxpayer. Which is organized with the wallet holder-verifier relationships and digital transactions conducted without presence of the issuer.

**Protected company data**

When it comes to the questions relating to sharing data from the legal person to another one, the basic principle is use of contracts between legal persons. Nevertheless, certain restrictions apply to guarantee at least rights of SMEs as contract parties or special secrecy of persons if a legal person holds data on natural persons.

**Suggestions:**

In Finland it should be clearly stated that the public authorities have a duty to enhance use of data on the public registries, like trade register and tax registers. This duty should also include the development of modern tools to share data. One key component of this approach is already available (Yhteentoimivuusalusta[6]). Using this modeling tool, the public authorities can model what data is available and make it available in a format which can be used like here: tax debt as a credential. In Sweden and in Norway sharing data and making it available in a modern format is one of the core tasks to develop in the future. In Finland we should take same approach. Common strategy also guarantees that data sharing is developed through a coordinated approach instead of service-by-service and data-by-data approach without common perspective.

Credential approach may also allow a taxpayer to share useful data to third parties, even though the data is secret. In order to enhance this approach a common understanding on the data which has this value to third parties should be agreed, because it is not useful to allow all data to be shared. Typically, these requests concern a specified tax data which has value to third parties, not all tax data. Also, this is in line with credential model, because credentials are precisely defined and used multiple times and benefit several taxpayers (scalability). Other possibility to organize this is authorization, like in Norway Altinn provides taxpayers a means to give an authorization to

[5] https://www.w3.org/TR/xmldsig-core/

[6] https://www.suomidigi.fi/ohjeet-ja-tuki/yhteentoimivuusalusta

retrieve all data or a specified data. This requires authorization management. And also, this approach requires regulatory changes in order to allow authorizations to secret data.

## Conclusion: Defining digital identity of a company (legal person)

Key aspects of a digital identity have been mentioned in several chapters of this document. As a summary we cannot define the digital company identity based only on this project. At least, we need to discuss and define it nationally and at the European Union level, because there does not exist a general definition. According to the experiences gained through this project we can state that the elements of a digital company identity are at least:

In general, the digital identity can be defined as a digital twin of a person or a legal person (company).

After acquiring the basic foundational digital identity a company is able to hold and use related verifiable credentials issued to their wallet to acquire other similar digital documents.

Natural persons may act digitally on behalf of a company once their role and identity have been validated through proper authentication, which may include a control of the person from the source state register or a certificate represented from source state indicating a status (a copy of a passport or TIN).

In this project we have used the following data as the basic digital identity: name, type and country of a company, registration authority, ID, status and registration date and VAT code (for taxation).

Based on this project we could state that the digital company identity requires

- Capability to send and receive facts (verifiable data) using a standard protocol that works in a national digital trust infrastructure, preferably this should work across the national borders
- A public address, which a company has in the aforementioned fact-transfer network
- An agent to which the aforementioned public address resolves onto, that controls/holds all verifiable data the owner of the wallet holds
- Actor(s) that can notarize facts about the company to this new digital wallet – both confirming verification of identity data from legacy registries (all Notary Services by definition via their KYC capacity), and when needed and in their authorized capacity, creating new foundational company identity to a registry and issuing this as a verifiable credential to company's digital wallet.

# Technical Proof of Concept Summary

## Verifiable Credentials Developed and Tested

The PoC setup involved credentials issued by the notary service ('onboarding credentials'), Finnish Tax Authorities and a 'credentialized' version of Vastuu Group's current Reliable Partner (Luotettava Kumppani) service's status report.

| **Onboarding credentials by Notary Service (Layer 0)** | **Tax Authorities' credentials (layer 1)** | **Reliable Partner credentials (Layer 2)** |
|---|---|---|
| Company ID | Company ID | Reliable partner status |
| Registration pending[7] | Tax debt status | |
| Unregistered association[8] | | |

The credentials can be found documented in full in Appendix B. Upon request we can also provide a pointer to the test ledger network where the credential definitions are visible in public.

## Definition of Data Products onto Credentials

The implemented method for creating data products that can be used as the information content in verifiable credentials included the following steps:

- Definition of *concepts* in a domain-specific terminology that describe the meaning the data owner (provider) gives to a certain term in his or her own business context. The aim is not to define terms too narrowly, but to allow for the use of commonly understood concepts in a number of specific business contexts.
- Linking the chosen terms representing these defined concepts to *data vocabularies* (or "conceptual data models"). A defined concept can provide the basis for the description of a class, attribute or association, that form reusable global or domain-specific "data components" to be specialized when describing the meaning of a specific data product.
- The creation of the final semantic description of a data product, an *application profile*, which utilizes the data components in common or domain-specific libraries, allowing for the addition of local extensions or additions when the contents of the libraries are not sufficient for the exact definition of the data.
- An automatically generated OpenAPI 3.0.2. description of the application profile is used as the basis of the API for the data product, which is then productized onto an operational API at the provider's system in question.

[7] Not used in the PoC use case
[8] Not used in the PoC use case

- Tools and solutions used in the process are provided by the Interoperability Platform, developed and maintained by the Finnish Digital and Population Data Services Agency (DVV).
- The control middleware responsible for managing provider's own presence (an agent) towards the trusted network will act as an API client towards the provider. Towards the trusted network, before issuing any verifiable credentials out in name of the provider, the agent 1) registers in public the definition of the application profile, and 2) registers itself as a trusted issuer for such credentials. Both realize as agent's digital transactions towards the network. Phase 1 could be omitted if there is already a suitable public definition available for the credential (application profile) at hand – in this case it suffices to register as a new issuer only.
- Having the profile originally as OpenAPI description helps in converting the data to a verifiable credential definition (utilizing either JSON-LD or just plain JSON) by the provider's IT developer responsible for the configuration of issuing agent.

# Moving Forward from a Proof of Concept

Next steps for progressing the creation of digital company identity will involve reaching out to other EU member state authorities with interest to test our concept across the borders, with potential multiple notary and wallet provider services. Interworking and mutual authorization of such entities needs to be managed both from legal and technical perspective across states - analyzing differences in local regulation, EU-wide regulation, and understanding that e.g., national trust networks currently testing with verifiable data may not share 100% common technology across the layers.

We are calling in partners for discussion and joint extension of our basic use case between Finland and other member states. In Finland, the list of identified and not-yet-implemented use cases gives a good trajectory on where to target next in terms of domestic piloting and co-development of verifiable data products in the companies' context.

# Appendix A - Glossary

| Term | Description | Further information |
|---|---|---|
| ID | identifier | https://en.wikipedia.org/wiki/Identifier |
| VC | Verifiable Credential | https://www.w3.org/community/credentials/ |
| VAT | Value Added Tax | https://ec.europa.eu/taxation_customs/business/vat/what-is-vat_en |
| PoC | Proof-of-concept | https://en.wikipedia.org/wiki/Proof_of_concept |
| FTA | Finnish Tax Administration | https://www.vero.fi/en/businesses-and-corporations/ |
| FTN | Finnish Trust Network | https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/electronic-identification |
| KYC | Know-Your-Customer | https://en.wikipedia.org/wiki/Know_your_customer |
| PRH | Finnish Patent and Registration Office | https://www.prh.fi |
| VAT | Value Added Tax | https://www.vero.fi/en/businesses-and-corporations/about-corporate-taxes/vat/ |
| JSON-LD | Javascipt Object Notation for Linked Data | https://www.w3.org/TR/json-ld11/ |

# Appendix B - Credential Definitions

The appendix contains the data model definitions of credentials developed and evolved during the project. First implemented use cases used only some of the credential types, others were defined but left for later use cases and concept development.

**1 - UnregisteredAssociation Credential** (not used in the demo)

```
## Hyperledger Indy credential format
{
"attrs":
[
    "name",
    "type",
    "id",
    "date",
    "country",
    "municipality",
    "url"
],
"name":"Unregistered Association",
"version":"0.1"
}

## W3C Example Credential
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
    "https://www.notaryregistry.findy.fi/credentials/v1"
  ],
  "id": "http://notary.vastuugroup.fi/credentials/242",
  "type": ["VerifiableCredential", "UnregisteredAssociationCredential"],
  "issuer": "https://notaari.vastuugroup.fi/issuers/02",
  "issuanceDate":"2020-11-01T08:13:01Z",
  "credentialSubject": {
    "id": "did:findy:fbfe36f712ebc6faa276e12ecda",
    "name":"Källarbandet",
    "type":"UnregisteredAssociation",
    "date":"2009-12-24"
    "country":"FI",
    "municipality":"Helsinki"
    "url":"https://källarbandet.hostyoursite.com"
    }
  }
```

**2 - CompanyID Credential** (used by both Notary Services in the demo)

```
## Hyperledger Indy credential format
{
"attrs":
[     "name",
      "type",
      "country",
      "reg_authority",
      "registration_id",
      "reg_status",
      "parent",
      "vat_code",
      "reg_date",
        "url"
],
"name":"Company",
"version":"0.1"
}

## W3C Example Credential
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
    "https://www.notaryregistry.findy.fi/credentials/v1"
  ],
  "id": "http://notary.vastuugroup.fi/credentials/013",
  "type": ["VerifiableCredential", "CompanyIDCredential"],
  "issuer": "https://notaari.vastuugroup.fi/issuers/02",
  "issuanceDate": "2020-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:findy:ebfeb1f712ebc6f1c276e12ec21",
    "name":"Keijon Konserni",
    "type":"Oü",
    "country":"EE",
    "reg_authority":"EEARIREG",
    "registration_id":"80189359",
    "reg_status":"active",
    "parent": {
      "id": "did:findy:ebfeb1f712ebc6f1c276e12ec21"
    }
    "vat_code":"EE80189359",
    "reg_date":"2003-08-19",
    "url":"https://keijonkonserni.ee"
    }
```

**3 - Reliable Partner Credential** (used by Vastuu Group Reliable Partner service in the demo)

```
{
"attrs":
[     "id",
      "LK_status",
      "date",
      "url"
],
"name":"Luotettava Kumppani",
"version":"0.1"
}


## W3C Example Credential
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
    "https://www.notaryregistry.findy.fi/credentials/v1"
  ],
  "id": "http://lk.vastuugroup.fi/credentials/007",
  "type": ["VerifiableCredential", "LuotettavaKumppaniCredential"],
  "issuer": "https://lk.vastuugroup.fi/issuers/06",
  "issuanceDate": "2020-10-05T14:00:21Z",
"credentialSubject": {
    "id": "did:findy:target-company-DID",
    "LK_status": "OK",
    "date": "17122020",
    "url": "www.example.com/company"
   }
}
```