DIACC Identity Networks Paper

Citizen One™ by Vivvo, Self-Assessment

This document is intended to be used by identity network providers that want to demonstrate how their solution fits into the framework and requirements as described in the “Making Sense of Identity Networks” whitepaper. This self-assessment is an informal way to illustrate the concepts discussed in the whitepaper and has been reviewed by Consult Hyperion to ensure it is objective, accurate, and aligns with the framework.

1. Introduction

CitizenOne™ is a trusted digital identity platform for government and healthcare. It enhances the digital experience for citizens (the primary subjects) by allowing them the ability to manage their information and the services they use with one simple profile. CitizenOne™ is capable of creating and contributing to different types of identity networks in various public sector contexts.

CitizenOne™ enables digital government and healthcare by providing citizens with single sign-on capabilities and a better citizen experience when using digital services. CitizenOne™ eliminates the need for the citizen to manage multiple accounts (identities) and passwords when accessing a variety of different services from their government(s).

CitizenOne™ includes a citizen identity and access management capability but also delivers a set of common enterprise services to the citizen that significantly improve their online service interaction. Along with brokering the connection between the citizen and digital service, CitizenOne™ secures the citizen's information and enhances consent and privacy management. This is done by providing the ability to "opt-into" the use of a digital service and allowing service providers to set discrete policy that a citizen must meet and accept to access the desired service through the digital channel.

CitizenOneTM provides:

- Mechanisms for connecting to data assets the customer can provide to enable digital identity proofing, this helps ensure sensitive services are delivered conveniently, securely and to the right people.
- A federated identity capability that can integrate with existing legacy applications as well as net-new services (SaaS or on-premise), allowing governments to rapidly and incrementally grow their digital service delivery program over time.
- Secure messaging to the citizen, consolidating messages into one secure, private, easy to access location with options to send calls to action to email/SMS if desired.
- Easy integration with external identity provider authentication for conveniently connecting people to critical online services using authentication methods and/or credentials they already have and trust (e.g. use authentication credentials from other parties to authenticate to CitizenOneTM).

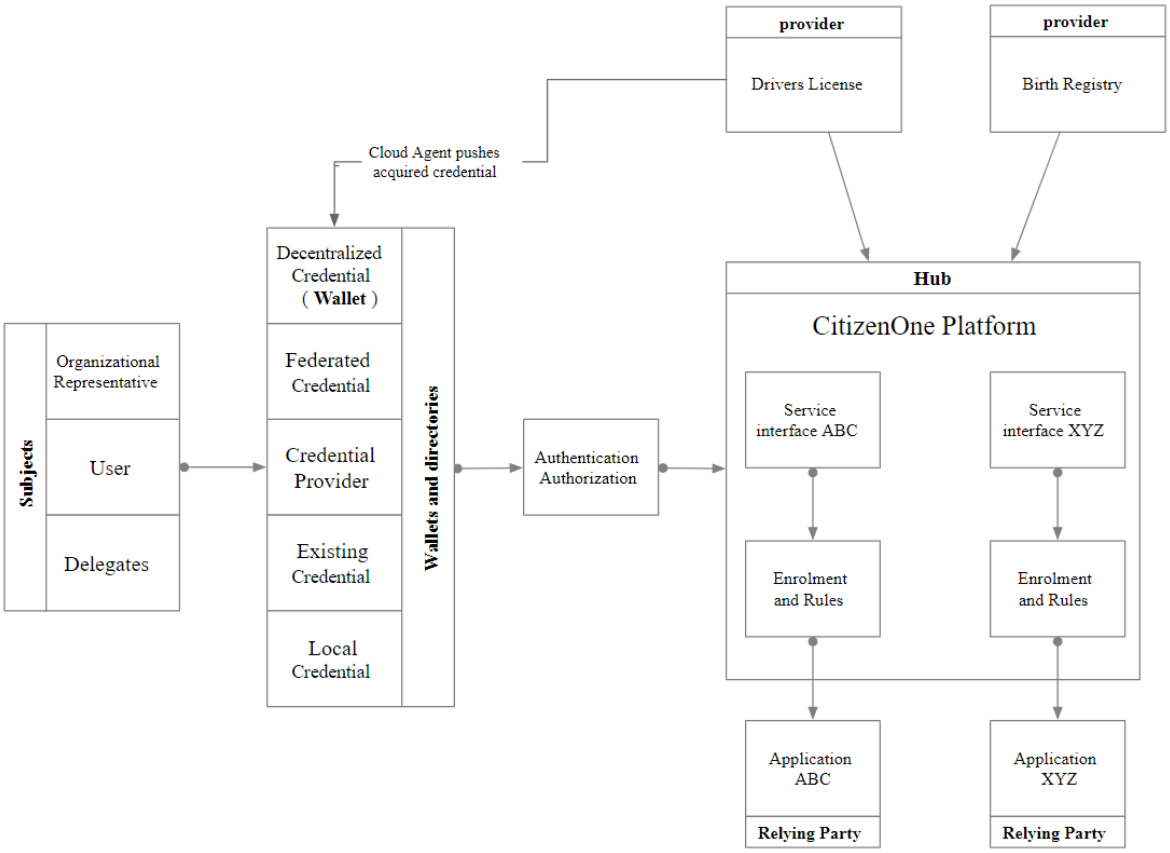

Figure 1 - CitizenOne™ context diagram

2. Identity Network Elements

For reference, this self-assessment section relates to Section 2 of the “Making Sense of Identity Networks” whitepaper. Included below is a description of how this identity network operates at each of the defined layers.

Connections

Definition
Before any communications can occur between parties in a network, there needs to be a means for parties to discover each other. In some cases, this may be automatic, as the parties wishing to share attributes may already be communicating about the service being requested. In other cases, a directory or automated service discovery method would allow parties to find and connect with each other.
Self-Assessed Network Description:
CitizenOne™ is delivered to customers on a contractual basis. Customers, typically governments and other public bodies, determine which services and relying parties may be part of the “identity network”. The CitizenOne™ platform allows relying parties to identify themselves manually so that their service can be listed in a catalogue (directory) for the particular customer. During the validation and listing of

the relying party, the relying party defines the policy that is required to be accepted to use their service, the attributes that are required to use the service, and the credentials and/or rules required to access the service.

The relying party is issued with a credential to be used with their application, which provides proof that the application is authorized and is not a fraudulent copy. At any point, if the relying party becomes a bad actor, the CitizenOne™ platform can revoke this credential and the service can be delisted.

As a subject selects the service they wish to use, the CitizenOne™ platform takes the subject through an enrolment process, the subject is stepped through a small workflow to review the policy and consent scope items and accept the conditions – effectively giving consent. Further conditions (defined by the relying party) are polled and if the user has not cleared these conditions previously, a workflow is invoked to request attributes and to acquire a credential proving the user has met the condition(s) (e.g. establishment of a verified person or business owner, or finer attributes such as at least 18 years of age). The CitizenOne™ platform requests the information from the subject and then relies on the other credential provider(s) to validate any information.

Once consent and conditions have cleared the subject is provided with an authorized link to use the service. These conditions, consent and policy are evaluated every time the subject uses the service. If policy changes or credentials have expired, or have been revoked, the subject must accept and/or clear conditions again.

Communications

Definition

The communications between parties carry the credentials that are to be shared. In some networks, this information is communicated directly from the provider to the relying party. In others, the information is only communicated indirectly, for example via a centrally operated hub or via the subject.

Self-Assessed Network Description:

In general, CitizenOne™ doesn't share credentials with relying parties. There is no mechanism to request this via SAML, OAuth, DID, etc. Our approach is to communicate indirectly, for example via a centrally operated hub. Subjects can request credentials be communicated from the provider to relying parties via the CitizenOne adapter framework, provided consent is given by the subject.

Credentials

Definition

The information that is to be shared including attributes together with the associated metadata that links those attributes to the subject and describes their provenance. The structure, content, and format of this information may vary between network types.

Self-Assessed Network Description:

The attributes shared are dependent on the requirements of the relying party and with the agreement of Vivvo's customer – a government or other public body with an instance of the CitizenOne™ platform.

Vivvo is following the development of open standards such as W3C Decentralised Identifiers and W3C Verifiable Credentials and intends to support them as they mature.

Vivvo takes steps to not lock its customers into proprietary solutions, and we are eager to work with other innovative initiatives to begin testing out what interoperability would look like.

Certifications

Definition

For a relying party to have confidence in the credentials received via an identity network, the relying party will need to be confident in the processes involved in the establishment of the credentials, and the attributes they contain, as well as in the secure transmission of it across the identity network. Often this will involve certification or audit of parties that are being relied upon to ensure the credentials and attributes are robust.

Self-Assessed Network Description:

Vivvo intends to align with the Pan Canadian Trust Framework (PCTF) and supports the values and principles it follows, helping customers choose the right privacy and security controls for their services. The approach of CitizenOne™ is to allow Vivvo's customers to have the choice over which credentials are trusted. As most of Vivvo's customers are governments typically credentials come from authoritative sources in the government. From an audit perspective, Vivvo is in the process of a SOC2 audit, we believe this will help provide greater confidence in our approach.

As an example, Vivvo has recently launched a new service with a government customer that allows individuals to view their electronic health records. To access their health records, the individual must first enrol providing evidence of birth and supporting documentation (in the form of a drivers license or an identity card). In this example, we are relying on the processes of government in the issuance of the driver's license and health card and then ensuring the subject has the required details from these "cards" in hand. Once this information is provided and validated to be correct this credential can now be trusted and used for services that also require high confidence of the user without asking for proofs again. This enrollment follows the requirements of the Verified Person Specification (PCTF) and positions the customer for process certification that we are hoping enables this credential as a trusted credential in other jurisdictions (e.g. provinces).

Our product can bind high confidence credentials to the authentication credential and achieve a verified authentication.

The CitizenOne™ Compliance module provides a compliance rating which can be used by network participants to assist them in their assessments.

3. Requirements of an Identity Network

For reference, this self-assessment section relates to Section 4 of the “Making Sense of Identity Networks” whitepaper. Identity networks are more than technology. For multiple parties to collaborate in a safe, secure and predictable way there need to be clearly defined legal, business, and technical rules that determine how participants behave.

The requirements are grouped into two areas:

- **Governance**: setting and enforcing the rules of the identity network
- **Operation**: implementing and operating the rules of the identity network

Identity networks meet the requirements of the network users through a combination of:

- **Trust**: The network user needs to trust the network to ensure that their requirements are met, and
- **Agency**: The network user can act independently and make their own free choice over how their requirements are met

Some identity networks place a greater emphasis on trust and the need to ensure that the participants in the network are trustworthy. Other identity networks place a greater emphasis on agency, seeking to give greater control to network users – which of course also brings with it, greater responsibility. In the end, all identity networks rely on a combination of trust and agency.

To work, identity networks need to serve and meet the needs of all network users. Included below is a description of how the CitizenOne™ identity network meets the requirements as defined in the whitepaper.

Governance

Participation			
Network User	Requirement	Self-Assessment	Basis
Subject	Be able to participate (inclusion)	The customer (which can be a single organization or a collection of RPs) determines the governance arrangements for the identity network (i.e. an instance of CitizenOne™). This will include the rules for subject participation. These typically specify the evidence that the subject needs to provide to participate in the service as well as acceptable sources of credentials and authentication.	Trust
Provider	Clear rules for participation and confidence in other participants	Providers participate based on their relationship with our customer. Vivvo's customers determine which relying parties can participate. Vivvo works with its customers to select the correct controls for privacy, security, and enrollment attributes that fit the level of assurance that each	Trust

		service requires. Each participant in the system is included based on their relationship with our customer. Typically, Vivvo's customers are governments or public bodies who only allow relying parties/providers from within government (or other governments) to participate. The solution can, however, be deployed in any sector.	
Relying Party	Clear rules for participation and confidence in other participants	As above. Vivvo works with its customers to assist them in selecting the appropriate privacy, policy and controls to participate in the network. The platform offers a continuous conformance service to monitor the health of the participants and scores their effectiveness as a friendly participant in the eco-system.	Trust
Transparency			
Network User	Requirement	Self-Assessment	Basis
Subject	Transparency over how credentials, and the attributes they contain, are used and clear straightforward means to manage credentials	The CitizenOne™ enrollment process informs the subject of how their data will be used before obtaining consent to the policy for the use of the service (and how it will use their data). We closely follow Privacy by Design recommendations and list the consent scopes requested, before any legal notice is displayed. This interaction is encapsulated as a "service card" where the subject can view and review consent receipts and choose to revoke their consent if they so choose. Service Cards in CitizenOne™ ensure a common onboarding process across a variety of disparate services and ensure subjects are provided with a straightforward means to manage their credentials.	Trust

Provider	Assurance that consent is correctly obtained, from the subject, to release credentials (when the consent is not obtained directly by provider) Transparency over downstream use of credentials.	As above. Each subject is stepped through a workflow on the CitizenOne™ platform to ensure consent is appropriately received and provided with mechanisms to ensure they understand how their credentials are used.	Trust
Relying Party	Transparency over the production and provenance of credentials that are relied upon	Credentials are obtained from known sources as determined by the customer. .	Trust
Accountability			
Network User	Requirement	Self-Assessment	Basis
Subject	Have recourse in the event something goes wrong, including being able to repair erroneous personal data and seek redress for harm caused	CitizenOne™ maintains appropriate state for credentials. If a credential is stolen, the issuer can revoke that credential and issue new attributes to represent it. The subject can withdraw consent at any time. The subject can rely on existing processes for correcting personal data when a particular credential (or attribute) is immutable in CitizenOne™. For example, if the user misplaces their driver license credential, or if their account is compromised, they can use a traditional workflow to notify the issuer and have a new license issued (with new verification numbers and revocation of the old verification). The user now simply re-enrols with that service to acquire the digital credential.	Trust
Provider	Relying parties of credentials are responsible and will be held accountable in the event of a breach	Vivvo's customers will put in place the necessary arrangements to ensure that RPs connected to its instance of CitizenOne™ are responsible and held accountable in their management credentials appropriately. Furthermore, CitizenOne™ validates credentials by polling authoritative sources in a "yes/no" context to validate the	Trust

		credential yet ensure no sensitive data is replicated in other systems.	
Relying Party	Clear liability arrangements Verifiable or audited evidence of provider processes	Liability and clear terms of use determined by the CitizenOne™ contracts.	Trust

Operation

Confidentiality			
Network User	Requirement	Self-Assessment	Basis
Subject	Credentials are only shared with consent Data is only used for purposes that the subject agrees to Network does not enable tracking or surveillance of a subject Network does not include honeypots that if breached would impact many subjects.	CitizenOne™ ensures that subjects are informed of the exact details of any sharing before consenting. Consent must be in place for the credentials to be shared. The CitizenOne™ policy service ensures policy and consent scopes are detailed to the subject and that the subject agrees to any policy and consent/sharing terms. Subjects are fully informed before making any sharing agreement. CitizenOne™ allows a relying party to choose what conditions are required to use their service as opposed to which specific credential is required. The condition may be "must be 18 years of age", and the subject gets to choose which issuer to enrol/use to satisfy this condition. This allows the relying party to have the confidence that the subject is of age but does not disclose who verified this. Additionally, the identifier that is shared with the relying party can be scoped unique, so it cannot be correlated with other relying parties. CitizenOne™ includes a rule and data bundle architecture. Data stays in source	Agency

		systems and can be used to validate rules or brokered via CitizenOne™.	
Provider	Legal basis to share data Being confident no data protection issues arise from downstream use of credentials	Clear policy and the subject consenting to terms is a prerequisite to sharing data. The subject can, at any time, revoke the consent.	Trust
Relying Party	Credentials received are minimized to mitigate data protection risks Data is only used for purposes that the subject agrees to	Before a relying party requests credentials to be used in their process, an agreement must be established between the relying party and the provider. We have completed a feature that ensures users are informed of any profile data they may be sharing with service providers. Subjects are prompted to consent to the data sharing, we refer to this concept as "consent scopes". Each subject must consent to the scope of data being supplied. Subjects are also presented with policy pertaining to the service they are attempting to access; this policy is used to provide clarity to the user of the intended use of the data.	Trust
Integrity			
Network User	Requirement	Self-Assessment	Basis
Subject	System protects against identity theft and other abuse	CitizenOne™ offers extended protection in the form of MFA techniques, policy lockouts, prevention of using a previously breached password to help subjects secure their identity. Our DiD authentication wallet extends this functionality further by allowing the user to bind their device security to the credential store, and using other credentials stored in the device as further evidence that the real user is authenticating.	Trust

Provider	Credentials cannot be altered downstream, resulting in fraud, disputes and/or inconvenience to subject	Credentials are provided via a back-channel communication or a citizen (subject) credential disclosure using a cryptographically verified credential that can be verified as true against the public key of the issuer.	Agency
Relying Party	Credentials are issued to the subject, have not been revoked and are received unaltered from the provider Network detects and mitigates against fraud	Relying parties can verify through cryptographic verification that a credential has not been altered by the subject or during transit.	Agency
Availability			
Network User	Requirement	Self-Assessment	Basis
Subject	Digital identity can be used when required Digital identity cannot be inappropriately taken away	Credentials that are issued to the subject, can be time-based and expired by the issuer (or cancelled by the subject at any time). These rules are conveyed to the subject during enrolment. If a credential is revoked, the user can always re-enrol with the issuer and receive a new credential to establish access once again.	Trust
Provider	System does not place onerous service level requirements on provider	CitizenOne™ is delivered as a Managed Service and the relying parties are not required to meet any particular SLA. It is up to the customer to decide which RPs are included at the SLAs that may apply.	Trust
Relying Party	System is available when needed, depending on whether it supports offline or online transactions	Availability is determined by the overall approach to deployment, depending on the needs of the customer and relying parties. CitizenOne™ is delivered to the specifications as determined by the customer. This means that the customer has the opportunity to ensure that the system is available. CitizenOne™ is primarily used in an online transactional model, however, we are working on wallet technology that could function in an offline manner.	Trust or Agency

4. Choosing an Identity Network

For reference, this self-assessment section relates to Section 6 of the “Making Sense of Identity Networks” whitepaper. There are many factors in determining whether to participate in an identity network or not. Included below is a self-assessment description of how this identity network meets the various factors to consider when choosing an identity network, as defined in the whitepaper.

Utility	
Identity transactions supported	The CitizenOne™ product supports identification and authentication transactions and allows service providers to set service access rules that support authorization. CitizenOne™ does not have to be the provider of the identity, the product can perform as a service provider and consume federated credentials via OAuth 2.0, SAML2, OIDC. CitizenOne™ also has a full IDP service for customers that need it. CitizenOne™ has the option to take any credential from the system and move it to a wallet. This ability is important as adoption from traditional forms of digital verification moves to a decentralized format.
Sector	At launch, CitizenOne™ was designed for interactions for government, public healthcare and other public institutions. We consider the credentials created inside these types of networks as valuable to relying parties outside of government. Traditionally governments have been providers of highly trusted documents that prove who we are, and private industry has depended on these. Moving to the digital world requires the same rigour of quality if these credentials are to be treated the same as their physical counterparts. From a technical perspective, CitizenOne™ can fit the requirements of a broad range of sectors.
Scope	CitizenOne™ is primarily an individual-to-organisation identity network. But from a technical perspective, it's engineered to meet a wide variety of scenarios (e.g. device to organization, device to device etc.). To provide capabilities that allow an organization to interact with another organization CitizenOne™ takes the approach that subjects have various roles they may play in their day to day lives and allows the subject to act in their various roles from the same identity (e.g. citizen, business owner, employee, representative of a business). Additionally, the CitizenOne™ wallet technology allows for a person to associate themselves to different entities and hold entitlements to act as that entity digitally.

	The CitizenOne™ relationship service allows an entity to relate to another through enrolment workflows. The organization responsible for enabling the relationship will select the criteria required to build the connection, and the CitizenOne™ workflow builds the process.
Mode	CitizenOne™ provides a flexible approach to mode. Depending on the trust requirements of the relying party, they may require one or more of: • Realtime verification of the credential • Time-based validation of the credential To accomplish time-based validation of the credential we rely on adapters to provide flexibility to integrate how our customers see fit. Customers can cache credentials in the adapter to achieve the time-based verification.
Identity migration	CitizenOne™ supports a unique way of migrating or connecting accounts across systems that may be part of the identity network (or even potentially outside the network). We allow the subject (user) to enrol themselves to another identity store with attributes they have knowledge of, binding that identity as a credential to the authenticated user.
Interoperability	Our product is compliant with SAML2, OIDC and OAuth 2.0 as both an IDP and SP. Our wallet technology is emerging and following the draft specifications, we are striving to be fully compliant with the Hyperledger and the Decentralized Identity Foundation specifications when released. Interoperating this credential across networks is currently challenging, as there currently are no standards for this.
Adoption	CitizenOne™ allows organisations or groups of organisations to set up a network to share subject information as part of a wider digital transformation, this includes numerous instances with wide geographical representation.
Trust	
Governance	CitizenOne™ is delivered to our customers (e.g. governments and other public bodies). These customers set the governance rules for participation and use of the identity network. Since many of the CitizenOne™ customers are governments the governance and policy that applies to the network are set down in various forms of public policy and/or legislation. From a technical point of view CitizenOne™. allows customers of the platform to create the policy and controls they feel appropriate for their use. The government customers we are working with are

	involved with DIACC and look to the PCTF to help choose controls for credentials and what credentials are required for each service.
Transparency	Our platform is built to allow for transparency to subjects of how their data is stored, managed and used. Our customers, largely being governments, often have audit requirements we must meet and provide results of to help ensure they are informed of the various service levels, security measures and processes we utilize to help provide transparency to subjects and to the public as a broader whole (and to ensure alignment to any governing policy). Subjects (users) of our platform have visibility to how they are connected to services and have the choice to revoke consent (sever the connection) at any time with their control. Subjects are also made aware of the policy and when policy changes for each service they choose to engage with.
Assurance	CitizenOne™ has a compliance module that allows the network operator to monitor state, privacy and health of the services in the catalogue. Services are scored and an overall network score is available. From an identity assurance perspective, subjects are stepped through processes that meet the network operators needs for assuring identity. Since the vast majority of our customers are governments this is most often the PCTF. Our customers make the choice to rely on an attribute of an identity provider. CitizenOne™ enables the workflow to allow for the validation to occur.
Funding	The CitizenOne™ product is funded by each organization (government, health care, private enterprise) that chooses to deploy it as part of its identity network. Data contained within the platform is not monetized (e.g. in a commercial model where subject data is “sold”). The data is owned by the organization (or the subject), and not available to Vivvo as the platform provider. Vivvo is not contractually permitted to commercialize the data contained within CitizenOne™. All data is encrypted only those with access to the encryption keys and platform (under certain circumstances can view the data).

Maturity	CitizenOne™ has been in production with customers since 2015, the platform has been tested at scale. The wallet technology in our product is new but fits very well with the controls in our core product. CitizenOne™ is deployed for a number of customers across Canada as unique managed services (e.g. separate instances for different government customers).
Privacy	
Choice	CitizenOne™ allows the user to take ownership of their digital self. The subject chooses which relying parties to connect to. Our product provides all the data required to make a good decision (clear policy, what is going to be shared and how it is used). The subject is also informed when policy or consent changes, and at any time can choose to disconnect (revoke consent) from the relying party. The network operators decide which services (and relying parties) will be part of the network. From a technical perspective, with the CitizenOne™ wallet technology, the subject can choose to provide credentials from their wallet to any provider in the network.
Data protection	CitizenOne™ allows a customer (a government) to select which data protection policies may apply to their network and then configure CitizenOne™ in such a way to meet that policy. In our proof of concept work, we have successfully transferred credentials between different levels of government with different governing policy.
Transparency	CitizenOne™ was built privacy first and has a very rich policy engagement. There is often a global policy that defines how the account is used from a network perspective, and then a service by service basis where policy can be extended and further defined.
Accountability	Vivvo takes privacy and security very seriously, as they are two of the key tenets of our product. We maintain ISO27001 and ITSG-33 compliance, perform routine security scans of all code and controls. We follow all obligations required from PIPEDA concerning disclosure of a potential breach.