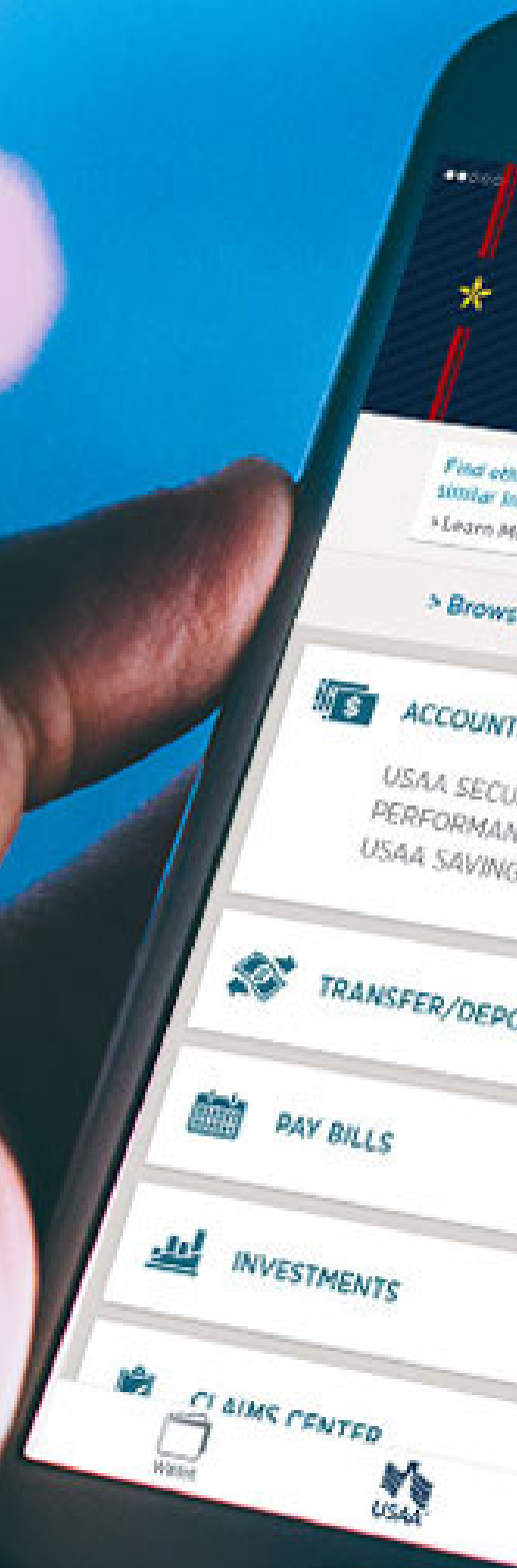


IDgov.digital

Identity for Digital Government

Architecture for seamless online services





This ebook will define and examine the keystone role Digital Identity plays in facilitating seamless online services, not just for Government but for all organizations and industries.

Digital Identity refers to the various usernames and log-on procedures we use to interact with web sites and other digital services. [Michael Gorriz explains](#) how Identity is a universal function, one that spans across government, banking and every other online service that we use.

For a review of Government Identity capabilities the examination will look across immediate, short and long term horizons:

Identity Programs and Best Practices Review

Government identity programs, such as [Gov.UK Verify](#), seek to leverage this interconnectedness through linking their authentication systems with others like banks to streamline the procedure from a users perspective, an approach known as 'federated identity'.

The types of challenges it has faced highlight the complexity and hurdles a successful scheme must overcome.

The Government has [halted its funding](#) and the Projects Authority [recommended it's termination](#); TechUK has recently [called for clarification](#) of future direction as a matter of urgency. Industry figures have called for alternative courses of action, such as [following the Nordic model](#). Other national approaches includes Canada's '[DIACC](#)'.

Key best practice scenarios will include the role the technology has played in streamlining digital services for users. For example North Lanarkshire Council implemented the Civica 'Multivue' solution to achieved a 'golden record' of each citizen giving them the ability to access all the services they need through only one login.

Government as a Platform

If ultimately Verify fails to succeed it can be seen as the poor implementation of a good idea, not a fundamentally bad idea. In particular it's role in enabling '[Government as a Platform](#)' is key.

The core ideal of this is one of architectural common sense – Reusing common components rather than continually reinventing the wheel, and so the medium term review will be to establish how this goal may ultimately be realized.

Identity is the keystone common service – Users don't want to have to repeat the username registration and signon process for each and every service they use, they want a simplified, streamlined approach, and in the light of the Verify woes we'll explore multiple options for how this end result may be best achieved.

The Identity Metasystem and PDS Architecture

The scope of the long term can principally be characterized through the evolution from centralized to decentralized approaches.

Currently Identity systems are built around a core premise that citizen data is held centrally by government agencies, and federated identity schemes implemented to achieved permissioned access to them.

In contrast the overall context of an emerging [Decentralized Web 3.0](#) again Identity will be one of the keystone foundations for this new paradigm, with users taking control over their own data directory.

Key capabilities accelerating this trend include decentralized identity systems notably 'Self Sovereign Identity', exemplified through early cutting edge pioneers like [British Columbia](#), and 'Personal Data Stores' - [This Medium article](#) by Irina Bolychevsky explores the emergent landscape of vendors offering apps and online services that enable users to store and control their own personal information.

Identity-Enabled Digital Services Architecture

Overall the goal is to define an architecture for Identity-Enabled Digital Services, explained through key use case scenarios such as Drivers Licence and Passport applications.

North Lanarkshire Council streamlines its citizen portal with MDM-enabled Single Signon



As documented in [this Civica case study](#) North Lanarkshire Council implemented their 'Multivue' solution to achieved a 'golden record' of each citizen giving them the ability to access all the services they need through only one login.

Digital Vision

In their [Digital Roadmap](#) the council describe their ambitions and vision for moving to a Digital delivery model, including key objectives such as:

We aim to empower and activate customers to be self-managing, direct them to the right resources, and anticipate their needs. This will make North Lanarkshire an attractive place to live, work and do business, both improving outcomes for residents and fostering economic growth.

and the case study documents the type of challenge they needed to overcome to realize this goal:

North Lanarkshire Council streamlines its citizen portal with MDM-enabled Single Signon

The Citizen Portal is an online service in which citizens of North Lanarkshire can sign in to access a variety of tasks and services, from having a pet microchipped to learning the recycling schedule in their neighborhood, to arranging repairs on their home or accessing council data.

Prior to the Citizen Portal going live in March 2017, there was a very disconnected online presence. Citizens had the ability to conduct their business online, but tasks were disjointed and difficult to find or access, and often required that they sign in multiple times to access various departments and services.

As they highlight in the Roadmap, a new digital platform was needed to address these types of issues:

We will reduce the cost base through the removal of duplication and fragmentation through consolidation of common activity/processes. Data and digital are key enablers to this model of service delivery. They provide access for our customers as well as the evidence base to change our services and respond to need on an ongoing basis. This will increase customers' use of self-support whilst allowing us to target our resources at those with greatest need.

To turn this into reality requires an improved IT architecture. This means a new digital platform on which we build the new technology and ways of working.

The transformation outcomes included:

- Improved user experience and simplified process for the citizen
- Single sign-in and integration with mygov.scot online account
- One 'golden record' for each citizen
- Tangible cost savings and efficient service delivery
- Used MDM solution to increase complete and accurate data records from 7,000 customers to 86,000

North Lanarkshire Council streamlines its citizen portal with MDM-enabled Single Signon



Roadmap : MDM-based Single Signon

The Civica solution defines 'MDM' ([Master Data Management](#)) as a keystone foundation to this new digital platform.

MDM system sits at the heart of the Portal, creating one "golden record" of each citizen, generated from the disparate information in the separate systems. The effect is that now, when the citizen logs on, that information can be called forth only one time, instantly. This gives the citizen access to all the services they need, through only one login.

It's a common requirement for all government agencies operating multiple business systems storing citizen data.

The [Aberdeen Digital Transformation Blueprint](#) describes a plan to implement a 'My Account' feature for users, that simplifies and streamlines services for them across the 400+ different applications that Aberdeen operates, and in [this document](#) define their business case for their own investment into an MDM capability.

Their Digital Plan lists a number of specific objectives towards this goal:

North Lanarkshire Council streamlines its citizen portal with MDM-enabled Single Signon

1. *Our Staff will spend less time inputting and updating information in systems as we join them up so they do it automatically.*
2. *Our Staff will have the right information to help customers, as we improve the way we share and join up our data.*
3. *Use our data to identify you so that you do not need to provide the same data many times.*
4. *Hold one set of customer information across all key systems.*
5. *Implement a single account for external customers.*
6. *Introduce a Single and staff account to allow for the federation of core systems with other organizations such as Aberdeenshire Council and the NHS.*

A critical point to highlight is that these are common requirements across all Scottish authorities.

For example in [their roadmap plans](#) East Ayrshire describes “*Unified Customer Accounts / Single-View – Wherever possible, services will be provided that allow a single ID to enable a consistent unified view of the customer*”, and similarly Dundee City Council describe the same functionality requirements in [their roadmap](#):

“Delivering on online customer portal and working towards creating a single identity for our citizens to make requesting services simpler, all linked through our citizen account, MyDundee.”

British Columbia pioneers Self-Sovereign Identity - Building Digital Trust into the Web



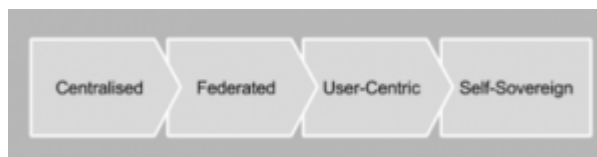
Digital Identity refers to the various usernames and log-on procedures we use to interact with web sites and other digital services.

[Michael Gorriz](#) explains how Identity is a universal function, one that spans across government, banking and every other online service that we use.

Government identity programs, such as [Gov.UK Verify](#), seek to leverage this interconnectedness through linking their authentication systems with others like banks to streamline the procedure from a users perspective, an approach known as 'federated identity'.

Self-Sovereign Digital Identity

However some in the industry will describe this as an 'old technology' approach, and that the future is one of 'Self-Sovereign Identity', being pioneered by organizations such as the [Sovrin Foundation](#).



As the diagram from [this Tieto article](#) describes it can be seen as the first step in a maturity journey, an improvement on from centralized model which means a duplicated identity procedure for each and every web site.

The article introduces Self-Sovereign Identity and positions it as the ultimate conclusion to this maturity journey.

Described in detail in [this ID2020 white paper](#) as the name suggests the primary feature is an identity mechanism owned and controlled by the user themselves, and introduced in [this short presentation](#) the fundamental principles are described as:

British Columbia pioneers Self-Sovereign Identity - Building Digital Trust into the Web

- Every individual human being is the original source of their own Identity.
- Identity is not an administrative mechanism for others to control.
- Each individual is the root of their own identity, and central to its administration.
- The role of names, citizenship, licences and other credentials should be distinct.

In short it places control and ownership of identity in the hands of the users themselves, not a third party like banks or the government, setting in place the keystone foundation for an entirely citizen-centric Digital Democracy.

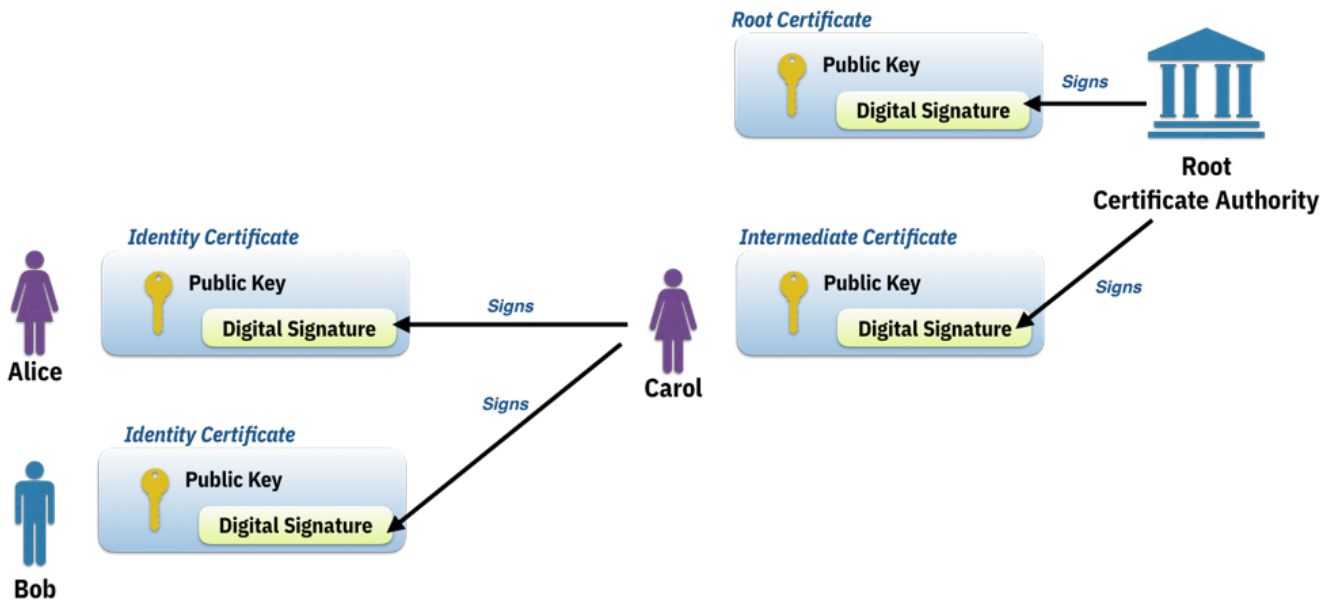
Via his [blog](#) tech industry luminary Phil Windley describes the launch of the [Sovrin Network](#), the world's first self-sovereign identity (SSI) network, intended to implement the technologies and these principles.

Self-Sovereign Identity – Rebooting the Web of Trust

Doing so highlights critical features of the required technical design for the blueprint, most importantly that Blockchain alone is not the complete answer. In particular, as exemplified by the role of our ID documents, the other essential piece of the jigsaw is Digital Identity, and within that field the emerging trend of 'Self-Sovereign Identity'.

Pioneered by the [Sovrin Foundation](#) this brings the decentralized web approach, rather than centralized, to the technologies we use to manage our digital identities, sign in to web sites, enable data sharing and so on. They combine and implement this architecture with Blockchain through their Hyperledger 'Indy' project, a code base that enables creating and managing decentralized, self-sovereign identities using distributed ledgers.

British Columbia pioneers Self-Sovereign Identity - Building Digital Trust into the Web



IBM joined Sovrin and their expert Dan Gisolfi explains [the terminology](#) and provides an overview of this ecosystem operates.

In [this blog](#) he explains how this technology combination enables “Trust Chains”, the core building block of the new Digital Economy now being built atop the first generation Internet, the “The Second Digital Age” Alexander Tapscott describes in the featured video.

British Columbia OrgBook - 'Tell Us Once' via Blockchain and Self-Sovereign Identity



As [the previous blog](#) describes Canada is beginning to adopt a 'Tell Us Once' approach for achieving integrated Digital Government.

Via their 'OrgBook' project British Columbia offers a technology blueprint for achieving this approach.

This is for a use case of business registrations, a very powerful case study that harnesses the latest technology innovations including the Blockchain and Self-Sovereign Identity.

Red Tape Reduction

As [their case study](#) explains a primary motivation for the project is to greatly reduce the bureaucracy associated with small business administration.

British Columbia OrgBook - 'Tell Us Once' via Blockchain and Self-Sovereign Identity

Small businesses in Canada face a daunting work load – Companies with less than five people pay C\$6,744 per worker just meeting regulations.

Even a sole proprietor in Canada must use at least three different tax numbers, and starting a new business is like navigating a maze with three levels: local, provincial, and federal.

The core benefit of a Tell Us Once approach is eliminating the need for citizens to repeatedly populate workflow forms with data they have already provided to another agency. In Estonia for example your tax return application application is pre-populated with data from other databases, indeed the requirement to do so is mandated by law.

How to reduce this type of bureaucracy to boost economic output is a key research focus for the EU, who have been conducting [extensive research](#) into this, publishing [this report](#).

Verifiable Organizations Network

The OrgBook project sought to bring this same efficiency to small business applications for British Columbia, launching the 'VON' – Verifiable Organizations Network.



British Columbia OrgBook - 'Tell Us Once' via Blockchain and Self-Sovereign Identity

The OrgBook is a repository of web-searchable public credentials, instances of **VON issuer/verifier agents**, the equivalent of “Permit to Operate” documents posted on businesses’ walls. It acts as a digital marketplace, matching organizations applying for permits to those who issue them, verifying the integrity of that process through Self-Sovereign Identity methods.

The register is a decentralized, Self-Sovereign identity network built on Blockchain technology, using the **Sovrin Foundation**’s Sovrin Network as the underlying Identity Registry Network.

As an organization goes through the online application processes to acquire registrations, licenses or permits, the services get proofs (and their associated verified claims) from verifiable credentials already stored in OrgBook about the organization. Once a service completes the approval process and decides to issue the organization a registration, licence or permit, they issue that public verifiable credential digitally to OrgBook about the organization.

This saves the users from having to re-type the information for each service (and eliminates typos in the data). Each service can trust the information because it comes from a trusted source, cryptographically proving:

- - The information was issued by the issuer.
 - The information was issued to OrgBook.
 - The information has not been tampered with (was not forged).
 - The information has not been revoked.

Blockchain and Self-Sovereign Identity

An especially helpful primer to this technology and case study is offered through this webinar (below) from **John Jordan** of the British Columbia ID team, one of the first governments to pioneer adoption of Blockchain and Self-Sovereign Digital Identity technologies for government use cases.

Particularly noteworthy points include:

British Columbia OrgBook - 'Tell Us Once' via Blockchain and Self-Sovereign Identity

- Enacting **the legislation required** to underpin the technology framework for Identity-enabled digital services.
- How previous Identity approaches (the “old technology”) resulted in semi-digital versions of the offline paper-based process, resulting in yet more multiple online accounts, an effect greatly exasperated by the many levels of government citizens must interact with to complete one process (eg. business permits etc.)
- A Continuous Integration capability enabled by RedHat Openshift-based Government as a Platform architecture.
- Starting off with a proof-of-concept to trial key technologies like the Blockchain, in conjunction with **DIACC** and based on an early version of the **Hyperledger Fabric**.
- How the key is to approach design models as an Ecosystem, the ‘Decentralized Identity Solar System’.