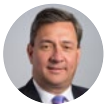
The Identity Revolution: How Digital IDs Are Reshaping Modern Registries

Exploring the Impact of Digital IDs on Legal Entities and Natural Persons

Authors

John Murray
VP Operations, Foster Moore, Europe

Bill Clarke
VP Business Development, Teranet, Canada



Ricco Dun
Senior Business Development Manager, Global Legal Entity Identifier Foundation (GLEIF), Switzerland

Tambet Artma
Business Register Team Lead, Centre of Registers and Information Systems (RIK), Estonia

Foreword

In our ever-evolving digital landscape, organizations worldwide are rethinking their business operations, data governance, and strategic frameworks to align with the dynamic demands of a data-centric future. This transformation necessitates a collaborative, internationally focused approach, emphasizing the adoption of a unified data strategy that encompasses shared visions, objectives, principles, standards, processes, and mechanisms. Central to this strategy is a user-centric approach that builds trust among stakeholders, ensuring data interoperability, security, and privacy.

The Paper "The Identity Revolution: How Digital IDs Are Reshaping Modern Registries" focuses on the transformative impact of digital identification systems for legal entities and natural persons. It highlights the crucial role of digital IDs in enhancing security, interoperability, and regulatory compliance, which collectively improve the delivery of government e-services, recording of payments, and financial transactions, among other benefits. This Paper offers a comprehensive review of best practices for digital identity systems and their adaptation in registries, incorporating legislative frameworks and technological innovations from global initiatives such as the UN, the European Union as well as national efforts underway in Canada focused on interoperability, trust, security and privacy, and user-centricity.

A notable example is the verifiable Legal Entity Identifier (vLEI) under the GLEIF, which facilitates cross-border identification of legal entities essential for monitoring and verification of financial transactions. Additionally, the United Nations Sustainable Development Goals (SDGs) are significantly supported by the advancement of digital IDs for natural persons, particularly SDG Target 16.9 ("legal identity for all, including birth registration by 2030") and SDG 17.19, which aims to enhance statistical capacity in developing countries through legal identity management.

Reading this Paper, and others published in the Series, from the perspective of a United Nations international standard setter for official statistics, I recognize the striking consistency and coherence of the proposed operating model for registries with the national and international data strategies and the more domain-specific statistical strategies. With a similar understanding of the current digital and technological environment and the transition to a future data model based on shared principles, business processes, and mechanisms, there is a seamless opportunity for industry and government experts to work together.

In this context, I would like to highlight a collaborative initiative, 'The Global Initiative on Unique Identifiers for Businesses,' developed by the United Nations Statistical Division (UNSD) in collaboration with the United Nations Committee of Experts on Business and Trade Statistics (UNCEBTS) and the GLEIF. This initiative aims to enhance transparency and improve the registration and availability of unique business identifiers in administrative data sources globally, promoting access to, and sharing of, administrative data for statistical business registers.

Engagement with this initiative by industry and registry domain experts would be mutually beneficial and align perfectly with the national and international collaborative principles and best practices outlined in this Paper. It underscores the call for industry and registry domain experts to work closely with government and international agencies to integrate the proposed domain-specific target operational model (TOM) for registries with broader national and global data strategies.

Ivo Havinga

Director 1 United Nations Statistics Division (retired)
Department of Economic and Social Affairs,
United Nations

Introduction

Digital identification (ID) systems are revolutionizing the way legal entities and natural persons interact and transact in the digital realm. The adoption of digital IDs has experienced a notable surge in recent years, propelled by factors such as interoperability, convenience, security, regulatory compliance, transparency, and the increasing digitization of services. Digital identities are the basis for trustworthy digital transactions.

To date, governments around the world have launched around 165 digital, or partially digital, ID schemes. However, their track record is mixed. Only a few programs, in particular Estonia, have achieved high levels of adoption, but predominantly across the board, use rates are often low, averaging just once or twice a year per person in some countries.[1]

These digital identifiers serve as standardised and secure authentication methods, facilitating seamless access to online platforms, government services, financial transactions, and more. Digital IDs can substantially streamline relations between governments and the private sector in areas including corporate registrations, taxes, economic support, permits, and authorizations. By enabling online interactions, the technology can lead to significant cost savings.[2]

Notably, the implementation of digital IDs has gained significant traction within the European Union (EU), where initiatives like the eIDAS Regulation have laid the foundation for a common legal framework governing electronic identification and trust services[3]. Equally notable is the work that has been underway in Canada with the development of the Pan-Canadian Trust Framework (PCFT) and its support in the evolving digital landscape, shaping the future of digital identity both domestically and on the global stage. These established frameworks are essential to fostering interoperability and cross-border recognition, marking them as a pivotal step towards a unified digital landscape.

As digital transactions continue to proliferate, digital IDs and portable digital wallets are poised to play a pivotal role in facilitating secure and convenient payments, identity verification, and access to services. Furthermore, advancements in technologies such as blockchain, biometrics, and decentralized identity solutions hold promise for enhancing the security and usability of digital wallets, paving the way for broader adoption and seamless integration into everyday life. As a result of this ongoing evolution, modern registries are undergoing a transformative shift with the need for integration of digital identification (ID) systems, revolutionizing the way legal entities and natural persons engage in digital interactions across government services.

In this paper, as we investigate the multifaceted impacts of digital IDs on legal entities and natural persons, exploring the historical evolution around identities, we will pinpoint how registration systems are key to the successful implementation and organization, the regulatory frameworks, technological adaptation, and market trends shaping their evolution.

We will also point to the innovations and learnings from the electronic Identification, Authentication and Trust Services (eIDAS) program in the EU and provide key insights around the developments and strategies from Estonia Centre of Registers and Information Systems (RIK). We will also highlight the evolution and adaptation of the Pan Canadian Trust Framework and its core applicability to enabling regional digital IDs. On the digital entity (i.e. corporate) relationship we will interrogate the international framework and directives supporting verifiable Legal Entity Identifiers (vLEIs) under the Global LEI Foundation (GLEIF).

Through these explorations, it is the aim of the authors to provide insights into the transformative power of digital IDs and their role in shaping the future of digital commerce, identity management and the evolution and maturity of modern registry platforms for government.

The Importance of Identifiers in Registration Systems

The basic units of social analysis are "neither individual entities (agent, actor, firm) nor structural wholes (society, order, social structure) but the relational processes of interaction between and among identities."[4] Registration systems are the record keepers, the bearers and sources of truth, with respect to their legislation or regulation. Registers keep records based on proof and other means of ensuring the accuracy of their records. One particular type of mechanism used by registers is called a credential. Credentials are not just any assertion of claims; rather they are meant to be trusted (to be accorded the status of truth) and, as a result, they need to meet a number of requirements that make them credible and reliable, in the relevant context of a register.[5] This credential within a register is created by (1) Face to Face – similar to a notarial system establishing the bona fides of a client with a physical presentation of identity; (2) Paper – presenting certified copies of organisations, identities and other claims; (3) Digital Identity – biometrics, online identity validation by the register, etc.

Identifiers in registration systems logically break down into two types, legal entity identifiers and natural person identifiers. Indeed, it could be argued that the sole purpose of a registration system (and a register) is to identify the natural person to which the asset (entity being registered) has a relationship to and create that link between such.

In 2021 the EU DG FISMA has explored where these relationships can be found in all the statutory and available registers, to be collated, to provide a holistic approach for AML purposes. Indeed, it is exploring the feasibility of a pan 'European Asset Register'[6].

History of Identities

In ancient Mesopotamia, around 3500 BCE, clay seals were used to establish personal identity. These seals, often engraved with unique symbols, acted as signatures on clay tablets, providing authenticity and authorisation. This practice enabled individuals to secure their identities and protect important documents, establishing the foundations of identity management.

With the advent of writing, written signatures emerged as a form of identity verification. Ancient civilisations such as the Egyptians and Greeks used signatures on papyrus scrolls and wax-sealed parchment to authorise documents and establish legal agreements. The transition from seals to signatures introduced a more portable and scalable means of identity management.

Digital Identities began with the age of the internet[7]. Before, such identities were representations in terms of identifiers within a database schema. These representations were limited and didn't constitute what we now consider digital identities. Identity was primarily established through physical documents like birth certificates, passports, and driver's licenses.

The popularisation of the internet brought about the need for digital identities to facilitate online interactions and transactions. Early forms of digital identities included usernames and passwords for accessing email accounts, online forums, and early social networking sites.

It quickly became apparent that identifying individuals and services on the anonymous internet was going to be of paramount importance for real commerce. Thus, the advent of Digital Certificates, Server Certificates, Identity and Access Management (IAM) systems, authentication protocols, and privacy-enhancing technologies. Various technologies emerged but multifactor authentication and biometrics have revolutionised digital identity services. Registration systems generally have been slow to adopt these technologies and much of the domain still relies on simple usernames and passwords and systems that offer little in terms of non-repudiation, much less have they been tested in their respective courts.

History of Legal Entity Identifiers

Legal entity identifiers reflect the actual evolution of registration systems and the increasing importance of standardised identifiers in the modern global economy. Early, registration systems, used unique identifiers within guilds and societies for the purposes of legally operating and participating within a certain trade activity. These identifiers were usually sequential numbers and unique only to the guild.

The concept of a jurisdictional register with unique identifiers, began with the advent of modern legislation, particularly in the early 19th century, with respect to company law. This legislation was adopted to support the increased economic activity, that marked the industrial revolution. A new entry, with a sequential identifier recorded physically as an entry in a ledger or book, that gave legal precedence to a corporate body/entity. And so, registration systems developed and expanded within jurisdictional contexts, by simply adding to a system of sequential numerical identifiers (with prefixes and suffixes in some cases for legal form). That is apart from states like New York, that does not currently assign any unique identifiers to companies registered within its jurisdiction. Similarly, legal entities within Germany, assign unique identifiers, per legal form, per commercial court. Regardless, each jurisdiction managed their own identifiers within their own registration system. This was all logical until the advent of cross border transactions, including registrations, and inevitably the need to identify/certify registration details out of a local jurisdiction.

Thus, began the era of interoperability, a multifaceted and complex issue, requiring support from policy makers, regulatory bodies and adoption from governmental and private sector actors to become truly successful. In our previous Paper, on Interoperability and Data Exchange Across Registries[8], we explore these complexities and look at key jurisdictions solving some of these longstanding issues.

Natural Person Identifiers

Unique natural person identifiers have been created for a broad range of social security, general security applications, government IDs, and tax purposes. These numbers have been typically issued by licensing, regulatory, health, registry, social security, and tax authorities. The variance of these numbers is not the subject of this paper, but our focus is how they have found their way into use within registration systems.

The numbers include passport numbers, social security numbers, health identity numbers, national identity numbers, personal identity numbers. Identifiers for any object/entity must consider the qualities of the identifiers in more detail: scope, uniqueness, granularity, intelligence, actionability, persistence, extensibility, and context.[9] Registration systems have used these identifiers in an attempt to tag the natural person being entered on their register, or to simply affect some signature process.

This whole area is now fraught with uncertainty, whereby data privacy regulations define what can be legitimately retained or not. This leads to the whole questions of personal and non-personal data. Notwithstanding the pivotal importance of the distinction between personal and non-personal data, it can, in practice, be extremely burdensome to differentiate between both categories. This difficulty is anchored in both technical and legal factors. From a technical perspective, the increasing availability of data points as well as the continuing sophistication of data analysis algorithms and performant hardware makes it easier to link datasets and infer personal information from ostensibly non-personal data. From a legal perspective, regulations rarely include a list of what is definitively personal data.

Jurisdictions that do not have the luxury of a unique national identifier have resorted to all and any available identifiers for individuals to be included on their registers. In non-notarial jurisdictions this has proved quite burdensome to the registration authority whereby individuals are not uniquely identified and more than often duplicated on the same register, e.g. when they have roles in multiple registered entities. Notwithstanding that the bona fides of the individual are rarely verified. This is highlighted most recently whereby the UK has reformed all their company legislation to enforce a regime of identification of all natural persons on their registers.

The notarial registration systems rely on intermediaries, agents, and or third parties to perform the KYC on the individual and then the registration system simply receives a summary of the information, whereby an identifier is created for the relationship. The authors assume that in most cases of this form, the registration authority would not have the ability to prove the identity of the relationship without recourse to the third party who performed the KYC validations.

We have seen a significant righting of the ship in terms of registration systems, from the heady days of the World Bank Doing Business Report (WBDBR) and their respective regulatory reforms. 'Quicker, faster and cheaper' in terms of registration systems has virtually lost all context with respect to register, where the value and integrity of the registers and its information, is now and in our opinion, correctly central. To that end, the validation of, exchange of, and the correct application of natural person identifiers, will become increasingly important for registers, and even more so for common law registers, where there has traditionally been very little KYC of the natural persons on their registers.

The Criticality of Interoperability – "Getting it Right"

A digital identity is only as useful as the context in which it can be used. A key determinant is its level of interoperability—the ability of the ID system to exchange data with other systems, databases, devices, and applications. A priority for governments can be to ensure interoperability across private and public service providers domestically, as well as ID systems in other jurisdictions. The risk of not ensuring interoperability is that digital ID schemes lose momentum, leading to fragmentation as service providers build authentication tools compatible with their own needs.[10]

Interoperability on the level of service provision is necessary to promote seamless integration with the systems and processes of service providers. Several early examples around interoperability across business registers, from across the US and Europe, identify some of the complexities around regulatory harmonization and operational efficiencies.

> The risk of not ensuring interoperability is that digital ID schemes lose momentum, leading to fragmentation as service providers build authentication tools compatible with their own needs.

Business Register Interoperability Throughout Europe (BRITE)

In 2004, the BRITE project funded by the European Commission (EC) and coordinated by the European Business Register sought to resolve the very real operational difficulties presented by the latest European Company Law Directives. The project was an integrated project funded by the EC with both private and public consortium members.

The issues were that in particular the 11th and 14th Company Law directives required Business Registers in the EU/EEA to interoperate with other business registers, to maintain compliance of the legal entities on their registers. The difficulties presented for these registers were simple – (1) How to uniquely identify the register they wished to communicate with and (2) how to uniquely identify the entities on those registers. The BRITE project created two unique constructs:

a. **Directory of Registers (DOR)** – in effect a register of European registers, this register authenticated the existence of the Business Register. This would seem like a trivial task, but business registration within the EU includes, private/public, administrative/judicial and centralised/decentralised registration authorities. A unique identifier was given to each register. A register was not the registration authority but the physical register per jurisdiction.

b. **Registered Entity Identifier (REID)** – a unique identifier for all legal entities in the business registers in Europe. It consisted of the concatenation of the two letter ISO country code, the DOR, the unique identifier in the register and a two-digit check sum. The REID followed a similar convention to the IBAN that originated in Europe in the early 1990s as part of the European Committee for Banking Standards (ECBS) initiative to standardise banking practices across the European Union (EU) and European Economic Area (EEA).

The BRITE project was deemed a success as it set out clearly the constructs and the path forward to facilitate the interconnection of business registers in Europe. The project ended in 2006 and shortly afterwards the green paper on the interconnection of Business Registers was published in 2009 by the EC[11.]

Business Register Interconnection System (BRIS)

Following on from the green paper, the directive was finally published in the EU on the Interconnection of Business Registers[12]. This stated the requirement to establish a platform to facilitate such interoperability. It took 5 years to implement the platform and it would not be unfair to state BRIS has not met the expectation of Business Registers in terms of the improvement of their operations, and the regulation of the entities on their register. These participatory Business Registers have also been mandated to integrate with said platform[13].

The pursuit of interoperability across identity frameworks, exemplified by initiatives such as the BRITE project and the subsequent development of the Business Register Interconnection System (BRIS), underscores the importance of cohesive and standardised approaches in facilitating seamless interactions between legal entities and natural persons across borders.

The use of the REID (now the EUID in BRIS) was envisaged for the exchange of information between EU/EEA business registers in the case of cross border mergers and to keep track of the relevant data of branches of companies in other Member States.

Data Universal Numbering System (DUNS)

DUNS numbers are private unique nine-digit identification numbers assigned to businesses by Dun and Bradstreet (D&B). D&B is a global data and analytics intermediary. As the system that evolved in the US under company law, each State assigned its own registration system, so at a federal level an identifier was needed to uniquely identify these registrations at a state level.

DUNS numbers are widely used internationally and are recognised as a standard business identifier in many countries. This was supported by the Federal US Government requiring a DUNS number of to contract with it. DUNS are not assigned by governments like their own jurisdictional and other identifiers (such as state-issued file numbers), they are commonly used by businesses to establish their identity and credibility in the business world. DUNS numbers are not mandatory and since 2021 the U.S. federal government has transitioned away from using DUNS numbers for certain purposes, such as for entity identification in the System for Award Management (SAM).

Overall, the failure of the DUNS system in the US underscores the importance of designing business identification systems that prioritize transparency, accessibility, interoperability, and government oversight to serve the needs of businesses and government agencies effectively.

Towards Seamless Integration: Interoperability in Digital Identity Solutions

While challenges persist, including the complexities of uniquely identifying registers and entities, these efforts represent significant strides towards harmonizing regulatory compliance and enhancing operational efficiency within the European Union and beyond. As the evolution of digital identification systems continues, guided by principles of interoperability and transparency, the potential for transformative impact on business practices and regulatory frameworks remains immense, promising a future where cross-border transactions are conducted with unprecedented ease and confidence.

The developments around the cooperation between business registers in Europe has one major limitation in that everything, including the use of the identifier (the EUID) is restricted to the EU/EEA area. It is important to think from a global perspective when looking at the topic of this paper.

There are two critical steps to achieving a high level of interoperability. The first is committing to standards in accordance with global best practice. These can help ensure interoperability in respect of technology (for example, biometrics, cards, digital signatures) and data, meaning the structure of information collected and used by the system. The second is implementing technologies enabling data transfer to and from other systems, including technical interoperability layers, web services, and application programming interfaces.[14]

These key thrust points as well as other global directives in the evolution of digital identification solutions can be further described as essential efforts that must incorporate:

Facilitating Trust and Security:

- Legal digital identifiers ensure authenticity and integrity in digital transactions, reducing the risk of fraud and identity theft.
- They enable secure access to sensitive information and services, fostering trust between parties involved in digital interactions.

Enhancing Efficiency and Interoperability:

- Standardised digital identifiers streamline processes such as payments, contracts, and regulatory compliance, reducing administrative burdens and costs.
- They promote interoperability (locally, regionally and globally) between different systems and platforms, enabling seamless data exchange and integration across diverse applications and organizations.

Enabling Regulatory Compliance and Governance:

- Legal digital identifiers help enforce regulatory requirements by providing a reliable means to track and monitor activities in regulated industries such as finance, healthcare, and telecommunications.
- They support government initiatives aimed at combating money laundering, tax evasion, and other illicit activities by improving transparency and accountability in digital transactions.

Empowering Digital Innovation and Economic Growth:

- By providing a foundation for digital infrastructure, legal digital identifiers stimulate innovation in emerging technologies such as blockchain, artificial intelligence, and the Internet of Things (IoT).
- They unlock new opportunities for digital entrepreneurship and market expansion, driving economic growth and job creation in the digital economy.

The transformational benefits brought about by digital identifiers extends beyond legal entities and natural persons, as noted above. For entities, digital IDs streamline operations, enhance security, and facilitate compliance with regulatory requirements. They enable organizations to conduct business seamlessly across borders, access government services digitally, and interact with customers in a secure and efficient manner.[15]

Global Frameworks for Digital Entity Identifiers

Legal Entity Identifier (LEI)

The Legal Entity Identifier (LEI) is a unique global identifier for legal entities. It was introduced by the G20 Ministers of Finance and the Financial Stability Board (FSB) in response to the global financial crisis of 2007-2008 to improve transparency and enhance risk management in financial markets.

The Legal Entity Identifier (LEI) is a 20-character[16], alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). As such, it is the only globally officially standardised identifier for legal entities. It connects to key reference information that enables clear and unique identification of legal entities. This data is validated with the information from the official business register in each country or from another relevant registration authority. All the basic data to adequately identify a legal entity are available in the LEI reference data, such as the official name of the entity, additional trading names (all names transliterated into Latin characters in case of languages with different character sets), the registration authority where the entity is the registered, the local registration number, the jurisdiction of formation, the legal form, the legal address and the headquarters' address.

Each LEI also contains information about an entity's ownership structure and thus answers the questions of 'who is who' and 'who owns whom'. This information is based on the accounting consolidating information and shows the direct and ultimate parents and the direct and ultimate children of an entity.

> Simply put, the publicly available LEI data pool can be regarded as a global directory, which greatly enhances transparency in the global marketplace. It is considered a 'broad public good'.

Simply put, the publicly available LEI data pool can be regarded as a global directory, which greatly enhances transparency in the global marketplace. It is considered a 'broad public good'.

Within the LEI, which is directly based on an ISO standard itself, more data are standardised to create the best possible reference data. GLEIF has developed a 'Registration Authorities list, which contains more than 1.000 business registers and other relevant registration and validation authority sources from around the world and assigns a unique code to each register / authority on the list.

Additionally, GLEIF acts as the Maintenance Agency Secretariat for the ISO 20275 Standard 'Entity Legal Forms (ELF) Codes'. The basic behind this is to have a list of all legal forms/types of all countries in the world, which substantially adds value to the standardisation of legal entity identifiers[17]. The current version lists more than 3,400 entity legal forms across more than 185 jurisdictions. The list contains legal forms/types in their native language, such as limited liability company (Ltd), Gesellschaft mit beschränkter Haftung (GmbH) or Société Anonyme (SA). The ELF Code List assigns a unique code to each entity legal form. The ELF code is an alpha-numeric code of four characters from the basic Latin character set. Integrating ELF codes into the standardised set of reference data on a legal entity available within the Global LEI Index further enhances the information included in each Legal Entity Identifier (LEI) record. The richer data provides an improved user experience, because it helps to categorize legal entities and therefore allows for more insight into the global marketplace.

Verifiable Legal Entity Identifier (vLEI)

GLEIF has also pioneered a new form of digitized organizational identity to meet the global need for automated authentication and verification of legal entities across a range of industries called the verifiable LEI (vLEI). The vLEI concept is simple: It is the secure digital counterpart of a conventional LEI. In other words, it is a digitally trustworthy version of the LEI code which is automatically verified, without the need for human intervention.

By wrapping new and existing LEIs in digital credentials that can be verified, the vLEI offers a digitally trustworthy version of the LEI which allows automated entity verification, thus can replace the manual processes conventionally required to access and confirm an entity's LEI data. Because the vLEI leverages the well-established Global LEI System, which is the only open, standardised and regulatory-endorsed legal entity identification system, it is capable of establishing digital trust between all organizations, everywhere.

The vLEI ecosystem utilizes the existing Global LEI System as the only open, standardised, and regulatory-endorsed system for legal entity identification. It is based on the Trust over IP Governance metamodel and leverages open standards including the ACDC (Authentic Chained Data Container) specification, the KERI (Key Event Receipt Infrastructure) protocol for key management, and the CESR (Composable Event Streaming Representation) capabilities for secure digital signing.

By using secure credentials and open standards, the vLEI creates a verifiable link between an organization and its representatives. These digital credentials are not only tamper-resistant but also verifiable in a decentralized manner, providing an ideal foundation on which to establish a secure chain of trust with GLEIF at the root.

Once an organization has obtained its vLEI it can proceed with the issuance of additional vLEI credentials to authorised representatives of the organization, allowing them to digitally confirm their authenticity (their name and their official role) when performing sensitive business activities, such as remotely approving transactions, or e-signing contracts.

To be able to use existing roles for such representations, GLEIF uses the ISO Standard 5009 'Official Organizational Roles'. A new ISO standard was published, supporting the uniform inclusion of 'official organizational roles' in LEI-based digital identity tools. The significance of ISO 5009 was its capacity to pave the way for vLEI credentials and digital certificates with embedded LEIs to become a universally trusted method of digitally confirming the authenticity of people authorised to act on behalf of an organization. The combination of LEIs and official organizational roles within digital identity credentials promotes greater trust in the authenticity of an entity's authorised representatives, enabling new digital identity management use cases.

GLEIF Role Credentials can be issued by persons whose Official Organizational Role can be verified both by the organization as well as against one or more public sources, or through official documents obtained from the organization such as Board minutes or resolutions, statutes or articles, which would validate the name and the role of the OOR Person.

GLEIF has recognised within the entity and natural person identifier domain a space that is currently not served. This approach is set to transform the nature of identity management and how person-to-entity, or entity-to-entity, interactions take place in the digital world. The need for the vLEI will continue to grow as we move into an automated, digitized future for organizations. Now, they can be equipped with a universally interoperable, decentralized trust system that can operate independently, with the highest levels of security, privacy, and ease of use.

UN Initiatives

The United Nations (UN) directives on digital IDs shape governments' future strategies. The United Nations is working on its Legal Identity Agenda for natural persons. Everyone has the right to be recognised as a person before the law, as enshrined in Article 6 of the Universal Declaration on Human Rights and Article 16 of the International Covenant on Civil and Political Rights. Several International human rights instruments, such as Article 7 of the Convention on the Rights of the Child and Article 24(2) of the International Covenant on Civil and Political Rights also recognised a right to birth registration.

Sustainable Development Goal Target 16.9 ("legal identity for all, including birth registration, by 2030") is key to advance the 2030 Agenda commitment to leave no one behind, and equally relevant is SDG 17.19 — support to statistical capacity-building in developing countries, monitored by the indicator "proportion of countries that have achieved 100 per cent birth registration and 80 per cent death registration".

The UN Secretary-General's Executive Committee has decided to "convene UN entities to develop, in collaboration with the World Bank Group, a common approach to the broader issues of registration and legal identity". To operationalize the decision of the Executive Committee, an inter-agency coordination mechanism — the UN Legal Identity Agenda Task Force (UNLIA TF) — was established where 13 UN agencies are working together to try to assist Member States achieve SDG target 16.9.

UN Principles on Identification promote inclusive, privacy-respecting systems. Digital Identity Guidelines provide standards for secure, interoperable systems . Adhering to these directives ensures citizen-centric, trustworthy digital ID initiatives fostering social inclusion and sustainable development.

On the topic of 'business identity', the United Nations Statistical Division (UNSD) in collaboration with the United Nations Committee of Experts on Business and Trade Statistics (UNCEBTS) and the Global Legal Entity Identifier Foundation (GLEIF) have developed 'The Global Initiative on Unique Identifiers for Businesses'. This initiative was developed to strengthen the transparency on businesses in countries by improving their registration, to improve the availability of unique business identifiers in administrative data sources in countries; and to promote access to and sharing of administrative data for statistical business registers. The LEI can play a vital role in this initiative, both as the overarching globally unique identifier to bring together data (with separate identifiers) from different sources, but is also available as the local identifier if in (developing) countries a new registration system is being set up.

UN Principles on Identification promote inclusive, privacy-respecting systems. Digital Identity Guidelines provide standards for secure, interoperable systems.

A Look at Progressive Regional Digital ID Frameworks

The EU Directives

The implementation of digital IDs has been particularly significant in the European Union (EU), who has been at the forefront of developing a legislative framework and implementing digital IDs through initiatives such as the eIDAS Regulation (electronic Identification, Authentication and Trust Services)[18]. eIDAS aims to establish a common legal framework for electronic identification and trust services across EU member states, enabling cross-border recognition of digital identities and facilitating secure electronic transactions.

Key aspects of the EU's legislative framework and implementation of digital IDs include:

- **eIDAS Regulation:** The eIDAS Regulation sets out rules for electronic identification and trust services, including electronic signatures, seals, timestamps, and website authentication. It establishes mutual recognition among 27 EU member states for electronic IDs issued by notified electronic identification schemes (eID schemes).

- **National eID Schemes:** EU member states are responsible for implementing their own national electronic identification schemes in compliance with eIDAS requirements. These schemes enable citizens and businesses to access public services and conduct electronic transactions securely.

- **Interoperability and Cross-Border Recognition:** eIDAS promotes interoperability by ensuring that electronic IDs issued in one EU member state are recognised and accepted in other member states. This facilitates cross-border e-government services, e-commerce, and digital interactions within the EU.

- **Trust Services Providers:** eIDAS regulates trust service providers (TSPs) who offer electronic identification, authentication, and electronic signature services. TSPs must comply with specific requirements regarding security, transparency, and liability to ensure the integrity and reliability of their services.

- **Secure and User-Centric Solutions:** The EU prioritizes the development of secure and user-centric digital identity solutions that protect individuals' privacy and data protection rights. eIDAS emphasizes the importance of user consent, data minimization, and confidentiality in electronic identification and trust services.

- **Digital Single Market Strategy:** The EU's Digital Single Market (DSM) strategy aims to remove barriers to the free flow of digital goods, services, and data within the EU. Digital IDs play a crucial role in enabling seamless cross-border transactions and fostering trust in digital markets.

The eIDAS (Electronic Identification, Authentication and Trust Services) program has undoubtedly brought positive impacts and outcomes to the digital landscape of the European Union by fostering cross-border trust and enabling secure electronic transactions. Its implementation has facilitated greater convenience and efficiency in online services, bolstering e-commerce, e-government initiatives, and digital interactions across borders. However, despite these achievements, eIDAS still faces challenges and gaps in certain key areas. These include issues related to interoperability between different national electronic identification schemes, varying levels of adoption and trust in eID solutions across member states, and the need for further harmonization of legal frameworks to ensure consistency and clarity in the application of eIDAS regulations.

Estonia's Digital ID Journey

One of the leading EU jurisdictions in digital developments is Estonia. Estonia stands as a beacon of digital governance, with its pioneering advancements in digital identity infrastructure garnering global recognition from institutions like the World Bank, Forbes, and the Financial Times. The genesis of Estonia's digital identity landscape can be traced back to two pivotal initiatives: the assignment of a unique personal identification number, known as the "Isikukood," to every citizen and resident, and the issuance of 10-year passports.[19] Digital identity systems are the core of a digital infrastructure that enables individuals to participate effectively in a society as digital citizens.[20].

One of the many possibilities for Estonians in leveraging their digital ID's is for electronic voting, in fact, the first application being utilized in the world, from anywhere in the world. This is enabled with advanced crypto solutions and security, which is the foundation of the solution ensuring digital trust. And this digitally secure trust solution has been in place since last parliamentary elections in 2023, where more than half of all votes were cast electronically. It is possible that mobile voting will likely available in Estonia in 2025.[21]

Estonia's digital government architecture revolves around two pillars: the X-Road[22] and digital identity. X-Road is a secure data exchange platform designed to facilitate interoperability between various public and private sector databases and information systems. It enables secure and standardised data exchange, ensuring the seamless flow of information between different organizations and government agencies, while maintaining data integrity and privacy.

Estonia's approach to digital identity, particularly through its e-Residency program developed over a decade ago, serves as a notable example for other countries.

These components synergize to automate e-government processes effectively. The smart card and X-Road, released simultaneously, facilitated seamless data exchange, with the X-Road handling nearly one billion queries annually, 95% of which are automated. Estonia's approach to digital identity, particularly through its e-Residency program developed over a decade ago, serves as a notable example for other countries[23].

The Estonian Digital ID landscape is unique both in terms of its complex legal framework, and the reliance of Estonian residents on their Digital IDs. Digital governance is viewed as integral parts of governance and identity and focuses more on sector specific applications rather than "digital" legislation.[24]

The Estonian legal system is designed such that there is little overarching legislation governing all aspects of the use of the ID. The ID is permitted to be used for any purpose provided there is a valid law that permits it. Thus, while the ID Act governs the issue of the ID, it does little to regulate any other aspect of the use of the ID itself — including the sharing of collected data — and thus leaves such critical matters unaddressed, to be determined by other laws or regulations. Although this is done deliberately, to have sector specific governance informed by the transaction that uses the digital ID, it creates a system where the Digital ID is not restricted by a purpose limitation, and just operates as a database of information to be leveraged by any sector and for any purpose.

Every citizen of Estonia gets ID code right at birth. Estonia also issues personal identification codes to all e-residents and people with residency permits. Also, there are future plans to issue Estonian ID code for all the foreigners that are at least in one of the key registries and doesn't already have Estonian personal identification number in their name. This idea helps to connect all of the different registries' data regardless of whether the person is a foreigner or not.

Personal identification code is one of the key IDs for aggregating the data inside different Estonian government registries. It's important to get a complete picture about the person to offer better personalized and proactive e-government services for the people. Good examples are the Estonian business register that combines personal ID codes with unique company registration numbers to an open data in different government registries to show out much more than just business registry data.

This approach allows to show a full picture about the company and all the people that are related to the company in different roles. Additionally, the same logic is being used to visualize Estonian business register data to give a fast overview about the interrelationships between companies and persons in those companies.

Having one standardised ID code greatly improves overall data quality, for example, in Estonia if the person name, sex, status or nationality in population registry changes then in business register automatically can also change the data accordingly. With the owner of the personal data the actual person, government provides a service where individuals can actually check who has asked their personal data related to the ID code and ask from the requester, the nature of the request was made and any additional information regarding the information/data shared.[25]

Since data is essentially the "new oil of insights", the more data you have about the legal entity or natural person, the more relevant and meaningful analysis can be derived. As an example, one of the ongoing projects in Estonia is to show entities their company entrepreneurial viability Index. This would provide companies with government support for growth and development, and where applicable, could also warn against the risk of insolvency and getting into future financial difficulties. The data gathered from different government registries is being used to create a value-added service for the business entrepreneurs.[26]

It is common knowledge across the Estonia government registry domain, that if you want to link and attribute data, you need unique digital IDs. There is nothing new in this approach in principle, combining standardised personal identification codes with X-Road and eID technologies like ID-cards, SmartIDs and mobileIDs, Estonia has been building secure e-services for over 20 years.

OECD has just released their new Digital Government Index[27], which surveys and benchmarks the OECD members' efforts to digitise their public sector. The survey shows that Estonia is a clear leader in developing a data-driven public sector. Its data-sharing interoperability system demonstrates a commitment to efficient digital government and integrated public services. Estonia's data rights reflect its focus on citizen-centric services, ensuring transparency, privacy, and security. This practice strengthens public trust and supports the country's broader digital transformation objectives.

Estonia's data quality framework also showcases its dedication to accuracy and reliability in government data, which is critical for informed decision-making and policy development. These practices demonstrate Estonia's strategic leveraging of data-driven solutions to create an efficient, transparent, responsive public sector.

Estonia stands as a trailblazer in digital governance, with its innovative approach to e-government and pioneering initiatives like the X-Road platform. It serves as the backbone of Estonia's digital infrastructure, facilitating secure data exchange between various government databases and systems. Through X-Road, Estonia has achieved seamless interoperability, enabling efficient delivery of public services and fostering a citizen-centric approach to governance. This experience underscores the importance of interoperability in modern registries, emphasizing the need for robust data exchange mechanisms to support connected government services.

The Evolving Identity Frameworks in Canada

In Canada, significant strides have been made in the realm of digital identity management, both at the federal and provincial levels. At the federal level, the establishment of the Digital Identity and Authentication Council of Canada (DIACC) in 2012 stands out as a pivotal initiative. Through DIACC, Canada has developed comprehensive digital identity standards and frameworks aimed at enhancing trustworthiness and interoperability across public and private sectors.

INGREDIENTS FOR SUCCESS - In order to drive economic growth and innovation across Canada, digital identity must be rooted in security, trust, and convenience so these solutions can truly benefit everyone - citizens, businesses, and government alike.[28]

The Pan-Canadian Trust Framework™ (PCTF) is a risk mitigation framework comprised of a set of rules, standards, specifications, regulations, and guidance that offers a high-quality and versatile defined code of practice for operating trustworthy and efficient digital identity, credential, and supporting services.[29]

INGREDIENTS FOR SUCCESS - In order to drive economic growth and innovation across Canada, digital identity must be rooted in security, trust, and convenience so these solutions can truly benefit everyone - citizens, businesses, and government alike.

The PCTF's guiding principles and core framework are aimed at:

- Enhancing the reliability and compatibility of digital trust and identity services across both public and private sectors, with a primary focus on user-centric design, privacy, security, and convenience.
- Consolidating leading methodologies, leveraging established standards, policies, and guidelines, while maintaining a commitment to incorporating inputs from diverse stakeholders. DIACC pledges to synchronize with global frameworks to foster interoperability and widespread acceptance.
- An approach that is inclusive, results-oriented, adaptable to various technologies, transparent, and flexible, bringing together and promoting best practices in the field.

DIACC stands as a beacon of collaboration and innovation, bringing together public and private sector stakeholders. A careful estimate of the potential value of trusted digital identity to the Canadian economy is at least one percent of GDP, or C$15 billion[30].Through DIACC, Canada has developed standardised frameworks to enhance trust, interoperability, and user-centric design principles. Aligning with international best practices, including those outlined in the EU's eIDAS program, underscores Canada's global leadership in digital identity management.

A careful estimate of the potential value of trusted digital identity to the Canadian economy is at least one percent of GDP, or C$15 billion.

Provincial Initiatives

British Columbia (BC) government continues to make significant advancements in the realm of digital identity (ID) innovation. With a focus on enhancing citizen-centric services, privacy, and security, BC has been actively developing and implementing digital ID solutions to streamline access to government services and transactions.

One of the key initiatives in BC's digital ID landscape is the BC Services Card program. This program integrates a person's healthcare and personal identity information into a single card, providing a secure and convenient means of accessing a wide range of government services online. The BC Services Card is designed to enhance efficiency, reduce administrative burdens, and improve the overall user experience for citizens interacting with government agencies.

Another innovation across the digital ID framework is the Org Book solution in British Columbia through its role in facilitating verifiable credentials and identity verification. The Org Book is essentially a registry of organizations and their associated legal entities, which can include businesses, government agencies, and other entities operating in British Columbia. This registry serves as a trusted source of information about these organizations.

In the context of digital IDs, the Org Book can play a crucial role in enabling verifiable credentials, which are digital representations of information that can be cryptographically verified. These credentials can include information such as identity attributes, qualifications, licenses, and more.

Ontario has been actively pursuing digital ID initiatives as part of its broader digital transformation strategy. One notable development is the Ontario Digital ID, a secure and user-centric digital identity solution designed to streamline access to government services and transactions online. This initiative aims to improve the user experience by providing residents with a convenient and efficient way to verify their identity and securely interact with government agencies. By leveraging advanced technologies and user-centric design principles, Ontario is enhancing accessibility and efficiency in public service delivery while prioritizing privacy and security.

Similarly, Alberta has been at the forefront of digital ID innovation, with a focus on enhancing security, interoperability, and user experience. The province has implemented various digital ID solutions to modernize government services and transactions, including the MyAlberta Digital ID. This digital identity platform enables residents to securely access a wide range of government services online, streamlining interactions and reducing administrative burdens. Alberta's commitment to digital ID innovation reflects its dedication to improving service delivery and fostering economic growth through digital transformation.

New Brunswick's government has been actively engaged in digital identity (ID) innovation, leveraging technology to enhance citizen services, privacy, and security. The province has embarked on several initiatives aimed at modernizing government services and transactions through digital ID solutions.

In Manitoba, initiatives such as the Manitoba Digital ID program have been launched to enhance access to government services and streamline digital interactions. Manitoba Digital ID offers residents a secure and user-friendly platform for verifying identity and accessing a wide range of online services. By embracing digital innovation and prioritizing user privacy, Manitoba aims to strengthen its digital identity ecosystem and enhance the overall digital experience for residents.

While some Canadian provinces have explored or are considering the use of blockchain technology for digital identity (ID) programs, it's important to note that not all provinces have publicly announced plans to implement blockchain in this context. Each province may have its own approach to digital ID development, influenced by factors such as technological feasibility, regulatory considerations, and stakeholder preferences.

Among the provinces that have shown interest in and are exploring blockchain technology for digital ID initiatives, British Columbia (BC) and Ontario have been notable in their exploration of blockchain-based solutions. BC, for example, has investigated the use of blockchain for digital identity verification as part of its broader digital transformation efforts. Similarly, Ontario has explored integrating blockchain technology into its digital ID ecosystem to enhance security and privacy in online transactions. In addition, New Brunswick has been exploring innovative approaches to digital ID verification, including the use of biometric authentication and blockchain technology.

The variance around the adoption of blockchain technology for digital ID programs is based on factors such as technological readiness, regulatory frameworks, and stakeholder engagement. Some provinces may prioritize alternative approaches to digital ID development, such as secure centralized databases or other decentralized technologies.

Challenges and Future Directions in the Canadian Landscape:

Despite the significant progress made in digital identity management, challenges persist that require continued attention and innovation. Legal and regulatory complexities, interoperability issues, and privacy concerns remain key areas of focus for policymakers and industry stakeholders. Addressing these challenges necessitates ongoing collaboration, stakeholder engagement, and a commitment to user-centric design principles.

Looking ahead, Canada is poised to further advance digital identity management, with a focus on enhancing security, privacy, and interoperability. By leveraging innovative technologies and fostering a culture of trust and collaboration, Canada aims to build a digital identity ecosystem that empowers individuals, enhances economic competitiveness, and fosters innovation across sectors.

“There’s a huge appetite from the private sector to leverage government [digital] ID, and as soon as it becomes fully adopted across Canada, we’re going to see a huge surge in private adoption.” [31]

Canada’s achievements in digital identity management reflect a collective commitment to innovation, collaboration, and user-centric design. Federally led initiatives, coupled with provincial developments, demonstrate leadership and progress in the field. Direct cooperation with the EU’s eIDAS program underscores Canada’s commitment to global interoperability and alignment with international best practices. Despite challenges, Canada remains poised to navigate the evolving digital landscape, shaping the future of digital identity both domestically and on the global stage.

The Target Operating Model (TOM) for the future design and development of both provincial and federal registries need to be aligned with and poised to adapt to digital identities and evolving trust frameworks. The key importance lies in modernizing and enhancing the efficiency, security, and accessibility of government services and transactions. The potential of integrating digital identities and evolving trust frameworks is vast. It enables registries to adapt to the digital age, meet the needs of a diverse population, and foster innovation in service delivery. Additionally, it enhances security measures, mitigates risks associated with identity theft and fraud, and lays the groundwork for future technological advancements.

“There’s a huge appetite from the private sector to leverage government [digital] ID, and as soon as it becomes fully adopted across Canada, we’re going to see a huge surge in private adoption.”

A Federated Approach to the Exchange of Digital Identifiers

We have seen how the introduction of an internationally recognised singular identity for legal entities, in the form of the LEI that has revolutionised the provision of certainty with respect to business entities. We as the authors believe the same should be true for natural person identities that exist on registers, also these should be exchanged with other registers.

Indeed, Credential Exchange Infrastructures (CEI) based on open standards are emerging with work ongoing across in many different jurisdictions, in several global standards bodies and industry associations, as well as at a national level. These endeavours are sometimes labelled simply as 'credentialing' at a national level. For the most part, these various initiatives are following the Self-sovereign identity model.[32] The statutory registers are central to all these initiatives.

The context of registration systems and registers is as follows:

- Most of these assets are held in centralized statutory registers. It is also accepted that these assets are also held in decentralized "on-chain" registers (i.e. Crypto Exchanges).
- Each register creates a unique identifier for each entity on their register.
- Each register creates a unique identifier for each natural person on their register.
- Registers are investing heavily on the verification of the identities of natural persons on their registers.
- Registers in many jurisdictions duplicate the identifier for the same natural person within their various statutory registers.
- Registers will always have natural persons on their registers which are foreign nationals, where the register cannot rely on the same validation routines as it does for other persons within their jurisdiction.
- Registers are increasingly demanded to interoperate with registers in their own jurisdictions and internationally.
- Registers have relationships to other registers at an entity level.
- AML, FATF, Anti-Terrorist Financing regulations and related initiatives demand greater cooperation between registers internationally. AML is solely about finding natural persons and the assets to which they own.
- A register assigning their own identifiers for the same natural persons as exist on other registers within their jurisdiction or internationally does not resolve many issues.
- The LEI/VLEI creates federated identifiers for all legal entities and there representatives.

The eIDAS 2 regulation sets out that digital identity wallets are to be made available to all EU citizens by 2024. It would however be fair to say that the development and adoption of an e-ID (electronic ID) accepted in all member states still has a very long way, to be successful. Only 14% of key public services in the EU allow cross-border authentication with an e-ID. For citizens, governments, and a myriad of different public and private sector service providers, the advent of eIDAS 2 and the European Digital Identity Wallet (EDIW) will bring a mix of challenges and opportunities. Registers will be required to provide for identities to wrapped in Digital Wallets and for those credentials to be shared in cross border transactions.

Consider the following simplified example, of three jurisdictions, with registers of different types (Land, Business and Asset). Each register persisting the ‘relationships’ between natural persons and the entities on their register. The register creates an identifier for the natural person and the title/folio number (land), entity ID (business), and asset tag/number (asset). In its simplest form the register is linking these two identifiers. However, there is no internationalised equivalent for the person ID created, similar to the Legal Entity Identifier. The authors strongly contend there should be.

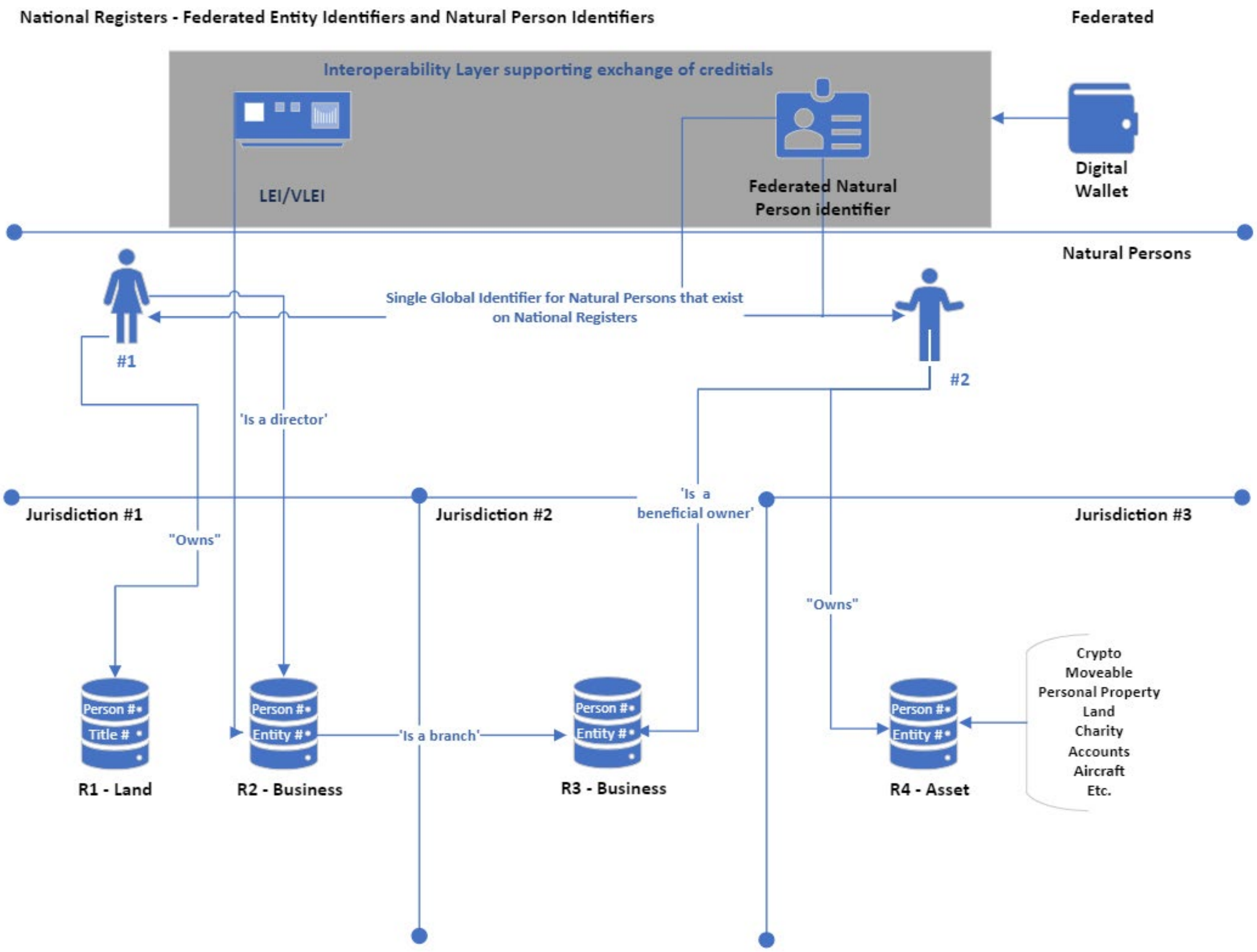


Figure 1: Federated Entity and Natural Persons Identifiers

It means each register independently creates a separate identifier for the same natural person. Registers do not harness the previous identity validation processes of their peers. Registers are very comfortable exchanging information on the particulars of the entities on their registers, but exchange little in terms of validated persons. Of course there will be data privacy regulations, but a register could acknowledge whether a natural person (with X personal attributes) exists on a separate register. Registers could become the source of truth, for other registers, for the identities that they have validated.

Key Digital Directives Informing the Future of Registers

As digital identity becomes increasingly central to modern governance, the Target Operating Model (TOM) for Registers of the future need to ensure alignment with key directives and initiatives[33]. These directives encompass various facets and challenges, from addressing duplication of identifiers and enhancing interoperability to facilitating the sharing of validated identities and ensuring compliance with international (global) standards and best practices such as those that will evolve from the EU Identity Wallet and eIDAS regulations, and the ongoing evolution of the Pan Canadian Trust Framework. Moreover, other initiatives like Connected Government and UN directives provide a comprehensive framework for the development of inclusive, secure, and interoperable digital identity systems.

1 **Non-duplication of Identifiers, interoperability equivalents** - In the future, registers will need to address the challenge of duplication of identifiers and ensure interoperability equivalents to facilitate seamless interactions within global digital identity ecosystems. Key aspects for future registers include the adoption of unique, standardised identifiers to prevent duplication and streamline identity verification processes. Additionally, interoperability frameworks must be established to enable registers to exchange information securely and efficiently, allowing for the seamless authentication of individuals and entities across different systems and platforms. The eIDAS 2 regulation sets out that digital identity wallets are to be made available to all EU citizens by 2024. It would however be fair to say that the development and adoption of an e-ID (electronic ID) accepted in all member states still has a very long way, to be successful. Only 14% of key public services in the EU allow cross-border authentication with an e-ID. For citizens, governments, and a myriad of different public and private sector service providers, the advent of eIDAS 2 and the European Digital Identity Wallet (EDIW) will bring a mix of challenges and opportunities. Registers will be required to provide for identities to wrapped in Digital Wallets and for those credentials to be shared in cross border transactions

2 **Sharing of validated identities** - registers must prioritize the seamless sharing of validated identities across systems to ensure efficient and secure digital identity management. Key aspects across the design of modern registers should include the establishment of standardised protocols and secure data exchange mechanisms to enable the sharing of validated identity information between different registers and government agencies. Additionally, robust authentication and authorization mechanisms should be implemented to verify the integrity and authenticity of shared identity data, while also safeguarding individuals’ privacy and rights.

3 **Natural Person Validation / Identity Validation Systems** - registers must prioritize the development of robust Natural Person Validation (NPV) or Identity Validation Systems (IVS) to ensure the accuracy and reliability of digital identity verification processes for individuals. Key aspects for future registers include the integration of advanced biometric authentication technologies, such as facial recognition and fingerprint scanning, to verify the identity of individuals with a high degree of certainty.

> As digital identity becomes increasingly central to modern governance, the Target Operating Model (TOM) for Registers of the future need to ensure alignment with key directives and initiatives.

4 **Digital "Identity" Wallet** - Key aspects when developing the future TOM should include the adoption, or at a minimum recognition, of standardised protocols and technical specifications to support digital wallets. There are some relevant examples to leverage the adaptation and integration as outlined by the EU Identity Wallet framework, facilitating seamless integration with digital ID systems across EU member states. Additionally, the design and interoperability within registers should prioritize adherence to regulations (e.g., eIDAS) and other like jurisdictional regulations that are evolving, ensuring the mutual recognition of electronic identification and trust services within the operating jurisdiction, thereby enhancing interoperability and trust in cross-border digital transactions.

5 **Connected Government** - The advent of digital identities (IDs) for both natural persons and business entities heralds a transformative shift in enabling connected government. With the proliferation of cellar coverage at a global level, enabling wireless communications and internet access to those previous disadvantaged, the applicability and use of digital IDs will continue to be critical to enable connected government, albeit at a varying pace across the globe.

Digital IDs streamline interactions between citizens, businesses, and government agencies, fostering a seamless ecosystem where information flows securely and efficiently. For natural persons, digital IDs offer a convenient and secure means of authentication, enabling access to a wide array of government services and resources online. This digitalization of identity verification processes reduces bureaucratic red tape and eliminates the need for physical documents, empowering individuals to engage with government services from anywhere, at any time.

Similarly, digital IDs for business entities revolutionize the landscape of government-business interactions, driving efficiency and transparency in regulatory compliance, taxation, and licensing processes. By digitizing business identities, governments can streamline registration procedures, facilitate cross-border transactions, and enhance regulatory oversight. This digital infrastructure enables businesses to operate more seamlessly within the regulatory framework, reducing administrative burdens and fostering a conducive environment for entrepreneurship and economic growth.

6 **Public Service Directives** - Registers will continue to focus on enhancing transparency by providing clear and comprehensive information about how personal data is collected, stored, and used within the digital identity ecosystem. All our future registers should be designed to prioritize interoperability and collaboration with public service agencies to streamline administrative processes and improve the delivery of government services. By aligning with Public Service Directives (or Government Guidelines), future registers can contribute to the development of inclusive, responsive, and citizen-centric digital identity systems.

These initiatives will impact the future TOM for registers across multiple areas is design and development, some of which we have already discussed, of which include:

- Inclusivity: Ensure accessibility for all, including marginalized groups.
- Privacy: Uphold data protection and privacy rights.
- Interoperability: Enable seamless data exchange between systems.
- Security: Implement strong measures to safeguard identity data.
- User-Centric Design: Prioritize user-friendly interfaces.
- Compliance: Adhere to international standards and best practices.

Aligning with these recommendations should guide the design and development of future register towards supporting more inclusive, secure, and user-friendly digital ID systems.

Final Thoughts: Advancing Digital Identifiers Through Modernized Registers

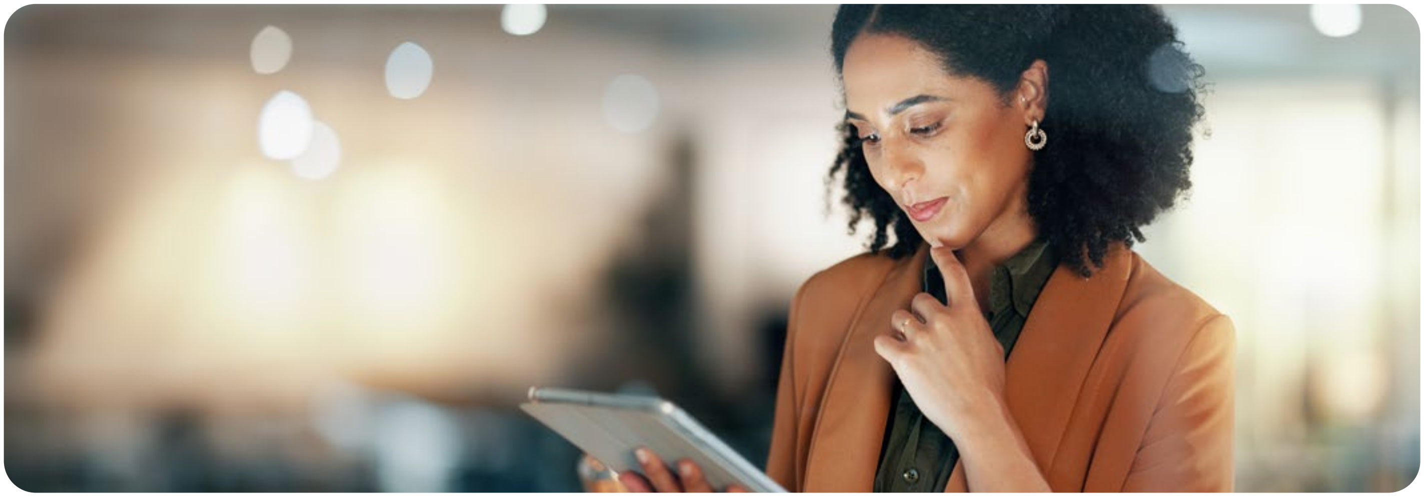
As digital identity continues to gain prominence in modern governance, the Target Operating Model (TOM) for registers of the future must align with key directives and initiatives to ensure efficiency, security, and inclusivity. Initiatives such as the EU Identity Wallet, eIDAS regulations, the PCTF, the Connected Government principles, and the UN directives all provide a comprehensive and detailed framework for the development of digital identity systems.

Government digital registers of the future need to address challenges such as duplication of identifiers, ensure interoperability, prioritize the sharing of validated identities, and develop robust Natural Person Validation (NPV) or Identity Validation Systems (IVS). Moreover, adherence to principles of inclusivity, privacy, interoperability, security, user-centric design, and compliance with international standards should guide the design and development of future registers, fostering more inclusive, secure, and user-friendly digital ID systems that empower individuals and businesses alike.

We encourage readers to closely examine the evolving landscape of digital identity within the European Union (EU) as an example for global developments, drawing insights from initiatives such as the eIDAS Regulation and Estonia's innovative approaches, and the continuing partnerships that are aligning towards building out the Pan Canadian Trust Framework. By delving into the legislative frameworks, technological innovations, and strategic initiatives outlined in this Paper, stakeholders can gain a deeper understanding of the principles underpinning effective digital identity ecosystems and how registries and interoperability are a critical component of success.

Moreover, we advocate for a holistic approach to digital identity management that prioritizes interoperability, trust, and user-centricity. As governments around the world grapple with the challenges of digital transformation, embracing global frameworks like the innovations around the verifiable Legal Entity Identifier (vLEI) under the GLEIF, and initiatives promoting inclusive digital identifiers becomes paramount we can ensure successful adoption across jurisdictional boundaries.

Ultimately, our purpose in crafting this Paper is to provide actionable insights and strategic recommendations that can inform policy decisions, drive technological innovation, and foster collaborative efforts in advancing digital governance and identity management. By leveraging the lessons learned and working collaboratively with trust frameworks being launched we can be more adaptive in underpinning these principles in the design of future Target Operating Model for registers worldwide. As common stakeholders we can, and should, work towards building a more connected, responsive, and trustworthy governance framework that empowers individuals and businesses alike in the digital age.



Teranet® is Canada's leader in the digital transformation, delivery, and operations of statutory registry services with extensive expertise in land and corporate and personal property registries. For more than three decades Teranet has been a trusted partner to governments and businesses in building stronger communities and economies. Teranet developed and currently operates Ontario's Electronic Land Registration System and Writs System, Manitoba's Land Titles and Personal Property Registries.

Foster Moore®, a Teranet company, – is a global leader and specialist registry software company focused on digital services for modernizing government. For two decades the team at Foster Moore has developed and maintained online business registry systems, and a host of other smaller electronic registries across the globe.

Global Legal Entity Identifier Foundation (GLEIF) was established by the Financial Stability Board in June 2014, is tasked to support the implementation and use of the Legal Entity Identifier (LEI). The foundation is backed and overseen by the Regulatory Oversight Committee, representing public authorities from around the globe that come together regularly to jointly drive forward transparency within the global financial markets.

Centre of Registers and Information Systems (RIK) is an agency in the jurisdiction of the Ministry of Justice, with the purpose of establishing an innovative environment providing good integrated e-services for a more efficient implementation of state administration, legal and criminal policy.

Key Terms and Terminology

AML – AML stands for anti-money laundering, which is legislation put in place to combat money laundering, which is a type of fraud. Certain organizations, such as banks, are mandated by law to follow AML risk assessment requirements in almost every country

Connected Government – The concept of 'Connected Government' holds immense importance in today's digital era. A connected government refers to a seamless integration of information, communication, and technology systems across various government entities, enabling efficient data sharing, collaboration, and service delivery. By fostering connectivity, governments can streamline processes, improve communication channels, and enhance the overall efficiency and effectiveness of public services

Crypto Exchanges – Crypto exchanges function similarly to online brokerage platforms, providing you with the tools you need to buy and sell digital currencies and tokens like Bitcoin, Ethereum, and Dogecoin.

eIDAS (electronic Identification, Authentication, and trust Services) – is a regulation that established a shared framework between all 27 European Union (EU) countries for safe and efficient business electronic interactions

Entity - Anything that can be referenced in statements as an abstract or concrete noun. Entities include but are not limited to people, organizations, physical things, documents, abstract concepts, fictional characters, and arbitrary text. Any entity might perform roles in the ecosystem if it is capable of doing so.

FATF – The Financial Action Task Force (FATF) is the global money laundering and terrorist financing watchdog. It sets international standards that aim to prevent these illegal activities and the harm they cause to society

Identity – Who a person or organization fundamentally is – a combination of attributes, beliefs, personal/ organizational history and behaviour that together constitute a holistic definition of the individual or organizational self.

Identification – The act of verifying identity; proving who people and organizations say they are.

Identity and Access Management (IAM) – IAM is for making sure that only the right people can access an organization's data and resources. It's a cybersecurity practice that enables IT administrators to restrict access to organizational resources so that only the people who need access have access.

Identity provider – An identity provider, sometimes abbreviated as IdP, is a system for creating, maintaining, and managing identity information for holders, while providing authentication services to relying party applications within a federation or distributed network. In this case the holder is always the subject. Even if the verifiable credentials are bearer credentials, it is assumed the verifiable credentials remain with the subject, and if they are not, they were stolen by an attacker. This specification does not use this term unless comparing or mapping the concepts in this document to other specifications. This specification decouples the identity provider concept into two distinct concepts: the issuer and the holder.

Issuer – A role an entity can perform by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder.

Pan-Canadian Trust Framework (PCFT) – The PCTF enables Canada's full and secure participation in the global digital economy through economic sector innovation and the enablement of modernized digital service delivery. The PCTF is developed through a collaborative approach between the Digital ID and Authentication Council of Canada (DIACC), a non-profit neutral forum, and the Pan-Canadian Identity Management Sub-Committee (IMSC) of the Joint Councils of Canada, a forum consisting of the Public Sector Chief Information Officer Council (PSCIOC) and the Public Sector Service Delivery Council (PSSDC).

Verifiable credential – A verifiable credential is a tamper-evident credential that has authorship that can be cryptographically verified. Verifiable credentials can be used to build verifiable presentations, which can also be cryptographically verified.

Verifiable data registry – A role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation registries, issuer public keys, and so on, which might be required to use verifiable credentials. Some configurations might require correlatable identifiers for subjects. Some registries, such as ones for UUIDs and public keys, might just act as namespaces for identifiers.

Endnotes

[1] https://www.mckinsey.com/industries/public-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id

[2] Ibid.

[3] Self-Sovereign-Identity & eIDAS: a Contradiction? Challenges and Chances of eIDAS 2.0, European Review of Digital Administration & Law - Erdal 2021, Volume 2, Issue 2, pp. 89-108

[4] Somers, M. R. (1998). We're Not Angels": Realism, Rational Choice, and Relationality in Social Science. Am. J. Sociol. 104 (No. 3), 722–784. doi:10.1086/210085

[5] Chango, Mawaki. "Building a credential exchange infrastructure for digital identity: A sociohistorical perspective and policy guidelines." Frontiers in Blockchain 4 (2022): 629790.

[6] Feasibility of a European Asset Register, EU DG-FISMA, https://etendering.ted.europa.eu/cft/cft-display.html?cftId=8792

[7] Windley, Phillip J. Digital Identity: Unmasking identity management architecture (IMA). " O'Reilly Media, Inc.", 2005.

[8] https://www.teranet.ca/wp-content/uploads/2023/02/Teranet-Foster-Moore_Interoperability-and-Data-Exchange-Between-Registries-01.30.23.pdf

[9] Campbell, Douglas. "Identifying the identifiers." Proceedings of the International Conference on Dublin Core and Metadata Applications. Dublin Core Metadata Initiative, 2007.

[10] https://www.mckinsey.com/industries/public-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id

[11] Green Paper on the interconnection of Business Registers - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52009DC0614

[12] Directive on the Interconnection of Business Registers - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012L0017

[13] Bregeš, Željka, and Tina Jakupak. "Digitalization of Business register." InterEULawEast: journal for the international and european law, economics and market integrations 4.2 (2017): 91-99.

[14] https://www.mckinsey.com/industries/public-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id

[15] Walke, Fabian, Till J. Winkler, and Michael Le. "Success of Digital Identity Infrastructure: A Grounded Model of eID Evolution Success." The 56th Hawaii International Conference on System Sciences. HICSS 2023. Hawaii International Conference on System Sciences (HICSS), 2023.

[16] Global LEI System: a Network of Federated Services - The Global LEI System - LEI – GLEIF (this does not show as a link)

[17] ISO 20275: Entity Legal Forms Code List - ISO 20275: Entity Legal Forms Code List - Code Lists - LEI – GLEIF

[18] https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

[19] https://cyber.ee/resources/news/the-history-of-digital-identity-in-estonia/

[20] Tammpuu, Piia, and Anu Masso. "Transnational digital identity as an instrument for global digital citizenship: The case of Estonia's E-residency." Information Systems Frontiers 21 (2019): 621-634.

[21] https://www.valimised.ee/en

[22] https://e-estonia.com/solutions/interoperability-services/x-road/

[23] https://e-estonia.com/solutions/e-identity/e-residency/

[24] https://digitalid.design/docs/CIS_DigitalID_EstoniaCaseStudy_2020.04.pdf

[25] https://www.ria.ee/en/state-information-system/people-centred-data-exchange/data-tracker

[26] https://katsetamine.riigikantselei.ee/naidistekogum/ettevtjaelujulisuseindeks/

[27] https://www.oecd.org/governance/2023-oecd-digital-government-index-1a89ed5e-en.htm

[28] https://canada.oliu.id/

[29] https://diacc.ca/overview/

[30, 31] https://www.itworldcanada.com/article/canada-is-moving-faster-on-digital-id-than-most-think-says-atb-ventures/532961

[32] Chango, Mawaki. “Building a credential exchange infrastructure for digital identity: A sociohistorical perspective and policy guidelines.” Frontiers in Blockchain 4 (2022): 629790.

[33] https://www.fostermoore.com/news/proposed-new-target-operating-model-for-registers