EUROPEAN UNION
UNION EUROPÉENNE

STUDY ON EU-CANADA DIGITAL IDENTITY AND TRUST SERVICES INTEROPERABILITY

Final Report

July 2025

PREPARED BY

KEITH JANSA
ELLIS JONATHAN SHAMAH

The present output was produced in the framework of the EU-Canada Policy Dialogue Support Facility, a project funded by the European Union.

EU-CANADA
Policy Dialogues
Support Facility
Funded by the European Union

I EXECUTIVE SUMMARY

This study, funded by the Delegation of the European Union to Canada through its Policy Dialogue Support Facility (PDSF), examines EU and Canadian frameworks related to digital identity, digital credentials and trust services[1].

The EU-Canada Summit (23 June 2025) was of paramount importance in establishing a strategic partnership between the EU and Canada. In the digital field, the joint statement makes specific reference to the EU-Canada Digital Partnership and includes many areas of cooperation including the establishment of " interoperable digital identities and digital credentials to facilitate interactions between our citizens and our businesses." The EU and Canada leaders also agreed to work on a Digital Trade Agreement.

The primary objective of this study is to evaluate and compare the legal and technical aspects as well as the standards of both frameworks which demonstrate both similarities and divergences.

As the EU has passed regulation establishing the EU Digital Identity Framework (EUDI Framework), this has become the legal determinant for EU wide governance and technical realisation for digital identities, Trust Services, and Digital Wallets. The timelines and mandatory nature of the regulation ensures that a consistent interoperable and functional digital wallet, together with the Trust Services will provide a pan-EU methodology made available to all EU citizens by the end of 2026 and must be accepted by public sector bodies and certain private sector relying parties by May 2027[2]. This solidification is the result of extensive consultation leading to a strong cross-EU consensus in methodology and legislative enforcement.

In Canada, the federation of 10 provinces deriving their power from the Constitution Act of 1867, and of 3 territories who receive their powers from the Federal Government (i.e., delegated to the Parliament of Canada) leads to a variance of differing approaches and methodologies which makes a single umbrella solution for the entirety of Canada challenging. There is a degree of commonality with the goals of simplification, security and interoperability between internal government services, but approaches and degrees of adoption vary depending on resources and infrastructure.

The study also examines at a high level how the differences between the EU and Canadian implementations could be bridged to establish the groundwork for closer collaboration resulting in smoother and more efficient digital trading and transactions between the EU and Canada. To achieve this objective, the authors of the study make an analysis on how both regions can use the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services and existing trade agreements like the Comprehensive Economic and Trade Agreement (CETA) to facilitate mutual recognition of digital identity/digital credentials and trust services.

The United Nations Commission on International Trade Law (UNCITRAL) was established to promote the modernization and harmonization of international trade law. It developed a Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT) in July 2022 to provide a uniform legislative framework for the use and cross-border recognition of Identity Management and Trust Services. The four sections of the model law address General Provision, Definitions, Scope of application, and general rules on the voluntary use of identity management and trust services. In this study the MLIT is used as a normative benchmark to match the variances in approach between Canada and the EU and establish a common basis for an agreement.

[1] "Digital identity" and "digital credentials" are used interchangeably in this study.

[2] Article 6b(2) – Acceptance by Relying Parties.

The EU-Canada Comprehensive Economic and Trade Agreement (CETA) is a modern and progressive EU trade agreement, which offers EU firms more and better business opportunities in Canada and protects consumers and the environment, allowing entrepreneurs and businesses of all sizes to benefit from improved market access opportunities.

Key Findings

The EU's Digital Identity Wallet (EUDI Wallet) as a core component of Electronic Identification, Authentication and Trust Services (eIDAS 2.0) and Canada's Digital Governance Standards Institute Technical Specification 115 (DGSI TS 115) are both designed to provide secure and trusted digital identity/digital credential and trust service solutions. However, they represent fundamentally different models: one rooted in a centralized, regulatory-driven European framework and the other reflecting a decentralized, standards-based Canadian approach.

Specifically:

1. The EU Digital Identity Framework in the EU provides a centralized and unified legal framework for digital identities and trust services, ensuring that they are legally recognised and consistently regulated across all EU member states.

2. In comparison, Canada's legal, regulatory and policy framework is decentralized, with different provinces and territories enforcing varying regulations and policies. While the Public Sector Profile Pan-Canadian Trust Framework represents a nationwide approach, it does not provide the same level of centralized governance or uniformity as the EU Digital Identity Framework. Canada has been incremental and diligent in developing a Pan-Canadian approach for digital trust and identity management systems where the Government of Canada is one of many partners working in concert with provinces, territories, the private sector, and the international community.

3. Nonetheless, both frameworks similarly recognise the importance of secure digital credentials, privacy protection, and the legal standing of electronic signatures. The EUDI framework and the Public Sector Profile Pan-Canadian Trust Framework share common objectives in promoting trust and security in digital transactions, though the legal mechanisms for achieving these goals differ in structure.

4. The World Trade Organisation Technical Barriers to Trade Agreement (WTO TBT) provides a framework for Canada and the EU to enhance cooperation on digital identity/digital credentials and trust services, facilitating the recognition of each other's regulatory, standards and conformity assessment approaches, even when policy and regulatory frameworks differ. The agreement's provisions on equivalence offer a mechanism for reconciling differences in regulatory structures while facilitating the smooth exchange of digital credentials and enhancing trust in digital systems. This cooperation is essential for supporting the growth of cross-border digital trade and fostering the secure and interoperable use of digital credentials and trust services between the two regions.

This study outlines a series of recommendations to foster technical interoperability between the two frameworks and pave the way for mutual recognition in the longer term.

Recommendation 1: Implement a use case-driven approach to demonstrate the practicality and relevance of the collaboration. The use cases could ideally re-use experiences gained from EU Large Scale Pilots that were launched in 2023 and 2025. The final list of use cases could be agreed at the first EU-Canada Digital Partnership Council.

Recommendation 2: Recognise the legal effects of identity management systems and trust services through a negotiated agreement on the basis of the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT).

Recommendation 3: Designate identity management systems and trust services in support of the first recommendation.

Recommendation 4: Agree on equivalent levels of assurance of identity management systems and system reliability of trust services between respective jurisdictions.

Recommendation 5: Establish a new equivalency agreement and add product coverage in the CETA Conformity Assessment Protocol to extend the existing mutual recognition agreement.

II INTRODUCTION

The EU-Canada Digital Partnership is a collaborative initiative with aims to strengthen digital cooperation between the EU and Canada.

It aims to create concrete deliverables of bilateral cooperation and strengthen regulatory convergence in areas such as artificial intelligence, cybersecurity, data governance, digital identities and digital credentials and online platforms. Aligning policies and standards to create a harmonised regulatory environment for digital innovation, collaboration and trade is an essential component of the partnership.

The goals of the partnership are to foster innovation and economic growth in the digital economy; uphold and promote democratic values and respect of fundamental rights in the global digital landscape; address the geopolitical and security challenges posed by rapid technological advancements; enhance transatlantic collaboration and establish leadership in setting global digital standards.

This study is supportive of the EU-CA Digital Partnership and aims to:

- Contribute to a deepened cooperation between the EU and Canada in the areas of digital identity, digital credentials and trust services
- Facilitate both parties to support a positive, inclusive, and human-centric vision where the design, development, governance, and use of the above-mentioned technology solutions are guided by democratic values and respect for fundamental rights.

In the EU, the Digital Identity Framework (EUDI) includes electronic identification, authentication, and trust services and provides a standardized framework for secure digital identification across member states, prescribed in regulation. It enables cross-border interoperability across the EU and serves as a basis for digital identity management at the member state level including Digital Wallets.

Canada, on the other hand, is developing platforms to provide a single point of access for government services using digital credentials provided by the different levels of federal, provincial, territorial and indigenous governments. These initiatives aim to ensure secure and efficient access to services like healthcare, finance, and e-government but degrees of implementation vary. Additionally, each level of government can implement its own solutions.

The primary focus of the study is to enhance comprehension of the digital identity, digital credential and trust services frameworks in both the EU and Canada. By deepening this understanding, stakeholders can be better assisted to align their approaches and can get clearer insights about the opportunities surrounding digital identity, digital credentials and trust services, including Digital Identity wallets.

This study aims also to equip EU and Canadian policymakers with a comprehensive understanding of the benefits for the EU and Canada from the use of digital identities and digital credentials to secure trusted online transactions between the businesses and citizens of both jurisdictions.

The study was informed by the following tasks:

- Comparing the European Digital Identity Wallet Architecture and Reference Framework (as made available on GitHub) and the EU Digital Identity Framework Implementing Acts, and relevant industry standards with the equivalent framework and standards in Canada.

- Identifying use cases where the EU-CA agreement can facilitate mutual recognition, with possible legal effect.
- Using the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT) as the common yardstick.
- Reviewing existing EU/CAN frameworks for mutual recognition of Canadian and EU consensus-based standards, including the Comprehensive Economic and Trade Agreement (CETA) Conformity Assessment Protocol with the view of expanding them to include digital trust services.
- Identification of the relevant technical and management standards (including international developments/initiatives on standards and interoperability like ISO, Open Wallet Foundation, FATF, etc.) that are applicable within the respective jurisdictional contexts (EU and CA) that can be directly linked to the articles within the MLIT.

III CONTEXT AND RATIONALE

III.1 World Trade Organisation Technical Barriers to Trade (WTO TBT) Agreement

The World Trade Organisation (WTO) Technical Barriers to Trade (TBT) Agreement plays a crucial role by providing a framework for mutual recognition and equivalence of technical regulations between jurisdictions. The TBT Agreement encourages Members to "give positive consideration to accepting as equivalent technical regulations of other Members, even if these regulations differ from their own, provided they are satisfied that these regulations adequately fulfil the objectives of their own regulations." This provision is designed to facilitate international trade by recognizing that different regulatory approaches can achieve similar public policy goals, such as ensuring safety, security and consumer protection. In the context of digital identity/credentials and digital trust services, this flexibility is important to facilitate Canada's and the EU's recognition of each other's regulatory frameworks, even if the technical and legal structures differ.

Both Canada and the EU aim to ensure the interoperability and security of digital credentials, which is critical for fostering cross-border digital transactions and trade. By engaging in discussions framed by the TBT Agreement both regions can work toward recognizing their technical regulations and policy frameworks governing digital trust services. This includes mutual recognition of digital signatures, electronic identification systems, and authentication protocols, even in the absence of identical regulatory structures. Such alignment could facilitate international digital transactions and enhance trust in cross-border digital interactions.

III.2 Article 218 of the Treaty on the Functioning of the European Union (TFEU)

Article 218 of the Treaty on the Functioning of the European Union (TFEU) lays down the procedures and powers of the EU institutions regarding the negotiation and adoption of agreements between the EU and non-EU countries or international organisations and as such lays down the legal framework for any collaboration between Canada and the EU. The article sets out the respective powers of the Council, the European Commission or the High Representative of the Union for Foreign Affairs and Security Policy, the European Parliament and the Court of Justice of the European Union in the process. In general, the Council has the power to open negotiations, adopt negotiating directives and sign and conclude agreements.

III.3 EU-CA Digital Partnership:

The EU-CA Digital Partnership is a strategic collaboration between the EU and Canada with aims to enhance cooperation in the digital domain. This partnership builds on the existing frameworks of the Strategic Partnership Agreement and CETA which have been in place since 2017.

The partnership establishes a framework for voluntary bilateral cooperation without creating legal obligations or financial implications for either side. It also aims to amplify the collective voice of the EU and Canada globally, bringing jointly developed solutions to international partners and advancing strategic priorities.

III.4 The role of digital transformation in enhancing economic security and supply chain resilience

Digital transformation plays a strong role in enhancing economic security and supply chain resilience, particularly within the context of EU-CA collaboration. This also includes, more broadly, the digital

context and the proliferation of online actors (e.g., AI agents) which may or may not have a real-world counterpart. The integration of advanced digital technologies has revolutionised the way economies operate, providing robust mechanisms to predict, mitigate, and respond to economic disruptions. Through digital technologies, both the EU and Canada can enhance their economic security, ensuring that their economies remain stable and competitive in the face of global uncertainties.

Trust services, digital identity and digital credentials are fundamental components of this digital transformation, contributing to economic security and supply chain resilience. Trust services are also fundamental components of defence and industrial policy and directly linked to sovereignty and broader security to ensure equitable nation-to-nation relationships. Trust services, ensure the authenticity, integrity, and confidentiality of digital transactions. These services build a secure environment for digital interactions, enhancing trust among parties and reducing the risk of fraud and cyber threats. In the context of EU-CA collaboration, trust services can facilitate seamless and secure cross-border transactions, bolstering economic security and supply chain resilience.

Digital identity and digital credentials play a crucial role in enabling secure access to digital services and platforms. It provides a reliable means of verifying the identities of individuals and entities, ensuring that only authorized parties can access sensitive information and resources. This is important in supply chain management where the verification of all participants is essential for maintaining the integrity and security of the supply chain. By implementing digital identity solutions, the EU and Canada can enhance the security of their supply chains, prevent unauthorized access and ensure the continuity of operations.

The collaboration between the EU and Canada in digital transformation extends to regulatory frameworks and standards. By examining their respective policies and regulations, both regions can create a cohesive environment that supports innovation and security. This examination is crucial for ensuring that digital identity and trust services are interoperable and universally accepted. It can help to facilitate the seamless exchange of information and resources, enhancing the overall resilience of supply chains and economic systems.

IV LEGAL AND REGULATORY LANDSCAPES

IV.1 Overview of EU Digital Identity Framework

The EU Digital Identity Framework, adopted into law across the entire European Union, represents a significant evolution in the EU's approach to digital identity and trust services. It is established through Regulation (EU) 2024/1183, which amends and builds upon the earlier Regulation (EU) No 910/2014, also known as eIDAS 1.0. This regulatory framework introduces advanced digital identity solutions, offering a more integrated and comprehensive framework for electronic identification (eID) within the EU. The primary objective of the framework is to provide EU citizens, residents, and businesses with a secure and trusted means of identification, both online and offline, with a particular emphasis on the use of eID to verify individuals and organisations. By promoting a seamless, standardized and interoperable digital identity ecosystem, the framework seeks to enhance trust in digital services, reduce administrative burdens, and foster greater digital inclusion across Member States.

A central feature of the framework is the introduction of the EU Digital Identity Wallet. This Wallet gives users full control over their digital identity and personal data, enabling the secure storage and management of verifiable credentials such as identification documents, professional qualifications, and health records. It also supports the use of legally valid electronic signatures. Another critical component is the principle of mutual recognition, which ensures that digital identities issued in one Member State are recognised and accepted across all others. This mutual recognition underpins cross-border digital interactions, facilitating access to public services, business operations, and secure online transactions throughout the EU. Additionally, the framework strengthens and expands the scope of trust services initially established under eIDAS 1.0, which include electronic signatures, seals, timestamps, and certificates. With eIDAS 2.0, new trust services such as remote qualified electronic signature creation devices and qualified electronic archiving services are introduced to meet evolving security needs, particularly in the context of increasing mobile transactions. Together, these elements create a robust foundation for secure, interoperable, and user-centric digital identity services across the European Union.

The European Union's approach to digital identity and trust is a regulatory-driven model designed to ensure legal certainty, cross-border interoperability between Member States, and mutual recognition across Member States. Anchored by the eIDAS Regulation and its recent update (eIDAS 2.0), the EU mandates a common legal framework for electronic identification and trust services, including the introduction of the European Digital Identity Wallet. This model emphasizes a consistent user experience and minimum assurance levels, while requiring each Member State to deploy at least one compliant wallet. The approach fosters cooperation among national authorities through structured legal obligations, shared technical standards, and conformity assessments, with a strong emphasis on safeguarding privacy, security, and data protection. The EU's digital identity strategy is explicitly designed to enable trusted digital interactions within its internal borders, promote digital sovereignty, and support the functioning of the internal market.

The European Commission plays a central leadership role in advancing digital identity across the European Union by coordinating efforts among Member States to establish a unified and trusted digital identity framework. Under the eIDAS Regulation and its successor, eIDAS 2.0, the Commission has mandated that each Member State formally notify at least one electronic identification scheme and, more recently, deploy a European Digital Identity Wallet. This regulatory framework ensures that digital identities and trust services are mutually recognised across borders, enabling individuals and businesses to access public and private sector services throughout the EU with a high level of assurance. Member States collaborate through structured mechanisms such as the eIDAS Cooperation Network and working groups to ensure conformance with legal, technical, and security requirements. The result is a legally binding, pan-European system of digital identity and trust services

that enhances interoperability, protects fundamental rights, and supports the functioning of the EU's digital single market.

The European Commission has also adopted a series of implementing acts under the original eIDAS Regulation to operationalize and standardize the requirements for cross-border digital identity and trust services. These implementing acts set out the minimum technical specifications, assurance levels, and procedural rules necessary for the mutual recognition of electronic identification schemes across Member States. They cover key areas such as the definition and application of assurance levels (low, substantial, high), interoperability requirements, notification procedures, and the security and liability obligations for electronic identification and trust service providers.

The implementing acts provide legal clarity and uniformity, ensuring that Member States interpret and apply the eIDAS Regulation consistently while retaining flexibility to tailor solutions to national contexts. These acts lay the foundation for the more detailed technical guidance provided in the Architectural Reference Framework (ARF), which serves as a practical reference for designing and implementing eIDAS-compliant digital identity systems, including the European Digital Identity Wallet (EUDIW) introduced under eIDAS 2.0.

The European Union's approach to digital identity and trust services is regulatory driven, with a strong emphasis on harmonization and compliance across Member States. Under the eIDAS Regulation and its recent update, eIDAS 2.0, Member States are required to adhere to the common legal and technical requirements, including the deployment of at least one European Digital Identity Wallet and the recognition of notified electronic identification schemes. This approach provides a uniform legal foundation for cross-border interoperability and mutual recognition, enabling consistent service delivery throughout the EU. By setting mandatory rules and standards, the EU aims to ensure legal certainty, enhance trust, and promote a cohesive digital single market, while allowing Member States flexibility in how they implement specific technical solutions within the established framework.

IV.2 Overview of Canada's Digital Identity Framework

The Canadian approach to digital identity and trust is grounded in a federated, multi-jurisdictional model, reflecting the country's constitutional division of powers between federal, provincial, and territorial (FPT) governments, that emphasizes collaboration, interoperability, and incremental progress. Rather than mandating a single national system, Canada supports a distributed network of trusted identity providers and governance arrangements that enable individuals and organisations to interact securely with a wide range of services across jurisdictions. This model does not mandate Person Identification Data (PID) as in the EU framework, but instead encourages cooperation among federal, provincial, territorial (FPT), and private sector actors, allowing for flexibility in implementation while maintaining a shared commitment to privacy, user control, and public trust. Canada's digital identity efforts are shaped by practical use cases and international collaboration, aligning with standards and legal frameworks to support cross-border interoperability.

The Government of Canada, through the Treasury Board Secretariat (TBS), has played a key leadership role in advancing digital identity by collaborating with provincial and territorial partners to establish trusted identity relationships. TBS is the central oversight department for the Government of Canada and responsible for setting Treasury Board policy, a standing Cabinet Committee. As part of this effort, TBS worked closely with the Provinces and Territories to formalize agreements recognizing their respective digital identity services as trustworthy for use in federal programs. In the case of Alberta and British Columbia, this collaboration culminated in the issuance of a letter of acceptance, wherein the federal government formally acknowledged trusted digital identities issued as meeting Treasury Board policy requirements. A 'trusted digital identity' is formally defined in the Treasury Board Policy on Government Security and is similar in concept to the Person Identification Data defined in the EU regulatory framework. The agreements were grounded in joint assessments and alignment on key principles such as mutual recognition, conformance with established identity

verification practices, and adherence to privacy and security expectations. This milestone enabled residents of Alberta and British Columbia to use their provincially issued digital identities to access participating federal services, demonstrating a practical step toward broader interoperability and cross-jurisdictional trust in Canada's digital identity ecosystem.

The Public Sector Profile Pan-Canadian Trust Framework (PSP-PCTF), developed through FPT Collaboration has served as a foundational instrument for evaluating the integrity and trustworthiness of digital identity programs within Canada's public sector. The PCTF is the foundation for the national standard CAN/DGSI 103-1 Digital Trust and Identity that defines a structured set of concepts, definitions, processes, designed to assess and ensure the reliability of digital identities and their associated services. The conformance criteria defined as part of the PCTF align directly with CAN/DGSI 103-1 and are intended to serve as the basis for a conformity assessment program going forward. The goal is to facilitate a common approach between various levels of government and the private sector and to promotes alignment, interoperability, and confidence in digital identity solutions intended to function across organisational, sectoral, and jurisdictional boundaries. The framework and standard are technology-agnostic and complements existing standards and policies, thereby supporting the acceptance and mutual recognition of digital identities and relationships across Canada.

In parallel, the Standards Council of Canada (SCC), a crown corporation in Canada, has advanced the standardization of digital credentials and trust services. Collaborating with the Digital Governance Standards Institute (DGSI), an SCC-accredited standards development organisation, and the Government of Canada, DGSI published a National Technical Specification, DGSI/TS 115, Digital Credentials and Digital Trust Services, that outlines minimum requirements to ensure interoperability between businesses and governments. This initiative aims to create a seamless experience for users by establishing a standardized approach to digital credentials, thereby enhancing privacy, security, and user control. SCC worked with 20 product developers, one conformity assessment body and an observation committee of more than 110 members who began piloting an ISO/IEC 17065 approach to conformity assessment for DGSI TS 115, while the Digital Governance Council tested a conformity assessment program for DGSI TS 115 in accordance with ISO/IEC 17029 methodology. Full-scale conformity assessment programs are expected to be ready in the next few years to support the consistent application of the technical specification.

In late 2024, the Government of Canada issued a Request for Information (RFI) to explore current and emerging industry solutions that can support the issuance, verification, and revocation of digital credentials. The RFI entitled, Common Set of Capabilities for Issuing and Verifying Digital Credentials (IVDC) for the Government of Canada, is seeking feedback from vendors offering components such as issuer and verifier services, holder components, and digital trust registries, to inform future procurement and help build a common set of capabilities that can enable a consistent, scalable, and interoperable approach to digital credentials across jurisdictions in Canada.

In March 2025, the Government of Canada issued an Invitation to Qualify (ITQ) for Issuing and Verifying Credentials. The intent of the ITQ is to qualify suppliers which can deliver an Issuing and Verifying Digital Credentials (IVDC) solution that meets the requirements for large-scale client facing processes of both the Government of Canada enterprise and departmental tiers of the solution. The ITQ is soliciting qualifying proposals for industry solutions that could provide a common set of capabilities to:1) Issue, verify, and revoke digital credentials, and 2) Enable external and internal clients and stakeholders to hold, share, and verify the digital credentials they issue. The stated goal of the ITQ is to make it easier for the Government of Canada and interested partners to implement and adopt digital credentials to make it quicker, easier, safer, more secure, and more cost-effective to deliver and obtain external and internal services digitally.

The issuance of the RFI and ITQ together demonstrate the Canadian approach to digital identity is by means of diligence, incrementalism, quiet engagement with industry, and most notably, deliberate

avoidance of political controversy. Canadian jurisdictions have opted for a pragmatic strategy that prioritizes collaboration, trust-building, and operational readiness over public fanfare. While there is interest among Canadians in the potential benefits that digital wallets and credentials can bring, such as optionality, convenience, privacy control, and improved access to services, these innovations must be introduced in a low-key, non-threatening manner. Public sensitivity to perceived overreach in digital initiatives and digital identity remains high; as demonstrated in across news outlets and reports including the Bank of Canada's decision to pause its central bank digital currency (CBDC) project following public consultation, Canadians are cautious about digital transformations that feel imposed or poorly understood. Likewise, within the provinces and territories, "digital identity programs" have been quietly refocused or rebranded to "online account" or "digital credentials" to deflect any potential negative perception associated with the term "digital identity".

This caution underscores the need for a careful, consultative rollout that earns public trust through transparency and clear value. This approach has been emphasized in the Ministerial Statement issued in December 2024 in response to the Auditor General's report on the Digital Validation of Identity. The Ministerial Statement provides clear direction that focuses on secure access to online programs and the sharing of digital credentials across federal programs while maintaining privacy. The intention is to "explore a collaborative national approach to digital credentials to support seamless service delivery for Canadians."

Digital wallets have also been introduced in a notably low-key manner in Canada, with public sector stakeholders deliberately avoiding the term in favour of more neutral language such as "digital credentials" or "digital accounts." Rather than focusing public attention on the concept of a digital wallet, which may carry unintended associations or spark privacy concerns, government communications have emphasized the underlying components—issuer, holder, and verifier—as well as the principles of security, privacy, and accessibility that govern their use. This subtle reframing allows the public sector to advance the infrastructure needed for trusted digital interactions while keeping market and policy options open. Whether digital wallets are ultimately provided by mobile platform providers, commercial vendors, or through government-approved applications, as seen in the European Union, the Canadian approach maintains flexibility and avoids locking into a single model too early, leaving room for broader consultation and evolution based on public comfort and industry innovation.

The Canadian approach, more aptly described as the "Pan-Canadian Approach", is fundamentally rooted in cooperation and collaboration across jurisdictions. It reflects a pragmatic model where the federal government assumes a facilitating and convening role, helping to coordinate efforts, align technical standards, and support mutual recognition of digital credentials across provinces, territories, and with international partners, such as the European Union. Rather than mandating a centralized solution, this approach respects jurisdictional autonomy while advancing interoperability and trust through shared frameworks and voluntary agreements. Importantly, all progress in this space occurs within the boundaries of existing legislation, intergovernmental agreements, and established policy frameworks, ensuring that any innovations in digital identity or credentials are both legally sound and publicly trusted.

Finally, at the time of writing this report, the political and economic landscape is shifting rapidly and in an uncertain direction. During the project, a new government has been elected with a new Prime Minister. The government mandate letter and Speech from the Throne, delivered in person by His Majesty, Charles III, may result in changes of sentiments and conditions described earlier.

IV.3 Benefits of technical interoperability and mutual recognition for businesses, governments, and citizens

The establishment of technical digital interoperability and mutual recognition between the European Union (EU) and Canada presents a transformative opportunity for businesses, governments, and citizens. This collaboration, particularly in the realms of trust services and digital identity, promises to enhance efficiency, security, and economic growth. By focusing on these areas, the multifaceted benefits that such interoperability brings to various stakeholders may be realised.

Trust services, including electronic signatures, seals, and time stamps, are fundamental to secure digital transactions. Interoperability between the EU and Canada ensures that these services are recognised and trusted across borders. This mutual recognition reduces the complexity and cost of cross-border transactions, fostering a more seamless and secure digital environment. For businesses, interoperability means simplified processes and reduced administrative burdens. Companies operating in both regions can leverage compatible digital identity frameworks, allowing for easier verification and authentication of partners and clients. This streamlining accelerates business operations, reduces fraud, and enhances overall efficiency.

The mutual recognition of digital identities and trust services stimulates economic growth by enabling smoother international trade and collaboration. Businesses can innovate without the constraints of incompatible digital identity systems, leading to the development of new products and services. This environment fosters a competitive market, driving economic prosperity in both regions. Governments benefit from interoperability through enhanced service delivery and operational efficiency. An equivalence in digital identity frameworks allows for better coordination parties, reducing duplication and improving the accuracy of data. This leads to more effective policy implementation and resource allocation.

For citizens, interoperability means greater access to services and opportunities. A recognised digital identity across borders simplifies interactions with government services, healthcare, education, and financial institutions. This equivalence enhances the quality of life and promotes social inclusion. Interoperability between the EU and Canada ensures that digital identities and trust services adhere to stringent security and privacy standards. This collaboration provides a safer digital environment for all stakeholders.

Mutual recognition complements the alignment of legal and regulatory frameworks. This alignment reduces legal uncertainties and compliance costs for businesses, making it easier to navigate the regulatory landscape in both regions. It also ensures that citizens' rights are protected consistently across borders. Public services benefit from interoperability through improved efficiency and reduced costs. Governments can share best practices and technologies, leading to more effective service delivery.

The digital economy thrives on interoperability, but requirements strategic alignment and real investment. By enabling seamless interactions between digital systems, the EU and Canada can build a robust digital marketplace that maximizes the return on investment This boost to the digital economy can support job creation, innovation, and sustainable growth. Further, a robust digital marketplace can promote cross-border collaboration in research, development, and innovation that includes academic institutions, research organisations, and businesses that will be able work together more effectively, leveraging shared digital identities and trust services.

V COMPARATIVE ANALYSIS: EU AND CANADA FRAMEWORKS

This section provides a comparative analysis of the EU and Canada's approaches to digital identity and trust frameworks, with particular attention to legal instruments, technical architectures and standardization efforts.

The analysis begins with the European Union's framework for trust services and digital identity, as established under Regulation (EU) No 910/2014 (eIDAS) and its subsequent amendments and updates. This includes a review of the legal recognition of trust services, the architecture and any Implementing Acts guiding the EU Digital Identity Wallet, and the alignment of EU standards with international norms such as ISO, FATF, W3C, OpenID Foundation, and the Open Wallet Foundation.

The analysis then turns to Canada's legislative and policy framework, which is a collection of varied legal, policy and technology instruments covering a federated model built through collaborative federal-provincial-territorial efforts. Emphasizing incremental and consensus-based progress, the Canadian approach reflects an ongoing collective partnership between levels of government, the private sector, and international actors.

Following this analysis, the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services is explored on how it can support legal and technical interoperability. The Model Law provides a globally recognised baseline for enabling mutual recognition and cross-border trust in identity frameworks—helping to bridge divergent systems and facilitate secure, reliable digital interactions internationally.

Finally, standardization and interoperability are explored, identifying key technical and legal alignment opportunities between EU and Canadian frameworks. Particular attention is given to the mutual recognition of digital credentials and the potential for convergence on common standards.

V.1 EU-CA Comparison

While the EU and Canada differ in their approaches to digital identity and trust, one being regulatory-driven and the other grounded in voluntary collaboration, they align in spirit on several key principles. Both jurisdictions prioritize user privacy, data protection, and security, and share a common goal of enabling secure, seamless digital interactions for citizens and businesses alike. They also recognise the need for interoperability, both domestically and internationally, and are committed to fostering trust in digital ecosystems that support economic growth and improved public service delivery. These shared values create a solid foundation for dialogue and cooperation.

However, the differences in governance structures, legal traditions and public expectations naturally lead to varying perspectives. The EU's model is grounded in supranational legal authority, with binding requirements for Member States, while Canada's federated system is decentralized with a high degree of jurisdictional autonomy. These differences are not obstacles, but rather important expressions of political and cultural context. The challenge lies in accommodating these distinctions in a way that enables mutual recognition and technical interoperability, while honouring the sovereign choices of each party. Success will depend on building flexible, respectful frameworks that ensure digital identity solutions are not only functionally compatible but also socially and politically acceptable to both EU and Canadian citizens.

It is beyond the scope of this study to conduct an in-depth analysis of each aspect of the European and Canadian digital identity frameworks. Instead, the following table is intended to provide a high-level comparison that highlights key differences and areas of alignment. These highlights provide a foundational understanding and a prompt for further inquiry into specific areas of interest. This

comparative overview delivers a starting point for deeper analysis, depending on context, objectives, or policy considerations.

Table 1: European and Canadian digital identity frameworks comparison

Aspect	EU	Canada
Overall Goal	Enable trusted cross-border digital identity and trust services	Foster a federated, interoperable digital identity ecosystem
Digital Wallet	European Digital Identity Wallet (EUDIW)	Holder Component
Definition	A secure app for storing, managing, and sharing identity and credentials	A component for holding digital credentials and consent artifacts
Mandatory Deployment	Yes, each Member State must provide one digital identity wallet on request.	No national mandate, but encouraged under voluntary national standards and specifications
Legal Basis	Defined in eIDAS 2.0 and legally binding across EU	Not legally mandated; based on cooperative agreements and best practices
Trust Services	Legally defined (e.g., e-signatures, timestamps, delivery services) by eIDAS and Implementing Acts.	Supported via trust framework components (e.g., credential, consent modules)
Assurance Levels	Three LOAs, (Levels of Assurance) Low, Substantial, High – standardized across EU	Four LOAs, defined as Qualifiers in the PSP-PCTF Conformance Criteria
Conformity Assessment	Mandatory certification of EUDI wallets (driven by a reference implementation) and trust services	Voluntary assessments against PCTF conformance criteria and DGSI/TS 115 conformity assessment programs in development by the Standards Council of Canada and Digital Governance Council.
Mutual Recognition	Trust Services are enforced through formal legal and technical rules between Member States; however, this applies to only Qualified Trust Services or third countries.	Encouraged through process mapping and alignment practices
Modularity	Defined components (wallets, credentials, trust services)	Modular architecture (PCTF atomic processes, compound services, and technical components defined in TS-115)

Summary:

- EU: Legally enforces a unified, interoperable digital identity system across Member States using certified wallets and standardized trust services.
- Canada: Encourages a collaborative, federated framework enabling public and private organisations to interoperate via voluntary conformance with a shared trust model.
- For the EU, the eIDAS regulations and implementing legislative framework is highly structured with mandatory recognition for notified eID schemes and strict requirements for qualified trust services.
- For Canada, the National Standard of Canada, CAN-DGSI-103-1, the techical specification CAN/DGSI TS-115 Techical Specification, and the Public Sector Profile Pan-Canadian Trust Framework are flexible and federated, allowing province-based identity management that is embodied as a Pan-Canadian Approach.

V.2 UNCITRAL Model Law on the Use and Cross-Border Recognition of Identity Management and Trust Services

The UNCITRAL Model Law on the Use and Cross-Border Recognition of Identity Management and Trust Services is a legislative framework developed by the United Nations Commission on International Trade Law (UNCITRAL) to facilitate global interoperability and legal certainty in the use of digital identity and trust services. The Model Law is designed to support the mutual recognition of identity management systems and trust services, such as electronic signatures, seals, timestamps, and authentication, across jurisdictions, thereby encouraging seamless cross-border digital transactions.

A key feature of the Model Law is its technology-neutral and functionally equivalent approach, which ensures that legal effect is not denied to identity or trust services simply because they are electronic or provided across borders. It outlines core legal principles, including the recognition of electronic identification, the obligations and liabilities of service providers and subscribers, reliability requirements, and criteria for designating services as "reliable." Importantly, it also provides mechanisms for cross-border recognition based on equivalence in assurance or reliability levels and encourages cooperation between jurisdictions to support mutual recognition. The Model Law serves as a flexible tool for countries looking to modernise their legal infrastructure for digital identity while enabling international alignment and trust.

The UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services offers a valuable opportunity for Canada and the European Union to "meet in the middle" in addressing their differences while building on their shared values and aspirations. While both jurisdictions place a strong emphasis on privacy, user control, and trust, their approaches diverge in terms of legal structure—Canada favouring a federated, consensus-driven model and the EU adopting a harmonised, regulatory framework. The Model Law provides a neutral, internationally recognised foundation that is both flexible and technology-agnostic, enabling jurisdictions with different legal systems and governance models to align without compromising their sovereignty or domestic policy priorities. It emphasizes functional equivalence and mutual recognition based on comparable levels of assurance or reliability, which could help bridge gaps between Canada's voluntary framework and the EU's mandatory regulatory environment.

Moreover, the adoption of the Model Law can lay the groundwork for a broader international framework for mutual recognition. It is common practice for countries to use UNCITRAL model laws as a basis for domestic legislation, making them trusted instruments for fostering global legal interoperability. For Canada and the EU, aligning with the Model Law would not only facilitate bilateral cooperation but also position each as leaders in shaping a scalable and inclusive global digital trust ecosystem. By using the Model Law as a reference point, both parties can promote a common language and legal foundation that supports cross-border trust services, creating a ripple effect that accelerates mutual recognition with other international partners and contributes to the development of a cohesive, rights-respecting global digital identity infrastructure.

It is beyond the scope of this project to conduct a detailed, article-by-article legal analysis of the UNCITRAL Model Law in direct relation to the frameworks of the European Union and Canada. However, the project team has reviewed the content of the articles of the Model Law and concluded that its structure and principles represent an acceptable and viable approach to support mutual recognition between the two jurisdictions. The following table provides a summary of key insights for each article of the Model Law, focusing on their relevance to EU and Canadian contexts, with a concluding assessment that reflects the overall alignment. More detailed working notes and analytical observations are included in the Appendix C for reference.

Table 2: UNCITRAL Model Law on the Use and Cross-Border Recognition of Identity Management and Trust Services Relevance to EU and Canadian contexts

Article	Summary, Key Insights and Recommendations
Article 1: Definitions	The terms and definitions are acceptable and can be applied in context. *It is recommended* that Canada support the Model Law's definitions as they align closely with Canadian terminology and existing standards. However, Canada often uses broader and more abstract definitions that allow for flexibility in implementation. *It is recommended* that the EU agrees in principle with the definitions set out in Article 1 of the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management (IdM) and Trust Services, while recognizing variations in terminology and conceptual frameworks within the EU Regulatory context of the EU Digital Identity framework.
Article 2: Scope	Emphasizes focus on commercial activities and trade-related services, while allowing for potential expansion into other electronic transactions involving businesses, governments, and consumers. *It is recommended* that Canada support the general principles outlined in Article 2 of the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management (IdM) and Trust Services while emphasizing that its implementation will be guided by existing national standards, applicable legislation, and regulatory frameworks. *It is recommended* that that the EU support the general principles outlined in Article 2 of the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management (IdM) and Trust Services while emphasizing that its implementation will be framed within the existing EU Digital Identity framework, and regulatory frameworks primarily intended for Government use towards citizens.
Article 3: Voluntary use of identity management and trust services	Using identity management and trust services is completely voluntary—no one is required to use them or a specific provider unless they choose to do so. People and businesses have the freedom to decide whether to use these services based on their needs and preferences. In summation, it is important to recognise that mutual recognition between the EU and Canada does not require full agreement on every aspect of digital identity governance, but rather a shared respect for each other's sovereignty and policy choices. The use of identity management and trust services remains voluntary in both jurisdictions—individuals and businesses are not compelled to use them or a specific provider unless they choose to do so. Canada's approach, rooted in provincial and territorial autonomy, aligns well with this principle, allowing each jurisdiction to determine its own participation based on local needs and capacities. It is therefore recommended that Canada support this principle as it reflects the flexibility and subsidiarity of the Pan-Canadian model. Conversely, the European Union may take a different stance. Under eIDAS 2.0, EU citizens and residents are guaranteed the right to a digital identity that is fully under their control and that enables access to services and participation in the digital economy. While this right does not mandate usage, it reflects a more assertive regulatory posture that

	goes beyond voluntary adoption. In this context, the EU may not support the article as written, given that it frames digital identity as entirely optional, which may not fully align with the legal entitlements and policy goals established under EU law. Nonetheless, recognizing these differences—rather than attempting to resolve them—is key to building a respectful and functional basis for cross-border interoperability. *It is recommended* that Canada agree with this article as it is consistent with the Pan-Canadian approach that allows for the Provinces and Territories to make their own determination. *It is recommended* that the EU agree with this article, whilst noting that according to eIDAS, education and legal services have specific regulatory requirements that mandate the use of the EUDIW for identity verification and authentication.
Article 4: Interpretation	*It is recommended* that Canada agree with this Article. *It is recommended* that the EU agree with this Article. Both the European Union and Canada could express their agreement to honour the intent and spirit of the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services. In doing so, both parties acknowledge the international origin of the Model Law and affirm their commitment to promoting uniformity in its application, consistent with the principle of good faith in international cooperation and trade. While each jurisdiction retains its own legal and policy frameworks, the EU and Canada agree that matters not expressly settled by the Model Law could be interpreted and addressed in accordance with its underlying general principles. This shared understanding reinforces a foundation of trust, flexibility, and mutual respect—enabling both parties to move forward collaboratively toward greater interoperability and recognition in the global digital identity landscape.
Article 5. Legal recognition of identity management	Ensures that electronic identification is legally recognised and cannot be dismissed simply because it is in digital form or because the identity management service is not officially designated under certain regulations. This means that electronic identity proofing and verification have the same legal validity as traditional, paper-based identification methods. Additionally, even if an identity management service has not been formally approved under specific laws, its results cannot be automatically rejected just for that reason. This provision helps promote trust in digital identity systems and supports their use in legal and commercial settings. *It is recommended* that Canada agree with this Article. Legal recognition is enabled by existing legislation at the Federal level, and in the Provinces and Territories, along with jurisprudence, provides a legal foundation that recognises and supports the admissibility of electronic documents and digital records as valid forms of evidence. These frameworks affirm that electronic communications and records can hold the same legal weight as their paper counterparts, provided they meet standards of reliability, integrity, and authenticity. This legal recognition ensures that digital identity credentials and trust services—when implemented—can be used in both public and private sector contexts,

	including legal proceedings, without requiring additional legislative changes. *It is recommended* that the EU agree with this Article. The EU has existing enacted legislation, on electronic identification and trust services for electronic transactions, the EU Digital Identity framework. This is further supplemented by ongoing legislation through a growing series of Implementing Acts.
Article 6. Obligations of identity management service providers	Identity management service providers must follow clear rules and policies to ensure their systems function properly and securely. They are responsible for enrolling users by collecting and verifying identity information and linking credentials to individuals. They must also manage identity credentials by issuing, updating, suspending, and renewing them, as well as handling electronic identification processes. Providers must operate their systems reliably, ensure they are accessible online, and follow their own stated policies. They could make their policies available to users and third parties, clearly communicate any limitations on service or liability, and provide a way for users to report security breaches. *It is recommended* that Canada agree with this Article as these requirements are comprehensively addressed in the Public Sector Profile Pan-Canadian Trust Framework (PSP-PCTF) Conformance Criteria and reflected in the National Standard of Canada, CAN/DGSI 103-1. Together, these instruments ensure that identity management services in Canada are held to rigorous standards of trust, accountability, and user protection. *It is recommended* that the EU agree with this Article as these requirements are explicitly detailed and enforced through the EU Digital Identity Framework, including the eIDAS Regulation (and eIDAS 2.0) and its associated implementing acts. These legally binding instruments establish comprehensive obligations for identity management service providers, including responsibilities for user enrolment, identity verification, credential lifecycle management, system reliability, and operational transparency. The regulatory framework ensures consistent application across all Member States, promoting trust, legal certainty, and cross-border interoperability within the European Digital Single Market.
Article 7. Obligations of identity management service providers in case of data breach	If an identity management service provider experiences a security breach or data integrity issue that significantly affects its system, it must take immediate action. This includes containing the breach by suspending affected services or revoking compromised credentials if necessary, fixing the issue, and notifying relevant parties as required by law. If someone reports a suspected breach, the provider must investigate the issue and take appropriate steps to resolve it, following the same process as if they had discovered the breach themselves. It is recommended that Canada agree with this Article, as it is already well reflected in Canada's policy, legal and regulatory landscape. The Personal Information Protection and Electronic Documents Act (PIPEDA), along with provincial privacy laws such as British Columbia's PIPA, Alberta's PIPA, and Québec's Law 25, impose clear and enforceable obligations on organisations—including identity

	management service providers—to take appropriate security measures to protect personal information. These laws require organisations to assess the impact of a breach, notify affected individuals, and report to the appropriate privacy authorities when there is a real risk of significant harm. **It is recommended that the EU agree** with this Article as these obligations are well-detailed in the EU Digital Identity Framework, namely in Article 10 of the Regulation, where either the electronic identification scheme notified within a Member State or the authentication referred to, is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission.
Article 8. Obligations of subscribers	The subscriber shall notify the identity management service provider, by utilizing means made available by the identity management service provider pursuant to article 6 or by otherwise using reasonable means, if: (a) The subscriber knows that the subscriber's identity credentials have been compromised; or (b) The circumstances known to the subscriber give rise to a substantial risk that the subscriber's identity credentials may have been compromised Both in Canada and the EU, a subscriber is not legally obligated to notify the identity management service provider. In Canada and the EU, individuals are not legally obligated to report breaches of their own personal data; however, they do carry a personal responsibility to act swiftly if they become aware that their information has been lost or compromised. It is generally expected that individuals will take proactive steps—such as notifying government services, local police, financial institutions, and credit bureaus—to protect themselves from further harm. While this responsibility is important, it should not be mandated by law. Instead, identity management systems and service providers could clearly outline these expectations in their terms and conditions, providing individuals with guidance on how to respond to data breaches, including monitoring for fraud and securing affected accounts. This approach respects individual autonomy while promoting awareness and accountability without imposing legal obligations. **It is recommended that the Canada and EU agree to a common interpretation to the Article** in that the identity management service provider is to provide a mechanism for the subscriber to notify them of their compromised credentials. While Canada and the European Union may hold differing positions regarding the obligations of individuals in responding to personal data breaches, this divergence does not undermine the overall integrity of

	their respective digital identity frameworks. These differences can be constructively addressed within a mutual recognition agreement that respects each jurisdiction's legal and cultural context. What remains consistent between both parties is a strong commitment to ensuring the reliability, accountability, and security of identity management and trust services. By focusing on shared principles—such as transparency, user protection, and system integrity—Canada and the EU can establish a foundation for mutual recognition that accommodates these variations while upholding high standards of trust and interoperability.
Article 9. Identification of a person using identity management	Where the law requires the identification of a person for a particular purpose, or provides consequences for the absence of identification, that requirement is met with respect to identity management services if a reliable method in accordance with article 10 is used for the identity proofing and electronic identification of the person for that purpose. **It is recommended that Canada agree** with this Article. The requirement for reliable identification of a person for legal purposes can be fulfilled using the CAN/DGSI 103-1 standard and the conformance criteria of the Public Sector Profile Pan-Canadian Trust Framework (PSP-PCTF). The standard and framework establish reliable methods for identity proofing and electronic identification, ensuring compliance. By adhering to the processes and assurance levels defined the standard and framework, identity management services can verify an individual's identity with a level of confidence appropriate to the legal requirements. This structured approach, verified under the auspices of a recognised conformity assessment program ensures that reliable identification mechanisms align with federal and provincial regulations, and abide with the MLIT articles in support of mutual agreement. **It is recommended that the EU agree** with this Article. EU citizens and residents have the right to a digital identity that is under their sole control and that enables them to exercise their rights in the digital environment and to participate in the digital economy to access public and private online and offline services throughout the EU. Member States may involve the private sector in their provision of those means. For use with Trust Services or interactions with public sector institutions, a High-Level Assurance (LOA3) identification could be used.
Article 10. Reliability requirements for identity management services	Identity Management Services could be reliable as appropriate for the purpose for which it is being used. The measure of reliability could consider the compliance of the identity management service provider with its own rules, policies and practices, recognised national and international standards and procedures, and with the level of assurance frameworks prevailing. **It is recommended that Canada agree** with this Article. Reliability requirements for identity management services can be met through assessment using the CAN/DGSI 103-1 standard and the conformance criteria of the Public Sector Profile Pan-Canadian Trust Framework (PSP-PCTF). **It is recommended that the EU agree** with this Article. As this is already a regulation in law, the provision of the services describe is mandatory by Member States. All trust service providers are subject to the requirements of this Regulation, particularly those on security and liability

	to ensure due diligence, transparency and accountability of their operations and Qualified Services. (eIDAS Recital 35). The Member State liability and that of the Qualified Trust Service Providers (QTSPs) located in its jurisdiction shall be applied in accordance with national rules on liability.
Article 11. Designation of reliable identity management services	A person, organisation or authority, whether public or private, specified by the enacting jurisdiction as competent, may designate identity management services that are presumed reliable. The person, organisation or authority, whether public or private, specified by the enacting jurisdiction as competent, shall consider all relevant circumstances, in designating an identity management service; and publish a list of designated identity management services, including details of the identity management service provider. Any designation shall be consistent with recognised international standards and procedures relevant for performing the designation process, including level of assurance frameworks. **It is recommended that Canada agree** with this Article in accordance with the jurisdictions under its sovereignty. The designation of reliable identity management and trust services under Article 11 can be carried out by a senior government official on behalf of the federal government, as well as the provinces and territories. Given the established coordination between federal and provincial authorities, this role could be assigned to the Chief Information Officer (CIO) of the Government of Canada, who operates within the Treasury Board Secretariat (TBS). As a key advisor on digital identity, cybersecurity, and information management, the CIO provides expert guidance to the President of the Treasury Board, a minister within the federal government, ensuring that designated services meet the necessary standards for security, privacy, and interoperability. This structured approach would enable a unified and consistent designation process across jurisdictions, reinforcing the trust and reliability of identity services used across Canada. **It is recommended that the EU agree** with this Article in accordance with the jurisdictions under its sovereignty. In the context of the EU Digital Identity Framework, the eIDAS Regulation ensures compliance of the notifying Member State and for all Qualified Trust Service Providers, the party issuing the electronic identification means and the party operating the authentication procedure. This is achieved via the use of national conformity assessment bodies and accreditation bodies.
Article 12. Liability of identity management service providers	The identity management service provider shall be liable for loss caused to the subscriber or to the relying party due to a failure to comply with its obligations. The rules on liability under the law and is without prejudice to any other basis of liability under the law, including liability for failure to comply with contractual obligations; or any other legal consequences of a failure of the identity management service provider to comply with its obligations under this Law. The identity management service provider shall not be liable to a subscriber for loss arising from the use of an identity management service to the extent that its use exceeds the limitations on the purpose or value of the transaction for which the identity management service is used; and those limitations are contained in the arrangement between the identity management service provider and the subscriber.

	The identity management service provider shall not be liable to a relying party for loss arising from the use of an identity management service to the extent that the use exceeds the limitations on the purpose or value of the transaction for which the identity management service is used; and the identity management service provider has complied with its obligations with respect to that transaction. **It is recommended that the Canada and EU agree** to a common interpretation to the Article with respect to liability under the law associated with contractual and regulatory obligations. While in principle, liability could be addressed, the distribution of liability and indemnity is typically managed through agreements and contracts, not through statutory provisions. In the Canadian context, there is no specific legislation governing the liability of identity management service providers. Instead, federal contracts follow the Mandatory Procedures for Limitation of Contractor Liability and Indemnification in Contracts, and intergovernmental agreements between federal, provincial, and territorial partners routinely include indemnity clauses to allocate risk appropriately. Where disputes arise involving multiple levels of government, they are generally resolved through intergovernmental agreements, administrative tribunals, or the courts. This approach provides the necessary accountability while preserving flexibility and respecting jurisdictional autonomy. Therefore, prescribing liability through legislation would not align with Canada's collaborative, agreement-based governance model. The eIDAS Regulation explicitly addresses the issue of liability within the EU Digital Identity Framework. Under eIDAS, the notifying Member State, as well as Qualified Trust Service Providers, the party issuing the electronic identification means, and the party operating the authentication procedure, are all held liable for failure to meet their obligations under the Regulation. However, it is important to emphasize that this liability framework is designed to be applied in alignment with national legal systems. The Regulation does not override national rules concerning the definition of damages, procedural requirements, or burden of proof. Member States retain autonomy in how liability is interpreted and enforced within their jurisdictions. Additionally, there is a strict notification and reporting process from Member States to the EU in cases of breaches or failures. This ensures that liability is enforced consistently, while allowing for necessary flexibility to respect the legal traditions and practices of individual Member States.
Article 13. Legal recognition of trust services	Same response as Article 5 as applied to legal recognition of trust services
Article 14. Obligations of trust service providers	Same response as Article 6 as applied to obligations of trust service providers
Article 15. Obligations of subscribers	Same response as Article 8 as applied to obligations of subscribers.
Article 16: Digital Signatures	Legal validity of digital signatures **It is recommended that Canada agree** with this Article as it aligns with existing Canadian legislation, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and the Canada Evidence Act, which recognise the legal validity of electronic signatures.

	Canadian law supports the use of electronic signatures as functionally equivalent to handwritten ones, provided they are reliable for identifying the person and confirming their intent. This principle is also reflected in provincial electronic commerce laws, making Article 16 consistent with Canada's legislative framework and practices. **It is recommended that the EU agree** with this Article, as it is consistent with the eIDAS Regulation**,** which provides a comprehensive legal framework for the use and the recognition of electronic signatures across all Member States. Under eIDAS, electronic signatures, including advanced and qualified electronic signatures, are legally valid and enforceable, provided they meet specific reliability and security requirements. The Regulation ensures that electronic signatures can be used in legal and commercial transactions with the same legal effect as handwritten signatures, supporting trust, cross-border recognition, and digital transformation across the EU.
Article 17. Electronic seals	Same response as Article 16 as applied to electronic seals.
Article 18. Electronic timestamps	Same response as Article 16 as applied to electronic timestamps. It should be noted that Canada does not currently have specific legislation dedicated solely to electronic timestamping, but electronic timestamps are recognised and supported within the broader legal and regulatory frameworks.
Article 19. Electronic archiving	Same response as Article 16 as applied to electronic archiving. It should be noted that Canada does not currently have specific legislation dedicated solely to electronic archiving but is recognised and supported within the broader legal and regulatory frameworks.
Article 20. Electronic registered delivery services	Same response as Article 16 as applied to electronic registered delivery services. It should be noted that Canada does not currently have specific legislation dedicated solely to electronic registered delivery services but is recognised and supported within the broader legal and regulatory frameworks.
Article 21. Website authentication	Same response as Article 16 as applied to website authentication. It should be noted that within the Canadian context, this requirement would be enforced by the various internet domain registration providers, for example the country code top-level domain (ccTLD) for Canada is ".ca" enforced by the Canadian Internet Registration Authority (CIRA) which has delegate authority from the Government of Canada.
Article 22. Reliability requirements for trust services	Same as response Article 10 as applied to reliability requirements for trust services.
Article 23. Designation of reliable trust services	Same response as Article 11 as applied to designation of reliable trust services.
Article 24. Liability of trust service providers	Same response as Article 12 as applied to liability of trust service providers
Article 25. Cross-border recognition of the result of electronic identification	Equivalencies of levels of assurance and legal effect. **It is recommended that Canada and the EU agree** to this Article with a common understanding between levels of assurance and system reliability in each respective jurisdiction to be recognised through an MRA. It is also recommended to build on the study conducted by the OECD on G7 Mapping of Digital Identity Approaches.

Article 26. Cross-border recognition of the result of the use of trust services	Equivalency of reliability and legal effect. **It is recommended that Canada and the EU agree** to this Article which enables the EU and designated national authorities to engage in international cooperation. This article provides the foundations for exchanging information, expertise and good practices; recognises legal effects enabled through an MRA; and aligns and harmonises criteria for levels of assurance and reliability.
Article 27. Cooperation	Recognition of legal effect **It is recommended that Canada and the EU agree** to this Article which enables the EU and designated national authorities to engage in international cooperation. This article provides the foundations for exchanging information, expertise and good practices; recognises legal effects enabled through an MRA; and aligns and harmonises criteria for levels of assurance and reliability.

V.3 Using the Analysis as an Approach to Mutual Recognition

Based on the analysis in the preceding table Articles 25 through 27 of the UNCITRAL Model Law would form the core provisions for enabling mutual recognition of identity management and trust services between jurisdictions. These articles can provide the legal basis, by means of an agreement, for accepting the reliability of foreign-originated services, recognizing the equivalence of assurance levels, and supporting cross-border interoperability without requiring complete alignment of the respective legal frameworks. An agreement would allow jurisdictions like Canada and the European Union to preserve their sovereignty, including data sovereignty, and differing governance models while establishing a foundation of trust that supports international digital interactions.

Building on this foundation, the preceding articles addressing elements such as liability, security, reliability, and user rights would be addressed through bilateral or multilateral negotiations and agreements that would map each party's frameworks to the general principles of the Model Law. By anchoring mutual recognition in Articles 25 to 27 and complementing them with agreements on the operational details found in the earlier articles, Canada and the EU could create a flexible, principles-based framework that enables cross-border digital trust. This approach not only respects the distinct legal and policy environments of both jurisdictions but also sets a precedent for engaging with other international partners in a consistent and scalable manner.

While the intentions of both Canada and the European Union generally align, particularly around user-centricity, privacy, security, and interoperability, their methods of implementation differ significantly. The EU has taken a prescriptive, regulatory-driven approach, codifying detailed technical and operational requirements within the eIDAS Regulation and its implementing acts. These binding legal instruments specify not only high-level obligations but also the architecture, assurance levels, wallet functionality, and certification processes that Member States and trust service providers must follow. This top-down approach aims to ensure consistency, legal certainty, and enforceability across all Member States, supporting a harmonised digital single market.
In contrast, Canada has pursued a more flexible, cooperative model, developing voluntary national standards and guidelines through collaboration among federal, provincial, territorial, and private sector stakeholders. Rather than codifying technical detail in regulation, Canada relies on frameworks such as the Public Sector Profile Pan-Canadian Trust Framework (PSP-PCTF) and the National Standard CAN/DGSI 103-1, which offer conformance criteria and best practices. These are intended to align with existing legal instruments, such as PIPEDA, the Canada Evidence Act and relevant provincial laws, avoiding the need for new legislation while promoting interoperability and trust. This

approach allows for greater jurisdictional autonomy and adaptability to local needs but also relies on consensus and coordination rather than legislative mandate to drive adoption.

Finally, the intent of this mutual recognition effort is not to export or impose one jurisdiction's model onto the other, as the domestic contexts, legal systems, and governance structures of Canada and the European Union are inherently different. Instead, the goal is to embrace these differences and build a practical, respectful middle road that allows for seamless interoperability. By focusing on shared principles and aligning on core elements such as assurance, trust, and user protection, Canada and the EU can create a seamless experience for individuals and businesses interacting across borders. This approach ensures that digital credentials and identity services remain reliable and secure, while also being adaptable to the unique realities and expectations of each jurisdiction's citizens.

VI MUTUAL RECOGNITION

Mutual Recognition Agreements (MRAs) serve as critical instruments in promoting international trade and cooperation between two or more jurisdictions by accepting each other's regulations, standards and/or conformity assessment procedures as equivalent. In the context of digital identity and trust services, the principles of mutual recognition aim to facilitate cross-border interoperability, ensuring that digital identities and electronic signatures are recognised and accepted across borders without the need for redundant or repetitive assessments.

The Comprehensive Economic and Trade Agreement (CETA) between the EU and Canada already includes provisions for mutual recognition of technical standards in several sectors. Expanding the conformity assessment protocol within CETA to cover digital credential and digital trust services would provide a structured and recognised mechanism for the mutual acceptance of conformity assessments related to digital identities.

This study includes analysis and provides the basis for the recognition of conformity assessments carried out by recognised bodies in both regions.

VI.1 Potential Use Cases for Mutual Recognition

Mutual recognition of digital credentials and trust services between the European Union and Canada holds transformative potential across a wide range of sectors. By enabling interoperability between trusted digital identity frameworks, including the European Digital Identity (EUDI) Wallet and Canada's Digital Governance Standards Institute (DGSI), both jurisdictions can foster secure, seamless, and privacy-preserving digital interactions. The following use cases were originally identified in highlight high-impact domains where mutual recognition can bring immediate benefits and the results obtained can be compared to existing similar Large-Scale Pilots for the EUDI framework within the EU.

Use Case UC1: Mobile Driver's Licences (mDLs)

Citizens from either jurisdiction could use a mobile driver's licence stored in a secure wallet as legal proof of identity and driving privilege. mDLs that adhere to ISO/IEC 18013-5/7, ISO-23220 and respective eIDAS Regulation or Canada's National Standard, CAN/DGSI 103-1, ensure seamless, contactless identity verification across borders. This supports use cases such as car rentals, traffic stops, and potentially identity checks, while maintaining user privacy and data minimization.

Use Case UC2: Travel and Immigration

Canadian and EU citizens could use secure digital travel credentials stored in compliant digital wallets to verify their identity at border control points, hotels, and other service providers. These credentials,

anchored in nationally issued and internationally recognised identity systems, would conform to the UNCITRAL Model Law, and respective EU eIDAS Regulation or Canada's DGSI Digital Credentials and Digital Trust Services Specification. Mutual recognition of these credentials would enhance traveler convenience, reduce manual checks, and support more efficient cross-border movement. Digital credentials can streamline immigration and travel-related documentation:

- Digital Passports and Visas: The ability to present verifiable, secure digital travel documents would improve processing times and security at borders.
- Residency and Work Permits: Digital verification of legal residency and work eligibility could simplify administrative processes for governments and employers, benefiting immigrants and expatriates.
- Proof of Funds: To show that the applicant has appropriate financial resources.

Use Case UC3: Educational, Professional and Financial Qualifications

As identified in bilateral technical and policy workshops, the mutual exchange of verifiable credentials in education and professional domains offers substantial value:

- University Degrees and Transcripts: Students moving between Canada and the EU could have their academic credentials verified and recognised efficiently, supporting mobility and reducing administrative barriers.
- Professional Certifications: Licenses and certifications in fields such as medicine, engineering, and law could be digitally verified, promoting workforce mobility and mutual professional recognition.
- Financial Qualifications: To prove an individual has sufficient funds or creditworthiness prior to an enrolment or registration transaction.

These applications form an ideal starting point for pilot projects, as they represent relatively low-friction domains and can generate valuable insights for broader implementation.

Use Case UC4: Medical Records and Vaccination Certificates

Interoperable digital health credentials offer significant advantages:

- Medical Records: Mutual recognition would allow healthcare providers in both jurisdictions to securely access patient records, enhancing continuity of care for travelers, migrants, and temporary residents.
- Vaccination Certificates: Verifiable digital certificates would ensure efficient and accurate verification of vaccination status, an essential function in both public health and cross-border mobility contexts.

Use Case UC5: Organisational Digital Identities (ODIs) and Business Document Exchange

Businesses engaged in cross-border trade face challenges related to trust, legal recognition, and interoperability. The mutual recognition of ODIs and digital business documents would:

- Enable legally binding document exchange, including contracts, invoices, and shipping documentation, using recognised electronic signatures and secure identities.
- Support compliance with data protection regulations, including the EU's GDPR and Canada's PIPEDA.

- Foster interoperability through international standards (e.g., W3C Verifiable Credentials), reducing ambiguity and improving digital document handling across systems.
- Enhance security and trust, allowing encryption and traceability to protect commercially sensitive information.
- Improve efficiency and transparency, lowering transaction costs and providing auditable digital records.

A pilot project focusing on business document exchange could demonstrate early economic value and showcase the trade and regulatory benefits of mutual recognition in commercial contexts.

Use Case UC6: Electronic Identity for Financial, Real Estate, and Legal Transactions

Sectors such as finance, real estate, and legal services operate under strict compliance obligations, including KYC/AML regulations, land title verification, and contractual due diligence. These industries are well-positioned to adopt electronic identity (eID) systems due to their regulatory maturity and transaction-based business models. The application of trusted digital identity and electronic attestations can:

- Streamline onboarding and verification processes by enabling secure, standards-based electronic identity and credential presentation compliant with FATF and FINTRAC regulations.
- Support legally recognised digital signatures and seals for binding agreements such as mortgage contracts, powers of attorney, and title transfers.
- Facilitate interoperability across jurisdictions and platforms through the use of verifiable credentials and digital wallets aligned with EUDI Framework and Public Sector Profile Pan-Canadian Trust Framework requirements.
- Enhance auditability, fraud prevention, and document traceability in high-value transactions through digital timestamps, archiving, and identity assurance mechanisms.
- Reduce friction in complex, multi-party transactions by enabling real-time identity validation, agent relationships, and delegated authority models (e.g., lawyers acting on behalf of clients).

VII TECHNICAL AND REGULATORY REQUIREMENTS

Both the European Union (EU) and Canada have established digital credential ecosystems that prioritize security, privacy, and user control. The EU Digital Identity Wallet (EUDI Wallet), governed by eIDAS 2.0, and DGSI TS 115, Canada's technical specification for digital identity and trust services, serve as foundational frameworks for their respective regions. Appendices 4 and 5 provides comprehensive analysis on the EUDI Wallet component of the EU Digital Identity Framework and Canada's DGSI TS 115 on digital credential and digital trust services.

While these systems differ in their approach, particularly in their trust models and regulatory oversight, they share the same core objectives: ensuring the authenticity of digital credentials, safeguarding personal data, and promoting economic collaboration through digital services. This section offers a structured comparison and contrast across the following core dimensions: legal foundations, trust models, technical architectures, privacy standards, and credential governance.

VII.1 Regulatory Foundations and Governance

The EUDI Wallet is governed by the Regulation on electronic identification and trust services (eIDAS 2.0), which mandates a pan-European digital identity ecosystem regulated by Member States. It provides a legal obligation for all EU countries to offer citizens and businesses access to a government-issued wallet that may be used across the EU for a wide range of public and private services.

In contrast to legislation or regulations, CAN/DGSI 103-1 is a voluntary national standard and DGSI TS 115 is a technical specification. These documents are governed by a voluntary standards-based approach, published by the Digital Governance Standards Institute (DGSI) in collaboration with Canadian stakeholders. While they align with federal and provincial digital identity strategies, it does not carry the force of law and relies instead on conformance through self- or third-party certification mechanisms.

The EUDI Wallet is built on a federated trust model, where identity providers and trust service providers are designated and supervised by national competent authorities. Trust and assurance are centralized through conformity assessment bodies and notified under EU law.

DGSI TS 115, by contrast, is based on a decentralized trust model inspired by self-sovereign identity (SSI) principles. It supports Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) issued by a variety of entities without requiring central authority oversight. Trust is instead derived through cryptographic proofs and governance frameworks that define the rules for how participants interact.

VII.2 Technical Architecture and Credential Model

Both frameworks share support for W3C Verifiable Credentials, providing a common technical substrate for credential issuance and presentation. However, their authentication, issuance, and assurance processes differ significantly:

- EUDI Wallet incorporates PKI, OAuth 2.0, eIDAS signature formats. Identity providers are authorized by Member States, and credentials must meet strict assurance levels (e.g., LOA2, LOA3).
- DGSI TS 115 supports DID-based authentication, quantum-safe cryptography, and TLS 1.3. Credential issuers are defined within trust frameworks, and assurance is provided through cryptographic validity and conformity with framework rules.

Moreover, the EUDI Wallet specifies wallet-level functional requirements, such as user consent, cryptographic protection, and device-level security, whereas DGSI TS 115 defines layered architecture roles (e.g., Holder, Issuer, Verifier) and places flexibility in wallet implementations.

VII.3 Privacy and Data Protection

The EUDI Wallet is required to comply with the General Data Protection Regulation (GDPR), one of the most stringent privacy frameworks globally. It enforces data minimization, purpose limitation, and user control, and mandates a legal basis for all processing operations.

DGSI TS 115 aligns with ISO/IEC 27018 and ISO/IEC 29100, focusing on privacy by design and user-centric control and is underpinned by national and provincial privacy laws (e.g., PIPEDA, Québec's Law 25), introducing variability in legal interpretations.

VII.4 Credential Issuance and Trust Services

The EUDI Wallet restricts credential issuance to Qualified Trust Service Providers (QTSPs) and designated public authorities. Each issuer must undergo a conformity assessment and be registered in a trusted list.

DGSI TS 115 enables a more pluralistic approach, where issuers can be governments, educational institutions, businesses, or even individuals—provided they operate within a defined governance framework. There is no requirement for state designation.

Table 3: EUDI Wallet and DGSI TS 115 Comparison

Feature	EUDI Framework	Canada Voluntary Standards
Regulatory Status	Legally mandated under EU law	Voluntary technical standard
Trust Model	Centralized/federated focused with support for decentralized standards.	Decentralized/Federated focused with support for decentralized standards
Credential Model	W3C format, PKI, OAuth 2.0, Verifiable Credentials. Also includes mDL/mDOC, SD-JWT and CBOR format	W3C format, PKI, DIDs, Verifiable Credentials, Quantum-safe crypto. Also includes mDL/mDOC, SD-JWT and CBOR formats.
Authentication	PKI, eIDAS compliant, DID Auth, TLS and cryptographic proofs.	TLS, cryptographic proofs, OAuth, OIDC
Governance	National authorities and utilises QTSPs	Market-based with governance frameworks
Privacy Compliance	GDPR	ISO/IEC 27018, PIPEDA, and provincial laws
Issuer Accreditation	Designated by state authorities	Self-attested or governed by framework rules

This research study examines the feasibility of achieving mutual recognition through an equivalence agreement, allowing both the EUDI Wallet and DGSI TS 115 to be recognised across jurisdictions without requiring structural changes to each system's regulatory framework. See Appendices for more information

By focusing on functional equivalence rather than harmonization, this study proposes a model for mutual recognition that preserves the autonomy of each framework while ensuring seamless interoperability.

VII.5 Pathway to an Equivalence Agreement

Historically, mutual recognition agreements between regulatory bodies have been achieved through equivalence frameworks rather than strict harmonization. This approach ensures that two systems can maintain their distinct regulatory and trust models while agreeing that their outcomes, such as security, privacy, and identity assurance, are functionally equivalent.

Following this precedent, an EU-Canada Digital Credential Equivalence Agreement (DCEA) could be established, allowing both frameworks to mutually recognise credentials and trust services without the need to modify their underlying structures.

An EU-Canada Digital Credential Equivalence Agreement (DIEA) could define:

1. Identity Assurance Levels: Mapping DGSI trust levels to eIDAS Levels of Assurance (LOA2 and LOA3) for credential verification.

2. Issuer Recognition: Ensuring that DGSI-verified identity providers are regarded as having met EU trust requirements through equivalency and vice versa.

3. Security and Privacy Compliance: Recognizing ISO/IEC 27018 and 29100 standards use in Canada as functionally equivalent to GDPR where applicable.

4. Technical Compatibility: Accepting W3C Verifiable Credentials and ISO/IEC 18013-5 as shared standards, allowing cross-verification without altering authentication methods.

5. Oversight Mechanisms: Establishing a Bilateral Digital Credential Oversight Committee to ensure ongoing compliance and resolve disputes.

VIII RECOMMENDATIONS

VIII.1 Recommendations for EU-Canada Cooperation

The increasing global need for secure and trusted digital identities necessitates cooperation among jurisdictions. Canada and the EU have an opportunity to strengthen their bilateral relationship by developing frameworks for cooperation on identity management and trust services. To operationalize this cooperation, it is essential to establish a structured approach to information exchange, best practices, and the mutual recognition of identity management systems and trust services.

Operationalizing Cooperation on Identity Management and Trust Services between Canada and the European Union

The following outline recommendations for operationalizing cooperation on identity management and trust services between Canada and the EU:

Recommendation 1: Implement a use case-driven approach to mutual recognition.

To accelerate progress toward mutual recognition of digital credentials and trust services between the European Union and Canada, it is recommended that stakeholders adopt a use case–driven approach. By prioritizing targeted, real-world scenarios such as verifiable education credentials, digital health records, mobile driver's licences, and secure business document exchanges, governments and industry partners can collaboratively develop, test, and scale interoperability mechanisms in controlled, high-impact environments. This practical, phased strategy would enable early wins, build trust among stakeholders, and inform the broader policy and technical frameworks needed to support full cross-border mutual recognition at scale.

Recommendation 2: Recognise the legal effects of identity management systems and trust services as per a negotiated agreement.

Establish a mutual understanding of how identity management systems and trust services in each jurisdiction can be recognised and accepted in the other, wherein:

- Canada and the EU could develop a formal bilateral agreement outlining the recognition of the legal effects of foreign identity management systems and trust services. This could be structured as a mutual recognition framework, where each jurisdiction recognises the equivalence of the other's systems. This agreement would cover both unilateral recognition (one jurisdiction recognizing the other's system without formalized mutual agreement) and mutual recognition.
- The agreement could include provisions for recognizing the legal and regulatory frameworks as equivalent in governing identity management and trust services in each respective jurisdiction.
- In instances where full mutual recognition cannot be achieved immediately, Canada and the EU could implement a case-by-case recognition process, considering the specific context and potential risks of recognition.

Recommendation 3: Designate identity management systems and trust services in support of first recommendation.

Develop a cooperative approach to designating trusted identity management systems and trust services to enhance interoperability between Canada and the EU.

- Establish a joint panel with representatives from both Canada and the EU to accept identity management systems and trust services that meet the established criteria through recognised conformity assessment approaches.
- Recognise the conformity assessment approaches, including ISO/IEC 17029 and ISO/IEC 17065 methodologies within both Canada and the EU to evaluate and designate based on established criteria. This would promote greater trust and acceptance of cross-jurisdictional identity management and trust services.
- Create a publicly accessible online registry where designated systems and services are listed, providing transparency and fostering trust among users and service providers across borders.

Recommendation 4: Agree on equivalent levels of assurance of identity management systems and system reliability of trust services between respective jurisdictions.

Ensure consistent standards for the assurance of identity management systems and the reliability of digital identity and trust services, so both Canada and the EU can confidently rely on one another's systems.

- Canada and the EU could mutually recognise and accept equivalent levels of assurance and reliability between each other's systems. This could ensure that a service recognised as trustworthy and secure in one jurisdiction is also recognised as such in the other.

- Both jurisdictions could commit to periodic reviews of frameworks to account for evolving technological advancements, emerging threats, and changing legal requirements. The framework could be flexible enough to incorporate new technologies, including blockchain or decentralized identifiers (DIDs).

Recommendation 5: Establish an equivalency agreement and include digital credentials and digital trust services in the CETA Conformity Assessment Protocol to extend the existing mutual recognition agreement.

Both Canada and the European Union (EU) have developed advanced frameworks for digital identity, electronic signatures, and trust services, which are essential for secure digital transactions. However, the absence of formal equivalency recognition between the two regions creates barriers to seamless cross-border digital interactions, affecting trade, security, and innovation. This recommendation proposes both an equivalency agreement between Canada and the EU for digital credentials and digital trust services, as well as their inclusion in the product coverage of the Comprehensive Economic and Trade Agreement (CETA) Conformity Assessment Protocol, specifically in the context of Article 18.

An equivalency agreement would recognise the mutual compatibility between frameworks and validity of digital credentials and digital trust services between Canada and the EU. In addition to the equivalency agreement, it is recommended that digital credentials and digital trust services be included in the product coverage of the CETA Conformity Assessment Protocol. This Protocol, under Article 18 of CETA, provides mechanisms for ensuring that goods and services exchanged between Canada and the EU meet agreed-upon standards and regulatory requirements.

The inclusion of digital credentials and digital trust services in the CETA Conformity Assessment Protocol, along with the establishment of an equivalency agreement between Canada and the EU, would significantly enhance cross-border trade, security, and the interoperability of digital services while facilitating mutual recognition between the jurisdictions. Mutual compatibility of the frameworks and mutual recognition across both regions would reduce barriers to digital commerce, support innovation, and ensure the security and trustworthiness of digital

transactions. This would help build a more resilient and integrated global digital economy, benefiting individuals, businesses, and governments in both Canada and the EU.

To support this recommendation, a comprehensive analysis of the 27 articles of the UNCITRAL Model Law on the Use and Cross-Border Recognition of Identity Management (MLIT) was conducted. An analysis of each article resulted in article-specific recommendations for the EU and Canada to support, to agree, or to develop a common interpretation of the article. The analysis concluded that all 27 MLIT articles were favourable to both the EU and Canada, noting considerations for differences in contexts and approaches between the EU and Canada. Overall, the MLIT provides an excellent basis to negotiate a mutual recognition agreement. Details of the analysis is found in Section V.2

Table 4: Model Law Recommendations – Summary

Article	EU / CAN Alignment	Article	EU / CAN Alignment
1	Yes	15	Yes
2	Yes	16	Yes
3	Yes	17	Yes
4	Yes	18	Yes
5	Yes	19	Yes
6	Yes	20	Yes
7	Yes	21	Yes
8	Yes	22	Yes
9	Yes	23	Yes
10	Yes	24	Yes
11	Yes	25	Yes
12	Yes	26	Yes
13	Yes	27	Yes
14	Yes		

IX CONCLUSION

This study underscores the strong potential for Canada and the European Union to establish a cooperative framework for the mutual recognition and interoperability of digital identity systems, digital credentials, and trust services. Despite notable structural and legal differences – centralized regulation under EUDI Framework in the EU versus Canada's decentralized, federated model – both jurisdictions share common objectives rooted in trust, security, transparency, and respect for fundamental rights.

Through detailed comparative analysis, including alignment with the UNCITRAL Model Law on Identity Management and Trust Services (MLIT), and exploration of trade facilitation instruments such as CETA and the WTO TBT Agreement, this study demonstrates that Canada and the EU are well-positioned to develop a shared pathway for cross-border digital identity cooperation. The commitment to democratic values and human-centric governance in both regions further strengthens the foundation for such collaboration.

Crucially, this study finds no insurmountable legal or technical barriers to a formal agreement between the two parties. On the contrary, it identifies a set of clear, actionable steps – ranging from establishing an equivalency agreement and mutual recognition of legal effects to shared definitions of assurance, reliability levels and conformity – that can facilitate the legal, technical, and operational interoperability of digital identities and wallets across jurisdictions. The analysis of the MLIT articles along with recommendations for both the EU and Canada can serve as a foundation for the parties to commence the agreement negotiation process. The inclusion of digital credentials and trust services in the CETA Conformity Assessment Protocol and the adoption of a use case–driven approach offers strategic pathways to demonstrate practical feasibility, build trust, and generate momentum.

Next Steps and Future Prospects

It is recommended that the path forward involve translating the recommendations of this study into concrete, operational governance. The authors of the study propose establishing a bilateral working group to formalize a mutual recognition framework, informed by the MLIT and supported by technical pilots. The technical pilots could be based on use cases focused on high-value areas such as digital education credentials, mobile driver's licences, and secure business exchanges. These use cases could help both jurisdictions to build practical experience, refine technical standards, and address legal and operational challenges in real time.

Over time, these early initiatives could serve as the basis for a more integrated and resilient transatlantic digital ecosystem. An equivalency framework could not only reduce friction in cross-border digital transactions but could also strengthen economic resilience, foster innovation, and enhance the global competitiveness of both Canada and the EU.

As the demand for trusted digital infrastructure accelerates worldwide, Canada and the EU have a timely opportunity to lead by example. By recognizing core elements of their respective trust and identity frameworks, they could unlock the full potential of cross-border digital services while setting a precedent for cooperative, rights-based digital governance. In doing so, they will not only strengthen their own digital economies, but also contribute to the development of an inclusive, secure, and interoperable global digital ecosystem grounded in mutual trust and democratic values.

X APPENDICES

Appendix A: Glossary – A Comparison of Terms

MLIT (Article 1)	CAN Reference 103-1	EU 2024/1183	Notes
Attribute	Attribute	Attribute	MLIT, Canada and EU terms and definition substantially equivalent
Data message	subject claim	Data Record	MLIT, Canada and EU definitions substantially equivalent
Electronic identification	identity management / digital representation	Electronic Identification	MLIT, Canada and EU definitions substantially equivalent
Identity	identity	identity	MLIT, Canada and EU terms and definition substantially equivalent
Identity credentials	credential	Identity credential	MLIT, Canada and EU terms and definition substantially equivalent
Identity management services	identity management, Digital identity system and services	European Union Digital Identity Framework (including eIDAS)	Variance between MLIT and Canada definitions of guidelines for systems and services, and EU legal regulation
Identity management service provider	entity	eID operator	MLIT, Canada and EU definitions substantially equivalent
Identity management system	Digital identity system and services	Electronic identification (eID) scheme	MLIT, Canada and EU definitions substantially equivalent
Identity proofing	Identity verification, identity information validation	Validation	MLIT, Canada and EU intent is substantially equivalent. EU mentions validation, with eID responsibility of Member States or PID providers
Relying party	cited in identity information notification and identity information retrieval but not formally defined.	Relying Party	MLIT, EU definitions substantially equivalent and consistent with usage of term in applicable Canadian standards.
Subscriber	Subject	User	MLIT, Canada and EU definitions substantially equivalent
Trust service	Digital identity system and services	Trust Service	MLIT, Canada and EU definitions substantially equivalent
Trust service provider	Digital identity system and services	Trust Service Provider	MLIT, Canada and EU definitions substantially equivalent

Appendix B: Glossary – EU Digital Identity Framework list of Common Terms

The EU has a rich set of definitions for the various components and services provided by the EU Digital Identity Framework.

eIDAS Term	Description under 2014/910 - 2024/1183
Electronic identification	the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing another natural person or a legal person
Electronic identification means	a material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service
Person identification data	a set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person.
Electronic identification scheme	a set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person
Authentication	an electronic process that enables the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form
User	a natural or legal person, or a natural person representing another natural person or a legal person, that uses trust services or electronic identification means provided in accordance with this Regulation
Relying party	a natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a trust service
Public sector body	a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate
Body governed by public law	a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council (15)
Signatory	a natural person who creates an electronic signature
Electronic signature	data in electronic form which is attached to or logically associated with other data in electronic form, and which is used by the signatory to sign
Advanced electronic signature	an electronic signature which meets the requirements set out in Article 26;
Qualified electronic signature	an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures
Electronic signature creation data	unique data which is used by the signatory to create an electronic signature
Certificate for electronic signature	an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person

Qualified certificate for electronic signature	a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I
Trust service	an electronic service normally provided for remuneration which consists of any of the following: (a) the issuance of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services; (b) the validation of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services; (c) the creation of electronic signatures or electronic seals; (d) the validation of electronic signatures or electronic seals; (e) the preservation of electronic signatures, electronic seals, certificates for electronic signatures or certificates for electronic seals; (f) the management of remote electronic signature creation devices or remote electronic seal creation devices; (g) the issuance of electronic attestations of attributes; (h) the validation of electronic attestation of attributes; (i) the creation of electronic timestamps; (j) the validation of electronic timestamps; (k) the provision of electronic registered delivery services; (l) the validation of data transmitted through electronic registered delivery services and related evidence; (m) the electronic archiving of electronic data and electronic documents; (n) the recording of electronic data in an electronic ledger.
Qualified trust service	a trust service that meets the applicable requirements laid down in the Regulation as 'Qualified'
Conformity assessment body	a conformity assessment body as defined in Article 2, point 13, of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides, or as competent to carry out certification of European Digital Identity Wallets or electronic identification means
Trust service provider	a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider
Qualified trust service provider	a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body
Product	hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of electronic identification and trust services
Electronic signature creation device	configured software or hardware used to create an electronic signature
Qualified electronic signature creation device	an electronic signature creation device that meets the requirements laid down in Annex II
Remote qualified electronic signature creation device	a qualified electronic signature creation device that is managed by a qualified trust service provider in accordance with Article 29a on behalf of a signatory
Remote qualified electronic seal creation device	a qualified electronic seal creation device that is managed by a qualified trust service provider in accordance with Article 39a on behalf of a seal creator;

Creator of a seal	a legal person who creates an electronic seal
Electronic seal	data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity
Advanced electronic seal	an electronic seal, which meets the requirements set out in Article 36
Qualified electronic seal	an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal
Electronic seal creation data	unique data, which is used by the creator of the electronic seal to create an electronic seal
Certificate for electronic seal	an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person
Qualified certificate for electronic seal	a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III
Electronic seal creation device	configured software or hardware used to create an electronic seal
Qualified electronic seal creation device	an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II
Electronic time stamp	data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time
Qualified electronic time stamp	an electronic time stamp which meets the requirements laid down in Article 42
Electronic document	any content stored in electronic form, in particular text or sound, visual or audiovisual recording
Electronic registered delivery service	a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations
Qualified electronic registered delivery service	an electronic registered delivery service which meets the requirements laid down in Article 44
Certificate for website authentication	an electronic attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued
Qualified certificate for website authentication	a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV
Validation data	data that is used to validate an electronic signature or an electronic seal
Validation	the process of verifying and confirming that data in electronic form are valid in accordance with this Regulation
European Digital Identity Wallet	an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals
Attribute	a characteristic, quality, right or permission of a natural or legal person or of an object

Electronic attestation of attributes	an attestation in electronic form that allows attributes to be authenticated
Qualified electronic attestation of attributes	an electronic attestation of attributes which is issued by a qualified trust service provider and meets the requirements laid down in Annex V of the eIDAS Regulation
Electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source	an electronic attestation of attributes issued by a public sector body that is responsible for an authentic source or by a public sector body that is designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45f and with Annex VII
Authentic source	a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice
Electronic archiving	a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to ensure their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period
Qualified electronic archiving service	an electronic archiving service which is provided by a qualified trust service provider, and which meets the requirements laid down in Article 45j
EU Digital Identity Wallet Trust Mark	a verifiable, simple and recognisable indication which is communicated in a clear manner that a European Digital Identity Wallet has been provided in accordance with this Regulation
Strong user authentication	an authentication based on the use of at least two authentication factors from different categories of either knowledge, something only the user knows, possession, something only the user possesses or inherence, something the user is, that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data
Electronic ledger	a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records
Qualified electronic ledger	an electronic ledger which is provided by a qualified trust service provider, and which meets the requirements laid down in Article 45l of the Regulation
Personal data	any information as defined in Article 4, point (1), of Regulation (EU) 2016/679
Identity matching	a process where person identification data, or electronic identification means are matched with or linked to an existing account belonging to the same person
Data record	electronic data recorded with related meta-data supporting the processing of the data
Offline mode	as regards the use of European Digital Identity Wallets, an interaction between a user and a third party at a physical location using proximity technologies, whereby the European Digital Identity Wallet is not required to access remote systems via electronic communication networks for the purpose of the interaction.

Appendix C: UNCITRAL Model Law Analysis

Article 1: Definitions

Article 1 of the UNCITRAL Model Law defines key terms that are used in the document.

- Canada Alignment
  The Model Law's definitions align closely with Canadian terminology and existing standards. While some Canadian definitions are broader or more abstract allowing for flexibility in implementation, they align conceptually with the Model Law's intent. Key variations and considerations in comparing the Model Law definitions with Canada's national standard, CAN/DGSI 103-1, include:
    - Attribute (1a): Definition in Canada is slightly broader, encompassing 'things' in addition to 'persons'.
    - Data Message (1b): Definition in Canada aligns, but uses a different term, 'subject claims'.
    - Electronic Identification (1c): Two separate but related definitions are used in Canada: 'identity management' and 'digital representation'.
    - Identity (1d): Identity is categorized in Canada into foundational and contextual identity.
    - Identity Credentials (1e): Definition in Canada is more abstract, considering a 'credential' as an assertion rather than a physical or data-based object.
    - Identity Management Services (1f): Terminology in Canada refers to 'digital identity systems and services', with a focus on broader system functionality.
    - Identity Management Service Provider (1g): This entity in Canada is defined more broadly as an 'organisation' or 'person' with specific legislative or regulatory obligations.
    - Identity Management System (1h): The term 'digital identity systems' with 'atomic processes' that comprise the system is used in Canada.
    - Identity Proofing (1i): The definition in Canada decomposes this process into multiple atomic functions, such as 'identity verification'.
    - Relying Party (1j): Usage of term is consistent with MLIT/EU definitions. There is no formal definition in the National Standard of Canada.
    - Subscriber (1k): The term in Canada that is used to refer to subscriber is 'a subject', which is an 'entity' about which claims are asserted.
    - Trust Service (1l): The term in Canada that is used to refer to trust service is 'digital identity systems and services', which may require contextual clarification.
    - Trust Service Provider (1m): This concept is referred more broadly in Canada to 'digital identity systems' and 'entities', which may require contextual clarification.

- EU Alignment
  The EU agrees in principle with the definitions set out in Article 1 of the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management (IdM) and Trust Services, while recognizing variations in terminology and conceptual frameworks within the EU Regulatory context of the EU Digital Identity framework. The following outlines the EU's stance on key definitions and areas where clarifications may be needed for mutual recognition.

  The Model Law's definitions align generally with the EU' Regulation 910/2014 as amended by EU regulation 2024/1183 and their implementing acts. However, the EU often uses more specific and detailed definitions and functionality descriptions that are appropriate for a

legally binding regulation in law, which is more outcome-based than the UNCITRAL Model Law. Key variations and considerations in comparing the Model Law definitions with EU's regulations and implementing acts:

- Attribute (1a): The EU's definition further defines to include natural Persons, Legal Persons and Objects as well as their attestations.
- Data Message (1b): The EU definition aligns with the definition but may extend to any data in electronic form.
- Electronic Identification (1c): The EU specifies to be in accordance with European Union or EU Member State national law which is used for the authentication to an online service or for an offline service.
- Identity (1d): The EU specifies the identity of a natural or legal person, or of a natural person uniquely representing another natural person or a legal person.
- Identity Credentials (1e): The EU maintains the concept of the tiered assurance levels of "Qualified" as the legally probative level in all its definitions,
- Identity Management Services (1f): The EU considers that the trust anchor for each citizen identity should be the responsibility of each Member State for its citizens.
- Identity Management Service Provider (1g): The EU considers this as Member State-based and operated but may be subcontracted to a third party under strict supervisory conditions.
- Identity Management System (1h): The EU defines the EU Digital Identity framework pertaining to this in law.
- Identity Proofing (1i): The EU describes this process in the appropriate EU Digital Identity Framework Implementing Act and relies on Member State for the initial identity of its respective citizens.
- Relying Party (1j): The EU specifies Natural Persons and Legal Persons and specifically includes Digital Identity Wallets as a delivery method of services that relied upon.
- Subscriber (1k): The EU defines this as a natural or legal person, (or a natural person representing another natural person or a legal person), that uses trust services or electronic identification means provided in accordance with the EU Digital Identity Framework.
- Trust Service (1l): The EU defines services in more detail and adds 'Qualified Trust Services' explicitly.
- Trust Service Provider (1m): The EU additionally describes the 'Qualified Trust Service Provider' explicitly.

- Considerations for Mutual Recognition Agreement
  - Canada and the EU may need to provide additional contextual clarifications on how certain concepts are defined or applied within Canadian standards and policies, and in EU regulations and implementing acts.
  - The MLIT's definitions form the basis for mapping within a Mutual Recognition Agreement (MRA) between Canada and the EU.
  - While Canada's CAN/DGSI-103 and EU eIDAS regulations share similar foundational concepts with MLIT, some distinctions exist that may require further alignment:
    - Attributes: The EU definition encompasses rights and permissions, whereas Canada includes broader characteristics applicable to entities beyond persons.
    - Data Messages: Canada aligns them with subject claims, whereas the EU defines them as electronic data without specific reference to claims.

        - Electronic Identification: The EU extends this concept to offline services, while Canada recognises it under identity management and digital representation.
        - Identity Credentials: The EU framework introduces tiered assurance levels, particularly emphasizing qualified electronic attestation of attributes.
        - Trust Services: The EU requires qualified trust service providers to ensure compliance with specific legal and security standards.
    - In pursuit of mutual recognition, the EU and Canada may:
        - Establish clarifications or equivalences for areas where terminology differs but intent aligns.
        - Acknowledge tiered assurance levels within EU regulations while maintaining the flexibility of the Public Sector Profile Canadian Pan-Canadian Trust Framework (PSP-PCTF).
        - Recognise that while MLIT does not inherently prioritize qualified services, the EU maintains stricter requirements for public sector adoption.
        - Through continued dialogue and process mapping, both parties affirm their commitment to cross-border interoperability of identity management and trust services in alignment with MLIT, eIDAS, and CAN/DGSI-103 frameworks.

The terms and definitions are acceptable and can be applied in context.

It is recommended that Canada support the Model Law's definitions as they align closely with Canadian terminology and existing standards. However, Canada often uses broader and more abstract definitions that allow for flexibility in implementation.

It is recommended that the EU agrees in principle with the definitions set out in Article 1 of the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management (IdM) and Trust Services, while recognizing variations in terminology and conceptual frameworks within the EU Regulatory context of the EU Digital Identity framework. The following outlines the EU's stance on key definitions and areas where clarifications may be needed for mutual recognition.

Article 2: Scope and Applicability

Article 2 of the UNCITRAL Model Law outlines the scope and applicability of the law, emphasizing its focus on commercial activities and trade-related services, while allowing for potential expansion into other electronic transactions involving businesses, governments, and consumers.
MLIT emphasizes focus on commercial activities and trade-related services, while allowing for potential expansion into other electronic transactions involving businesses, governments, and consumers.

It is recommended that Canada support the general principles outlined in Article 2 of the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management (IdM) and Trust Services while emphasizing that its implementation would be guided by existing national standards, applicable legislation, and regulatory frameworks.

It is recommended that that the EU support the general principles outlined in Article 2 of the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management (IdM) and Trust Services while emphasizing that its implementation would be framed within the existing EU Digital Identity framework, and regulatory frameworks primarily intended for Government use towards citizens.

Article 3: Voluntary use of identity management and trust services

Article 3 of the UNCITRAL Model Law affirms that identity management and trust services are entirely voluntary. Individuals and organisations may choose whether and how to use such services, without obligation to adopt a specific system or provider.

- Canada Alignment
    - Voluntary use is consistent with Canadian privacy law, digital policy, and the principle of individual choice. Canada's approach emphasizes:
        - Informed Consent: Aligned with PIPEDA and provincial laws.
        - Service Flexibility: No mandated providers; organisations may choose according to their needs.
        - Technological Neutrality: Support for multiple interoperable models.
        - Clarification on Implied Consent: Recognised but must be explicit in context.

- EU Alignment
    - While citizen use of Digital Identity Wallets is optional, the EU:
        - Mandates Member States to issue digital wallets to citizens if requested.
        - Embeds Digital Identity Wallets as part of strategic digital infrastructure.
        - Maintains user consent and control through selective data sharing.
        - Defines a specific wallet-based architecture, limiting broad tech-neutrality.

- Considerations for Mutual Recognition Agreement
    - Ensure text affirms voluntary use for mutual recognition without undermining the EU's systemic mandates.
    - Emphasize interoperability and user control as shared principles.
    - Address differences between issuance requirements and user adoption.
    - Using identity management and trust services is completely voluntary—no one is required to use them or a specific provider unless they choose to do so. People and businesses have the freedom to decide whether to use these services based on their needs and preferences.
    - It is important to recognise that mutual recognition between the EU and Canada does not require full agreement on every aspect of digital identity governance, but rather a shared respect for each other's sovereignty and policy choices. The use of identity management and trust services remains voluntary in both jurisdictions—individuals and businesses are not compelled to use them or a specific provider unless they choose to do so. Canada's approach, rooted in provincial and territorial autonomy, aligns well with this principle, allowing each jurisdiction to determine its own participation based on local needs and capacities. It is therefore recommended that Canada support this principle as it reflects the flexibility and subsidiarity of the Pan-Canadian model.
    - Conversely, the European Union may take a different stance. Under eIDAS 2.0, EU citizens and residents are guaranteed the right to a digital identity that is fully under their control and that enables access to services and participation in the digital economy. While this right does not mandate usage, it reflects a more assertive regulatory posture that goes beyond voluntary adoption. In this context, the EU may not support the article as written, given that it frames digital identity as entirely optional, which may not fully align with the legal entitlements and policy goals established under EU law. Nonetheless, recognizing these differences—rather than attempting to resolve them—is key to building a respectful and functional basis for cross-border interoperability.

It is recommended that Canada agree with this article as it is consistent with the Pan-Canadian approach that allows for the Provinces and Territories to make their own determination.

It is recommended that the EU agree with this article, whilst noting that according to eIDAS, education and legal services have specific regulatory requirements that mandate the use of the EUDIW for identity verification and authentication.

Article 4: Interpretation

Article 4 emphasizes that the law should be interpreted with consideration for its international origins, ensuring uniformity in its application across different jurisdictions while promoting good faith in international trade. If the law does not explicitly address a particular issue, it should be resolved based on its underlying principles rather than solely relying on local legal interpretations, ensuring consistency and fairness in identity management and trust services globally.

- Considerations for Mutual Recognition Agreement
    - Ensure that there is text recognizing both the principle-based approach of MLIT and Canada, and the regulatory-based approach of the EU.
    - Both the European Union and Canada could express their agreement to honour the intent and spirit of the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services. In doing so, both parties acknowledge the international origin of the Model Law and affirm their commitment to promoting uniformity in its application, consistent with the principle of good faith in international cooperation and trade. While each jurisdiction retains its own legal and policy frameworks, the EU and Canada agree that matters not expressly settled by the Model Law could be interpreted and addressed in accordance with its underlying general principles. This shared understanding reinforces a foundation of trust, flexibility, and mutual respect—enabling both parties to move forward collaboratively toward greater interoperability and recognition in the global digital identity landscape.

It is recommended that Canada agree with this Article.

It is recommended that the EU agree with this Article.

Article 5: Legal Recognition of Identity Management

Article 5 affirms that electronic identification is legally recognised and cannot be dismissed simply because it is in digital form or because the identity management service is not officially designated under certain regulations. This means that electronic identity proofing and verification have the same legal validity as traditional, paper-based identification methods. Additionally, even if an identity management service has not been formally approved under specific laws, its results cannot be automatically rejected just for that reason. This provision helps promote trust in digital identity systems and supports their use in legal and commercial settings. The Article ensures that electronic identification is legally recognised and cannot be dismissed simply because it is in digital form or because the identity management service is not officially designated under certain regulations. This means that electronic identity proofing and verification have the same legal validity as traditional, paper-based identification methods. Additionally, even if an identity management service has not been formally approved under specific laws, its results cannot be automatically rejected just for that reason. This provision helps promote trust in digital identity systems and supports their use in legal and commercial settings.

- Canada Alignment
    - Legal recognition enabled by existing legislation in the Provinces and Territories

- EU Alignment
    - The EU has existing enacted legislation, on electronic identification and trust services for electronic transactions, the EU Digital Identity framework. This is further supplemented by ongoing legislation through a growing series of Implementing Acts.

- Considerations for Mutual Recognition Agreement
    - Ensure there is text recognising the evolving identity management systems in Canada, as well as the existing enacted legislation in the EU.

It is recommended that Canada agree with this Article. Legal recognition is enabled by existing legislation at the Federal level, and in the Provinces and Territories, along with jurisprudence, provides a legal foundation that recognises and supports the admissibility of electronic documents and digital records as valid forms of evidence. These frameworks affirm that electronic communications and records can hold the same legal weight as their paper counterparts, provided they meet standards of reliability, integrity, and authenticity. This legal recognition ensures that digital identity credentials and trust services—when properly implemented—can be used in both public and private sector contexts, including legal proceedings, without requiring additional legislative changes.

It is recommended that the EU agree with this Article. The EU has existing enacted legislation, on electronic identification and trust services for electronic transactions, the EU Digital Identity framework. This is further supplemented by ongoing legislation through a growing series of Implementing Acts.

Article 6: Obligations of identity management service providers

Article 6 affirms that identity management service providers are to follow clear rules and policies to ensure their systems function properly and securely. They are responsible for enrolling users by collecting and verifying identity information and linking credentials to individuals. They must also manage identity credentials by issuing, updating, suspending, and renewing them, as well as handling electronic identification processes. Providers must operate their systems reliably, ensure they are accessible online, and follow their own stated policies. They should make their policies available to users and third parties, clearly communicate any limitations on service or liability, and provide a way for users to report security breaches.

- Canada Alignment
    - Covered by the requirements of the National Standard of Canada, CAN/DGSI 103-1 and associated conformance criteria of the Public Sector Profile Pan-Canadian Trust Framework (PSP-PCTF).

- EU Alignment
    - These obligations are outlined fully in the EU Digital Identity Framework's regulations and implementing acts and are legally binding in the EU.

- Considerations for Mutual Recognition Agreement
    - Ensure there is text recognising these obligations and note that they are enacted in existing legislation in the EU.

It is recommended that Canada agree with this Article as these requirements are comprehensively addressed in the Public Sector Profile Pan-Canadian Trust Framework (PSP-PCTF) Conformance Criteria and reflected in the National Standard of Canada, CAN/DGSI 103-1. Together, these instruments ensure that identity management services in Canada are held to rigorous standards of trust, accountability, and user protection.

It is recommended that the EU agree with this Article as these requirements are explicitly detailed and enforced through the EU Digital Identity Framework, including the eIDAS Regulation (and eIDAS 2.0) and its associated implementing acts. These legally binding instruments establish comprehensive obligations for identity management service providers, including responsibilities for user enrolment, identity verification, credential lifecycle management, system reliability, and operational transparency. The regulatory framework ensures consistent application across all Member States, promoting trust, legal certainty, and cross-border interoperability within the European Digital Single Market.

Article 7: Obligations of identity management service providers in case of data breach

Article 7 affirms that if an identity management service provider experiences a security breach or data integrity issue that significantly affects its system, it must take immediate action. This includes containing the breach by suspending affected services or revoking compromised credentials if necessary, fixing the issue, and notifying relevant parties as required by law. If someone reports a suspected breach, the provider must investigate the issue and take appropriate steps to resolve it, following the same process as if they had discovered the breach themselves.

- Canada Alignment
    - In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) and various provincial privacy laws govern how organisations handle security breaches related to personal information, including identity management systems.
    - Under PIPEDA, organisations must take appropriate security measures to protect personal data and, in the event of a breach of security safeguards, they are required to assess whether it poses a real risk of significant harm to individuals. If so, they must notify affected individuals and report the breach to the Office of the Privacy Commissioner of Canada (OPC).
    - Similarly, provincial privacy laws such as British Columbia's Personal Information Protection Act (BC PIPA), Alberta's Personal Information Protection Act (AB PIPA), and Québec's Law 25 (formerly Bill 64) impose strict breach notification and response requirements.
    - Alberta's PIPA mandates organisations to report all breaches with a real risk of significant harm to the Information and Privacy Commissioner of Alberta.
    - Québec's Law 25 has recently strengthened breach notification obligations, requiring organisations to keep a record of all privacy incidents and notify both affected individuals and Québec's Commission d'accès à l'information (CAI) when the breach presents a risk of serious harm.
    - In principle, these laws align with the obligations outlined in Article 7 of the UNCITRAL Model Law, ensuring that identity management service providers take swift action to contain, investigate, and mitigate data breaches while complying with transparency and accountability requirements.

- EU Alignment
    - In the EU, these obligations are detailed in the EU Digital Identity Framework, namely in Article 10 of the Regulation.
    - Where either the electronic identification scheme notified within a Member State or the authentication referred to, is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission. When the breach or compromise is remedied, the notifying Member State shall re-establish the cross-border authentication and shall inform other Member States and the Commission without undue delay.
    - If the breach or compromise referred to is not remedied within three months of the suspension or revocation, the notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme. The European Commission shall publish the notification in the Official Journal of the European Union without undue delay.
    - The process in each EU member state designates a national authority responsible for overseeing electronic identification and trust services. If a breach occurs, it could be reported to this authority.
    - Service providers offering trust services (like electronic signatures and seals) are required to report any security incidents that could affect the integrity, availability, or confidentiality of their service
    - Coordination with Other Authorities: In cases where a breach may affect multiple jurisdictions, coordination with other national authorities and relevant bodies (like ENISA - the European Union Agency for Cybersecurity) is essential.
    - User Notification: Depending on the severity of the breach, affected users may also need to be informed so they can take appropriate action.
    - In principle, these laws align with the obligations outlined in Article 7 of the UNCITRAL Model Law, ensuring that swift action is taken to contain, investigate, and mitigate data breaches while complying with transparency and accountability requirements.

- Considerations for Mutual Recognition Agreement
    - Ensure there is text recognising these obligations and note that they are enacted in existing legislation in Canada and the EU.

It is recommended that Canada agree with this Article, as it is already well reflected in Canada's policy, legal and regulatory landscape. The Personal Information Protection and Electronic Documents Act (PIPEDA), along with provincial privacy laws such as British Columbia's PIPA, Alberta's PIPA, and Québec's Law 25, impose clear and enforceable obligations on organisations—including identity management service providers—to take appropriate security measures to protect personal information. These laws require organisations to assess the impact of a breach, notify affected individuals, and report to the appropriate privacy authorities when there is a real risk of significant harm.

It is recommended that the EU agree with this Article as these obligations are well-detailed in the EU Digital Identity Framework, namely in Article 10 of the Regulation, where either the electronic identification scheme notified within a Member State or the authentication referred to, is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border

authentication or the compromised parts concerned, and shall inform other Member States and the Commission.

Article 8. Obligations of Subscribers

Article 8 affirms that the subscriber shall notify the identity management service provider, by utilizing means made available by the identity management service provider pursuant to article 6 or by otherwise using reasonable means, if the subscriber knows that the subscriber's identity credentials have been compromised; or the circumstances known to the subscriber give rise to a substantial risk that the subscriber's identity credentials may have been compromised.

- Canada Alignment
    - In Canada, individuals are not legally obligated to report breaches of their own personal data.
    - If an individual discovers that their personal data has been lost or compromised in Canada, it is their responsibility to act quickly to notify relevant authorities such as government services, local police, financial institutions, and credit bureaus.
    - The obligation to take immediate action in the event of a personal data loss or breach could be explicitly outlined in the terms and conditions. This could include clear guidance on notifying relevant authorities, monitoring for fraudulent activity, and securing personal accounts to mitigate potential harm.

- EU Alignment
    - If there has been a security breach involving a notified electronic identification (eID) or Qualified Trust Service in the EU, steps could be taken to report the incident, including notification to the relevant National Authority. Each EU member state has established a designated national authority responsible for eID and trust services.

- Considerations for Mutual Recognition Agreement
    - Ensure there is text recognising these obligations and note that they are enacted in existing EU Member State and EU legislation.

It is recommended that Canada and the EU agree to a common interpretation of the Article in that the identity management service provider is to provide a mechanism for the subscriber to notify them of their compromised credentials.

While Canada and the European Union may hold differing positions regarding the obligations of individuals in responding to personal data breaches, this divergence does not undermine the overall integrity of their respective digital identity frameworks. These differences can be constructively addressed within a mutual recognition agreement that respects each jurisdiction's legal and cultural context. What remains consistent between both parties is a strong commitment to ensuring the reliability, accountability, and security of identity management and trust services. By focusing on shared principles—such as transparency, user protection, and system integrity—Canada and the EU could establish a foundation for mutual recognition that accommodates these variations while upholding high standards of trust and interoperability.

Article 9: Identification of a person using identity management

Article 9 affirms that where the law requires the identification of a person for a particular purpose, or provides consequences for the absence of identification, that requirement is met with respect to

identity management services if a reliable method in accordance with Article 10 is used for the identity proofing and electronic identification of the person for that purpose.

- Canada Alignment
    - The requirement for reliable identification of a person for legal purposes could be fulfilled using the CAN/DGSI 103-1 standard and the conformance criteria of the Public Sector Profile Pan-Canadian Trust Framework (PSP-PCTF). The standard and framework establish reliable methods for identity proofing and electronic identification, ensuring compliance. By adhering to the processes and assurance levels defined the standard and framework, identity management services can verify an individual's identity with a level of confidence appropriate to the legal requirements. This structured approach, verified under the auspices of a recognised conformity assessment program ensures that reliable identification mechanisms align with federal and provincial regulations, and abide with the MLIT articles in support of mutual agreement.

- EU Alignment
    - EU citizens and residents have the right to a digital identity that is under their sole control and that enables them to exercise their rights in the digital environment and to participate in the digital economy to access public and private online and offline services throughout the EU. Member States may involve the private sector in their provision of those means.
    - For use with Trust Services or interactions with public sector institutions, a High-Level Assurance (LOA3) identification must be used.

- Considerations for Mutual Recognition Agreement
    - Ensure there is text recognising these obligations and note that they are enacted in existing EU legislation.

It is recommended that Canada agree with this Article. The requirement for reliable identification of a person for legal purposes could be fulfilled using the CAN/DGSI 103-1 standard and the conformance criteria of the Public Sector Profile Pan-Canadian Trust Framework (PSP-PCTF). The standard and framework establish reliable methods for identity proofing and electronic identification, ensuring compliance. By adhering to the processes and assurance levels defined the standard and framework, identity management services can verify an individual's identity with a level of confidence appropriate to the legal requirements. This structured approach, verified under the auspices of a recognised conformity assessment program ensures that reliable identification mechanisms align with federal and provincial regulations, and abide with the MLIT articles in support of mutual agreement.

It is recommended that the EU agree with this Article. EU citizens and residents have the right to a digital identity that is under their sole control and that enables them to exercise their rights in the digital environment and to participate in the digital economy to access public and private online and offline services throughout the EU. Member States may involve the private sector in their provision of those means. For use with Trust Services or interactions with public sector institutions, a High-Level Assurance (LOA3) identification must be used.

Article 10: Reliability requirements for identity management services

Article 10 affirms that identity Management Services should be reliable as appropriate for the purpose for it is being used. The measure of reliability should consider the compliance of the identity

management service provider with its own rules, policies and practices, recognised national and international standards and procedures, and with the level of assurance frameworks prevailing.

- Canada Alignment
    - Reliability requirements for identity management services could be met through assessment using the CAN/DGSI 103-1 standard and the conformance criteria of the Public Sector Profile Pan-Canadian Trust Framework (PSP-PCTF).

- EU Alignment
    - As this is a regulation in law, the provision of the services describe is mandatory by Member States. All trust service providers are subject to the requirements of this Regulation, particularly those on security and liability to ensure due diligence, transparency and accountability of their operations and Qualified Services (eIDAS Recital 35). The Member State liability and that of the QTSPs located in its jurisdiction shall be applied in accordance with national rules on liability.

- Considerations for Mutual Recognition Agreement
    - Ensure there is text recognising obligations and liability and note that they are already enacted in existing EU legislation. Any liability could extend to services delivered in jurisdictions covered by any MRA, but only for the cross-border transactions. There could be pre-agreed liability limits in the MRA to avoid uncertainty.

It is recommended that Canada agree with this Article. Reliability requirements for identity management services could be met through assessment using the CAN/DGSI 103-1 standard and the conformance criteria of the Public Sector Profile Pan-Canadian Trust Framework (PSP-PCTF).

It is recommended that the EU agree with this Article. As this is already a regulation in law, the provision of the services describe is mandatory by Member States. All trust service providers are subject to the requirements of this Regulation, particularly those on security and liability to ensure due diligence, transparency and accountability of their operations and Qualified Services. (eIDAS Recital 35). The Member State liability and that of the Qualified Trust Service Providers (QTSPs) located in its jurisdiction shall be applied in accordance with national rules on liability.

Article 11: Designation of reliable identity management services

Article 11 affirms that a person, organ or authority, whether public or private, specified by the enacting jurisdiction as competent, may designate identity management services that are presumed reliable. The person, organ or authority, whether public or private, specified by the enacting jurisdiction as competent, shall consider all relevant circumstances, in designating an identity management service; and publish a list of designated identity management services, including details of the identity management service provider. Any designation shall be consistent with recognised international standards and procedures relevant for performing the designation process, including level of assurance frameworks. In designating an identity management service, no regard shall be had to the geographic location where the identity management service is provided; or to the geographic location of the place of business of the identity management service provider.

- Canada Alignment
    - The designation of reliable identity management and trust services under Article 11 could be carried out by a senior government official on behalf of the federal government, as well as the provinces and territories. Given the established

coordination between federal and provincial authorities, this role could be assigned to the Chief Information Officer (CIO) of the Government of Canada, who operates within the Treasury Board Secretariat (TBS). As a key advisor on digital identity, cybersecurity, and information management, the CIO provides expert guidance to the President of the Treasury Board, a minister within the federal government, ensuring that designated services meet the necessary standards for security, privacy, and interoperability. This structured approach would enable a unified and consistent designation process across jurisdictions, reinforcing the trust and reliability of identity services used across Canada.

- Alternatively, the designation of reliable identity management and trust services could be carried out by a private sector or not-for-profit entity. For example, a certification body, such as Digital Governance Council, once accredited by its national accreditation body, could be able to designate reliable identity management providers. Such an approach would closely mirror the EU context.

- EU Alignment
  - In the context of the EU Digital Identity Framework, the eIDAS Regulation ensures compliance of the notifying Member State and for all Qualified Trust Service Providers, the party issuing the electronic identification means and the party operating the authentication procedure. This is achieved via the use of national conformity assessment bodies and accreditation bodies.

- Considerations for Mutual Recognition Agreement
  - Canada could delegate to a Conformity Assessment Body(ies) or keep in house, and a note should be made of the existing regime to ensure and monitor reliability of the EU Digital Identity Framework in the EU.

It is recommended that Canada agree with this Article. The designation of reliable identity management and trust services under Article 11 could be carried out by a senior government official on behalf of the federal government, as well as the provinces and territories. Given the established coordination between federal and provincial authorities, this role could be assigned to the Chief Information Officer (CIO) of the Government of Canada, who operates within the Treasury Board Secretariat (TBS). As a key advisor on digital identity, cybersecurity, and information management, the CIO provides expert guidance to the President of the Treasury Board, a minister within the federal government, ensuring that designated services meet the necessary standards for security, privacy, and interoperability. This structured approach would enable a unified and consistent designation process across jurisdictions, reinforcing the trust and reliability of identity services used across Canada.

It is recommended that the EU agree with this Article. In the context of the EU Digital Identity Framework, the eIDAS Regulation ensures compliance of the notifying Member State and for all Qualified Trust Service Providers, the party issuing the electronic identification means and the party operating the authentication procedure. This is achieved via the use of national conformity assessment bodies and accreditation bodies.

Article 12: Liability of identity management service providers

Article 12 affirms that the identity management service provider shall be liable for loss caused to the subscriber or to the relying party due to a failure to comply with its obligations. The rules on liability under the law and is without prejudice to any other basis of liability under the law, including liability

for failure to comply with contractual obligations; or any other legal consequences of a failure of the identity management service provider to comply with its obligations under this Law.

In addition, the identity management service provider shall not be liable to a subscriber for loss arising from the use of an identity management service to the extent that its use exceeds the limitations on the purpose or value of the transaction for which the identity management service is used; and those limitations are contained in the arrangement between the identity management service provider and the subscriber.

Furthermore, the identity management service provider shall not be liable to a relying party for loss arising from the use of an identity management service to the extent that the use exceeds the limitations on the purpose or value of the transaction for which the identity management service is used; and the identity management service provider has complied with its obligations with respect to that transaction.

- Canada Alignment
    - There is no specific legislation or regulation for the liability of identity management. Contract with service providers would abide by Mandatory Procedures for Limitation of Contractor Liability and Indemnification in Contracts.
    - Agreements between different levels of governments use indemnity clauses in agreements to allocate risks appropriately.
    - When liability involves multiple levels of government, legal disputes may be resolved through intergovernmental agreements or via administrative tribunals and courts.

- EU Alignment
    - In the context of the EU Digital Identity Framework, the eIDAS Regulation provides for the liability of the notifying Member State and for all Qualified Trust Service Providers, the party issuing the electronic identification means and the party operating the authentication procedure, for failure to comply with the relevant obligations under this Regulation. However, this Regulation could be applied in accordance with national rules on liability. Therefore, it does not affect those national rules on, for example, definition of damages or relevant applicable procedural rules, including the burden of proof. There is a strict notification process to the EU from the Member States for breaches or failures.

- Considerations for Mutual Recognition Agreement
    - Any liability could extend to services delivered in jurisdictions covered by the MRA, but only for the cross-border transactions. There could be pre-agreed liability limits in the MRA to avoid uncertainty in future transactions.
    - Specific indemnification clauses may need to be negotiated between the EU and Canada.
    - Any breaches in either the EU or Canadian conformity assessment schemes could be notified to each responsible authority and other relevant bodies (like ENISA - the European Union Agency for Cybersecurity). This would minimise future potential losses and liabilities.

It is recommended that the Canada and EU agree to a common interpretation to the Article with respect to liability under the law associated with contractual and regulatory obligations. While in principle liability must be clearly addressed, the distribution of liability and indemnity is typically managed through agreements and contracts, not through statutory provisions. In the Canadian context, there is no specific legislation governing the liability of identity management service providers. Instead, federal contracts follow the Mandatory Procedures for Limitation of Contractor

Liability and Indemnification in Contracts, and intergovernmental agreements between federal, provincial, and territorial partners routinely include indemnity clauses to allocate risk appropriately. Where disputes arise involving multiple levels of government, they are generally resolved through intergovernmental agreements, administrative tribunals, or the courts. This approach provides the necessary accountability while preserving flexibility and respecting jurisdictional autonomy. Therefore, prescribing liability through legislation would not align with Canada's collaborative, agreement-based governance model.

The eIDAS Regulation explicitly addresses the issue of liability within the EU Digital Identity Framework. Under eIDAS, the notifying Member State, as well as Qualified Trust Service Providers, the party issuing the electronic identification means, and the party operating the authentication procedure, are all held liable for failure to meet their obligations under the Regulation. However, it is important to emphasize that this liability framework is designed to be applied in alignment with national legal systems. The Regulation does not override national rules concerning the definition of damages, procedural requirements, or burden of proof. Member States retain autonomy in how liability is interpreted and enforced within their jurisdictions. Additionally, there is a strict notification and reporting process from Member States to the EU in cases of breaches or failures. This ensures that liability is enforced consistently, while allowing for necessary flexibility to respect the legal traditions and practices of individual Member States.

Article 13: Legal recognition of trust services

Article 13 affirms that the result deriving from the use of a trust service shall not be denied legal effect, validity, enforceability or admissibility as evidence on the sole ground that it is in electronic form; or the trust service is not designated pursuant to the designation of reliable trust services (Article 23).

- Canada Alignment
    - This affirmation aligns with Canada's established legal and policy frameworks, including the Public Sector Profile Pan-Canadian Trust Framework (PSP-PCTF) and national standards such as CAN/DGSI 103-1: Digital Trust and Identity. Together, these frameworks emphasize a technology-neutral and outcome-focused approach to trust services, promoting functional equivalence across digital and paper-based transactions.

- EU Alignment
    - In the EU, the automatic legal recognition of Trust Services is limited to Qualified Trust Services under the EU Digital Identity Framework. The legal admissibility of Non-Qualified Trust Services may be challenged by the legal process.

- Considerations for Mutual Recognition Agreement
    - A clear recognition of the trust services in Canada that are legally recognised must be determined and listed so that there is an equivalence with EU Trust Services in any dispute. There should not be any reduction in trust of digital services delivered or supplied in either the EU or Canada.

The recommendation is the same as Article 5 as applied to legal recognition of trust services

Article 14: Obligations of trust service providers

Article 14 affirms that a trust service provider shall, at a minimum have in place operational rules, policies and practices, including a plan to ensure continuity in case of termination of activity, as

appropriate to the purpose and design of the trust service; act in accordance with its operational rules, policies and practices, and any representations that it makes with respect to them; make its operational rules, policies and practices easily accessible to subscribers, relying parties and other third parties; provide and make publicly available means by which a subscriber may notify the trust service provider of a security breach pursuant to Article 15; and provide easily accessible means that enable a relying party to ascertain, where relevant: any limitation on the purpose or value for which the trust service may be used; and any limitation on the scope or extent of liability stipulated by the trust service provider.

In addition, if a breach of security or loss of integrity occurs that has a significant impact on a trust service, the trust service provider shall, in accordance with the law take all reasonable steps to contain the breach or loss, including, where appropriate, suspending or revoking the affected service; remedy the breach or loss; and notify the breach or loss.

- Canada Alignment
    - These provisions are reflected in the Public Sector Profile of the PCTF and in CAN/DGSI 103-1: Digital Trust and Identity.

- EU Alignment
    - These provisions are integrated into the EU Digital Identity Framework.

- Considerations for Mutual Recognition Agreement
    - Ensure there is text recognising these obligations and note that they are enacted in existing legislation in the EU.

The recommendation is the same as Article 6 as applied to obligations of trust service providers.

Article 15: Obligations of subscribers

Article 15 affirms that the subscriber shall notify the trust service provider, by utilizing means made available by the trust service provider pursuant to Article 14, paragraph 1, or by otherwise using reasonable means, if: the subscriber knows that data or means used by the subscriber for access and usage of the trust service have been compromised; or the circumstances known to the subscriber give rise to a substantial risk that the trust service may have been compromised.

- Canada Alignment
    - Individuals are not legally obligated to report breaches of their own personal data; however, they do carry a personal responsibility to act swiftly if they become aware that their information has been lost or compromised. It is generally expected that individuals will take proactive steps such as notifying government services, local police, financial institutions, and credit bureaus to protect themselves from further harm.

- EU Alignment
    - Individuals are not legally obligated to report breaches of their own personal data; however, they do carry a personal responsibility to act swiftly if they become aware that their information has been lost or compromised. It is generally expected that individuals will take proactive steps—such as notifying government services, local police, financial institutions, and credit bureaus—to protect themselves from further harm.

- Considerations for Mutual Recognition Agreement
    - Ensure there is text recognising these obligations and note that they are enacted in existing legislation in the EU.

The recommendation is the same as Article 8 as applied to obligations of subscribers.

Article 16: Electronic signatures

Article 16 affirms that where the law requires a signature of a person, or provides consequences for the absence of a signature, that requirement is met in relation to a data message if a reliable method in accordance with Article 22, paragraph 1, or Article 22, paragraph 4, is used: (a) to identify the person; and (b) to indicate the person's intention in respect of the information contained in the data message.

- Canada Alignment
    - Canada has in place electronic signature regulations and applicable guidelines at the federal and provincial levels.

- EU Alignment
    - Already enacted in the EU.

- Considerations for Mutual Recognition Agreement
    - Ensure there is text recognising these obligations and note that they are enacted in existing legislation in the EU.

It is recommended that Canada agree with this Article as it aligns with existing Canadian legislation, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and the Canada Evidence Act, which recognise the legal validity of electronic signatures. Canadian law supports the use of electronic signatures as functionally equivalent to handwritten ones, provided they are reliable for identifying the person and confirming their intent. This principle is also reflected in provincial electronic commerce laws, making Article 16 consistent with Canada's legislative framework and practices.

It is recommended that the EU agree with this Article, as it is consistent with the eIDAS Regulation, which provides a comprehensive legal framework for the use and the recognition of electronic signatures across all Member States. Under eIDAS, electronic signatures, including advanced and qualified electronic signatures, are legally valid and enforceable, provided they meet specific reliability and security requirements. The Regulation ensures that electronic signatures can be used in legal and commercial transactions with the same legal effect as handwritten signatures, supporting trust, cross-border recognition, and digital transformation across the EU.

Article 17: Electronic seals

Article 17 affirms that where the law requires a legal person to affix a seal, or provides consequences for the absence of a seal, that requirement is met in relation to a data message if a reliable method in accordance with Article 22, paragraph 1, or Article 22, paragraph 4, is used: (a) to provide reliable assurance of the origin of the data message; and (b) to detect any alteration to the data message after the time and date of affixation, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display.

- Canada Alignment

- Canada does not have standalone or explicit legislation specifically governing electronic seals. However, Canada's legal framework does support similar concepts functionally through a combination of laws, standards, and regulations.

- EU Alignment
  - The EU has both Qualified and Advanced Seals.
    - An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.
      - A Qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked. A qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States.
      - An Advanced electronic seal presumes with a high level of confidence that the electronic seal creation device is under the control of the seal creator and is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

- Considerations for Mutual Recognition Agreement
  - Ensure there is text recognising, that they are enacted in existing legislation in the EU, but with the concepts of Qualified and Advanced.

The recommendation is the same as Article 16 as applied to electronic seals.

Article 18: Electronic timestamps

Article 18 affirms that where the law requires a document, record, information or data to be associated with a time and date, or provides consequences for the absence of a time and date, that requirement is met in relation to a data message if a reliable method in Accordance with Article 22, paragraph 1, or Article 22, paragraph 4, is used (a) To indicate the time and date, including by reference to the time zone; and (b) To associate that time and date with the data message.

- Canada Alignment
  - Canada does not have standalone or explicit legislation specifically governing electronic timestamps. However, Canada's legal framework does support similar concepts functionally through a combination of laws, standards, and regulations. Additionally, there is an opportunity for a Standards Development Organization (SDO) to develop voluntary standards.

- EU Alignment
  - The timestamp binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably; The timestamp is based on an accurate time source linked to Coordinated Universal Time; and is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

- Considerations for Mutual Recognition
    - Ensure there is text recognising, that they are enacted in existing legislation in the EU.

The recommendation is the same as Article 16 as applied to electronic timestamps.

Article 19: Electronic archiving

Article 19 affirms that where the law requires a document, record or information to be retained, or provides consequences for the absence of retention, that requirement is met in relation to a data message if a reliable method in accordance with Article 22, paragraph 1, or Article 22, paragraph 4, is used: (a) to make the information contained in the data message accessible so as to be usable for subsequent reference; (b) to indicate the time and date of archiving and associate that time and date with the data message; (c) to retain the data message in the format in which it was generated, sent or received, or in another format which can be demonstrated to detect any alteration to the data message after that time and date, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display; and (d) to retain such information, if any, as enables the identification of the origin and destination of a data message and the time and date when it was sent or received.

- Canada Alignment
    - Canada does not have standalone or explicit legislation specifically governing electronic archiving. However, Canada's legal framework does support similar concepts functionally through a combination of laws, standards, and regulations.
    - As stated in the previous article, there is an opportunity for a Standards Development Organization (SDO) to develop voluntary standards.

- EU Alignment
    - Electronic data and electronic documents preserved using an electronic archiving service shall not be denied legal effect or admissibility as evidence in legal proceedings on the sole grounds that they are in electronic form or that they are not preserved using a qualified electronic archiving service. Electronic data and electronic documents preserved using a qualified electronic archiving service shall enjoy the presumption of their integrity and of their origin for the duration of the preservation period by the qualified trust service provider. A Qualified Preservation Service also maintains the integrity and validity of the signing or sealing qualified signature.

- Considerations for Mutual Recognition
    - Ensure there is text recognizing that they are enacted in existing legislation in the EU.

The recommendation is the same response as Article 16 as applied to electronic archiving.

Article 20: Electronic registered delivery services

Article 20 affirms that where the law requires a document, record or information to be delivered by registered mail or similar service, or provides consequences for the absence of delivery, that requirement is met in relation to a data message if a reliable method in accordance with Article 22,

paragraph 1, or Article 22, paragraph 4, is used: (a) to indicate the time and date when the data message was received for delivery and the time and date when it was delivered; (b) to detect any alteration to the data message after the time and date when the data message was received for delivery to the time and date when it was delivered, apart from the addition of any endorsement or information required by this article, and any change that arises in the normal course of communication, storage and display; and (c) to identify the sender and the recipient.

- Canada Alignment
    - Canada does not have standalone or explicit legislation specifically governing electronic registered delivery services. However, Canada's legal framework does support similar concepts functionally through a combination of laws, standards, and regulations.
    - As stated previously, there is an opportunity for a Standards Development Organization (SDO) to develop voluntary standards.

- EU Alignment
    - Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.
    - Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.

- Considerations for Mutual Recognition
    - Ensure there is text recognizing that they are enacted in existing legislation in the EU described as Qualified Registered Delivery Services.

The recommendation is the same as Article 16 as applied to electronic registered delivery services.

Article 21: Website authentication

Article 21 affirms that where the law requires website authentication, or provides consequences for the absence of website authentication, that requirement is met if a reliable method in accordance with Article 22, paragraph 1, or Article 22, paragraph 4, is used: (a) to identify the person who holds the domain name for the website; and (b) to associate that person to the website.

- Canada Alignment
    - Within the Canadian context, this requirement would be enforced by the various internet domain registration providers, for example the country code top-level domain (ccTLD) for Canada is ".ca" enforced by the Canadian Internet Registration Authority (CIRA) which has delegate authority from the Government of Canada.

- EU Alignment
    - The EU agrees in principle but subject to the EU Digital Identity Framework, using qualified certificates

- Considerations for Mutual Recognition
    - Ensure there is text recognizing that this is enacted in existing legislation in the EU.

The recommendation is the same as Article 16 as applied to website authentication.

Article 22: Reliability requirements for trust services

Article 22 affirms that:

1. For the purposes of Articles 16 to 21, the method shall be:
    a. as reliable as appropriate for the purpose for which the trust service is being used; or
    b. deemed to be as reliable as appropriate if proven in fact by or before a court or competent adjudicative body to have fulfilled the functions described in the article, by itself or together with further evidence.
2. In determining the reliability of the method, all relevant circumstances shall be taken into account, which may include:
    a. Compliance of the trust service provider with the obligations listed in article 14;
    b. Compliance of the operational rules, policies and practices of the trust service provider with any applicable recognised international standards and procedures relevant for the provision of trust services;
    c. Any relevant level of reliability of the method used;
    d. Any applicable industry standard;
    e. The security of hardware and software;
    f. Financial and human resources, including the existence of assets;
    g. The regularity and extent of audit by an independent body;
    h. The existence of a declaration by a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method;
    i. The purpose for which the trust service is being used; and
    j. Any relevant agreement between the parties, including any limitation on the purpose or value of the transactions for which the trust service might be used.
3. In determining the reliability of the method, no regard shall be had:
    a. To the geographic location where the trust service is provided; or provider.
    b. A method used by a trust service designated pursuant to Article 23 is presumed to be reliable.
4. Paragraph 4 does not limit the ability of any person:
    a. To establish in any other way the reliability of a method; or
    b. To adduce [cite] evidence of the non-reliability of a method used by a designated trust service.

- Canada Alignment
    - Canada does not have standalone or explicit legislation regarding the legal recognition of qualified trust services. This may be incorporated into the mutual recognition agreement.

- EU Alignment
    - In the EU, the automatic legal recognition of Trust Services is limited to those Qualified Trust Services under the EU Digital Identity Framework. The legal admissibility of Non-Qualified Trust Services may be challenged by the legal process.

- Considerations for Mutual Recognition
    - The EU considers the reliability of Trust Services to be described within the definitions of 'Qualified Trust Service'.

The recommendation is the same as Article 10 as applied to reliability requirements for trust services.

Article 23: Designation of reliable trust services

Article 23 affirms that:

1. A [person, organ or authority, whether public or private, specified by the enacting jurisdiction as competent] may designate trust services that are presumed reliable.
2. The [person, organ or authority, whether public or private, specified by the enacting jurisdiction as competent] shall:
    a. Consider all relevant circumstances, including the factors listed in Article 22, in designating a trust service; and
    b. Publish a list of designated trust services, including details of the trust service provider.
3. Any designation pursuant to paragraph 1 shall be consistent with recognised international standards and procedures relevant for performing the designation process.
4. In designating a trust service, no regard shall be had:
    a. To the geographic location where the trust service is provided; or
    b. To the geographic location of the place of business of the trust service Provider.

- Canada Alignment
    - Canada does not have standalone or explicit legislation regarding the designation of reliable trust services. This may be incorporated into the mutual recognition agreement.

- EU Alignment
    - Member States lay down rules on penalties for infringements such as direct or indirect practices that lead to confusion between non-qualified and qualified trust services.

- Considerations for Mutual Recognition
    - The EU considers the reliability of Trust Services to be described within the definitions of 'Qualified Trust Service'.

The recommendation is the same as Article 11 as applied to designation of reliable trust services.

Article 24: Liability of trust service providers

Article 24 affirms that:

1. The trust service provider shall be liable for loss caused to the subscriber or to the relying party due to a failure to comply with its obligations under Article 14.
2. Paragraph 1 shall be applied in accordance with rules on liability under the law and is without prejudice to:
    a. any other basis of liability under the law, including liability for failure to comply with contractual obligations; or

b. any other legal consequences of a failure of the trust service provider to comply with its obligations under this Law.

3. Notwithstanding paragraph 1, the trust service provider shall not be liable to a subscriber for loss arising from the use of a trust service to the extent that:
    a. That use exceeds the limitations on the purpose or value of the transaction for which the trust service is used; and
    b. Those limitations are contained in the arrangement between the trust service provider and the subscriber.
4. Notwithstanding paragraph 1, the trust service provider shall not be liable to a relying party for loss arising from the use of a trust service to the extent that:
    a. That use exceeds the limitations on the purpose or value of the transaction for which the trust service is used; and
    b. The trust service provider has complied with its obligations under Article 14, paragraph 1 (e), with respect to that transaction.

- Canada Alignment
    - The mutual recognition agreement would need to include clear provisions regarding liability, including the allocation of responsibilities, any limitations or exclusions, and mechanisms for addressing potential claims.

- EU Alignment
    - This Regulation is to be applied in accordance with Member State national rules on liability. Therefore, it does not affect those national rules on, for example, definition of damages or relevant applicable procedural rules, including the burden of proof. The burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph.
    - The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage occurred without the intention or negligence of that qualified trust service provider.

- Considerations for Mutual Recognition
    - The mutual recognition agreement would need to clearly specify how representation is handled on both sides. For the European Union, it could outline how member states are collectively represented under the EU framework, ensuring consistent application of the agreement across all jurisdictions. Similarly, in Canada, the agreement must address how provinces and territories are represented by the federal government, recognizing their jurisdictional authority in matters related to identity management and trust services. Clear provisions would be essential to ensure alignment, accountability, and seamless cross-border cooperation.

The recommendation is the same as Article 12 as applied to liability of trust service providers.

Article 25: Cross-border recognition of the result of electronic identification

Article 25 affirms that:

1. The result of electronic identification provided outside [the enacting jurisdiction] shall have the same legal effect in [the enacting jurisdiction] as electronic identification provided in [the enacting jurisdiction] if the method used by the identity management system, identity management service, or identity credential, as appropriate, offers:

a. At least an equivalent level of assurance, where the assurance levels recognised by such jurisdictions are identical; or
b. Substantially equivalent or higher level of assurance, in all other cases.

2. For the purposes of determining satisfaction of paragraph 1, regard shall be had to recognised international standards.
3. An identity management system, identity management service or identity credential shall be presumed to satisfy paragraph 1 if [the person, organ or authority

- Canada Alignment
    - CAN/DGSI 103-1 includes the following requirement: "Where an Organisation will issue and/or consume Identity and/or Credentials as part of its identity context, including as part of a federation, the Organisation shall define and implement criteria for selecting a trust framework that may inform the operation of its identity management system and the rights and obligations of the federation participants, so as to ensure the trustworthiness of its identity management system and those of the federation participants." A trust framework includes: the Electronic Identification, Authentication, and Trust Services (eIDAS) in the European Union.

- EU Alignment
    - Trust services provided by trust service providers established in a third country shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country in question or an international organisation in accordance with Article 218 TFEU.

- Considerations for Mutual Recognition
    - When setting out the conditions under which the trust frameworks of third countries could be considered to be equivalent to the trust framework for qualified trust services and providers thereof under the EU Digital Identity Framework , compliance with the relevant provisions in the Directive (EU) 2022/2555 of the European Parliament and of the Council (13) and Regulation (EU) 2016/679 should be ensured, as well as the use of trusted lists as essential elements to build trust.
    - A recent study conducted by the OECD (October 2024) entitled G7 Mapping of Digital Identity Approaches. A link to the report is found in the bibliography.

It is recommended that Canada and the EU agree to Article 25 with a common understanding between levels of assurance and system reliability in each respective jurisdiction to be recognised through an MRA.

Article 26. Cross-border recognition of the result of the use of trust services

Article 26 affirms that:

1. The result deriving from the use of a trust service provided outside [the Enacting jurisdiction] shall have the same legal effect in [the enacting jurisdiction] as the result deriving from the use of a trust service provided in [the enacting jurisdiction] if the method used by the trust service offers:
    a. At least an equivalent level of reliability, where the reliability levels recognised by such jurisdictions are identical; or
    b. Substantially equivalent or higher level of reliability, in all other cases.

2. For the purposes of determining satisfaction of paragraph 1, regard shall be had to recognised international standards.
3. The trust service shall be presumed to satisfy paragraph 1 if [the person, organ or authority specified by the enacting jurisdiction pursuant to Article 23] has determined the equivalence, taking into account Article 22, paragraph 2.

- Canada Alignment
    - The mutual recognition agreement shall ensure that the requirements applicable to trust service providers and trust services originating from outside of Canada are substantially equivalent to those applicable to trust service providers and trust services established in Canada.

- EU Alignment
    - Agreements shall ensure that the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country or international organisations with which the agreement is concluded, and by the trust services they provide; the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or international organisation with which the agreement is concluded.

- Considerations for Mutual Recognition
    - When setting out the conditions under which the trust frameworks of third countries could be considered to be equivalent to the trust framework for qualified trust services and providers thereof under the EU Digital Identity Framework , compliance with the relevant provisions in the Directive (EU) 2022/2555 of the European Parliament and of the Council (13) and Regulation (EU) 2016/679 should be ensured, as well as the use of trusted lists as essential elements to build trust.

It is recommended that Canada and the EU agree to Article 26 which enables the EU and designated national authorities to engage in international cooperation. This article provides the foundations for exchanging information, expertise and good practices; recognises legal effects enabled through an MRA; and aligns and harmonises criteria for levels of assurance and reliability.

Article 27: Cooperation

Article 27 affirms that [The person, organ or authority specified by the enacting jurisdiction as competent] may cooperate with foreign entities by exchanging information, experience and good practice relating to identity management and trust services, in particular with respect to:

a. Recognition of the legal effects of foreign identity management systems and trust services, whether granted unilaterally or by mutual agreement;
b. Designation of identity management systems and trust services; and
c. Definition of levels of assurance of identity management systems and of levels of reliability of trust services.

It is recommended that Canada and the EU agree to Article 27 which enables the EU and designated national authorities to engage in international cooperation. This article provides the foundations for exchanging information, expertise and good practices; recognises legal effects enabled through an MRA; and aligns and harmonises criteria for levels of assurance and reliability.

XI REFERENCES AND BIBLIOGRAPHY

1. European Commission. (2022). European Digital Identity Wallet Architecture and Reference Framework (Version 1.7).
2. European Parliament and Council. (2014). Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation).
3. European Parliament and Council. (2024). Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (eIDAS 2.0).
4. European Union-Canada Summit 2025. Joint Statement: Enduring Partnership, Ambitious Agenda
5. UNCITRAL. (2022). Model Law on the Use and Cross-Border Recognition of Identity Management and Trust Services.
6. World Trade Organisation. (1995). Agreement on Technical Barriers to Trade (TBT Agreement).
7. Treaty on the Functioning of the European Union (TFEU), Article 218, Consolidated Version.
8. Digital Governance Standards Institute. (2023). Technical Specification 115:2023 – Digital Credentials and Digital Trust Services.
9. Digital Governance Standards Institute. (2023). CAN/DGSI 103-1:2023 – Digital Trust and Identity Standard.
10. Decision No 1/2024 of the Joint Committee on Mutual Recognition of Professional Qualifications of 10 October 2024 setting out an agreement on the mutual recognition of professional qualifications for architects.
11. European Union - Canada Organic Equivalency Arrangement (EUCOEA). Government of Canada. (2025). Request for Information (RFI) – Common Set of Capabilities for Issuing and Verifying Digital Credentials (IVDC).
12. Government of Canada. (2025). Invitation to Qualify (ITQ) for Issuing and Verifying Digital Credentials (IVDC).
13. Open Wallet Foundation. (2024). Open Wallet Foundation Technical Specifications.
14. Financial Action Task Force (FATF). (2020). Guidance on Digital Identity.
15. ISO/IEC. (2019). ISO/IEC 18013-5:2019 — Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application.
16. ISO/IEC. (2022). ISO/IEC 23220-1:2022 — Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 1: General framework.
17. ISO/IEC. (2023). ISO/IEC 23220-2:2023 — Building blocks for identity management via mobile devices — Part 2: Authentication
18. OECD G7 Mapping of Digital Identity Approaches

XII ABOUT THE AUTHORS

Keith Jansa

Chief Executive Officer, Digital Governance Council

Keith Jansa is the Chief Executive Officer of the Digital Governance Council. He works with senior leaders from across Canada to address digital governance opportunities and challenges to safeguard Canadians in an increasingly digital world. His unparalleled acumen in devising strategies for responsible data and digital governance has earned the Digital Governance Council the distinction as preeminent technology leadership council globally.

Keith is a specialist in the strategic application of standards. Keith was named one of the 10 most influential business leaders in 2023 by The Inc Magazine. Keith graduated with honors from the University of Ottawa with a degree in health sciences.

Ellis Jonathan Shamah

Director, EJ Consultants Ltd, Chair, Global Trust Foundation

Jon Shamah, a Southampton University Aeronautics & Astronautics graduate, is an international expert in Digital Identity & Trust, named in the *One World Top 100 Leaders in Identity*. He has advised governments, worked with organisations such as ENISA, Hitachi, and Thales, contributed to major EU research programmes, and addressed the UN on eID's role in tackling child trafficking.

A former co-chair of the ITU-T SG17 Identity group, Jon is known for turning complex issues into clear messages for decision-makers. Through E J Consultants, he represents clients at high-level meetings and global conferences, extending their presence with trusted expertise in digital identity and trust.