G7 MAPPING EXERCISE OF DIGITAL IDENTITY APPROACHES

REPORT PREPARED FOR THE 2024 ITALIAN G7 PRESIDENCY AND THE G7 DIGITAL AND TECH WORKING GROUP

15 October 2024

Table of contents

Executive summary

Digital identity plays a crucial role in fostering a secure, inclusive, and efficient digital transformation by enabling individuals and businesses to prove their identity and share verified information through digital means. The rising demand for digital services across the public and private sector, along with concerns about digital exclusion, cybersecurity threats, and the misuse of personal data, underscore the need for well-designed digital identity systems supported by appropriate governance frameworks. While traditional forms of identification and authentication means like physical identity cards, passports, passwords and eID cards remain significant, they alone are insufficient to address the complexities of today's digital landscape.

As highlighted in the OECD Recommendation on the Governance of Digital Identity[1], there is a growing recognition of the importance for individuals and businesses to be able to use their digital identities across borders, calling for increased bilateral and multilateral co-operation. This includes comparing digital identity approaches across different countries and regions to inform policy development and support interoperability efforts.

This report was prepared at the request of the 2024 Italian G7 Presidency and G7 members to inform discussions within the G7 Digital and Technology Working Group. The goal of the mapping exercise has been to identify commonalities in digital identity approaches among G7 members that can support work on future interoperability.

The findings from the mapping exercise highlight significant similarities in the G7 approaches to digital identity, forming a solid foundation for further co-operation on cross-border alignment and interoperability. G7 members could prioritise using this mapping exercise as a springboard for discussions during their respective presidencies. A relevant future exercise could also be to discuss the design and adoption of relevant solutions, such as digital wallets.

[1] The OECD Recommendation of the Council on the Governance of Digital Identity encourages international collaboration to foster trust in each other's digital identity systems, including through the assessment and mapping of existing legal requirements, trust frameworks and use of technical standards. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491

1. Introduction

In March 2024, Italy hosted the G7 Industry, Digital and Tech Ministerial Meeting in Verona and Trento. In their Declaration[2], the Industry, Tech & Digital Ministers of the G7 reaffirmed their "*commitment to the OECD Recommendation on the Governance of Digital Identity, promoting the development of digital identity systems that are user-centred and inclusive, supported by appropriate governance, including security and privacy safeguards*" and looked forward to *"developing the Mapping Exercise of Digital Identity Approaches across the G7 to find commonalities in G7 members' approaches to digital identity*".

Digital identity refers to a set of electronically captured and stored attributes and/or credentials that can be used to prove a feature, quality, characteristic, or assertion about a user, and, when required, support the unique identification of that user. A *user* can be a natural person or a legal person, or a natural person representing a natural or legal person[3].

This report compares the digital identity approaches of Canada, the European Union (covering France, Germany, and Italy), Japan, the United Kingdom, and the United States across three main elements:

1. Concepts and definitions;
2. Approaches to levels of assurance[4]; and
3. Use of international technical standards.

The mapping is based on a template and report first developed by the EU-US Trade and Technology Council (TTC) in 2023. The results of the mapping exercise are expected to feed into future discussions of the G7, as well as support discussions on the governance of digital identity and cross-border use among other international fora.

[2] https://innovazione.gov.it/notizie/articoli/en/g7-ministerial-declaration-on-industry-technology-and-digital/

[3] Definitions are from the OECD Recommendation of the Council on the Governance of Digital Identity

[4] Level of Assurance (LoA) refers to the extent to which a service provider can be confident in the claimed identity of a user and is determined by the practices employed by the digital identity solution provider in the issuing of a given digital identity solution. Source: OECD Recommendation of the Council on the Governance of Digital Identity

2. Overview of G7 digital identity frameworks

This section provides an overview of the digital identity frameworks of Canada, the European Union, Japan, the United Kingdom, and the United States that are covered in the mapping exercise.

2.1. Canada: Directive on Identity Management

The Directive on Identity Management is part of the Government of Canada's Policy of Government Security. The Directive applies to the federal government and has the objective to ensure effective identity management practices by outlining requirements to support federal departments in the establishment, use and validation of identity information. The Directive is supported by two guidelines and one standard:

- Guideline on Defining Authentication Requirements: The purpose of this guideline is to assist departments and agencies in defining their authentication requirements for the delivery of their programmes and services in accordance with the Standard on Identity and Credential Assurance and in compliance with the relevant policies and legislation. This guideline is also supported by User authentication guidance for information technology systems (ITSP.30.031 v3) - Canadian Centre for Cyber Security.
- Guideline on Identity Assurance: This guideline supports implementation of the minimum requirements for establishing the identity of an individual to a given level of assurance.
- Standard on Identity and Credential Assurance: This standard provides details on the requirements set out in subsection 4.1.7.2 (Identity assurance and credential assurance) of the Directive on Identity Management.

Together, these policy tools form the basis of the Government of Canada's[5] approach to digital identity covered in the mapping exercise.

2.2. European Union: Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

In 2021, the European Commission proposed a framework for a European digital identity that would be available to all EU citizens, residents, and businesses, via interoperable European digital identity wallets. The new framework amends the Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

On 26 March 2024, both the European Parliament and the Council had adopted the revised regulation, which came into force on 21 May 2024. Under the new law, member states will, most likely by the end of 2026 or beginning of 2027, offer citizens and businesses digital wallets that will be able to link their national digital identities with proof of other personal

[5] These are tools of the Government of Canada and do not apply to private entities or provincial governments.

attributes (driving licence, qualifications, bank account, among others). A set of implementation acts will be developed within the course of 12 month from the adoption of the revised regulation.

During the time of writing this report, revised implementation acts had not yet been adopted. Therefore, this mapping exercise covers the Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (see consolidated version), as well as Implementing Regulation (EU) 2015/1502 adopted under the revised Regulation (EU) No 910/2014, and that will remain in force until new implementing acts amend or substitute it.

2.3. Japan: DS-500 Guidelines Concerning Online Identity Verification Methods in Administrative Procedures

The DS-500 Guidelines Concerning Online Identity Verification Methods in Administrative Procedures[6] are part of the Government of Japan's standard guidelines for the promotion of a digital society. These guidelines outline the necessary methods for online identity verification for digital public services and cover the following three areas:

- Methodology for determining the level of risk impact from threats related to online procedures and the threats themselves.
- Methodology for determining the assurance level of authentication methods required for online procedures based on the derived level of risk impact.
- "Countermeasure standards" required at each authentication assurance level derived from the above method.

The guidelines are currently under revision by Japan's Digital Agency, supported by a group of experts from the private sector, standardisation organisations, and academia. The revised guidelines are expected to be released in 2025, with consideration of the trends of online identity verification and revision of guidelines in other countries.

2.4. United Kingdom: Good Practice Guide (GPG45): How to prove and verify someone's identity; Good Practice Guide (GPG44): Using authenticators to protect and online service

There are two parts to the United Kingdom's digital identity programme:

- GOV.UK One login – a single-sign on and identity verification service that supports the more effective delivery of public services in collaboration with other government departments.
- A technologically agnostic framework of standards, governance and legislation that will enable digital identities to be secure and inclusive across the wider UK economy. The wider framework includes four elements:
    - Standards for what good digital identities look like in the form of the UK Digital Identity and Attributes Trust Framework (UKDIATF);

[6] The Guidelines are available in Japanese only.

- Certification of organisations that wish to join the UK's trusted digital identity ecosystem as providers of products and services;
- Governance to oversee the developing market, issue a trust mark, enforce the trust framework, and keep it up to date; and
- Legislation as part of a new data bill announced by His Majesty King Charles III in the UK Parliament on 17 July 2024.

The UK's digital identity programme is underpinned by the following good practice guides issued by the UK Government, and referenced throughout the mapping:

- Government guidance on how to prove and verify someone's identity (GPG45) last updated in January 2024: This guidance help service providers decide how to check the identity of a customer, employee, or someone acting on behalf of a business.
- Government guidance on using authenticators to protect an online service (GPG44) last updated in May 2020: This guidance helps service providers choose the authenticator that will give them the level of protection that is right for their service.

2.5. United States: NIST Digital Identity Guidelines SP-800-63-3

The US identity guidelines take the format of 'Digital Identity Guidelines' published by the National Institute of Standards and Technology (NIST) (Special Publication 800-63). These guidelines are grouped into four volumes, of which three are covered in this mapping exercise:

- Base Volume - digital identity and risk management
- Volume A - identity proofing and enrolment
- Volume B - authentication and lifecycle management

These guidelines provide foundational technical and process requirements for organisations implementing digital identity services, and cover identity proofing and authentication of users, as well as federation of identity information between authorised parties. The NIST guidelines are not mandatory unless specified by law or policy, and they are commonly adopted on a voluntary basis by industry, academia and governments.

NIST is currently developing a Revision 4 of the Digital Identity Guidelines[7]. The purpose of the revision is to respond to the changing digital landscape that has emerged since the last major revision of this suite was published in 2017. The Revision 4 seeks to include considerations for increasing equity and accessibility through greater optionality (including processes that do not mandate automated biometrics) as well as integration of new technology including Mobile Driver's Licences, Verifiable Credentials, wallet technology, and syncable authenticators.

[7] More info at: https://pages.nist.gov/800-63-4/

3. Commonalities between G7 digital identity frameworks

This section summarises the mapping of G7 digital identity frameworks across three elements: concepts and definitions, levels of assurance, and the use of international technical standards. It provides a basis for understanding both similarities and differences to identify a way forward in collaborating around digital identity.

3.1. Concepts and definitions

When digital identity systems from different countries need to work together, having a shared understanding of key definitions and concepts is essential. It ensures that systems can communicate and interact smoothly across borders. It can also assist policymakers to identify areas of alignment or divergence and work towards greater consistency in regulations, guidelines, and frameworks. Box 1 shows the ten concepts and definitions mapped across G7 members, based on the original EU-US TTC report.

Box 1. Concepts and definitions mapped across G7 members

- Attribute
- Authentication
- Authentication factor
- Authoritative source
- Certificate
- Identity
- Person identification data
- Signature
- Relying party
- Risk management

The mapping of definitions and concepts used by G7 members reveals a significant degree of alignment. None of the definitions used (refer to Annex A for mapping) are drastically different. Most concepts exhibit partially matching definitions, such as authentication, authoritative source, certificate, identity, person identification data, signature, relying party, and risk management. Two key concepts – attribute and authentication factor – share nearly identical definitions across all G7 members. Furthermore, the G7 members' definition of attribute coincides with that outlined in the OECD Recommendation on the Governance of Digital Identity[8].

As observed in the mapping of the EU-US TTC, variations in the precise concepts employed can be attributed in part to the diverse nature of the authoritative documents involved. For instance, there is a distinction between the European Union regulation, which

[8] Attribute refers to a verified feature, quality or characteristic ascribed to a user, for example biometric data, name, date of birth, place of birth, uniqueness identifier (e.g. personal ID number, social security number, company registration number) and address, in electronic form.

spans multiple countries, and national guidelines in Canada, Japan, the United Kingdom, and the United States, each with its own scope. The EU Regulation, for example, has a broad focus encompassing various definitions relevant to trust services. Likewise, the UK Digital Identity and Attributes Trust Framework addresses concepts associated with certification and accreditation within its framework, as well as privacy-enhancing digital identity technologies (e.g., zero knowledge proofs, verifiable credentials).

Main findings and their implication for interoperability: The alignment of definitions for the ten key concepts among G7 members is a positive indicator for interoperability efforts. While some variations exist and are understandable, this highlights the relevance of advancing international consensus on digital identity terms, where possible, to prevent friction, delays, and potential vulnerabilities. Building on these findings, G7 members could use the mapping of concepts as a basis for more detailed discussions on digital identity semantics to support interoperability.

3.2. Approaches to levels of assurance

Levels of assurance (LOAs) acts as a scale that measures how much trust you can have in a digital identity. A higher level of assurance means you can be more confident that the person or entity using that digital identity is who they say they are. If you are operating in multiple countries, you need to understand the varying levels of assurance each country employs to ensure digital identity systems are compatible and compliant with local regulations. A mapping of approaches to levels of assurance is like a guidebook that helps navigate the complex landscape of digital identity, helping to ensure that systems are secure, trustworthy, and interoperable. Governments and organisations can use this mapping to compare their own approaches to digital identity with those of other countries, helping them develop more effective policies and regulations.

The G7 approaches to levels of assurance all leverage either three or four ascending levels to indicate increasing confidence in the means of identification and authentication deployed (see Table 2 and Table 3). Since the majority of G7 members use three levels of assurance, the G7 approaches are mapped and compared across three reference assurance levels:

- Level of Assurance 1 (LOA1, Low)
- Level of Assurance 2 (LOA2, Medium)
- Level of Assurance 3 (LOA3, High)

LOA1 represents the lowest level of assurance, where there are generally few identity assurance and authentication requirements, suitable for low-risk services and applications. LOA2 is a medium level of assurance, suitable for services or applications where there is a moderate acceptance of risk. LOA3 is the highest level of assurance, where relying parties need to be confident with a high level of degree that the user accessing their service or application is the same person they claim to be.

Country requirements are mapped for each level of assurance across 1) identity proofing and enrolment, and 2) authentication. For identity proofing and enrolment, the requirements are divided into four components[9], and for authentication, in eight components[10] (see Table 1).

[9] Evidence requirements, Validation process, Verification method, Issuance and binding

10 Allowed authenticators, Information security, Binding, Issuance, Suspension and revocation, Renewal and replacement, Cryptographic validation, Threats addressed.

Table 1. Requirements compared in the mapping exercise

Identify proofing and enrolment		Authentication	
Component	*Description*	*Component*	*Description*
Evidence requirements	Requirements on the type of evidence collected	**Allowed authenticators**	The types of authenticators allowed
Validation process	The process of checking the accuracy, authenticity and integrity of the evidence and related information	**Information security**	Requirements on information security controls
Verification method	The method of confirming and establishing a link between the claimed identity and the real-life existence of the subject presenting the evidence	**Binding**	The establishment of an association between a specific authenticator and a subscriber's account, enabling the authenticator to be used to authenticate for that account.
Issuance and binding	Requirements related to issuance and binding at enrolment	**Issuance**	Requirements related to the issuance of an authenticator
		Suspension and revocation	Requirements for suspending and revoking authenticators
		Renewal and replacement	Requirements related to the renewal or replacement of authenticators
		Cryptographic validation	Requirements related to cryptographic validation
		Threats addressed	Threats to authenticators addressed

Note: The descriptions are meant to support readers in understanding the scope of the mapping exercise; they are not agreed-upon definitions by G7 members.
Source: Some of the descriptions are from the SP 800-63 Digital Identity Guidelines document suite by NIST.

Table 2. Mapping of G7 levels of assurance: identity proofing and enrolment

Reference level	Canada	European Union	Japan	United Kingdom	USA
LOA1 (Low)	Level 1	Low	IAL1	Low confidence	IAL1
LOA2 (Medium)	Level 2 and Level 3	Substantial	IAL2	Medium confidence	IAL2
LOA3 (High)	Level 4	High	IAL3	High confidence, Very high confidence	IAL3

Note: LOA stands for Level of Assurance and IAL stands for Identity Assurance Level. See Annex B for a detailed description of G7 members' levels of assurance for identity proofing and enrolment.

Table 3. Mapping of G7 levels of assurance: authentication

Reference level	Canada	European Union	Japan	United Kingdom	United States
LOA1 (Low)	LOA 1 and LOA 2	Low	AAL1	Low quality authenticator	AAL1
LOA2 (Medium)	LOA 3	Substantial	AAL2	Medium quality authenticator	AAL2
LOA3 (High)	LOA 4	High	AAL3	High quality authenticator	AAL3

Note: LOA stands for Level of Assurance and AAL stands for Authentication Assurance Level. See Annex C for a detailed description of G7 members' levels of assurance for authentication.

3.2.1. Summary of LOA mapping across the G7

LOA1: Overall, there are significant similarities in G7 members' requirements for LOA1 (low level of assurance). None of the G7 members have evidence requirements at this level, nor require multi-factor authentication. However, small differences are noted with the approach to identity proofing and enrolment, where, for example, the United Kingdom include options for evidence collection, validation and verification, and the EU and Japan have requirements for binding and issuance. For authentication, there are some differences between G7 members in the level of detail covered for authenticators.

LOA2: The main similarities in the requirements for LOA2 across all G7 frameworks is the requirement for identity evidence collection, as well as the use of multi-factor authentication. However, there are notable differences. Japan, Canada, the UK, and the US have specific evidence requirements, while the EU focuses on member state-recognised evidence. Remote identity proofing is explicitly allowed in Japan and the US but not in other frameworks. Verification approaches differ in depth, with the EU requiring checks against authoritative sources. Canada, the US, and the EU include provisions for address confirmation. For authentication, only the US, UK, and Canada reference information security standards, and only Canada and the US mandate cryptographic validation.

LOA3: For LOA3 identity proofing and enrolment, all G7 frameworks share a focus on validating strong identity evidence against authoritative sources to ensure genuineness and that the identity corresponds to a real person. Differences arise in the evidence requirements: while the EU and Japan emphasise official state-issued IDs with photos, the UK, Canada, and the US offer additional combinations. Issuance and binding requirements differ too, with face-to-face activation mandated by the EU, US, and Japan but not by the UK or Canada. In authentication, all frameworks require multi-factor authentication and address Man-in-the-Middle attacks, but the US, UK, Japan and Canada include phishing resistance and the US, UK, and Canada also include cryptographic validation. Additionally, the EU requires verification with authoritative sources for renewal, while only the US, UK, and Canada explicitly reference information security standards.

Main findings and their implication for interoperability: While there are significant similarities in the foundational requirements across G7 members' digital identity frameworks, especially at the lower levels of assurance (LOA1 and LOA2), the differences in the specifics of identity proofing, evidence requirements, validation, and verification processes at higher assurance levels (LOA2 and LOA3) present challenges for achieving interoperability. The limited uniformity suggests that the current frameworks are tailored to domestic needs, and that further dialogue and co-operation would be required to achieve global compatibility. Based on these findings, G7 members could work towards alignment and interoperability of approaches at higher assurance levels, particularly those related to identity proofing, verification, and authentication.

3.3. Use of international technical standards

The mapping of international standards referenced by each G7 member's digital identity framework shows evident differences. The mapping, covering more than 50 international technical standards references, reveals that there are no overlaps in any of the standard references across all G7 members. Nonetheless, there are six overlaps between at least two G7 members:

- ISO/IEC 29115:2013 for identity assurance of persons and non-person entities (**European Union and United States).**

- RFC 5280 describing Internet X.509 Public Key Infrastructure Certificate and CRL Profile (**EU and United States).**
- ISO/IEC Information assurance and security standards for eID node operators **(European Union and United Kingdom).**
- OpenID Connect **(United Kingdom and United States).**
- ISO/IEC 9594-8 Information technology — Open systems interconnection — The Directory: Public-key and attribute certificate framework **(Canada and European Union).**
- ISO 3166-1 Codes for the representation of names of countries and their subdivisions — Part 1: Country codes **(Canada and European Union).**

As noted in the section on concepts and definitions this can be attributed to the different nature of the digital identity frameworks and their scope (regulation vs. guideline). The European Union's framework contains several references to international technical standards related to electronic signatures and trust services. As a former member state of the European Union, the United Kingdom shares international standards references regarding eID node operators. The United Kingdom and United States refer to a number of international technical standards focused on security techniques. The digital identity frameworks of Japan and Canada overall does not refer to any international technical standards. However, in Japan, the only G7 country that does not use the Latin alphabet, all use of the technology referred to in the guidelines is premised on the use of non-alphabetical characters.

Main findings and their implication for interoperability: The mapping of the use of international technical standards indicates diversity in how digital identity systems are developed and managed at domestic level. Several G7 members refer to many technical standards with little overlap between them, while others do not. This may be the result of differences in administrative, legal, and cultural contexts. Based on these findings, G7 members could explore further discussions on the relevance of different international technical standards to support future interoperability, while respecting their different contexts and approaches.

4. The way forward

Given the rapidly evolving digital identity landscape, the G7 serves as a crucial forum to advance discussions on digital identity and interoperability among like-minded countries. These discussions are grounded in the respect for human rights and on upholding the highest standards in privacy and security safeguards.

The findings from this mapping highlight significant similarities in the G7 approaches to digital identity, forming a solid foundation for further co-operation and dialogue on cross-border alignment and interoperability. While there are some differences, particularly concerning technical standards references, the overall mapping shows promising results. This creates an opportunity for G7 members to build on this exercise by:

- Using the mapping of concepts as a basis for more detailed discussions on digital identity semantics to support interoperability.
- Working towards alignment and interoperability of approaches, particularly those related to identity proofing, verification, and authentication at higher assurance levels.
- Exploring further discussions on the relevance of different international technical standards to support future interoperability, while respecting their different contexts and approaches.

In the future, G7 members could prioritise using this mapping exercise, and the above recommendations, as a springboard for discussions during their respective presidencies. This could include additional efforts to seek alignment and interoperability of existing approaches. It could also explore further co-operation in the design and development of solutions such as mobile driver's licenses and digital wallets, at both national and subnational level. This could leverage the expertise on digital identity within G7 members as well as continued partnership with the OECD.

Insights from this report can also support ongoing bilateral discussions between G7 members, such as those within the EU-US Trade and Technology Council (TTC) and the EU-Japan Digital Partnership. Moreover, it can inform bilateral and multilateral discussions on digital identity among G7 members and likeminded countries across various regions or forums.

Annex A. Mapping of concepts and definitions

Concept	Canada	European Union	Japan	United Kingdom	United States
Attribute	**Identity attribute:** A property or characteristic associated with an identifiable individual, also known as an identity data element (Source)	A characteristic, quality, right or permission of a natural or legal person or of an object (Source)	A property or characteristic that a subject possesses, and such information is called "attribute information". (Source)	Pieces of information that describe something about a person or an organisation. (Source)	A quality or characteristic ascribed to someone or something. (Source)
Authentication	The process of establishing truth or genuineness to generate an assurance (Source)	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 (Source)	A process that establishes trust that the "performing entity" is the person (or device) pre-associated with the identity by verifying equivalence between the "performing entity" of an act and the identity claimed by the "performing entity". (Source)	The process for managing and controlling access of a known user, to a system or service	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources. (Source)
Authentication factor	**Multi-Factor:** A characteristic of an authentication system or a token that uses more than one authentication factor. The three types of authentication factors are 1) something a user knows, 2) something a user has, and 3) something a user is. (Source)	A factor confirmed as being bound to a person, which can be possession-based (something the person owns), knowledge-based (something the person knows) or inherent (something based on a physical attribute) (Source)	**Three Authentication Factors:** What you know, what you have, what you are (attribute information regarding your body.) (Source)	This will usually be one of the following: - something the user knows, - something the user has - something the user is. Sometimes an authenticator can fit into more than one of these categories. (Source)	The three types of authentication factors are something you know, something you have, and something you are. Every authenticator has one or more authentication factors. (Source)
Authoritative source	A collection or registry of records maintained by an authority that meets established criteria. (Source)	**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 (Source)	N/A	To have high confidence in someone's identity you might have to check things with an authoritative source. To be authoritative for a particular piece of information, the source must make sure; the integrity of the information is protected; the information is up to date. The source must also do one of the following: issue evidence; get information from an organisation that issues evidence; get information from another authoritative source. (Source)	An entity that has access to, or verified copies of, accurate information from an issuing source such that a CSP can confirm the validity of the identity evidence supplied by an applicant during identity proofing. An issuing source may also be an authoritative source. Often, authoritative sources are determined by a policy decision of the agency or CSP before they can be used in the identity proofing validation phase. (Source)

Concept	*Canada*	*European Union*	Japan	*United Kingdom*	United States
Certificate	**Public key certificate:** A digital document issued and digitally signed by the private key of a certificate authority that binds the name of a Subscriber to a public key. The certificate indicates that the Subscriber identified in the certificate has sole control and access to the private key (Source)	**Certificate for electronic signature:** electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person. (Source)	N/A	**Digital certificate:** a trust service which can be used to verify that a sender or receiver of data are exactly who they claim to be. Comprising a public and private key infrastructure or use of verifiable credentials to ensure access is only granted to the authorized entity.	**Public key certificate:** a digital document issued and digitally signed by the private key of a certificate authority that binds an identifier to a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. (Source)
Identity	A set of attributes that uniquely describe a person within a given context. (Source)	**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. (Source)	An information or set of information that uniquely distinguishes an individual or other entity. (Source)	A combination of 'attributes' (characteristics) that belong to a person (Source)	An attribute or set of attributes that uniquely describe a subject within a given context (Source)
Person identification data	**Personal information:** Information that is about an identifiable individual and recorded in any form, as defined in section 3 of the Privacy Act. **Identity information:** The set of identity attributes that is sufficient to distinguish between individuals and sufficient to describe the individual as required by the service or program. (Source)		**Personal Information:** Information relating to a living identified or identifiable individual which falls under any of the items described in the Article 2 of the Act on the Protection of Personal Information	**Personal Identification data:** A set of data enabling the identity of a natural or legal person, or a natural person representing a legal person, to be established. (Source)	**Personally Identifiable information**: information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (Source)
Signature	**Electronic signature**: a signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document. (Source)	**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. (Source)	**Electronic signature:** The term "electronic signature" means a measure taken with respect to information that can be recorded in an electronic or magnetic record (a record that is prepared by an electronic form, a magnetic form or any other form not perceivable by human senses and that is used for information processing by computers), and which falls under both of the following requirements: (i)a measure to indicate that the relevant information was created by the person who has taken that measure; and (ii)a measure to confirm whether the relevant information has been altered. (Source)	**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 (Source) **Digital signatures:** A type of electronic signature that is used to validate the authenticity and integrity of a message, like an email, credit card transaction or a digital document. (Source)	**Digital signature**: An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation, but not confidentiality protection. (Source)

Relying party	A federation member that relies on assurances of credential or identity from other members (authoritative parties). (Source)	A natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a trust service (Source)	N/A	An organisation that receives, interprets and - depending on the use case - stores information received from other trust framework organisations (Source)	An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system. (Source)
Risk management	**Security authorisation:** The ongoing process of obtaining and maintaining a security risk management decision and to explicitly accept the related residual risk, based on the results of security assessment. (Source) **Security categorisation:** The process of assigning a security category to information resources, assets or services based on the degree of injury that could reasonably be expected to result from their compromise. (Source)	**Information security management system:** Set of processes and procedures designed to manage to acceptable levels risks related to information security. (Source)	N/A	A process to identify, assess, manage and control potential events or situations to provide reasonable assurance regarding the achievement of the organisation's objectives.	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. (Source)

Annex B. Overview of identity and authentication assurance levels

Identity assurance levels					
	Canada	*European Union*	*Japan*	*United Kingdom*	*United States*
Identity assessment type	Identity Assurance Levels	eIDAS Levels of assurance	Identity assurance level (IAL)	Level of confidence in someone's identity	Identity assurance level (IAL)
Description	Different identity assurance levels allow government programs and services to carry out transactions commensurate with the level of risk.	Assurance levels should characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned	A category that conveys the degree of confidence that a person's claimed identity is their real identity, as defined in [NIST SP 800-63-3] in terms of three levels	You can reach a level of confidence by meeting an identity profile. The results of your services risk assessment will help you decide which level to meet. You should aim to get a higher level of confidence in someone's identity if you or your service are at high risk of identity-related crime	A category that conveys the degree of confidence that a person's claimed identity is their real identity, as defined in [NIST SP 800-63-3] in terms of three levels
Nr of Levels	4	3	3	4	3
Levels	Level 1 (little confidence), Level 2 (Some confidence), Level 3 (High confidence), Level 4 (Very high confidence)	Low, Substantial, High	IAL 1 (Some confidence) IAL 2 (High confidence) IAL 3 (Very high confidence)	Low confidence, medium confidence, high confidence, very high confidence	IAL 1 (Some confidence) IAL 2 (High confidence) IAL 3 (Very high confidence)
Authentication assurance levels					
	Canada	*European Union*	*Japan*	*United Kingdom*	*United States*
Identity assessment type	Assurance level	eIDAS Levels of assurance (LOA)	Authenticator Assurance Level (AAL)	Quality of authenticator	Authenticator Assurance Level (AAL)
Description	The Guideline will enable departments to use a standardized approach to defining authentication requirements. ITSP.30.031 v3 is a complementary document to the guidelines.	Assurance levels should characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned	A measure of the strength of an authentication mechanism and, therefore, the confidence in it, as defined in [NIST SP 800- 63-3] in terms of three levels	An authenticator can be low, medium or high quality. The quality of an authenticator will depend on how secure it is.	A measure of the strength of an authentication mechanism and, therefore, the confidence in it, as defined in [NIST SP 800- 63-3] in terms of three levels
Nr of Levels	4	3	3	3	3
Levels	Level of Assurance 1 (LOA1), Level of Assurance 2 (LOA2), Level of Assurance 3 (LOA3), Level of Assurance 4 (LOA4)	Low (LOA 1), Substantial (LOA 2), High (LOA 3)	Authentication Assurance Level 1 (AAL1) Authentication Assurance Level 2 (AAL2) Authentication Assurance Level 3 (AAL3)	Low quality, medium quality, high quality	Authentication Assurance Level 1 (AAL1) Authentication Assurance Level 2 (AAL2) Authentication Assurance Level 3 (AAL3)

Annex C. Identity proofing and enrolment – summary of mapping

LOA1

Similarities in identity proofing and enrolment for LOA1

- None of the G7 members have requirements for evidence collection at LOA1.

Differences in identity proofing and enrolment for LOA1

- **Evidence requirements**
  - The United Kingdom framework includes the possibility to request that users provide low quality physical evidence (e.g. documents without biometrics or security features) or digital evidence that supports and represents their claimed identity. The quality of this evidence is scored depending on the number of attributes associated with the claimed identity and if it includes information that is unique to that identity or the evidence, e.g. reference number.
- **Validation process**
  - If evidence is requested at LOA1 (not a requirement), the United Kingdom framework includes limited checking of physical evidence to ensure its genuine and valid, or by checking the digital evidence with an authoritative source.
- **Verification method**
  - The United Kingdom framework includes verification that the identity belongs to the person who is claiming it by proving they know information that only the claimed identity should know.
- **Issuance and binding**
  - For the European Union, after issuance, the electronic identification means is required to be delivered via a mechanism by which it can be assumed to reach only the intended person.
  - For Japan, credentials and tokens are sent to the e-mail address of the applicant. If an e-mail address is registered, the validity of the e-mail address shall be verified.
  - For the United Kingdom, once the identity proofing is verified as having been performed at low confidence, binding is established in line with procedures to check that the genuine user controls their claimed identity. Once created, the electronic identity is issued and managed in accordance with all relevant standards, including security and data protection regulations.
  - The European Union has specific requirements on binding procedures for natural persons acting on behalf of legal persons.

LOA2

Similarities in identity proofing and enrolment for LOA2

- All G7 frameworks require identity evidence collection at this level.

Differences in identity proofing and enrolment for LOA2

- **Evidence requirements**
  - Japan, Canada, United Kingdom, and United States have requirements on the number and strength of the identity evidence. The European Union specifies the need for Member State-recognised evidence.
  - Both Japan and the United States explicitly allow for remote and in-person identity proofing, which is not specified in the other G7 member frameworks.
  - LOA2 is a combination of Canada's Level 2 and Level 3 (see Table 2). Canada's Level 2 has slightly lower requirements than Level 3, including the need for only one identity evidence compared to two. Canada's framework separates between foundational evidence of identity (e.g. records of birth, immigration, or citizenship) and supporting evidence of identity (e.g. social insurance records), where Level 3 require at least one of the pieces of evidence to be foundational.
- **Validation process**
  - The United Kingdom provides detailed requirements on the process of validating the evidence, including its authenticity and the accuracy of details, with different requirements depending on whether it is a physical document or digital information.
  - Japan requires that the name and address of the applicant is checked against the official registry (authoritative source), or official certificates such as a residence certificate. This detail is not prescribed by other G7 frameworks. The European Union requires checks to determine that evidence is genuine, which could include consulting authoritative sources.
  - The United States requires validation of each piece of evidence, including both the authenticity of the evidence and the accuracy of the details, with a process that can achieve the same strength as the evidence presented.
  - For Canada, Level 2 requires that the identity information acceptably matches assertion by an individual and evidence of identity, whereas Level 3 requires validation that the identity information acceptably matches all instances of evidence of identity.
- **Verification method**
  - For the United States, at minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of strong + knowledge-based verification shall not be used for in-person identity verification.
  - For the European Union, an authoritative source must be able to verify that the claimed identity exists, and it may be assumed that the person claiming the identity is one and the same. Additional requirements also apply, such as that

the person has been verified being in possession of evidence recognised by the Member State that represent the claimed identity.

- For the United Kingdom, it is verified that the identity belongs to the person who is claiming it by performing the following checks: ensuring the person physically matches the photo on or associated with the strongest piece of genuine evidence provided of the claimed identity; ensuring the person's biometric information matches biometric information from the strongest piece of genuine evidence provided or an authoritative source; asking the person to complete multiple 'dynamic' Knowledge Based Verification (KBV) challenges, that only the claimed identity should be able to do (can only receive a score 2 out of 3).
- For Canada, at Level 2, there is confirmation that evidence of identity originates from an appropriate authority. At Level 3, there is confirmation of the foundational evidence of identity using an authoritative source, and confirmation that supporting evidence of identity originates from an appropriate authority, using an authoritative source.
- Japan has not specified verification requirements.

- **Issuance and binding**
  - The European Union has specific binding requirements for natural persons acting on behalf of a legal person, which are increased at LOA2 compared to LOA1.
  - The LOA2 frameworks of the United States, Japan, and the European Union include address confirmation for issuance.
  - For Level 3, Canada requires at least one of the following binding methods (there are no requirements at Level 2):
    - Knowledge-based confirmation.
    - Biological or behavioural characteristic confirmation.
    - Trusted referee confirmation.
    - Physical possession confirmation.

LOA3

Similarities in identity proofing and enrolment for LOA3

- Validation requirements all focus on the checking of strong evidence against authoritative sources to determine genuineness and that the identity to which the evidence pertains exists and relates to a real person.

Differences in identity proofing and enrolment for LOA3

- **Evidence requirements**
  - Evidence requirements for all G7 members at LOA3 centre on the provision of strong evidence, including photo or biometric information. The European Union and Japan include similar requirements for official state-issued IDs with photo, while the United Kingdom, Canada, and United States also provide other options and combinations.

- **Validation process**
  - The United States requires validation of each piece of evidence, including both the authenticity of the evidence and the accuracy of the details, with a process that can achieve the same strength as the evidence presented.
  - For the European Union, evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person AND the evidence is checked to determine that it is valid according to an authoritative source.
  - For the United Kingdom, there are requirements to check if the evidence is protected by cryptographic security features and ensure these security features are genuine OR for non-cryptographic evidence complete the following checks:
    - confirm the evidence is valid or check the evidence has not been cancelled, lost or stolen.
    - confirm any physical security features are genuine.
    - check the evidence has not expired.
  - For Canada and Japan, the validation process is the same as for LOA2.
- **Verification method**
  - For the European Union, the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source.
  - For Canada, there is either of the two following verification methods:
    - Confirmation of the foundational evidence of identity using an authoritative source, and confirmation that supporting evidence of identity originates from an appropriate authority, using an authoritative source, or;
    - Inspection by a trained examiner.
  - For the United Kingdom, the same checks as for LOA2 are performed plus the following:
    - Checks to tell when someone is spoofing the system using a sophisticated artefact that has taken a lot of time, money, effort or criminal activity to create. The biometric information on the evidence and the biometric information of the person must also be captured under ‘controlled conditions’ which usually require an element of face-to-face checking.
- **Issuance and binding**
  - Binding for the EU LOA3 is similar to LOA2 with increased requirements, including verification based on a unique identifier representing the legal person used in the national context.
  - The LOA3 frameworks of the European Union, United States and Japan require face-to-face activation or issuance/delivery. The United States’ framework also requires address confirmation. This is not specified in the United Kingdom’s or Canada’s frameworks.

- Canada requires the use of at least three of the following binding methods:
  - Knowledge-based confirmation.
  - Biological or behavioural characteristic confirmation.
  - Trusted referee confirmation.
  - Physical possession confirmation.

Annex D. Authentication – summary of mapping

LOA1

Similarities in authentication for LOA1

- All G7 LOA1 frameworks allow for single factor authenticators.

Differences in authentication for LOA1

- For Canada, the reference LOA1 is covered by Canada's LOA1 and LOA2 (See Table 3). Canada's LOA1 has no, or lower, requirements than LOA2, including on threats addressed. Canada's LOA2 is more similar to other G7 LOA1 frameworks.
- Some level of criteria for information security management, binding, issuance, suspension, revocation, renewal and replacement are explicitly covered in all G7 LOA1 frameworks, except Japan.
- The LOA1 frameworks of the United States, European Union, Canada, and Japan specify the need to address guessing, Man-in-the-Middle (MitM) attacks, replay and eavesdropping. The United Kingdom's framework specifies that low quality authenticators are designed to prevent unprotected access, impersonation of log in details, and eavesdropping.
- The United States and Canada have minimum requirements for cryptographic validation.

LOA2

Similarities in authentication for LOA2

- All G7 LOA2 frameworks require multi-factor authentication.
- The LOA2 processes for binding and issuance, renewal and replacement are equivalent to LOA1 for all G7 frameworks, except Japan that has not specified equivalent criteria.

Differences in authentication for LOA2

- Canada introduces requirements for suspension and revocation at LOA2.
- The United States, United Kingdom and Canada introduces explicit reference to standards and requirements for information security controls.
- Only Canada and the United States have requirements for cryptographic validation.
- The LOA2 frameworks of the United States, European Union, Canada, and Japan specify the need to address guessing, MitM attacks, replay and eavesdropping. The United Kingdom framework specifies that medium quality authenticators are designed to prevent most attacks; MitM, distributed denial of service (DDOS),

impersonation, and phishing, depending on the combination of two-factor authentication deployed. Canada and Japan also specify preventing phishing.

LOA3

Similarities in authentication for LOA3

- All G7 LOA3 frameworks require multi-factor authentication and addresses MitM attacks.
- The LOA3 processes for issuance and suspension and revocation are equivalent to LOA2 for all G7 frameworks, except Japan that has not specified equivalent criteria.

Differences in authentication for LOA3

- The United States, Canada, Japan, and the United Kingdom cover impersonation/pharming/phishing resistance.
- For renewal and revocation, the European Union's framework requires the identity data to be verified with an authoritative source where renewal is based on a valid electronic identification means.
- The United States, United Kingdom and Canada have requirements for cryptographic validation.
- The United States, United Kingdom and Canada make explicit reference to standards and requirements for information security controls.

Annex E. Mapping of international technical standards

International technical standard	Scope/name	Canada	European Union	Japan	United Kingdom	United States
ISO/IEC 9241-11	Ergonomic requirements for office work with visual display terminals (VDTs) — Part 11: Guidance on usability					Yes
ISO 29003	Information technology — Security techniques — Identity proofing					Yes
ISO 29115	Information technology — Security techniques — Entity authentication assurance framework		Partially			Yes
ISO/IEC 2382-37	Information technology — Vocabulary — Part 37: Biometrics					Yes
ISO/IEC 10646	Universal Coded Character Set					Yes
ISO/IEC 24745	Information technology — Security techniques — Biometric information protection					Yes
ISO/IEC 30107-1	Information technology — Biometric presentation attack detection — Part 1: Framework					Yes
ISO/IEC 30107-3	Information technology — Biometric presentation attack detection — Part 3: Testing and reporting					Yes
BCP 195	Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)					Yes
OpenID Connect	OpenID Connect Core 1.0 incorporating errata set 1				Yes	Yes
RFC 20	ASCII format for network interchange					Yes
RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2					Yes
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and CRL Profile		Yes			Yes
RFC 6238	TOTP: Time-Based One-Time Password Algorithm					Yes
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP					Yes
Unicode	Unicode Normalization					Yes

Standard Annex #15	Forms					
RFC 4120	The Kerberos Network Authentication Service (V5)					Yes
RFC 6113	A Generalized Framework for Kerberos Pre-Authentication					Yes
RFC 7591	OAuth 2.0 Dynamic Client Registration Protocol					Yes
RFC 7636	Proof Key For Code Exchange					Yes
SAML	Security Assertion Markup Language (SAML) V2.0 Technical Overview					Yes
ETSI TS 119 612	Electronic Signatures and Infrastructures (ESI); Trusted Lists		Yes			
ISO/IEC 9594-8	Information technology — Open systems interconnection — The Directory: Public-key and attribute certificate framework	Yes	Yes			
ISO 3166-1	Codes for the representation of names of countries and their subdivisions — Part 1: Country codes'	Yes	Yes			
ISO 32000	Document management — Portable document format		Yes			
ISO 19005	Document management — Electronic document file format for long-term preservation		Yes			
RFC 3739	Internet X.509 PKI: Qualified Certificates Profile		Yes			
ETSI TS 103171	XAdES Baseline Profile		Yes			
ETSI TS 103173	CAdES Baseline Profile		Yes			
ETSI TS 103172	PAdES Baseline Profile		Yes			
ISO/IEC 15408	Evaluation criteria for IT security,		Yes			
ISO/IEC 18045	Methodology for IT security evaluation		Yes			
EN 419 211	Protection profiles for secure signature creation device,		Yes			
ISO/IEC 27001	Information assurance and security standards for eID node operators		Yes		Yes	
EN 301 549 V3.2.1 (2021-33)	ETSI standard for accessibility requirements				Yes	
EN 301 549 V1.1.2 (2015-04)	Accessibility requirements suitable for public procurement of ICT products and services in Europe				Yes	
ISO/IEC 18013-5:2021	Use of mobile credentials				Yes	

ISO/IEC 19795-1:2001	Biometric performance testing and reporting				Yes	
BS 8878:2010	Web accessibility Code of practice				Yes	
ISO/IEC 27001:2017	Staff and resources				Yes	
BS 7858:2019	Screening of individuals working in a secure environment. Code of practice				Yes	
ETSI TS 103 458	Application of Attribute Based Encryption (ABE) for PII and personal data protection on Internet of Things (IoT) devices, WLAN, cloud and mobile services				Yes	
ISO/IEC 18033 family Part 1-5	Information technology — Security techniques — Encryption algorithms				Yes	
ETSI TS 119 312	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites				Yes	
ISO 20000:2018	Information technology — Service management				Yes	
ISO 9001:2015	Quality management systems — Requirements				Yes	
ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems — Requirements				Yes	
ISO/IEC 27005:2018	Information technology — Security techniques — Information security risk management				Yes	
ISO 31000:2018	Risk management				Yes	
ISO/IEC 27701:2019	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines				Yes	
W3C Verifiable Credential Data Model	Specification to express credentials on the Web				Yes	

Annex F. Reference documents

Canada:

- Policy on Government Security- Canada.ca
- Directive on Identity Management- Canada.ca
- Directive on Identity Management - Appendix A: Standard on Identity and Credential Assurance- Canada.ca
- Guideline on Identity Assurance- Canada.ca
- Guideline on Defining Authentication Requirements- Canada.ca
- User authentication guidance for information technology systems (ITSP.30.031 v3) - Canadian Centre for Cyber Security

European Union:

- Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Consolidated version: EUR-Lex - 02014R0910-20240520 - EN - EUR-Lex (europa.eu)
- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014

Japan:

- DS-500 Guidelines Concerning Online Identity Verification Methods in Administrative Procedures

United Kingdom:

- Government guidance on how to prove and verify someone's identity (GPG45)
- Government guidance on using authenticators to protect an online service (GPG44)
- UK Digital Identity and Attributes Trust Framework

United States:

- NIST Special Publication 800-63-3 - Digital Identity Guidelines
    - Base Volume - digital identity and risk management
    - Volume A - identity proofing and enrolment
    - Volume B - authentication and lifecycle management