# Recommendation of the Council on the Governance of Digital Identity

**OECD Legal Instruments**

OECD

BETTER POLICIES FOR BETTER LIVES

This document is published under the responsibility of the Secretary-General of the OECD. It reproduces an OECD Legal Instrument and may contain additional material. The opinions expressed and arguments employed in the additional material do not necessarily reflect the official views of OECD Member countries.

This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

For access to the official and up-to-date texts of OECD Legal Instruments, as well as other related information, please consult the Compendium of OECD Legal Instruments at http://legalinstruments.oecd.org.

**Please cite this document as:**
OECD, *Recommendation of the Council on the Governance of Digital Identity*, OECD/LEGAL/0491

Series: OECD Legal Instruments

**Photo credit:** © metamorworks/Shutterstock

© OECD 2023

This document is provided free of charge. It may be reproduced and distributed free of charge without requiring any further permissions, as long as it is not altered in any way. It may not be sold.

This document is available in the two OECD official languages (English and French). It may be translated into other languages, as long as the translation is labelled "unofficial translation" and includes the following disclaimer: *"This translation has been prepared by [NAME OF TRANSLATION AUTHOR] for informational purpose only and its accuracy cannot be guaranteed by the OECD. The only official versions are the English and French texts available on the OECD website http://legalinstruments.oecd.org"*

## Background Information

The Recommendation on the Governance of Digital Identity was adopted by the OECD Council meeting at Ministerial level on 8 June 2023 on the proposal of the Public Governance Committee (PGC). The Recommendation aims to guide Adherents in their efforts to successfully establish domestic approaches to digital identity that are user-centred, trusted and well-governed and in so doing create the conditions for achieving the ambition of full international interoperability to realise the value of digital identity across geography, technology and sectors.

***The need for a standard on digital identity***

Identity verification is essential for the functioning and resilience of societies, economies, and political systems. While physical documents such as ID cards and passports have enabled individuals to access essential services and cross borders, they are not adequate to meet the opportunities and challenges of the digital age. To ensure the long-term sustainability of digital identity, governments need to establish robust governance foundations and treat digital identity as critical digital public infrastructure.

Governments are working to ensure reliable and trusted access to a digital identity for natural and legal persons that is portable across platforms, sectors, and borders. However, challenges exist both at national and international level to implement this ambition, including public perception, user experience and adoption, digital inclusion, data sharing, interoperability, liability, data privacy and security. Often these challenges are shaped by technology and underpinned by foundational questions of governance that include strategy, public-private collaboration, regulation, and international co-operation. Developing a strategic and systematic approach is necessary to create a trustworthy and robust digital identity system that accounts for the emergence and management of new models and technologies. To achieve this, governments need to balance different goals depending on their national context. This requires a governance framework that is flexible, adaptable and promotes interoperability across borders.

The Recommendation builds on the work of the Working Party of Senior Digital Government Officials (E-Leaders Working Party, under the PGC), complementing initiatives undertaken by the OECD Committee on Digital Economy Policy as well as other international organisations and fora. It provides a standard for the governance of digital identity in line with OECD values, enabling accessible, user-friendly, highly trusted, secure, and equitable approaches to digital identity that will simplify and accelerate interactions, achieve more proactive and personalised services, and reduce the opportunities for error, fraud and other illicit activities.

***Process for developing the Recommendation***

The development of the Recommendation involved extensive consultations both within and outside the OECD. Based on responses from 30 OECD Members and non-Members to the OECD Survey on Digital Identity and extensive interviews with government representatives and units responsible for digital identity, the E-Leaders Working Party started to discuss the findings and identified priority policy issues for the development of an OECD Recommendation in 2022.

Expert stakeholders from the digital identity ecosystem were engaged to provide their views on the draft of the Recommendation. The draft was also submitted to public consultation and distributed widely among relevant OECD bodies. To finalise the text of the Recommendation, multiple rounds of comments were held on the draft text in the E-Leaders Working Party and the PGC.

***Scope of the Recommendation***

The Recommendation is structured around three pillars:

- The first pillar emphasises the importance of developing user-centred and inclusive digital identity systems. This involves designing and implementing digital identity systems that are effective, usable and respond to the needs of users and service providers. This pillar also highlights the need for digital identity systems to prioritise inclusion and minimise barriers to access, while preserving non-digital ways to prove identity.

- The second pillar focuses on strengthening the governance of digital identity. This requires taking a strategic approach to digital identity and defining roles and responsibilities across the digital identity ecosystem. It also emphasises the importance of protecting privacy and prioritising security to ensure trust in digital identity systems. Additionally, it concentrates on the need to align legal and regulatory frameworks, and provide resources to enable interoperability across different systems and services.

- The third pillar is dedicated to the cross-border use of digital identity. This requires identifying evolving needs of users and service providers in different cross-border scenarios and co-operating internationally to establish the basis for trust in other jurisdictions' digital identity systems and issued identities. Achieving cross-jurisdictional portability of digital identity is complex, but international collaboration and the development of international instruments can help set expectations, create consensus, and build trust.

Overall, the Recommendation provides a framework that promotes the development of reliable and trusted access to digital identity for natural and legal persons that is portable across platforms, sectors, and borders. It addresses challenges at national and international levels to implement this ambition, including public perception, user experience and adoption, data sharing, interoperability, liability, data privacy and security, governance, and international cooperation. The Recommendation does not focus on technical aspects or imply changes to the nature of any domestic identity systems.

***Next steps***

The PGC, through the E-Leaders Working Party, will serve as a forum for exchanging information and fostering multi-stakeholder dialogue on user-centred and inclusive digital identity systems, governance, and cross-border use. The discussions will support peer learning and propagate good implementation practices among Adherents.

The PGC will monitor activities and emerging trends around digital identity, provide guidance and tools to support implementation, and report to Council on the implementation, dissemination, and continued relevance of the Recommendation in 2028.

*For further information please consult: https://www.oecd.org/gov/digital-government/.*
*Contact information: eleaders@oecd.org.*

**THE COUNCIL**,

**HAVING REGARD** to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;

**HAVING REGARD** to the standards developed by the OECD in the area of electronic authentication, regulatory policy and governance, agile regulatory governance, international regulatory co-operation, protection of privacy and transborder flows of personal data, cross-border co-operation in the enforcement of laws protecting privacy, digital government strategies, cryptography policy, internet policy making, digital security, children in the digital environment, and open government;

**HAVING REGARD** to the technical standards developed by other fora, such as the European Committee for Standardization (CEN), European Telecommunications Standards Institute (ETSI), the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the United States National Institute of Standards and Technology (NIST) and the World Wide Web Consortium (W3C), as well as related work undertaken by the European Commission, the Financial Action Task Force (FATF), the United Nations Commission on International Trade Law (UNCITRAL), and the World Bank;

**RECOGNISING** that effective, usable, secure and trusted digital identity systems can enhance privacy, facilitate inclusion and simplify access to a wide range of services, and thereby contribute to social and economic value;

**RECOGNISING** that digital identity can transform the way service providers operate and interact with their users, both in-person and online, by providing an optional alternative to physical credentials as part of a seamless omni-channel experience;

**RECOGNISING** that the governance, design and implementation of digital identity systems should be rooted in democratic values and respect for human rights;

**RECOGNISING** the need to ensure the accessibility, affordability, usability, and equity of digital identity solutions for all, continually promoting the inclusion of vulnerable groups and minorities;

**RECOGNISING** that the rapidly evolving technology landscape creates the need for governments to regularly evaluate and assess the opportunities and risks of new technologies and architectural paradigms, including cost-benefit analyses as well as environmental, privacy, data protection, ethical and human rights impact assessments, complemented by open and transparent processes for mitigating the harms of any potential unintended consequences;

**RECOGNISING** that the deployment of digital identity systems can introduce risks, including fraud, identity theft, and cybercrime, as well as potential threats to human rights, privacy, and data protection;

**RECOGNISING** that both the public and private sector contribute to the success of digital identity systems, and that their roles and relative contributions in the digital identity ecosystem might be different across countries;

**RECOGNISING** that trust between the different actors of the digital identity ecosystem is critical for the proper functioning of digital identity, and should be underpinned by domestically appropriate policies and solutions, supported by relevant technical standards and technologies;

**RECOGNISING** that stakeholder engagement and consultation is essential to foster public trust in the digital identity system as a whole;

**RECOGNISING** that Members and non-Members having adhered to this Recommendation (hereafter the “Adherents”) have differing approaches to the development and refinement of their digital identity systems with different roles and contributions from the public and private sectors, varying underlying identity management systems (centralised, federated and decentralised) and links with civil registry systems,

legacy infrastructure, levels of digital maturity, existing digital identity adoption, trust between actors of the digital identity ecosystem, and public discourse about the role and nature of digital identity;

**RECOGNISING** that the different approaches taken by Adherents create a need for interoperability of secure and trusted digital identity systems across borders, which calls for international collaboration and the development, adoption, alignment or mapping of the use of technical standards to ensure that all users are always able to access essential services;

**RECOGNISING** the value of trust services such as electronic signatures, electronic time-stamps, and electronic seals to support the usability of digital identity solutions, including across borders, based on technical standards and regulatory frameworks, such as international agreements;

**RECOGNISING** that while the principles relating to the governance of digital identity for natural and legal persons should be the same, the use cases, user experience, challenges, and mechanisms for implementation will differ, including those relating to privacy and other potential issues;

**RECOGNISING** the relevance of international development co-operation for supporting the governance and funding of digital identity systems in low- and middle-income countries;

**CONSIDERING** that the governance of digital identity is a shared responsibility across branches and levels of government, and that therefore this Recommendation is relevant to all of them, in accordance with their national and institutional frameworks, some of which also provide for responsibilities of the private sector.

**On the proposal of the Public Governance Committee:**

**I.** **AGREES** that, for the purposes of the present Recommendation, the following definitions are used:

- **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;
- **Authentication** refers to a function for establishing the validity and assurance of a claimed identity of a user, device or another entity in an information or communications system;
- **Credential** refers to a set of one or more electronically recorded and verifiable assertions about a user made by a credential issuer, for example, a driver's licence, ID card, permit, or qualification. Some Adherents may refer to or understand the terms Attribute and Credential interchangeably, depending on their context;
- **Credential issuer** refers to any entity, public or private, that issues credentials to users;
- **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;
- **Digital identity ecosystem** refers to the different actors involved in the digital identity system, such as policymakers, regulators, government supervisory bodies, technical standards organisations, digital identity solution providers, credential issuers, service providers, civil society organisations, and users. The ecosystem may include different domain-specific solutions and their associated actors;
- **Digital identity lifecycle** refers to the series of stages and processes involved in the management of a digital identity from its creation to termination, including identity proofing, registration or enrolment, issuance, use, possible lost or theft, expiration or revocation, and maintenance or repair;

- **Digital identity solution** refers to a material and/or immaterial unit allowing users to store, retrieve and/or share attributes and/or credentials, and which is used for authentication for an online or offline service;
- **Digital identity solution provider** refers to any entity, public or private, that issues digital identity solutions to users;
- **Digital identity system** refers to the entirety of the system under which digital identity solutions, credentials and attributes are provided to users and relied upon by service providers, including the policies, regulatory frameworks, trust frameworks, technical standards, and roles and responsibilities;
- **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;
- **Service provider** refers to any entity, public or private, that relies on secure and trusted digital identity solutions for user authentication and verification of attributes and/or credentials, in order to provide their service, whether online or offline;
- **Trust framework** refers to a set of common requirements, including cybersecurity requirements, for digital identity solutions that digital identity solution providers follow for the purpose of facilitating trust within a digital identity ecosystem. The requirements can be divided into different Levels of Assurance (LoA);
- **User** refers to a natural person or a legal person, or to a natural person representing a natural or legal person. In cross-border scenarios, a user should be understood as a natural or legal person from another jurisdiction.

## Developing User-Centred and Inclusive Digital Identity

**II. RECOMMENDS** that Adherents **design and implement digital identity systems that respond to the needs of users and service providers**. To this effect, Adherents should:

1. Take into account the domestic context, including digital maturity and existing digital identity developments, when considering the design, implementation or iteration of a digital identity system;

2. Use service design methodologies to ensure that digital identity systems respond to the needs of users and achieve accessible, ethical, and equitable outcomes, particularly by:

   a) identifying the needs of users, service providers, and other affected parties;

   b) considering the end-to-end user experience of the digital identity lifecycle;

   c) measuring operational performance in order to iterate the digital identity system and solutions, as appropriate.

3. Encourage the development of digital identity solutions that are portable for users in terms of:

   a) location, including in-person, remotely, at all levels of government, and across borders;

   b) technology, including availability through the most convenient device, mobile form factors or communication medium and without being constrained by the speed or quality of internet connection;

   c) sector, to allow access to public services as well as the wider economy as appropriate.

4. Encourage the development of privacy-preserving and consent-based digital identity solutions that give users greater ownership over their attributes and credentials, and the ability to more easily and securely control what attributes and credentials they share, when, and with whom.

**III. RECOMMENDS** that Adherents **prioritise inclusion and minimise barriers to access to and the use of digital identity**. To this effect, Adherents should:

1. Promote accessibility, affordability, usability, and equity across the digital identity lifecycle in order to increase access to a secure and trusted digital identity solution, including by vulnerable groups and minorities in accordance with their needs;

2. Take steps to ensure that access to essential services, including those in the public and private sector is not restricted or denied to natural persons who do not want to, or cannot access or use a digital identity solution;

3. Facilitate inclusive and collaborative stakeholder engagement throughout the design, development, and implementation of digital identity systems, to promote transparency, accountability, and alignment with user needs and expectations;

4. Raise awareness of the benefits and secure uses of digital identity and the way in which the digital identity system protects users while acknowledging risks and demonstrating the mitigation of potential harms;

5. Take steps to ensure that support is provided through appropriate channel(s), for those who face challenges in accessing and using digital identity solutions, and identify opportunities to build the skills and capabilities of users;

6. Monitor, evaluate and publicly report on the effectiveness of the digital identity system, with a focus on inclusiveness and minimising the barriers to the access and use of digital identity.

## Strengthening the Governance of Digital Identity

**IV. RECOMMENDS** that Adherents **take a strategic approach to digital identity and define roles and responsibilities across the digital identity ecosystem**. To this effect, Adherents should:

1. Set out a long-term vision for realising the benefits and mitigating the risks of digital identity for the public sector and wider economy either in a dedicated strategy or as part of a broader strategy;

2. Secure national strategic leadership and delivery oversight and define and communicate domestic roles and responsibilities within the digital identity ecosystem;

3. Encourage co-operation and co-ordination between government agencies and competent authorities at all levels of government, as relevant and applicable;

4. Take steps to ensure that government agencies, and competent authorities at all levels of government, as well as other relevant actors, as applicable, take responsibility for stewarding, monitoring, and protecting the digital identity ecosystem, including by safeguarding the rights of users, and prioritising inclusion;

5. Promote collaboration between the public and private sectors by supporting the development of a healthy market for digital identity solutions, as appropriate, that encourages innovation and competition and explores the potential value of alternative models and technologies;

6. Establish a national or regional trust framework, or where applicable, align with relevant regional trust frameworks, to set out common requirements, including cybersecurity requirements, against different Levels of Assurance (LoA) for digital identity solutions that digital identity solution providers can follow to facilitate trust within the digital identity ecosystem;

7. Establish clear responsibilities for the regulation and oversight of digital identity systems, such that the rights of users and affected parties are protected and that adequate and effective mechanisms for dispute resolution, redress and recovery are in place;

8. Promote a sustainable and resilient digital identity system by taking into account the environmental impact of technology choices, and the need for ongoing investment to reflect the costs for all relevant actors throughout the digital identity lifecycle;

9. Oversee the digital identity system to adapt to new needs, threats, risks and opportunities.

**V. RECOMMENDS** that Adherents **protect privacy and prioritise security to ensure trust in digital identity systems**. To this effect, Adherents should:

1. Recognise security as foundational to the design of trusted digital identity systems and ensure that digital identity solution providers and solutions comply with all relevant requirements, in a manner that is consistent with defined Levels of Assurance (LoA) and/or is consistent with a risk-based approach, to protect users, service providers, and societies, including from possible identity theft or alteration;

2. Treat user control, privacy and data protection as fundamental tenets of digital identity systems, and encourage the adoption of privacy-by-design and privacy-by-default approaches that include informed consent, integrity, confidentiality, selective disclosure, purpose specification, as well as collection and use limitations regarding personal data, including by considering the need for specific standards and mechanisms to protect against the misuse of special categories of personal data, including biometric data;

3. Prevent the aggregation of datasets between services or the retention of unnecessary personal data trails being left when users use digital identity solutions to access different services;

4. Enforce accountability obligations under existing data protection and privacy laws;

5. Introduce robust arrangements to ensure that any attributes and credentials shared through a digital identity solution are accurate, complete, kept up-to-date, and relevant;

6. Identify the specific needs concerning how to safely accommodate and protect children and vulnerable groups and minorities in the design and use of digital identity systems;

7. Consider taking steps to establish legally recognised mechanisms, as deemed necessary, by which users can use digital identity solutions to mandate someone, or delegate representation rights, to act on their behalf in a manner that is visible to, manageable for, and traceable by, the user;

8. Promote the use of open standards and open-source software in the design of the digital identity system and other relevant actions to mitigate the risks to users, service providers and societies associated with dependency on any single hardware or software vendor.

**VI. RECOMMENDS** that Adherents **align their legal and regulatory frameworks and provide resources to enable interoperability**. To this effect, Adherents should:

1. Ensure that, as appropriate, domestic policies, laws, rules and guidelines for the digital identity system cover issues such as governance, liability, privacy, resilience and security, to encourage and facilitate interoperability and portability in terms of location, technology and sector;

2. Ensure that digital identity solutions are technology and vendor neutral as long as they comply with all relevant security requirements, and promote the use of internationally recognised technical standards and certification;

3. Provide access to a catalogue of resources intended to support service providers onboard with the digital identity system such as common technical components, documentation or relevant technical support as appropriate;

4. Support the creation of mechanisms, such as regulatory sandboxes, to provide a secure and controlled environment in which to explore the risks and opportunities of emerging technologies, and/or updates to digital identity systems that might affect interoperability;

5. Monitor and report on compliance with existing domestic rules and internationally recognised technical standards across the digital identity ecosystem, as appropriate.

**Enabling Cross-Border Use of Digital Identity**

**VII. RECOMMENDS** that Adherents **identify the evolving needs of users and service providers in different cross-border scenarios**. To this effect, Adherents should:

1. Identify the priority use cases for cross-border interoperability of digital identity systems according to their context and the experience of their users by identifying the activities that require the sharing of attributes and/or credentials in a different jurisdiction;

2. Co-operate internationally to identify the needs of service providers in other jurisdictions for recognising, integrating and trusting a digital identity solution;

3. Identify the risks associated with the cross-border interoperability of digital identity systems and associated use cases, and adopt mitigation measures as necessary.

**VIII. RECOMMENDS** that Adherents **co-operate internationally to establish the basis for trust in other countries' digital identity systems and issued digital identities**. To this effect, Adherents should:

1. Designate a national point of contact to engage as appropriate and applicable with international counterparts and activities in support of cross-border digital identity;

2. Engage in international regulatory co-operation to enable cross-border interoperability of digital identity systems, such as by assessing and/or mapping the coherence, compatibility or equivalence of existing legal requirements, trust frameworks and technical standards, exploring collaboration through free trade agreements, and identifying opportunities for cross-border regulatory experimentation;

3. Engage in bilateral and multilateral co-operation in collaboration with relevant stakeholders from across the digital identity ecosystem by participating in international technical standards work, exchanging experiences and best practices, and aligning innovation programmes;

4. Ensure that the cross-border interoperability of digital identity is not used to unduly discriminate against foreign users in their access to essential services or commercial transactions;

5. Work towards clarifying the basis for liability related to the use of digital identity in cross-border transactions;

6. For cross-border public services, enable, as appropriate, the matching of identity attributes stored in a particular public sector body abroad with the attributes or information shared about the user through the digital identification process, to ensure matching between the identity and digital identity of the user trying to access the service;

7. Produce a roadmap scoping out steps that would be needed to enable:

   a) domestically recognised digital identity solutions and associated attributes and credentials to be used internationally;

b) digital identity solutions and associated attributes and credentials from other countries to be recognised domestically.

**IX.** **CALLS ON** all actors in the digital identity ecosystem to implement or, as appropriate according to their role, support and promote the implementation of this Recommendation.

**X.** **INVITES** the Secretary-General to disseminate this Recommendation.

**XI.** **INVITES** Adherents to disseminate this Recommendation at all levels of government.

**XII.** **INVITES** non-Adherents to take account of and adhere to this Recommendation.

**XIII.** **INSTRUCTS** the Public Governance Committee to:

a) serve as a forum for exchanging information on the implementation of this Recommendation, fostering multi-stakeholder dialogue on user-centred and inclusive digital identity systems, the governance of digital identity systems, and cross-border use of digital identity for accessing public and private sector services;

b) monitor activities and emerging trends around digital identity which may impact the implementation of this Recommendation, through relevant data collection, analysis, and dissemination of results to Adherents;

c) develop the processes, guidance and tools to support the implementation of this Recommendation; and

d) report to Council on the implementation, dissemination and continued relevance of this Recommendation no later than five years following its adoption and at least every ten years thereafter.

# Related documents

## EXPLANATORY NOTE[1]

*Prior work carried out by the OECD related to digital identity*

The OECD Recommendation on the Governance of Digital Identity was developed building on work carried out by the OECD related to digital identity over many years.

The OECD's Committee on Digital Economy Policy (CDEP) developed several key documents and standards relating to electronic authentication. In 2004, the report *Summary of Responses to the Survey of Legal and Policy Frameworks for Electronic Authentication Services and E-Signatures in OECD Member Countries* identified gaps and commonalities across jurisdictions with different legal and regulatory approaches. In 2005, the report *The Use of Authentication across Borders in OECD Countries* gave a focus to the opportunities for cross-border use of authentication methods in OECD Member countries, including information on factors that were identified as promoting or hampering the national use of authentication technologies and digital signatures. These reports provided the basis for the Council to adopt the 2007 *Recommendation on Electronic Authentication* (hereinafter "the 2007 Recommendation"), recalling the *OECD Guidance for Electronic Authentication* to assist OECD Members in developing effective and compatible approaches to electronic authentication, both at the national and international level.

In 2008, the *Declaration for the Future of the Internet Economy* (The Seoul Declaration) saw OECD Members and a number of non-Members commit to strengthen confidence, trust, and security through policies that ensure the protection of digital identities on Internet and interconnected digital networks. The following year, *The Role of Digital Identity Management in the Internet Economy* provided a brief introduction to digital identity management and then in 2011, the report on *Digital Identity Management for Natural Persons* included guidance for policymakers building on the results of a comparative analysis of national strategies for digital identity management in OECD Member countries.

This Recommendation complements the work of CDEP with the work carried out by the OECD's Public Governance Committee (PGC) since 2003, when OECD e-Government and Digital Government reviews included brief country-specific assessments of digital identity systems. The report *Digital Government in Chile - Digital Identity* provided the first comprehensive country-specific assessment of an OECD Member's digital identity system. The study compared the approach to digital identity in Chile to 13 countries, using an analytical framework considering the existing national identity infrastructure, policies and governance, technical solutions, adoption, and the approach to data, transparency, and measurement. The *OECD Digital Government Policy Framework – Six Dimensions of a Digital Government* provides the basis for measuring digital government maturity through the Digital Government Index and identified digital identity as a core part of the digital public infrastructure that enables the transformation of public services through digital technologies.

In 2018, the Working Party of Senior Digital Government Officials (the "E-Leaders Working Party") convened an informal thematic group dedicated to digital identity. The work of this group has contributed to developing a deeper understanding of how to implement and expand digital identity as a service and enable citizen-initiated sharing of their information and data.

The principles of the OECD Guidance on Electronic Authentication, and thus the scope of the 2007 Recommendation, relate to the authentication of electronic communication in its broadest sense. The

[1] This explanatory note was prepared by the Secretariat. The opinions expressed and arguments employed in this explanatory note do not necessarily reflect the official views of OECD Member countries.

Guidance defines authentication as "a function for establishing the validity and assurance of a claimed identity of a user, device or another entity in an information or communications system." Well-functioning electronic authentication and the acceptance of authentication solutions are an important part of any digital identity system used by any actor. However, these efforts were conducted in a period where a fully joined up system was still some way off in terms of technology and governance. Today, governments need to consider how to put in place the necessary governance framework, to deliver a comprehensive identity ecosystem that allows easy and secure access to a full range of public and private services in a way that is tailored to the needs of individuals and businesses.

As such, this Recommendation seeks to address the wider issues involved in the governance of digital identity systems and provides guidance acknowledging the important interplay between electronic authentication and digital identity for trusted digital transactions, while focusing on the governance of electronically captured and stored attributes and/or credentials that can be used to prove a feature, quality, characteristic, or assertion about a natural or legal person, and, when required, support the unique identification of that natural or legal person. It does not cover the identity of services, objects or goods, including Internet-of-Things (IoT) devices, or electronic authentication per se, which is of more relevance for the CDEP community and the existing 2007 Recommendation.

*Work carried out by other international organisations and fora*

The discussion about digital identity is globally resonant and has been the focus of several other international organisations and fora. The activities of the European Committee for Standardization (CEN), European Telecommunications Standards Institute (ETSI), European Union (EU), Financial Action Task Force (FATF), G20, GovStack, International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), National Institute of Standards and Technology (NIST), United Nations Commission on International Trade Law (UNCITRAL), the World Bank, and World Wide Web Consortium (W3C) have covered both policy and technical standardisation.

- **CEN**: CEN is one of three bodies officially recognised by the EU in setting standards within Europe. CEN supports standardization activities in relation to a wide range of fields and sectors. Of most relevance to this draft Recommendation is the work providing standards for strengthening the interoperability and security of personal identification and related personal devices, systems, operations and privacy in a multi sectorial environment.
- **ETSI**: ETSI is one of three bodies officially recognised by the EU in setting standards within Europe. ETSI's focus is on technical standards for telecommunications, broadcasting and electronic communications networks and services. It has produced several standards relevant to this draft Recommendation, such as on requirements for identity proofing (*ETSI TS 119 461 V1.1.1 (2021-07)*; *ETSI TR 119 460 V1.1.1 (2021-02)*) and requirements for accessibility of ICT products and services (*EN 301 549 V3.2.1, (2021-03)*; *EN 301 549 V1.1.2 (2015-04)*);
- **EU**: The *Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS regulation)* adopted on 23 July 2014 is a prominent example of a cross-border legal framework that supports trusted recognition of digital identities. In June 2021, the European Commission published a *proposal for a regulation to amend the current eIDAS regulation and establish a framework for a European Digital Identity* that includes provisions to foster greater cross-sectoral and cross-border usability within the EU single market and to allow citizens to take greater control over their data. This is critical in relation to the Commission's *Digital Decade Policy Programme 2030* that sets out a number of targets and milestones, including that by 2030, all key public services should be available online, all citizens will have access to electronic medical records; and all citizens should have use of an eID solution;
- **FATF**: In 2020, FATF issued *Guidance on Digital Identity* in support of global requirements on anti-money laundering, countering the financing of terrorism and proliferation of weapons of mass destruction. It provides guidance on how to use a risk-based approach to using digital identity solutions to conduct customer identity verification at onboarding and to support other

elements of Customer Due Diligence, leveraging the digital identity technical standards and policy frameworks developed by NIST and the EU;

- **G20**: The 2018 *G20 Digital Identity Onboarding* developed under the Argentinian Presidency analysed the role that ID systems, with a particular focus on digital ID, can play in enhancing financial access and inclusion. The 2021 *Declaration of the G20 Digital Ministers* welcomed the *"emphasis on secure, interoperable and trusted digital identity solutions that can provide better access to public and private sector services while promoting privacy and personal data protection"*. The Declaration was informed by the OECD report *G20 Collection of Digital Identity Practices* developed in collaboration with the G20 Digital Economy Taskforce. The OECD has continued to provide support for the digital identity agenda to the G20 during Indonesia's Presidency in 2022 with the *G20 Digital Economy Ministers' Meeting Chair's Summary* noting *"the importance of continuing the discussion on the use and development of interoperable digital identity frameworks in alignment with the human-centric approach in facilitating digital identity solutions that respect human rights, including the right to be free from arbitrary or unlawful interference with privacy.";*
- **GovStack:** The GovStack initiative is a multi-stakeholder initiative focused on promoting the use of interoperable and reusable building blocks for digital services led by the German Federal Ministry for Economic Cooperation and Development, (Gesellschaft für Internationale Zusammenarbeit, GIZ) the Estonian Ministry of Foreign Affairs, the International Telecommunication Union (ITU) and the Digital Impact Alliance (DIAL). The initiative has developed specifications focused on *identity and verification*.
- **ISO and IEC**: The ISO and IEC have developed several technical standards relevant for the design, development and maintenance of digital identity including *ISO/IEC 29115:2013 Information Technology – Security techniques – Entity authentication assurance framework*, *ISO/IEC 24760-1:2019 A framework for identity management – Part 1: Terminology and concepts* and all the standards associated with physical identity cards, the technology in smartcards and handling of biometrics;
- **NIST**: Although this organisation operates as part of the United States Department of Commerce, NIST is globally influential, particularly in terms of standardising the approach to defining and applying Levels of Assurance (LoA). These are contained in *NIST Special Publication 800-63-3, Digital Identity Guidelines*, which was most recently revised in 2017;
- **UNCITRAL**: Since 2015, UNCITRAL has conducted preparatory work on legal aspects of identity management and trust services. Following the drafting efforts by the Working Group IV (Electronic Commerce) of the Commission, the *Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services* was adopted in 2022, with a view to promote uniformity in the development and application of operational rules, policies and practices for identity management in the context of commercial activities and trade-related services;
- **World Bank**: The World Bank has played a significant role in supporting the global development of digital identity systems through policy advice and standards development, especially in its stewarding of the Identity for Development (ID4D) initiative. In 2018, the World Bank supported the G20 in analysing the role of digital identity systems in enhancing financial access and inclusion through the report *G20 Digital Identity Onboarding*. In 2021, the World Bank published the *Principles on Identification for Sustainable Development: Toward the Digital Age*. The Principles have been endorsed by 30 different organisations, including Digital Nations, UNHCR, UNDP, UNICEF, GSMA, and ITU. In 2023, the World Bank published a *How-to Note on Mobile Government*, highlighting the increasing ubiquity of access to mobile networks and the role of mobile digital identity solutions as a route to increasing inclusion and access to services;
- **W3C**: The goal of the W3C is to develop guidelines, protocols and technical standards which support the World Wide Web. In this regard, the W3C has a keen interest in digital identity and

most recently has provided leadership with respect to decentralised identity in developing a *Recommendation on Decentralized Identifiers (DIDs)*. A DID refers to any subject (e.g., a person, organisation, thing, data model, abstract entity, etc.) as determined by the controller of the DID. Unlike typical, federated identifiers, DIDs are designed so that they may be decoupled from centralised registries, identity providers, and certificate authorities.

## About the OECD

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD Member countries are: Australia, Austria, Belgium, Canada, Chile, Colombia, Costa Rica, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

## OECD Legal Instruments

Since the creation of the OECD in 1961, around 460 substantive legal instruments have been developed within its framework. These include OECD Acts (i.e. the Decisions and Recommendations adopted by the OECD Council in accordance with the OECD Convention) and other legal instruments developed within the OECD framework (e.g. Declarations, international agreements).

All substantive OECD legal instruments, whether in force or abrogated, are listed in the online Compendium of OECD Legal Instruments. They are presented in five categories:

- **Decisions** are adopted by Council and are legally binding on all Members except those which abstain at the time of adoption. They set out specific rights and obligations and may contain monitoring mechanisms.

- **Recommendations** are adopted by Council and are not legally binding. They represent a political commitment to the principles they contain and entail an expectation that Adherents will do their best to implement them.

- **Substantive Outcome Documents** are adopted by the individual listed Adherents rather than by an OECD body, as the outcome of a ministerial, high-level or other meeting within the framework of the Organisation. They usually set general principles or long-term goals and have a solemn character.

- **International Agreements** are negotiated and concluded within the framework of the Organisation. They are legally binding on the Parties.

- **Arrangement, Understanding and Others**: several other types of substantive legal instruments have been developed within the OECD framework over time, such as the Arrangement on Officially Supported Export Credits, the International Understanding on Maritime Transport Principles and the Development Assistance Committee (DAC) Recommendations.