Organisation for Economic Co-operation and Development

C/MIN(2023)8

For Official Use **English - Or. English**

30 May 2023

COUNCIL

Meeting of the Council at Ministerial Level, 7-8 June 2023

DRAFT RECOMMENDATION OF THE COUNCIL ON THE GOVERNANCE OF DIGITAL IDENTITY

JT03520019

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; and
    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; and
    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; and
    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.