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.