Financial Action Task Force

FATF/PDG(2019)3/REV1

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

4 June 2019

Policy Development Group

DRAFT GUIDANCE ON DIGITAL IDENTITY

17 - 18 June 2019, Wyndham Orlando Resort International Drive, Orlando, Florida, USA

Issue: How do the CDD requirements in R.10 apply in the context of digital identity systems and solutions?

Action: Provide preliminary views on the Draft Guidance and approve the next steps until October 2019.

FATF-XXX
Please bring this document with you to the meeting, as no paper copies will be available at that time.
This document is for Official Use by FATF members and observers only. This document must not be made publicly available, or distributed to third parties, without prior authorisation from the FATF.

Tom NEYLAN, Tel.: +(33-1) 45 24 98 53, Tom.NEYLAN@fatf-gafi.org
Shana KRISHNAN, Tel.: +(33-1) 85 55 60 03, Shana.KRISHNAN@fatf-gafi.org

JT03448395

Digital Identity – Draft Guidance

Discussion paper

Issue:	How do to the CDD requirements in R.10 apply in the context of digital identity systems and solutions?
Action & Recommendations:	1. Provide preliminary views on the Draft Guidance (**Annex A**), including on the following issues: a. Definition of legal identity b. Categorisation of digital IDs (depending on provision by the government or the private sector, or level of government authorisation of the scheme) c. Discussion of risk-based approach set out in the Guidance (Section V) d. General feedback– scope, structure, level of detail, areas for further work etc. 2. Approve the next steps for the project (Draft Guidance to be approved for consultation in October and adopted in February 2020).
Timing:	PDG does not need to approve text at this meeting but a discussion on the above issues will assist the Project Team to finalise the report by October and determined the course of required private sector consultation.

Background

1. PDG decided to conduct policy work on digital identity (ID) in February 2018 in order to clarify the application of FATF Standards in relation to the use of digital forms of identification for CDD purposes.[1] The Guidance is intended to address two main questions:

- What are the principal requirements for digital ID for it to be considered as "reliable and independent sources" of identification?
- Under what circumstances can digital ID be used by financial institutions/DNFBPs and what are the risk factors that need to be considered?

2. In October 2018, PDG decided that the Guidance should focus on the reliability and independence features of digital IDs, and describe potential risks as well as opportunities for their mitigation in that context. PDG also agreed that the Guidance should mainly deal with the requirements under Recommendation 10, leaving Recommendations 11 and 17 out of scope.[2]

3. In February 2019, PDG agreed in principle on the direction and the scope of the paper. There was a consensus that digital IDs issued by the government or in the framework of a government-endorsed process should be the primary focus of the paper, noting that, there should be flexibility to accept private-issued IDs on a risk-sensitive basis. PDG asked that the paper include definitions of the concepts used in the digital ID context, describe potential risks (such as impersonation attacks) as well as the relevant mitigation measures, and provide more use cases.

[1] See FATF/PDG(2018)13; FATF/PDG(2018)20 and FATF/PDG(2019)3 for further reference.

[2] FATF/PLEN/RD(2018)20

Progress made

4. Following the PDG meeting in February 2019, co-leads were selected (the United States and the World Bank) and a project team formed.[3] Building on the outline approved by PDG in February 2019, the co-leads provided the substantial input for the Draft Guidance at Annex A, with members of the project team providing relevant case studies.

5. The Private Sector Consultative Forum also in May 2019 provided an opportunity to seek early feedback from the private sector from their perspective as: (1) providers of digital ID services, or (2) users of digital ID services for CDD purposes. The co-leads identified several private sector experts as being able to add significant value to the project moving forward.

6. The Draft Guidance includes a substantial amount of new content which is preliminary text and has not yet been subject to a round of comments by the project team. The Secretariat has provided preliminary edits to simplify the content but further editorial and consistency checks need to be undertaken. Some conceptual issues have arisen in the drafting of the guidance which are outlined below.

Issues for discussion

A. Definition of legal identity

7. There is no generally accepted definition of legal identity and the FATF has not previously defined this concept in the context of traditional documentary ID. Various sources recognise that legal identity is difficult concept to define. There are two alternative descriptions of legal identity provided by the co-leads:

> ***United States (US)**: For the purposes of this Guidance, legal identity is the specification of a unique natural (or legal) person that is: (1) is based on certain pre-specified characteristics (identifiers or attributes) of the person that are intended to establish the person's uniqueness in the population or particular context(s); (2) is recognised by the state under national law; and (3) is used to ascribe legal rights and duties to that person, such as the right to obtain access to certain regulated financial products and services or to obtain certain government benefits and services, or the obligation to pay taxes or serve in the military. Legal identity provides the basis for a person's ability to enforce his/her rights under national law, and to satisfy government requirements for certain activities.*
>
> ***World Bank** (on behalf of the United Nations Legal Identity Expert Group - UN LEIG[4]): Legal identity is defined as the basic characteristics of an individual's identity. e.g. name, sex, place and date of birth conferred through registration and the issuance of a certificate by an authorised civil registration authority following the occurrence of birth. In the absence of birth registration, legal identity may be conferred by a legally-recognised identification authority; this system should be linked to the civil registration system to ensure a holistic approach to legal identity from birth to death.*

[3] United States (co-lead), World Bank (co-lead), Belgium, China, European Commission, Netherlands, Sweden, Switzerland & United Kingdom.

[4] This definition has not yet been put to UN Member States. It is the result of over a year of negotiation by 15 international bodies and the World Bank.

8. While there are a lot of similarities in these definitions, some of the key differences are that:

- The US definition focuses on the 'specification of a unique person' (based on certain characteristics) whereas the UN LEIG definition focuses on 'the basic characteristics of a person' themselves.
- The US definition has been developed with the FATF Guidance in mind while the UN LEIG is broader definition that is suited to a variety of contexts. References to birth or other registration in the UN LEIG definition link to development outcomes, namely Sustainable Development Goal 16.9 which calls for states to provide 'legal identity for all, including birth registration'.
- The UN definition does not reference the rights that ensue from being granted a legal identity (the third limb of the US definition) as they do not want to link concepts of nationality/citizenship with legal identity. The US included text in the chapeau of the definition to de-link the concept of legal identity and citizenship.

9. While it is not strictly necessary for the FATF to develop a definition, it may have an impact on the scope and application of Section V of the Draft Guidance and how we define 'legal identity' could also impact financial inclusion and development initiatives. Delegations are invited to provide views on this issue, including definitions used in a domestic context. As specialist expertise is required to come to a conclusion on this topic, the Secretariat proposes to gather initial views from PDG and consult further with experts prior to proposing a definition for the purposes of this Guidance.

B. Categorisation of public and private sector digital ID systems/solutions

10. The Secretariat seeks delegations' views on the categorisation of digital ID systems/solutions. The text in the Draft Guidance aligns with the outline provided to PDG in February and draws the distinction between digital ID solutions based on whether the government or the private sector is the *provider* of the system (either the technical solution itself or the broader framework for the solution) (see paragraphs 53-65 of Annex A).

11. The World Bank has provided an alternative, which suggests delineating the categories based on whether the digital ID solution is *recognised* by the government or not. Under this alternative, a digital ID is government recognised if it provides proof of identity for official, government transactions. While the authoritative sources for these systems are typically (though not necessarily) government-operated, the digital ID infrastructure itself—including credentials and authentication—may be provided through multiple arrangements. See **Annex B** for an outline of this alternative.

12. A third another option suggested by a member of the project team and envisaged in earlier outlines for this Draft Guidance, is to have three categories of solutions: (1) purely government systems, (2) public and private solutions (including a spectrum of different options for public and private sector involvement), and (3) purely private sector solutions.

13. The categorisation of the digital ID systems/solutions is linked to how they are treated under Section V, therefore it is important to have an understanding of the key factors that impact how the risk based approach to digital ID is applied. The categorisation should also be broad and flexible enough to capture the range of solutions that exist today, and could come into fruition in the future. Lastly, how the FATF defines these categories (and applies the risk based approach set out in Section V) could impact on how the private sector develops solutions in their field and the role and involvement of the government in those solutions.

C. Risk-based approach to digital ID for CDD purposes

14. Sections IV and V address the main questions this guidance is intended to answer. Section V sets out a two-component RBA assessment for the use of digital ID in CDD: (1) an assessment to technical reliability, and (2) an assessment of the level of technical reliability required in the context of the risks that the customer, product, jurisdiction etc., presents.

15. The RBA assessment varies depending on: (1) whether the digital ID is government-provided or certified for use in CDD, and (2) whether the regulated entity has options in terms of the digital ID solutions it can use and whether those solutions propose products with different levels of technical reliability.

16. Regulated entities that use digital ID systems/solutions which are government-provided or certified can assume they are technically reliable (i.e. they do not have to undertake component one of the RBA assessment). In this sense, the Draft Guidance is consistent with the decision in PDG in October 2018 that digital IDs that are issued on the basis of a process agreed, regulated or supervised by a national authority should be treated in the same manner as the traditional documentary ID.

17. The Secretariat seeks delegation views on whether the approach set out in Section V of the Draft Guidance maintains parity in the treatment of digital ID vis-à-vis traditional documentary ID under the FATF Standards.

D. General Feedback

18. The Secretariat invites delegations to provide initial views on the Draft Guidance, highlighting in particular:

- This version of the guidance includes more practical examples but further examples could be included in relation to the types of digital ID solutions that exist, how they are being applied to CDD and the application of the RBA. These examples could come from FATF members, FSRB members, other international standard setting bodies and the private sector.
- Whether Section III strikes the right balance between technical precision and accessibility to a wide audience, including non-digital ID experts (noting that a level of technical understanding is required for the application of a risk-based approach to digital ID).
- Whether Section IV could benefit from a more sophisticated analysis of the risks associated with digital ID and how these products are being exploited by bad actors and whether RTMG could add value to this portion of the Guidance.
- Potential areas where further work is required include describing levels of government certification/supervision/regulation and addressing issues of ultimate responsibility in case of a breach of the integrity of the digital ID solution which are not addressed in the current draft.
- The scope of the guidance covers digital ID for natural persons and does not include the range of solutions being developed for legal persons.

Next steps

19. The suggested next steps are set out in Table 1 below. The Secretariat proposes to seek two rounds of comments from delegations prior to finalising a consultation draft for consideration in October 2019.

20. The project team has highlighted the importance of consulting with private sector experts. The Secretariat proposes two forms of private sector consultation. Firstly, consultation with a small group of digital ID experts from the private sector and other international standard setting bodies, between June and October 2019, to gather more use-cases and practical examples for the Draft Guidance. The group would be formed using the list of experts developed for the Private Sector Consultative Forum, augmented by project team and delegations' nominations. A broader consultation could take place after October 2019, particularly to seek the views of regulated entities on the implementation of the RBA and to mitigate against any unintended negative impact on financial innovation and financial inclusion initiatives.

Table 1. Indicative timeline for completion of the Guidance

Delegations provide high-level written feedback on draft guidance and co-leads/project provide any additional material to the Secretariat.	14 July 2019
Secretariat circulates revised Guidance to delegations and small group of private sector experts	9 August 2019
Delegations provide comments on revised draft guidance	13 September 2019
Circulate final draft guidance to delegations	27 September 2019
FATF Plenary	14-18 October 2019
Consultation with private sector on the guidance, any final changes presented to PDG in February 2020.	October 2019 – February 2020

Annex A. Draft Guidance on Digital Identity

I. INTRODUCTION

1. The Financial Action Task Force (FATF) is committed to ensuring that the global standards encourage responsible financial innovation. In this regard, the FATF supports the use of new technologies in the financial sector to strengthen the implementation of anti-money laundering/counter financing of terrorism (AML/CFT) objectives and financial inclusion goals.[5]

2. A series of outreach events on financial innovation (FATF's FinTech/Regtech initiative) highlighted that the rapid pace of innovation in the digital identity (ID) space has reached an inflection point. The technology, processes, and technical standards have evolved to a point where trustworthy digital ID solutions are commercially available at scale. Some of these relevant technologies include: more reliable, lower-cost biometric technology (including fingerprints; facial recognition; iris scans); the near-ubiquity of the Internet and mobile phones (and the wide use of 'smart phone' technology); digital device identifiers (e.g., IP addresses, mobile phone numbers, SIM cards and GPS location); behavioural biometrics; high-definition scanners (for scanning drivers licenses and other identity documentation); high-resolution video transmission (allowing for more trustworthy remote identification and verification); artificial intelligence/machine learning (e.g., for determining validity of government-issued documentary identity evidence); and, potentially, Distributed Ledger Technology.

3. Digital ID solutions that meet high technical standards hold great promise for improving the trustworthiness, security, privacy and convenience of identifying natural and legal persons in a wide variety of settings, such as banking, health, and e-government in the global economy of the digital age.

4. In the financial sector, trustworthy digital ID solutions could improve customer on-boarding and authorising account access; facilitate other customer due diligence (CDD) measures; and strengthen AML/CFT compliance, general risk management and anti-fraud efforts. They also have potential to generate cost savings and efficiencies for financial services firms.

5. Trustworthy digital ID solutions can significantly contribute both to efforts to combat ML/TF and to increase financial inclusion. In light of this recognition, the FATF has developed this Guidance to clarify how digital ID solutions can be used to comply with specific AML/CFT requirements under its standards.

Legal Identity

6. Identity is a complex concept with many meanings. For FATF's purposes, identity refers to legal or official identity, which is distinct from broader concepts of personal and social identity, which may be relevant for unofficial purposes (e.g., unregulated commercial or social, peer-to-peer interactions in person or on the Internet).

[5] See the FATF's position on *FinTech and RegTech* (November 3, 2017), available at http://www.fatf-gafi.org/publications/fatfgeneral/documents/fatf-position-fintech-regtech.html.

7. For purposes of this Guidance, **legal identity** is the specification of a unique natural or legal person that: (1) is based on certain pre-specified characteristics (identifiers or attributes) of the person that are intended to establish the person's uniqueness in the population or particular context(s); (2) is recognised by the state under national law; and (3) refers to a status that ascribes legal rights and duties to that person.

8. **Proof of legal identity** generally depends on some form of officially recognised registration, documentation or certification (e.g., a birth certificate, identity card or digital identity credential) which sets out evidence of core identifiers or attributes of ID (e.g., name, sex, place and date of birth) for establishing and verifying legal identity.[6]

9. There are two types of legal ID: ***universal/foundational identity*** or ***functional identity***. **Universal/foundational ID** is used for all legal identity purposes in a jurisdiction and is provided by (or on behalf of) the government (typically, national identity cards or numbers). **Functional ID** is intended to be used for a particular, limited purpose(s) such as tax administration; access to specific government benefits and services; access to medical services and personal health records; voting; authorisation to operate a motor vehicle; and (in some jurisdictions) access to financial services. Functional ID evidence (credentials) include, e.g., taxpayer identification numbers; driver's license numbers; passport numbers; voter registration cards; social security or in-kind subsidy ration cards.

10. In the exercise of their sovereignty, national governments specify the required attributes, evidence and proofing process required to prove legal identity. They can use either prescriptive, rules-based criteria or criteria that is principles-, performance-, and/or outcomes-based The latter approach, which is more flexible, enables jurisdictions to better future-proof the requirements for proving legal identity (identification/verification), given the rapid evolution of digital ID technology and related technical standards.

11. As reflected by the UN's sustainable Development Goals,[7] official birth registration ideally provides the basis of legal identity for individuals. However, proof of legal identity does not necessarily require birth registration. Providing legal identity is conceptually distinct from civil registry and vital statistics (CRVS) functions. Other reliable forms of official recognised registration and documentation/certification can provide evidence of core attributes required to prove legal identity. This is particularly important for providing legal identity solutions in developing countries that do not yet have adequate civil registry and vital statistics (CRVS) and cannot provide official birth registration and documentation for most natural persons in the jurisdiction. In such situations, official government registration could take the form of registration of an individual in a government-provided identity system, based on biometrics and biographical information obtained during the enrolment process, and documentation/credentialing that fixes the individual's unique identity at the point of identity registration and credentialing. Alternative forms of official identity registration and documentation are also relevant for providing legal identity evidence for forcibly displaced persons (FDPs), such as refugees, who may have lost or lack access to their official home country identity documentation. [8]

[6] In the case of refugees, host countries are primarily responsible for issuing proof of legal identity, including identity papers. The issuance of proof of legal identity to refugees may also be administered by an internationally recognised and mandated authority: 1951 Convention on the Status of Refugees, Article 25.

[7] Sustainable Development Goal (SDG) Target 16.9 requires countries to "By 2030, provide legal identity for all, including birth registration."

[8] For example, with the consent of host countries, the UN Human Rights Commission (UNHCR) may provide identity registration and certification/documentation (credentials) for refugees when host countries when host countries do not do so.

Box 1. India's Universal ID (UID) number

India's Universal ID (UID) number—or Aapka Aadhaar (henceforth, Aadhaar) identity program has provided a model for other developing countries on using biometrics and available biographic information, as well as official identity documentation where it exists, to build national digital ID systems that can overcome obstacles, including lack of birth certificates and other identity documentation as source evidence. The Unique Identity Authority of India (UIDAI) enrolment process does not necessarily depend on pre-existing birth registration or other official civil registration and documentation.

At enrolment, UIDAI accepts specific government Proof-of-Identity and Proof-of-Address documents as evidence of core attributes, including: an election photo ID card, Ration card, passport, driving license, and a photo ID PAN card. Proof-of-Address documents also include water, electricity, or telephone bills from the preceding three months. However, if an individual does not have any of this evidence, UIDAI also accepts a Certificate of Identify with a photo, issued by a Gazetted Officer or Tehsildarn (i.e., a tax official) on letterhead, as valid Proof-of-Identity. Alternative Proof-of-Address can be provided by a Certificate of Address with a photo, issued by a Gazetted Officer, Tehsildar, a member of Parliament, or a member of a state legislative assembly on letterhead, or by Village Panchayat head (i.e., local government official) or its equivalent authority (for rural areas).

If a family member does not have individual valid documents, the individual can still enrol in Aadhaar if his/her name exists in a family entitlement document and the Head of Family in the entitlement document enrols in Aaadhar, using valid Proof-of-Identity and Proof-of-Address documents. The head of the household can then introduce other members in the family while they are enrolling. UIDAI accepts eight document types as Proof of Relationship. Where no documents are available, a resident may also use Introducers notified by the Registrar, who are available at the enrolment centre.

Aadhaar is also noteworthy for providing legal identity to all residents above a specified age, and not restricting Aadhaar numbers to citizens.

Basic Types of Digital ID Products and Services

12. ***Digital* legal identity products and services** (referred to in this Guidance as digital ID) use electronic means to unambiguously assert and authenticate a person's unique legal identity in online (digital) and/or in-person environments. Digital ID solutions may rely on various types of technology, and may use digital technology in various ways, including:

- Electronic databases to obtain, confirm, store and/or manage identity evidence
- Electronic credentials to authenticate identity for accessing mobile, online, and offline applications
- Digital biometrics to identify and authenticate individuals, and
- Digital application program interfaces (APIs), platforms and services that facilitate online identification/verification and authentication of identity.

13. Not all elements of a digital ID system are necessarily digital (see Section III for an explanation of the basic steps in digital ID). Digital ID products and services are rapidly evolving, and may come to rely on technologies, architectures, and operational and business models that did not exist at the time this Guidance was developed.

14. This Guidance addresses two broad categories of digital ID: **Government-provided digital identity *systems*** and **private-sector provided digital identity *solutions*** for use in the financial sector (see Section III for further information). Digital ID systems/solutions can involve different operational models, with different roles for the government and private sector in developing and operating them. This Guidance is flexible to accommodate a range of solutions and does not seek to prefer any particular solution. There are a number of examples of digital ID systems and solutions included in boxes throughout the Guidance.

Purpose and Target Audience

15. This Guidance is intended to help government financial sector authorities (regulators, supervisors, examiners, and policymakers), as well as government authorities responsible for increasing financial inclusion, develop a clearer understanding of how digital ID works and to clarify how they can be used under the global AML/CFT standards.

16. The Guidance is also intended to help private sector stakeholders, including financial institutions, DNFBPs, technology service providers, the International Financial Institutions (IFIs), the United Nations (UN) and other international organisations; as well as relevant non-governmental organisations (NGOs) and others in the development and humanitarian assistance communities understand how digital ID can satisfy the requirements established by the FATF Recommendations for on-boarding and account access.

Scope

17. This Guidance addresses the application of Recommendation10 to the use of digital ID systems and solutions for on-boarding and authorising customer account access. Third Party Reliance is discussed only with respect to situations in which financial institutions provide digital ID solutions for conducting customer identification/verification to other financial institutions. The Guidance does not address the application of Recommendation 17 to providers of digital ID solutions which are not financial institutions.

18. Under the principle of technology neutrality, the requirements of Recommendation 11 apply equally to recordkeeping in digital form and in documentary form. Accordingly, digital ID does not raise distinctive issues for complying with Recommendation 11 requirements, and they will not be addressed in the Guidance.

19. In relation to CDD, this Guidance focuses on the use of digital ID systems only to: (1) conducting customer identification and verification for individuals (i.e. natural persons) when establishing business relations (on-boarding) and (2) authenticate the identity of on-boarded customers to authorise access to their accounts and other financial products and services. It does not address digital ID outside the context of proving legal ID in the financial sector—i.e., it does not address digital ID more broadly, for example, identity for use in online commercial transactions or on social media, or for accessing regulated products and services outside the financial sector (e.g., healthcare). Nor does it address the use of digital ID systems to identify and verify the identity of legal persons.

20. The Guidance also does not cover the use of digital ID systems or solution to help conduct other elements of the CDD process—apart from the essential role that customer identification/verification and authentication of customer identity for account access plays in conducting ongoing due diligence on the business relationship and transaction monitoring (see Section V). In particular, the Guidance does not address the use of digital ID systems or solutions to identify and verify the identity of a legal person's

representative(s); identify and verify the identity of beneficial owner(s); or understand and obtain information on the purpose and intended nature of the business relationship—although trustworthy digital ID systems and solutions are critically important for all of these CDD functions.

21. With respect to government-provided digital ID systems, the Guidance focuses on universal/foundational digital ID systems, although it also discusses government-provided functional digital ID systems, such as voter registries or databases, when the government authorises their use and makes them available to regulated entities for CDD purposes.

22. The Guidance does not establish technical standards for assessing the trustworthiness of digital ID systems and solutions. It relies on technical standards for assurance, data security, and privacy developed or being developed by: other Standard Setting Bodies (SSBs) such as the International Standards Organisation (ISO) or the International Telecommunications Union (ITU); individual or supra-national jurisdictions; and certain technology-based industry associations, such as GSMA.[9]

23. In addition, while digital ID systems and solutions present potential privacy, data protection, and governance risks that should be mitigated through comprehensive legal, operational, and technical controls, these issues are only considered to the extent they relate to the integrity of digital ID and the application of R.10's trustworthiness criteria.

24. This Guidance is non-binding. It clarifies rather than revising the current FATF Standards which are technology-neutral.

[9] GSMA is the global industry association for mobile communication network operators, and is involved in the development of a variety of technical standards applicable to mobile communications platforms, including standards for user identification and authentication.

SECTION II: FATF STANDARDS ON CUSTOMER DUE DILIGENCE

Customer identification/verification requirements (Recommendation 10)

25. Recommendation 10 requires each country to impose specified customer due diligence (CDD) obligations on financial institutions and, in certain circumstances, and Designated Non-Financial Businesses and Professions (DNFBPs), referred to as 'regulated entities' for the purpose of this Guidance.

26. Under Recommendation 10(1)(a) regulated entities are required to "identify the customer and verify that customer's identity, *using reliable, independent source documents, data or information"* when establishing business relations (i.e., at on-boarding).

27. In addition, regulated entities are also required to authenticate the identity of on-boarded customers, when authorising the customer to access his/her account and conduct account-based transactions. This is an implicit requirement because customer identification/verification at on-boarding would be a meaningless formality if the regulated entity is not also required to authenticate that the person seeking to access the account to conduct financial activities *is* the individual identified by the financial institution at on-boarding as the account holder. The requirement to authenticate customer identity to authorise account access and customer (account-based) financial transactions is also part of the requirement in Recommendation 10(d) that regulated entities must conduct "ongoing due diligence (on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship." Unless a financial institution can reliably determine that the person seeking to access the customer's account and conduct transactions is in fact the identified and verified customer, it cannot conduct meaningful ongoing due diligence throughout the business relationship.

28. This Guidance uses the phrase, "customer identification/verification*"* to refer to both of these CDD use-cases (i.e. at on-boarding and authorising account access/use).

Documentary or digital form

29. Recommendation 10 is technology neutral. Recommendation 10 (a) permits financial institutions to use "documents" as well as "information or data," when conducting customer identification and verification. Recommendation 10 (a) does not impose any restrictions on the form (documentary or digital) that "information or data" can take.

30. Moreover, although Recommendation 10 *does* require financial institutions to link a customer's verified identity to the individual in some "reliable" way, nothing in the FATF standards sets forth requirements for *how* a verified customer identity *should be linked* to a unique, real-life individual for purposes of authenticating the on-boarded customer's identity to authorise account access. Recommendation 10 thus does not impose limitations as to the use of digital ID systems or solutions for that purpose. The FATF standards leave the matter to each jurisdiction, as part of its national legal framework for proving legal ID when conducting CDD.

31. In a face-to-face in-branch financial transaction, traditional documentary authentication of a customer typically takes the form of the customer's presenting an official document, such as a national identity card, a driver's license, or some other form of official, authoritative identity evidence. Digital ID systems or solutions, particularly digital ID in some developing countries, now permit digital authentication, for both face-to-face and remote account access and transactions.

Box 2. To be included: Example of digital face-to-face authentication

E.g. Aadhaar illustration with fingerprint reader

Reliable and independent sources

32. The key to determining how digital ID systems and solutions can be used for customer identification/verification is understanding what Recommendation 10's requirement of "using *reliable, independent* source documents, data or information" means in the context of digital ID systems and solutions. This Guidance paper will use the term "trustworthy" as an equivalent to "reliable and independent" for the sake of brevity.

33. Recommendation 12 in the original FATF Forty Recommendations (July 1990) required regulated entities to identify their clients "on the basis of an official or other reliable identifying document". This language was carried forward unchanged through the June 1996 and June 2003 revisions of the Recommendations, and remained in place until the current version of the Recommendations, adopted in February 2012, added the "verification of identity" requirement and "independent" as a specific criteria for identity evidence, but took a more flexible, expansive approach to the types of identity evidence – source documents, but also digital data or information – that could be used for customer identification/verification.

34. In the context of documentary identification/verification, source documents, and documentary data or information, are reliable when they are genuine and the information they contain is accurate, and independent when they are created or generated by a neutral entity, under an appropriate legal and governance framework, and are not subject to the influence of any outside party, including the identified individual or any natural or legal person associated with the identified individual.

35. Digital ID products and services are more complex. In the digital ID context, the broad requirement that digital "source …data or information" must be "reliable, independent" means that the digital ID used to conduct customer identification/verification relies upon technology and processes that provide an appropriate level of trustworthiness, and are not subject to internal or external manipulation or falsification (including by cyberattack), to fabricate and credential false identities or authenticate unauthorised users.

Risk-based approach to CDD

36. Regulated entities are required to use a risk-based approach (RBA) to determine the extent of the CDD measures to be applied set out under Recommendation 10, including customer identification/verification. Under Recommendation 1 and its Interpretive Note, regulated entities are required to identify, assess and take effective action to mitigate their ML/TF risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). Enhanced measures are required in situations of higher risk and simplified measures may be appropriate in situations where low-risk is established.

37. The Interpretative Note to Recommendation 1 highlights that when assessing risk, regulated entities should consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level of mitigation to be applied. It specifically gives the example that regulated entities may differentiate the extent of measures, depending on the type and level of risk for the various risk factors (e.g. in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa).

Non face-to-face transactions

38. The Interpretative Note to Recommendation 10 includes "non-face-to-face business relationships or transactions" as an example of a potentially higher-risk situation in undertaking customer due diligence.

39. By its terms, this statement does not require appropriate authorities and financial institutions to always treat non-face-to-face business relationships or financial transactions as higher risk for ML and TF. Rather, non-face-to-face business relationships and transactions are examples of circumstances where the risk of ML or TF may *potentially* be higher.

40. Given the evolution of digital ID technology and architecture, and the emergence of consensus-based open digital ID technical standards, it is important to clarify that non-face-to-face customer-identification and non-face-to-face transactions that rely on digital ID systems and solutions that are appropriately trustworthy under the RBA discusses in this Guidance are typically standard risk, and may even be lower-risk.

SECTION III. DIGITAL IDENTITY

Description of basic digital ID systems

41. This section provides a brief explanation of the basic steps in a digital ID system[10], and its participants, with relevant definitions. These elements are presented in a technology-neutral way (i.e. not assuming the use of any particular identity technology, such as biometrics or mobile phone technology) and at a high-level in order to apply to a broad range of systems. This simplified description focuses on the elements of a digital ID system that are most directly relevant for customer identification/verification at on-boarding, and provides the basis for the discussion in Section V on how Recommendation 10—and in particular, its "reliable and independent" criteria—comes into play. This section does not provide a detailed explanation of digital technology or processes or a glossary of digital identity technology.

Summary of the digital ID process

42. As reflected in the digital ID technical standards, the digital ID process involves three basic stages (also referred to as the 'digital ID lifecycle'):

a. Identity proofing and enrolment (with initial binding/credentialing) (essential);

b. Authentication and identity lifecycle management (essential); and

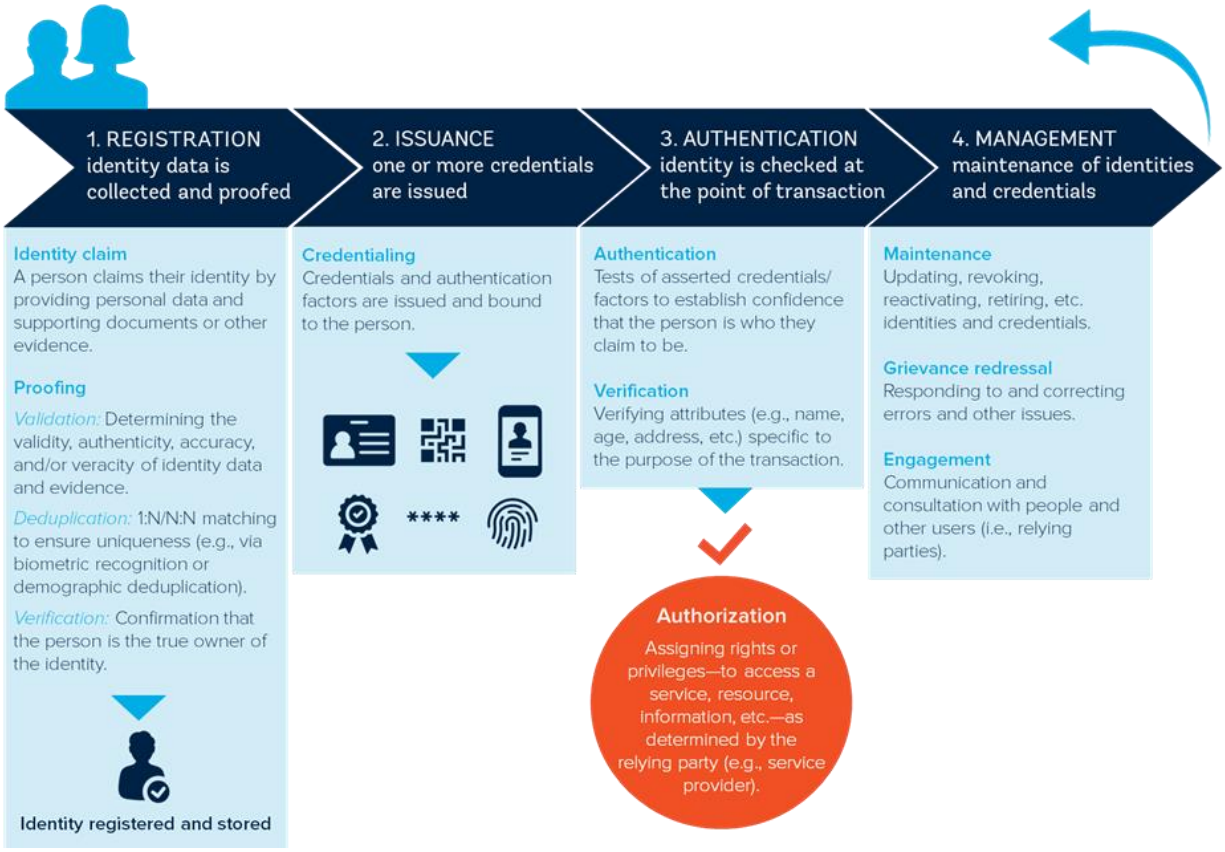
c. Federation/portability (optional).

43. Identity proofing and enrolment may be either digital (and in-person or remote) or documentary (and in-person). In a digital ID system, binding/certification, authentication and federation are always, and necessarily, digital.

44. The terminology used by different organisations may differ slightly depending on the system being described. The diagram below has been developed using ID4D terminology but summarises stages A and B above (ID proofing/enrolment and authentication/management). A more detailed description of each of the stages follows.

[10] In this section, a reference to digital identity systems also refers to digital identity solutions.

Figure 1. ID4D Digital ID Lifecycle



Source: ID4D Practitioner's Guide (forthcoming)

Stage 1: Identity proofing and enrolment

45. Together, identity proofing and enrolment (with initial binding/ credentialing) constitute the first stage of a digital ID system.

46. **Identity proofing** is the process by which an identity service provider (IDSP) collects, validates and verifies information about a person and resolves it to a unique individual, answering the question, "Who are you?". Identity proofing verifies a person's association with their real-world identity, and involves three actions: (1) identification, (2) validation, and (3) verification.

Table 2. Identity proofing process

Actions involved	Description	Examples
IDENTIFICATION	Involves obtaining attributes (identifiers), collecting attribute evidence; and resolving identity evidence and attributes to a single unique identity within a given population or context(s). Attribute evidence may be either physical (documentary) or purely digital, or a digital representation of physical attribute evidence (e.g., a digital representation of a paper or plastic driver's license). At present, in most jurisdictions, required (core) legal identity attributes typically include: full legal name; date of birth; home address; and a unique government-issued identity number. However, various other attributes are also relevant, including biometric attributes. The process of resolving identity evidence and attributes to a single unique identity within a given population or context(s) is called **de-duplication**.	Identity evidence (formerly called "identity documentation") has traditionally taken a physical form, such as (for natural persons) a government-issued document bearing a photograph and hologram or similar safeguards—e.g., a birth certificate, national identity card, driver's license or passport. With the development of digital technology, identity evidence may now be generated digitally (or converted from physical to digital form) and stored in electronic databases, allowing the identity evidence to be obtained remotely and/or identity attributes and other information to be remotely verified and validated against a digital database(s). Identifiers may also be biometric—i.e., based on an individual's personal biological or behavioural characteristics. • Biophysical biometric attributes include fingerprints, iris patterns, voiceprints, and facial features captured by facial recognition technology. • Biomechanical biometric attributes, such as keystroke mechanics, are the product of unique interactions of an individual's muscles, skeletal system, and nervous system. • Behavioural biometric attributes consist of an individual's various patterns of movement and usage in geospatial temporal data streams, and include, e.g., an individual's email or text message patterns, file access log, mobile phone usage, and geolocation patterns.
VALIDATION	Involves determining that the evidence is genuine (not counterfeit or misappropriated) and the data the evidence contains is accurate by checking the identity information/evidence against an acceptable (authoritative/reliable) source to establish that the information matches reliable source data/records.	For instance, in a private sector provided identity solution, the IDSP could check the physical identity evidence (identity document), such as a driver's license and/or passport, or the digital images of the applicant's physical identity evidence, and (1) determine that: there are no alterations; the data encoded in the license or passport's QR codes matches the plain-text information; the identification numbers follow standard formats; and the physical and digital security features are valid; and (2) query the government issuing sources for the license and/or passport and validate (confirm) that the information matches.
VERIFICATION	Involves confirming that the validated identity relates to the individual (applicant).	For example, the IDSP could ask the applicant to take and send a mobile phone video of themselves, or a mobile phone photo with other liveness checks; compare the applicant's submitted photo to the photos on the license and passport identity evidence; and determine they match to a given level of certainty. To tie this identity evidence to the actual real-person applicant, the IDSP could then send an enrolment code to the applicant's validated phone number; require the applicant to provide the enrolment code to the IDSP and confirm the submitted enrolment code matches the code the IDSP sent, verifying that the applicant is a real person, in possession and control of the validated phone number. At this point, the applicant has been successfully identity proofed.

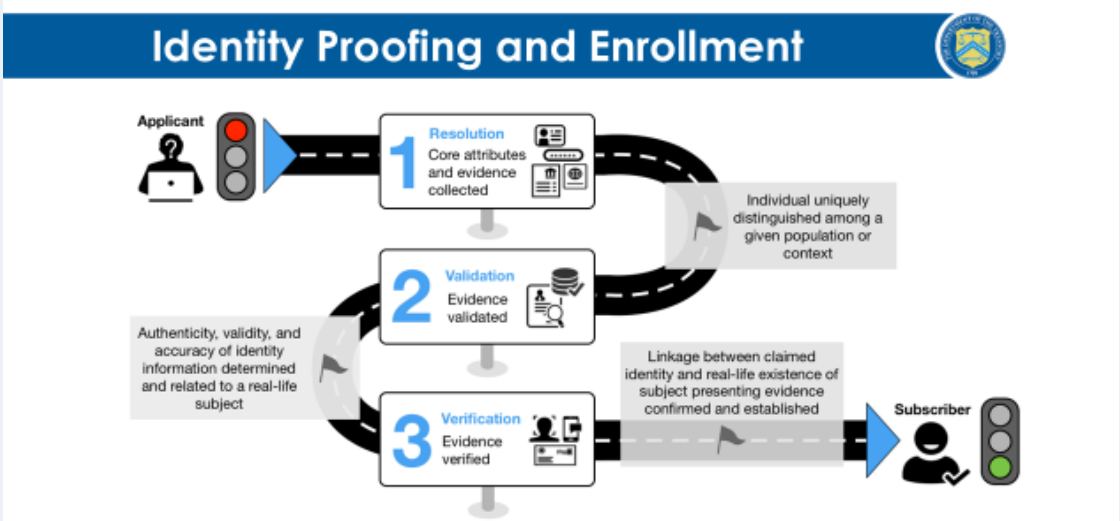
47. **Enrolment** is the process by which an IDSP registers (enrols) an identity-proofed applicant as a 'subscriber' and establishes their identity account. This process authoritatively binds the subscriber's unique verified identity (i.e., the subscriber's attributes/identifiers) to one or more authenticators possessed and controlled by the subscriber, using an appropriate **binding** protocol. The process of binding the subscriber's identity to authenticator(s) is can also be referred to as 'credentialing'.

48. As noted below, typically, the IDSP issues the authenticator(s) to the subscriber and registers the authenticator(s) in a way that ties them to the subscriber's proofed identity at enrolment. However, the IDSP can also bind the subscriber's account to authenticators provided by the subscriber that are acceptable to the IDSP (acting as a credential service provider (CSP)). Moreover, while binding is an essential part of trustworthy enrolment, the IDSP can also bind a subscriber's credentials to additional or alternative authenticators at a later point, as part of identity lifecycle management, discussed below.

49. The identity proofing process can be delivered by a single service provider, or by multiple service providers (see the summary of digital ID system participants, below). In the former case, it is possible that a single entity, process, technique, or technology could conduct each of the identity proofing process steps. Similarly, binding the proofed identity during enrolment can be accomplished by a single service provider or by a separate entity that does not also perform identity proofing.

Box.3. Identity Proofing and Enrolment/Binding Process Flow

Identity Proofing and Enrolment/Binding Process Flow Diagram to be inserted – revised version of diagram at to be inserted.



50. At the end of step one, the following results are achieved:

- Identity Proofing: Identity proofing resolves a claimed identity to a single, unique identity within the population or a particular context(s) to a stated level of certitude; validates that all identity evidence relied upon is correct and genuine, that the claimed identity exists in the real world, and is associated with the real person to whom the identity evidence relates (typically, the real person supplying the identity evidence to the IDSP or to a RP), to a stated level of certitude measured by one of three identity levels of assurance (ILA).
- Enrolment/Binding: Obtains and maintains identity records (including in particular identity or attribute evidence) and concludes with the identity service provider's authoritatively binding the individual's unique proofed identity to authenticator(s) possessed and controlled by that subscriber.

Stage 2: Authentication

51. Authentication can rely on various types of authentication factors and processes as set out below. The trustworthiness of the authentication depends on the type of authentication factors used and the security of the authentication processes.

Authentication factors

52. Traditionally, there are three basic categories of authentication factors:

- Knowledge factors: Something you know such as: a shared secret (e.g., password or passphrase), a personal identification number (PIN), or a response to a pre-selected security question.
- Ownership factors: Something you have, such as: cryptographic keys stored in hardware (e.g., in a mobile phone, tablet, computer, or a USB-dongle) or software that the subscriber controls, an out-of-band device[11], a one-time password (OTP) in a hardware device, or a software OTP generator installed on a digital device, such as a mobile phone.
- Inherence factors: Something you are (biometrics, such as facial, fingerprint or retinal pattern biometrics, and advanced behavioural biometrics, based on the unique way an individual interacts with digital devices, such as how the individual holds the mobile phone, swipes the screen, keyboard cadence, or uses certain keyboard or gestural shortcuts).

53. Some traditional authentication factors do not apply directly to digital authentication. For example, a physical driver's license is something you have and may be useful when authenticating identity in person to a human being (e.g., to a bank teller), but is not in itself an authenticator for digital authentication purposes.

54. Moreover, under the technical standards for digital ID, authenticators must always contain a secret. Knowledge authentication factors (something you know) are not necessarily secrets. Knowledge-based authentication, in which the claimant is prompted to answer questions that are presumably known only by the claimant, does not constitute an acceptable secret for digital authentication under the technical standards. Similarly, a biometric inherence factor does not constitute a secret, and the technical standards allow the use of biometrics for authentication only when strongly bound to a physical authenticator (see Section V and Appendix A, for a discussion of an identity risk management framework and the technical standards, including for authentication).

55. At the same time, new kinds of technology-based ownership and inherence authenticators (including advanced digital device authenticators and behavioural biometric patterns), many of which have been or are being developed and deployed primarily for anti-fraud purposes, have significant potential to strengthen digital ID authentication processes for AML/CFT compliance purposes.

Authentication processes

56. Authentication processes are generally categorised by the number and type of authentication factors the process requires. The more factors an authentication process employs, the more robust and trustworthy the authentication system is. Types of authentication protocols/processes by increasing levels of security include:

- **Single-factor authentication (1FA)** uses only one authenticator to authenticate a person's identity.
- **Two-factor authentication (2FA)** is the minimum level of multi-factor authentication (MFA) (see point below). It uses a combination of two independent authenticators from two different factor categories to confirm the individual's identity. For example, where a claimant has logged on to their online bank account using a knowledge-based authenticator (username and password) and seeks to complete an online transaction, the person would need to enter an additional

[11] [Definition or explanation to be included]

authentication factor, from a different authentication factor category. An online banking customer might use an ownership authentication factor, such as sending a a One Time Password (OTP) on an out-of-band device or mobile phone and confirming the customer's possession of the OTP.

- **Multi-factor authentication (MFA)** combines use of two or more authentication factors for enhanced security. MFA may be implemented either by presenting multiple factors directly to the verifier or by using one or more factors to protect a secret, which in turn is presented to the verifier. I.e., MFA can be performed using a single authenticator that provides more than one factor, or by a combination of authenticators that provide different factors.

57. Strong authentication requires either 2FA or MFA that uses two or more mutually independent authentication factors of different types, at least one of which is non-reusable and non-replicable and cannot be surreptitiously stolen via the internet.

58. The authentication has three basic steps. A single IDSP may conduct all of the authentication processes. Alternatively, independent entities, with names (verifier and credential service provider (CSP)) reflected by their separate functions, may conduct each (or several) the authorisation processes. In addition, the same entity may be both the verifier and the relying party (RP), or even the CSP, the verifier and the relying party—as is the case with certain large banks. The description of authentication processes, below, assumes a legitimate claimant with valid authenticators, and a positive result of the authentication process verifying the claimant's identity. Authentication can also produce a negative result, based on the failure of any of the following steps:

- Authentication begins with the claimant's asserting his/her identity and demonstrating possession and control of an authenticator(s) that is bound to the asserted identity by an IDSP (acting as a Verifier) through a secure authentication protocol. To confirm the claimant's possession and control of valid authenticators, the verifier may also need to confirm that the credentials linking the authenticator(s) to the subscriber's account are valid.

- Once the claimant demonstrates possession and control of the authenticator(s) to the IDSP/verifier, the verifier confirms that the authenticators are valid by interacting with the IDSP (acting as a **Credential Service Provider (CSP))** and the verifier generates an **assertion**,[12] a digital object or data structure that communicates the results of the authentication process (i.e., verifies the claimant's identity) and optionally, information about the claimant over the authentication protocol to the **relying party (RP).** Assertions typically are communicated directly from the CSP/verifier to the RP, but they may also be forwarded to the RP through the subscriber.

- The RP determines that the assertion came from a verifier the RP trusts, and processes any additional information in the assertion, such as personal attributes or credential/authenticator expiration times, and makes an authorisation decision. The RP is the final arbiter of whether a specific assertion presented by a verifier meets the RP's established criteria for system (e.g., account) access, regardless of the technical level of identity assurance, authorisation assurance, and/or federation assurance (see the discussion of the digital ID technical standards, Section V and Appendix B.

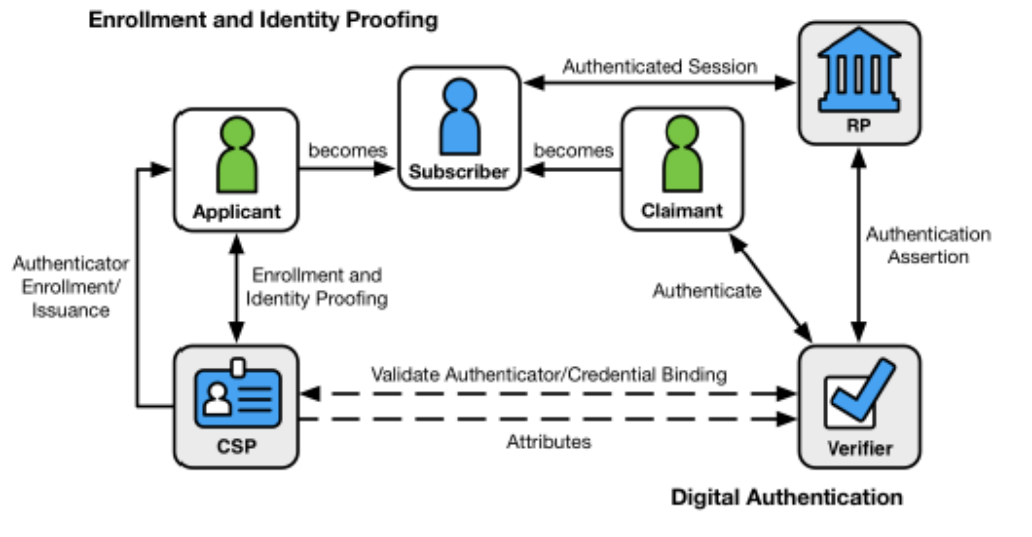
59. The figure below illustrates the authentication process using the example of a typical financial transaction. In this diagram, an existing customer wants to initiate a

[12] An **assertion** is a digital object or data structure (sometimes called a statement) sent from a verifier to a RP that contains information about a subscriber (claimant) and may also contain verified attributes or other information or identity evidence.

financial transaction and must first prove, via one or more authenticators, that he/she is who he/she claims to be—i.e., is the account owner. The customer (claimant) proves his/her possession and control of authenticators by communicating with the IDSP (verifier) over a secure authentication protocol. The verifier confirms the validity of (verifies) the authenticators with the credential service provider (CSP) and provides an authentication assertion to the financial institution, which is the RP in the illustrated scenario.

Box.4. Authentication Process Flow

[Diagram below, from the NIST Identity Guidelines, SP 800-63-3, to be adapted for the Guidance.]



Lifecycle management

60. **Authenticator lifecycle management** refers to the actions IDSPs should take in response to events that can occur over the lifecycle of a subscriber's authenticator that affect the use, security and trustworthiness of the authenticator. These events could include: issuing or binding credentials either at enrolment or post-enrolment, loss, theft, unauthorised duplication, expiration, and revocation of authenticators and/or credentials.

61. An **authenticator** is something the claimant possess and controls—typically, a cryptographic module or password—that is used to authenticate the claimant's identity. A **credential** is a digital object or data structure that authoritatively binds a subscriber's proofed identity, via an identifier/s, to at least one authenticator possessed and controlled by the subscriber.

62. The discussion below uses the function-based term, credential service provider (CSP), in describing the actions that should be taken in response to a specific type of authenticator lifecycle event even though a single IDSP may undertake authenticator lifecycle management, as well as identity proofing and enrolment, and/or authentication.

- **Issuing and recording credentials:** The CSP issues the credential and records and maintains the credential and associated enrolment data in the subscriber's identity

account throughout the credential's lifecycle. Typically, the subscriber possesses the credential, but the CSP/verifier may also possess credentials. In all cases, the subscriber necessarily possesses the authenticator/s, which, as discussed above, is used to claim an identity when interacting with a relying party.

- **Binding (a.k.a. credentialing or credential issuance):** Throughout the digital ID lifecycle, the CSP must also maintain a record of all authenticators that are, or have been, associated with the identity account of each of its subscribers, as well as the information required to control authentication attempts. When a CSP binds (i.e., issues credentials that bind) a new authenticator to the subscriber's account post-enrolment, it should require the subscriber to first authenticate at the assurance level (or higher) at which the new authenticator will be used.
- **Compromised Authenticators—Loss, Theft, Damage, Unauthorised Duplication**: If a subscriber loses (or otherwise experiences compromise of) all authenticators of a factor required for MFA, and has been identity proofed at IAL2 or IAL3, the subscriber must repeat the identity proofing process, confirming the binding of the authentication claimant to previously proofed evidence, before the CSP binds a replacement for the lost authenticator to the subscriber's identity/account. If the subscriber has MFA and loses one authenticator, the CSP should require the claimant to authenticate, using the remaining authentication factors.
- **Expiration and Renewal**: CSPs may issue authenticators that expire and are no longer usable for authentication. The CSP should bind an updated authenticator before an existing authenticator expires, using a process that conforms to the initial authenticator binding process and protocol, and then revoke the expiring authenticator.
- **Revocation (a.k.a. Termination):** CSPs must promptly revoke the binding of authenticators when an identity ceases to exist (e.g., because the subscriber has died or is discovered to be fraudulent); when requested by the subscriber; or when the CSP determines that the subscriber no longer meets its eligibility requirements.

Stage 3: Federation (optional)

63. Federation refers to the use of digital ID systems to convey identity and authentication information across an interoperable set of networked systems. Federation allows digital legal identity to be portable. Portable identity means the individual's verified identity credentials can be used to establish legal identity for new customer relationships at unrelated financial institutions or government entities (or other unrelated entities/services that require proof of legal identity), without each financial institution or government entity having to obtain and verify personally identifiable information (PII) to meet regulatory requirements. Portability requires developing interoperable digital identification products, systems, and processes—which federated identity architecture provides.

64. Federation is an optional component of a digital ID system, but is generally part of government-provided universal digital ID systems. Federated digital ID architecture and protocols are also being developed and adopted in various jurisdictions to enable interoperability and portable identity across many national-level functional identity systems.

65. In the absence of government-provided digital universal identity, trustworthy federation, enabling interoperable private sector digital ID solutions could provide many

significant benefits. For example, it could potentially save relying parties (e.g., financial institutions and government entities) time and resources in identifying, verifying, and managing customer identities, including for account opening and access. Federation could also potentially save customers the inconvenience of having to prove and authenticate identity for each unrelated financial institution or government service, and reduce the risk of identity-theft stemming from the repeated exposure of PII.

Summary of the participants involved in the digital ID system

66. As noted above, digital ID system or solutions can involve different operational models, with different roles for the government and private sector in developing and operating digital ID system or solutions and/or providing specific DIDPS.

67. The following table describes the basic participants in a generic digital ID system or solution, with the understanding that in the provider/operator space, the government in national digital ID system or solutions may conduct all or most of the provider processes, and that in cases where the private sector plays a leading role in the development and delivery of DIDPS, a single entity or multiple entities may play some or all of the provider participate roles.

Table 3. Participants in digital ID systems/solutions

IDENTITY SERVICE PROVIDERS	
Identity Service Provider (IDSP)	Generic umbrella term that refers to all of the various types of entities involved in providing and operating the processes and components of a digital ID system or solution. IDSPs provide DIDPS to users and relying parties. As noted above, a single entity can undertake the functional roles of one or more IDSPs
Identity Provider (IDP)	Entity that manages a subscriber's primary authentication credentials and issues assertions derived from those credentials to RPs. An IDP is usually also the Credential Service Provider (CSP), but may rely on a third party for identity proofing and credentialing.
Credential Service Provider (CSP)	Entity that issues and/or registers authenticators and corresponding electronic credentials (binding the authenticators to the verified identity) to subscribers. The CSP is responsible for maintaining the subscriber's identity credential and all associated enrolment data throughout the credential's lifecycle and for providing information on the credential's status to verifiers. A CSP typically also acts as a Registration Authority (RA) and a Verifier, but may delegate certain enrolment, identity proofing, and credential/authenticator issuance processes to an independent entity, known as a RA or an Identity Manager (IM)—i.e., CSPs can be comprised of multiple independently operated and owned business entities. A CSP may be an independent third-party provider, or may issue credentials for its own use (e.g., large financial institution or a government entity). A CSP may also provide other services, in addition to digital ID services, such as conducting additional CDD)/KYC compliance functions on behalf of a Relying Party (RP).
Registration Authority (RA) (or Identity Manager)	The entity that is responsible for enrolment. The RA registers (enrols) the applicant and the applicant's [credentials and] authenticators after identity proofing.
Verifier	Entity that verifies the Claimant's identity to a Relying Party (RP) by confirming the claimant's possession and control of one or more authenticators, using an authentication protocol. The verifier confirms that the authenticators are valid by interacting with the Credential Service Provider (CSP) and provides an assertion over the authentication protocol to the RP. The assertion communicates the results of the authentication process and optionally, information about the subscriber to the RP. To confirm the claimant's possession and control of valid authenticators, the verifier may also need to confirm that the credentials linking the authenticator(s) to the Subscriber's account are valid. The verifier is responsible for providing a mechanism by which the RP can confirm the integrity of the assertion it communicates to the RP. The verifier's functional role is frequently implemented in combination with the CSP, the RP, or both.
USER	

User	The unique, real-life individual who is identity proofed, enrolled, credentialed, and authenticated by a digital ID system or solution and uses the DIDPS to prove his/her (legal) identity. Users are typically referred to by different names at different stages in a digital ID system or solution, depending on their activities-based role with respect to each of the three components of a digital ID system or solution, as set out below.
Applicant	Person to be identity proofed and enrolled. Applicant refers to the person undergoing the processes of identity proofing and enrolment/binding (credentialing) and applies to the user from the point the user applies for a digital ID and provides supporting identity evidence until the user's identity has been verified and an identity account established and bound to the authenticator(s), at which point the applicant becomes a SUBSCRIBER
Subscriber (a.k.a. Subject)	Person whose identity has been verified and bound to authenticators (credentialed) by a Credential Service Provider (CSP) and who can use the authenticators to prove identity. Subscribers receive an authenticator(s) and a corresponding credential from a CSP and can use the authenticator(s) to prove identity.
Claimant	A Subscriber who asserts ownership of an identity to a RELYING PARTY (RP) and seeks to have it verified, using authentication protocols. A claimant is a person who seeks to prove his/her identity and obtain the rights associated with that identity (e.g., to open or access a financial account).
Relying Party (RP)	Person (natural or legal) that relies on a subscriber's credentials or authenticators, or a verifier's assertion of a claimant's identity, to identify the Subscriber, using an authentication protocol. An RP trusts an identity assertion based on the source, the time of creation, how long the assertion is valid from time of creation, and the corresponding trust framework that governs the policies and processes of CSPs and RPs. The RP is responsible for authenticating the source of an assertion (i.e., the verifier) and for confirming the integrity of the assertion. A RP relies on the results of an authentication protocol to establish confidence in the identity or attributes of a subscriber for establishing a business relationship (account opening) or authorising account access and/or conducting a transaction. RPs may use a subscriber's authenticated identity, the IAL, AAL, and FAL, metadata, providing information about the trustworthiness of each of the digital ID components and processes, and other factors to make a final identity/verification or authorization decision. Typical RPs include financial institutions and government departments and agencies.
Trust Framework Provider / Trust Authority	Trusted entity that certifies and audits IDSP compliance with technical standards (processes and controls) for identity, authentication, and federation assurance levels (IAL, AAL, and FAL). Trust Framework Providers may also be responsible for setting technical standards for these levels of assurance. Trust Framework Providers may be government entities (e.g. EU/ eIDAS government digital ID certification authority) or a trusted industry organization, such as Open Identity Exchange (OIX); FIDO (Faster Identity Online) Alliance (specifications and certifications for hardware- mobile- and biometrics-based authenticators that reduce reliance on passwords and protect against phishing, man-in-the-middle and replay attacks using stolen passwords); Kantara; or GSMA (for mobile communications devices).

Government and Private-Sector Provided Digital ID Systems

68. As noted in the Introduction, this Guidance addresses the application of the global standards—and in particular, Recommendation 10—to two broad categories of digital ID products and services: (1) government-provided digital ID systems, (2) private-sector legal digital ID solutions.

69. The Guidance has adopted this distinction for the purpose of analysing how Recommendation 10's trustworthiness criteria applies to digital ID because these two categories of products and services envisage different roles for the government and private sector. The use of government-provided or private sector-developed digital ID for customer identification/verification at on-boarding and authorising account access raises distinct issues, particularly for regulated entities that are deciding whether to adopt or accept them. These issues are explored in Section V, which separately discusses the application of a risk-based identity management framework and Recommendation 10's "reliable and independent" criteria to government-provided and private sector provided digital ID products and services.

70. The discussion below briefly describes some of the operational models adopted by government-provided systems, and the three basic sub-categories of private-sector solutions. The characteristics of the three types of private sector digital ID solutions are particularly important for evaluating their trustworthiness, as explained in Section V.

Government-Provided Digital ID Systems

71. Government-provided digital ID systems can involve different operational models, and include both government-developed and operated digital ID systems, and systems developed and/or operated on behalf of the government by private sector entities, via a variety of legal and contractual arrangements. For purposes of this Guidance, the defining characteristic of government-provided digital ID systems is that the national government provides and stands behind the authoritativeness and trustworthiness of the system's identity proofing, credentialing, and authentication processes—including the integrity of its technology, design, and delivery.

72. The following descriptions are illustrative rather than comprehensive. See Appendix C for additional examples of government-provided digital ID systems.

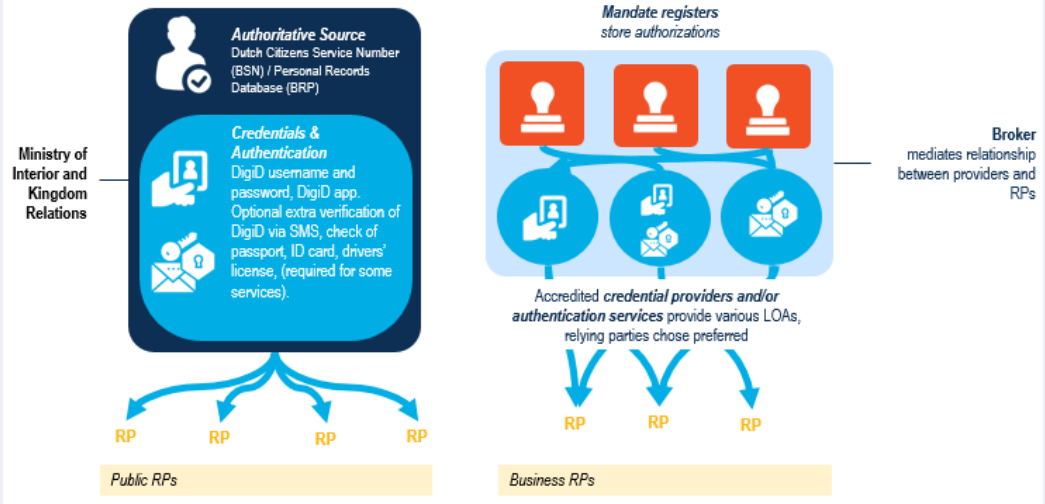
Government as Centralised Identity Service Provider

73. National government provides and operates the universal and/or functional digital ID system(s), acting as a centralised IDSP that conducts: identity proofing (using government databases as authoritative source of identity evidence, enrolment and binding, authentication and lifecycle management; and, where applicable, federation.

- Jurisdictions with foundational (universal) legal identity: The same government entity that manages the country's foundational legal identity registration system operates a centralised digital ID system. Examples: Belgium/eCard, Netherlands/DigiD, India/Aadhaar, and eIDs in Estonia, Singapore, and Peru.
- Jurisdictions without foundational legal identity: The government acts as a centralised IDSP by linking to multiple national-level functional identity systems or to regional government identity systems, and relying on their digital databases as authoritative identity evidence for identity proofing and enrolment. Examples: Australia/myGovID.

Box 5. Netherlands - DigiD

For more than 10 years the Dutch government issues a digital identification and authentication tool: 'DigiD'. DigiD can be used by citizens in the public domain. Citizens can access online services of many government organizations by identifying themselves with a DigiD username and password (and optional authentication code via a text message). Via DigiD the service provider receives the unique "Dutch Citizens Service Number (in Dutch: burgerservicenummer) of the user. This means that only service providers that are competent to process the Dutch Service Number (governments and organizations that perform a public service) can use DigiD. At this time, approximately 13.5 million citizens use DigiD. It is the aim of the Dutch government that DigiD meets the standards 'substantial' and 'high' with regard to the European regulation on electronic identities and trust services (eIDAS). The legislative process is pending. For more information: https://www.digid.nl/en/.



Source: Netherlands and World Bank

Federated Government Digital ID Systems

74. The national government provides the Trust Framework and establishes an interoperable federated digital ID system, in which multiple IDSPs (acting as CSPs/Verifiers), using federated identity architecture, convey identity-proofed claimants' identity assertions and authenticate identity to RPs across separate, but networked, digital ID systems.[13]

75. A **Trust Framework** is the set of interdependent specifications, rules, and agreements that make up the operating policies of a federated identity system. Federation is a process that allows authentication results and attribute information to be communicated across networked, interoperable digital ID systems to unrelated RPs. Federation enables an individual to be identity-proofed once and use the issued credential at multiple RPs, across multiple, networked identity systems.

76. A government-provided federated identity system may include IDSPs that are government entities or it may also authorise certified private sector IDSPs (CSPs/Verifiers) to participate and authenticate identities in the government-provided federated identity system.

77. Typically, the national government operates the federated digital ID infrastructure, acting as the **Trust Authority** that certifies participant IDSPs. However, the government can also authorise an independent Trust Authority to act on its behalf certify that a given IDSP complies with the Trust Framework, accrediting it to participate in the federated identity system.

[13] Private sector digital identity solutions can also be federated. The trustworthiness of federated digital identity services, whether government- or private sector-provided, depends in part on the robustness, or level of assurance (LoA), of its federated identity architecture—in particular, the LoA of the assertion protocol the federation uses to communicate authentication and attribute information (if applicable) to a RP (i.e., its Federation Assurance Level (FAL)).

78. To date, government-provided federated identity systems are almost exclusively used for proving claimants' legal identity to access government benefits and services, with government entities as the RPs. However, the use of government-provided federal identity systems in the financial sector, to conduct customer identification/verification at on-boarding, and to authenticate identity for account access, is being explored in a number of jurisdictions (for example, EC under e-IDAS; UK/Gov.Verify).

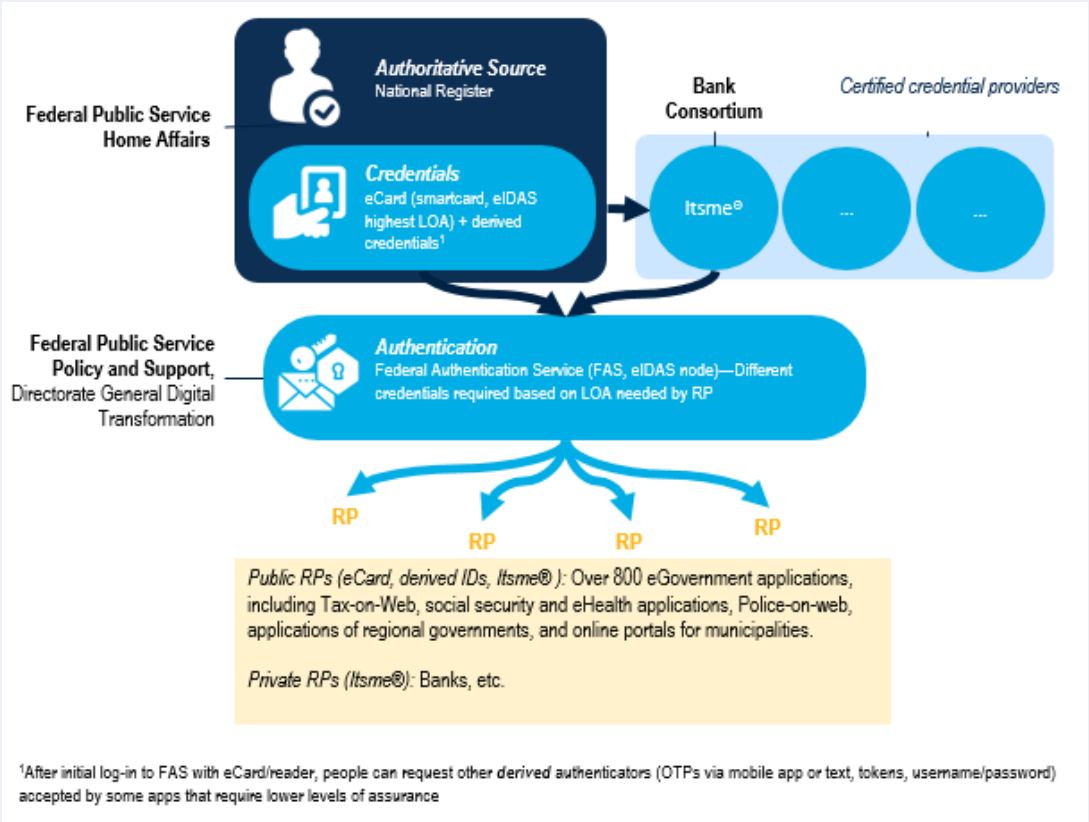
79. Some countries are also in the process of establishing a government-provided federated identity system, where government authorities – acting as a Trust Framework Provider – initially verify and confirm the identity of a person at the enrolment stage and issue credentials for the eID and authenticate users (e.g., Switzerland[14]).

[14] Swiss Draft E-ID Law, https://www.parlament.ch/en/ratsbetrieb/suche-curia-vista/ratsunterlagen?AffairId=20180049&k=PdAffairId:20180049; Commentary of the Federal Council on the Swiss Draft law on the E-ID, https://www.admin.ch/opc/fr/federal-gazette/2018/4031.pdf (in French) or https://www.admin.ch/opc/de/federal-gazette/2018/3915.pdf (in German)

Box 6. Belgium - eCards

The eCards include the Belgian Citizen eCard and the Foreigner eCard (together referred to as the Belgian eCards). The Belgian eCards satisfy the Level of Assurance 'high' for the context of the eIDAS notification. Municipalities / consulates and embassies are responsible for the enrolment, issuance, and delivery of the eCard. The Federal Authentication Service (FAS) is responsible for authenticating users. The authentication flow between the citizen or foreigner and the FAS, using the eCard, is based on the TLS mutual authentication standard. During this authentication flow, the internet browser sends the citizen or foreigner authentication certificate to the FAS. The FAS performs the necessary certificate verifications to ensure the integrity, validity and authenticity of the presented TLS client authentication certificate. This certificate can only be used by providing the PIN code, which is known only by the citizen or foreigner holding the eCard. Access to the requested government application is provided after the correct entry of the PIN code, a successful verification of the authentication certificate and completion of the authentication flow.

Today, almost all Belgian citizens and residents have an eCard, which now grants access to a wide range of over 800 eGovernment applications, including Tax-on-Web, social security and eHealth applications, Police-on-web, applications of regional governments, and online portals for municipalities.



Source: Belgium and World Bank

Box 7. Sweden – BankID

Sweden has a long history of robust federal identity ecosystem with a foundational/universal identification system characterised by a unique ID number in place since 1974. This has allowed administrative frameworks and the broader public to adapt relatively easily to digitisation. The Swedish government opted to pursue a market-based digital ID system rooted in the financial services sector to spur competition between identity service providers, thus facilitating innovation and driving per transaction costs down, creating trusted identity integrations into a greater variety of e-services, and reducing initial implementation costs for the public sector.

First launched in 2003 and managed by a consortium of 10 Swedish banks, BankID is a PPP-based identification system. All customers of participating banks are given an eID free of charge, which can be used to authenticate transactions across the private and public sector. Companies looking to integrate BankID with their services establish a contract with a bank in the BankID network, which facilitates a direct revenue stream to participating financial institutions. Identity credentials themselves are available in "hard" form—encoded on a smart chip—or "soft" form, which is available on a user's personal computer, tablet, or phone. As at 2016, BankID facilitated 2 billion transactions per year and was used by more than 80 percent of Swedish citizens. Sweden has additional plans for the program's continued expansion, as well. BankID has integrated next generation identity verification and authentication mechanisms based on behavioural biometrics to minimize reliance on passwords. Six of the country's largest banks also cooperatively launched a common mobile payment app, Swish, in 2012, building on BankID's functionality.

Source: World Bank ID4D, Private Sector Economic Impacts from Identification Systems, 2018

Private-Sector Provided Digital ID Solutions

80. Private sector-provided digital ID solutions can be divided into three types:

- **Government regulated/certified/supervised:** The national government provides the technical standards for levels of assurance for each of the steps (processes) of a digital ID system or solution, and regulates, supervises and examines private sector identity providers that seek to be government-certified as providing digital ID solutions at specified levels of assurance. For example: European Member States/e-IDAS; Canada/Treasury Board of Canada Standard on Identity and Credential Assurance; Australia/TBC.
- **Private-sector audited and certified:** Private sector IDSPs are audited and certified as complying with a given set of technical standards for trustworthiness by an independent, non-governmental standards and certification body, which may be national or international (including, in some cases, technology-based industry associations). Examples: Open Identity Exchange (OIX); FIDO Alliance (hardware-based authentication standards); GSMA (mobile communications industry digital ID standards)
- **Unaudited/uncertified:** Private Sector IDSPs offer digital ID solutions that have not been audited and certified as complying with relevant technical standards, including standards for assurance levels of various digital ID processes.

Box 8. Netherlands – iDIN

iDIN is a service offered by banks which allows consumers to use their bank's login methods to identify, log in of confirm age on the websites of participating organizations (mainly other banks). The aim of iDIN is that customers or consumers can authenticate their identity easily and significantly reduce the number of accounts they use. As a result, there is less chance of forgetting passwords and they are assured of a secure login method. It also means that they do not have to provide their data repeatedly. For merchants, this can save time, manpower and paperwork and increases conversion rates. For more information: https://www.idin.nl/en/about-idin/

Whether iDIN can also be used by banks to on-board new clients is currently being reviewed by the Dutch Central Bank.

Source: Netherlands

SECTION IV: BENEFITS AND RISKS OF DIGITAL ID SYSTEMS AND SOLUTIONS FOR AML/CFT COMPLIANCE

81. Digital ID systems and solutions that meet appropriate, risk-based technical standards for trustworthiness—i.e., that have appropriate levels of assurance (LoA) for their various steps and processes—offer significant potential benefits for improving customer identification/verification at on-boarding, and authenticating the identity of customers to authorize account access. Moreover, accurate customer identification is an essential enabler of other CDD measures, including effective ongoing due diligence on the business relationship and transaction monitoring (element (d) of the CDD measures set out in Recommendation 10). Similarly, robust customer identification facilitates the identification and reporting of suspicious transactions. Trustworthy digital ID products and services could therefore strengthen these preventive AML/CFT measures, as well as improve general risk management and anti-fraud efforts, while potentially reducing compliance costs.

Box 9. Nigeria Bank Verification Numbers (BVN)

In 2015, Nigeria began a biometric verification pilot for all civil servants in an effort to get an accurate record of the personnel and ensure that 'ghost' salaries were not paid out. The Central Bank of Nigeria, required that all customers enrol with their banks to get their unique Bank Verification Numbers (BVN), operated by the Nigeria Inter-Bank Settlement System (NIBSS). In early 2016, they announced the removal of 24,000 (ghost) workers,42 and that number has since doubled – saving the tax payer equivalent of USD $74million.

Source: Digital ID On-boarding, The World Bank 2018

82. In addition, the use of trustworthy digital ID systems or solutions could help enable more individuals and businesses, especially low-income, unserved and underserved persons, to access regulated financial services, facilitating financial inclusion and helping combat the risk financial exclusion poses to the reach and effectiveness of AML/CFT regimes.

83. At the same time, digital ID products and services that are not sufficiently robust present a variety of risks that may undermine AML/CFT safeguards and facilitate illicit financing activities. It is certainly the case that traditional, documentary methods of proving legal identity in the financial sector also pose risks. For example, the use of fraudulent or forged identity documents, such as driver's licenses or Social Security cards, may facilitate ML, TF, and fraud activities. This and other risks associated with documentary customer identification/ verification have been exacerbated in recent years by massive online identity theft in many jurisdictions. Moreover, traditional documentary methods of conducting customer identification/verification largely rely on front-line personnel, such as bank tellers, who are unlikely to have access to the tools and skills required to identify counterfeit or stolen documents.

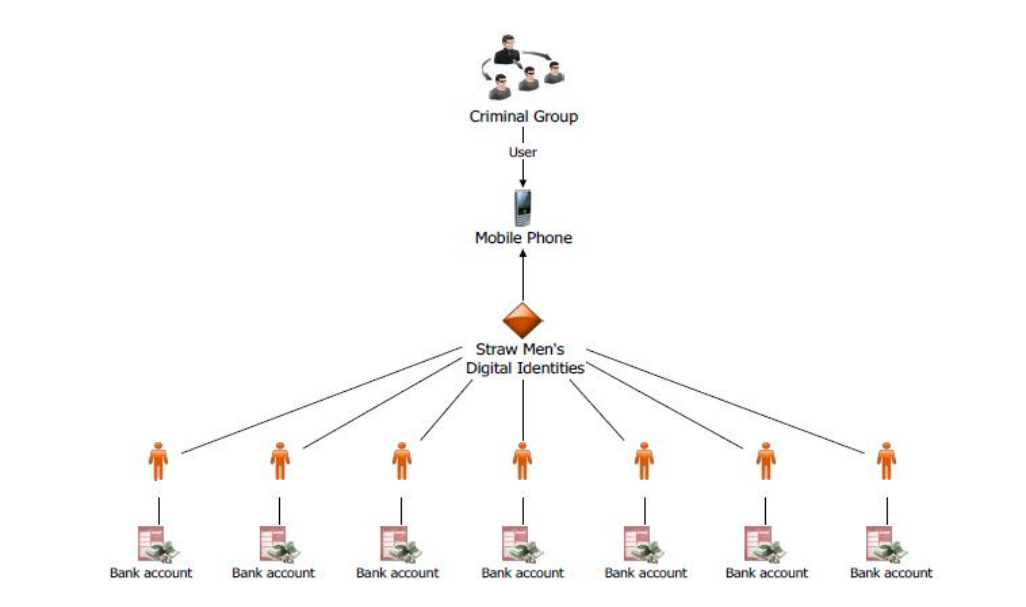
84. For the purposes of this Guidance, is that potential ML, TF, and fraud risks associated with certain digital ID systems and solutions—including in particular weaknesses in identity proofing and binding at enrolment, and post-enrolment authentication—must be understood and effectively mitigated in order to comply with Recommendation 10 requirements.

85. Without careful consideration of relevant risk factors and implementation of appropriate levels of assurance to address them, criminals, terrorists, money launderers and other bad actors may be able to exploit vulnerabilities in for digital ID processes to generate false identities and credentials to facilitate their illicit activities. Poor identity credential life cycle and access management can, wittingly or unwittingly, enable unauthorised persons to access and misuse customer accounts, undermining the purpose of customer identification/verification and ongoing due diligence requirements in protecting the financial system from abuse.

Box 10. Misuse of digital ID by straw men

Sweden highlighted the ML/TF risks arising from a criminal's systematic use of straw men's digital ID to launder proceeds of crime. The services of payment service providers that offer real-time transactions are especially useful for criminals, as they, together with misused digital IDs, make it possible to quickly transfer money between various accounts.

When criminal groups wish to launder money by misusing digital IDs, they first need to open bank accounts, which are done by straw men. The role of a straw man is to open a bank account, obtain a digital ID and a security code, and provide their credentials to the criminal group, in exchange for money. Multiple digital identities can be used on a single mobile phone or tablet (see diagram below). The bank accounts are then controlled by the criminal group. It is important to note that the overwhelming majority of digital IDs that are opened by straw men, and misused by criminal groups, are issued on this basis of legitimate identity evidence (i.e. proof of identification).



Source: Sweden

86. The use of digital ID also has an important part to play in ongoing CDD and the detection of ML/TF. Where digital ID solutions are outsourced by the regulated entity, it may have less information available to it on the customers' behavior and transaction patterns. If the use of a third-party IDSP fragments the information landscape, it may become more difficult for regulated entities to see the bigger picture. The monitoring of how a digital ID is being used should enable the detection of any systematic misuse of digital IDs, including compromised, stolen or sold digital IDs. IDSPs can detect the misuse of their products but, if they are not a regulated entity, they may not be under an obligation to report suspicious behavior to financial intelligence units.

87. Digital ID systems and solutions that do not meet high technical standards also themselves pose a risk of massive identity theft, including new forms of online synthetic identity theft; wide scale online commercial and financial services fraud; and cyberattacks—including attacks aimed at disabling broad swaths of the financial sector, or at disabling the identity systems or solutions themselves. Moreover to the extent that digital ID systems or solutions fail to cover all or most persons in a jurisdiction, or exclude certain populations—for example, because of the greater failure rates of certain kinds of biometrics for some vulnerable groups (e.g., inability to read the worn fingerprints of manual labourers; match failure of older individuals, due to aging, disease, or other confounding factors; or disproportionate facial recognition failures for certain ethnic groups, or individuals with certain physical characteristics, such as darker skin tones or facial hair) they may drive—or at least fail to mitigate—financial exclusion as a ML/TF risk.

88. In addition, digital ID systems and solutions may pose critical challenges with respect to the technical capacity to develop, implement, operate and evolve trustworthy digital ID products and services. In many cases, technical design (architecture) flaws, undermining trustworthiness, may not become apparent until they are exploited by bad actors in ways that disclose how the digital ID system or solution can be hacked. For instance, today, basic facial recognition capabilities are built into everyday computer systems and software. However, experience has shown that facial recognition factors can be obfuscated by facial expressions of different moods, lighting conditions, and other factors.

89. Digital ID systems or solutions also present challenges with respect to connectivity and resilience in the face of unreliable electrical grids, as well as access challenges where "smart" mobile phones and other digital devices have not yet reached near-ubiquity. Lack of reliable infrastructure can potentially undermine, for meaningful periods, the availability and/or reliability of the primary means for conducting customer identification/verification and authentication in a jurisdiction or in particular areas of a country.

90. The examples below illustrate some of the potential risks associated with digital ID systems or solutions that bad actors can exploit or have exploited to facilitate ML/TF. Some of the examples relate to identity proofing and enrolment vulnerabilities (e.g., synthetic identity theft fraud cases); others involve authentication flaws:

- **Two Factor Authentication (TFA) Vulnerabilities:** Passwords, which are supposed to be "shared secret" knowledge authenticators, are very easily defeated. Some more recent variations of TFA include texting a unique passcode to a subscriber's mobile phone. However, bad actors can take over and divert cell phone numbers, or steal the physical device. A bad actor can then trigger a text to the phone number, and needs only one additional factor to authenticate the subscriber's identity and obtain access to that individual's account.

- **Biometric Authenticators:** Although (biophysical) biometric authenticators, such as fingerprints and iris scans, are more difficult to defeat than TFA and are increasingly ubiquitous (most smartphones have built-in fingerprint scanners; next-generation smart phones have built-in iris scanners; and facial recognition capabilities are built into many personal computer systems), they can be spoofed or fraudulently validated. For instance, the Chaos Computing Club of Germany replicated Apple's TouchID within 48 hours, using a high-resolution photo of a subscriber's [user's?] fingerprint that was on the phone's surface and using a 3-D printer of the photo to create a fingertip simulacrum.

Box 11. Behavioural biometric data

Monitoring behavioural biometric data can be a risk-mitigating method to ensuring the digital ID is used by the same person it was issued to (i.e. that it is properly authenticated). Monitoring behavioural data, such as the dominant hand the user uses to hold their phone, or the speed of typing in a code, can identify changes in these behaviours. This can help detect when a legitimate digital ID is being used by a different person (i.e. someone who is not the subscriber), which may occur with stolen, compromised or sold digital IDs. However, it is important to note that changes in behavioural biometric data will not be able to spot situations where issues in enrolment or authentication have occurred and the straw man's behavioural biometrics become the base line for measurement.

Source: Sweden

Box 12. Further input required

Delegations are requested to provide other examples of potential risks associated with digital ID systems or solutions that bad actors can exploit or have exploited to facilitate ML/TF.

Benefits and Risks of Digital ID for Financial Inclusion Objectives

91. The 2019 FATF Ministerial Declaration accompanying the Mandate of the FATF commits the FATF to continuing to promote financial inclusion.[15] Financial inclusion policy objectives are viewed as complementary to FATF's financial integrity objectives as inclusion broadens the scope of transparency and crime protection afforded by AML/CFT.[16]

92. Legal identity, in turn, is recognised as a key enabler of financial inclusion and of broader, sustainable development. Digital ID and digital financial services have emerged as core components of effective financial inclusion. Easier identification and verification

[15] FATF Mandate (April 2019), paragraph 13.

[16] FATF Revised Guidance on AML/CFT and Financial Inclusion (2017) par 29; Bester, H., et al (2008), Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines. The FIRST Initiative. The World Bank, Washington, DC; Chatain, P-L., et al (2011), Protecting Mobile Money Against Financial Crime: Global Policy Challenges and Solutions. The World Bank, Washington, DC, 145.

processes supports the efforts of regulators and financial service providers to combine more efficient and convenient customer on-boarding with effective and efficient AML/CFT measures, even in non-face-to-face situations. The importance of digital ID has grown as the range of internet services, including financial services, expanded and as access to the internet increased, especially in developing economies.

93. An overly cautious, non-risk-based approach to AML/CFT safeguards can have adverse effect on financial inclusion. In recognition of the complementarity of financial integrity and financial inclusion goals the FATF recognised "financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes" as an example of a potentially lower risk scenario for the purposes of Recommendation 10. The FATF has also issued guidance on financial inclusion and supplemented these with examples of simplified CDD in 2017.[17]

94. Digital ID can improve the ability of many more individuals in developing countries to engage in electronic commerce, e-government and many other online interactions. As many of these remote transactions involve financial services, the availability of digital ID has become critical in facilitating access to a broad range of such services. ID infrastructure is key to digitalising Government-to-Person (G2P) payments, [18] such as social benefit transfers (e.g. conditional cash transfers, child support payments and student allowances), government employee salaries and pensions and tax refunds. Access to a transaction account is necessary to facilitate these payments which is predicated by the need to provide reliable proof of identity, even in remote (non-face-to-face) situations.

95. Availability of credit histories has become a key condition to access credit for both individuals and firms. Credit histories are built through consolidation of information collected from different sources which require the identification of the consumer with the underlying payment behaviour data items collected and consolidated typically through Credit Reporting Systems (CRS). The International Committee on Credit Reporting (ICCR) recognised that credit reporting systems to be effective for disadvantaged individuals require reliable mechanisms for identifying individuals and firms as well as for linking them unequivocally with their financial obligations.

96. A digital ID that would enable access to financial services, while also meeting risk management policies, is especially relevant for marginalised segments of society such as women, poor rural farmers, refugees, asylum seekers, returnees, youth and MSMEs. The 2017 Global Findex Survey shows that the lack of documentation was the primary barrier to access to financial services cited by 26 percent of unbanked individuals in low-income countries.

97. The benefits of a digital ID can be amplified through collaborative CDD models such as centralised KYC and provide the basis for the development of KYC utilities and registries. This means that once a CDD check is conducted for a person linked with a digital ID, the identity and its corresponding check can be held on a KYC registry for example. Later on, if the consumer wanted to access a new financial product or service with a different service provider, they will not need to go through the process of submitting various documents to prove their identity again. On the other hand, the benefits of Digital ID can me underscored and lead to exclusion if they do not allow broad coverage and access by all financial service providers. Where the private-sector is involved in providing digital ID services, anti-competitive motivations could create the risk of exclusion.

[17] FATF Revised Guidance on AML/CFT and Financial Inclusion (2017).

[18] http://www.worldbank.org/en/topic/financialinclusion/brief/pafi-task-force-and-report

Box 13. Pakistan Mobile Service Provider

Identification is vital to the mobile and telecommunications industry, not only due to their need to identify customers as part of their core business processes, but also because they provide mobile identity platforms and services to other industries and sectors.

High levels of mobile penetration contribute open the door to mobile financial services including payments and lower the cost of financial services allowing mobile service providers to operate an important gateway to expanded digital ID services through their authentication processes.

The development of Pakistan's Computerized National ID Card (CNIC) and its relationship with mobile finance illustrates these mutually reinforcing goals of identity ecosystem development and mobile sector growth. In 2014, the Government of Pakistan mandated that all SIM card registrations be verified with biometric data drawn from the country's national ID system, managed by the National Database and Registration Authority (NADRA). This integration proved to be a turning point for the expansion of mobile industry development in the country.

A few key contextual factors made Pakistan an especially promising area for mobile development facilitated by digital ID. First, most citizens already carried a CNIC, which included coded fingerprint data along with additional personal information. Requiring CNIC registration for SIM cards created a positive network effect, allowing the CNIC system to enrol the last 10 percent of Pakistani citizens who had previously lacked an identity. Second, Pakistan had very low levels of financial inclusion. In 2014, only 13 percent of the adult population in Pakistan had access to formal financial services, including just 5 percent of women. The mobile penetration rate was comparatively high, however, reaching nearly 50 percent of the total population.

Telenor, at the time the second largest mobile network operator in Pakistan, took advantage of the opportunity to expand its financial offerings through its Easypaisa payments service. The company successfully negotiated for the Bank of Pakistan to accept CNIC-verified SIM registration information as sufficient identity authentication for its own KYC purposes. This reduced on-boarding time to under one minute, and allowed for Telenor to offer mobile money services to their clients at the point of SIM registration.

Source: Groupe Speciale Mobile Association (GSMA), 2016

Data Protection and Privacy Risks

98. Digital ID involves the collection and processing of personal information. Information collected in databases to create an individuals' identity typically refer to inherent attributes for individuals including age, height, date of birth, and fingerprints of the individual or other biometric information. Identity information might also include other set of attributes that are attached to the individual but are not related to its intrinsic nature such as e-mail address, login IDs and passwords, telephone number, social security ID, and passport number. Misuse of identification data and breaches in security can result in identity theft, physical harm, discrimination, and emotional distress to individuals causing them to lose trust in the system. Financial institutions can also suffer reputational damage and financial loss.

99. Although it will be the responsibility of the Government to establish the overall data protection and privacy framework in each jurisdiction, there are functions, such as the preservation of the confidentiality and integrity of the data, which are primary responsibility of the data controller (aka Identity Provider). In addition, security measures and other safeguards that preserve personal information from unauthorised access, data loss, data corruption or data abuse are also necessary considerations for Digital ID Providers but also for all others that access such information for verification purposes.

100. Moreover, in countries where there is no data protection laws in place privacy risks can be exacerbated resulting in a lack of trust in the system.

Box14. Challenges to Digital ID frameworks

In India, the Supreme Court's decision challenged the right of privacy to Aadhaar number holders. A number of privacy issues were raised based on such Court Decision including; (i) whether the data collected, stored and used by the national ID system violated any privacy rights, including use of biometric data and authentication data which can facilitate improper surveillance of individuals, (ii) whether it is appropriate to require data subjects to link their national ID number to their income tax number, bank account, or mobile phone, (iii) whether, and under what circumstances, the private sector should be entitled to use the national ID and related authentication services, (iv) to what extent can national ID data or the results of authentication transactions be linked to other government databases.

The India Supreme Court decision in the Aadhaar case highlights the critical need for a legal framework to govern any identity system (particularly a national ID system), and the vital importance of ensuring that such framework adequately and appropriately addresses the key issues.

Source: World Bank

101. In order to mitigate privacy and data protection and privacy related risks, Digital ID Providers could conduct a privacy impact assessment (PIA) to identify potential areas that could create challenges when developing the system in consultation with Data Protection Authorities, where relevant. Some of the key aspects related to the use of personal information under a Digital ID environment relate to the following;

- Implementation of data minimisation principle: what type of information should be included in the digital records and what data items could be accessed by third parties?
- Including clear rules to access Digital ID under the data governance framework; the data governance framework should take into consideration scenarios of legitimate interest (i.e. financial intelligence units) and those that call for individual's consent.
- When applicable, design a consent mechanism that adequately ensures individuals choice regarding third parties accessing their Digital ID and clearly identify the purposes for such use.

102. Cybersecurity risks are present in any information systems. However, under a system containing personal information that is critical for the individual but also for the provision of services and enabling access to financial services and others, the risks should be mitigated allowing a prompt restoration to the situation before the event and have in place sufficient mechanisms to allow business continuity. Digital ID service providers could undertake threat-modelling exercises to assess potential internal and external threats throughout the identity lifecycle, and conduct regular audits of the legal, technical, and procedural security measures to ensure that personal data is well protected.

SECTION V: ASSESSING THE TRUSTWORTHINESS OF DIGITAL ID

103. In the digital ID context, the broad requirement that digital "source …data or information" must be "reliable, independent" means that the digital ID products or services used to conduct customer identification/verification and authentication of customer identity rely upon technology and processes that provide an *appropriate* level of trustworthiness/reliability, and are not subject to internal or external manipulation or falsification (including by cyberattack), to fabricate and credential false identities or authenticate unauthorised users.

Risk-Based Approach to the Use of Digital ID Systems and Solutions

104. Governments, financial institutions, and other stakeholders should use a risk-based approach (RBA) to determine whether a given digital ID system or solution is sufficiently trustworthy to comply with Recommendation 10.

105. The RBA to digital ID has two components:

(1) An *assessment of the technical reliability*[19] of the digital ID system or solution's technology, architecture and governance to determine the *reliability* of the digital ID system or solution *as a technical matter*; and

(2) A *broader, risk-based determination* of whether, given its technical reliability, the particular digital ID system or solution provides an *appropriate* level of *trustworthiness* for Recommendation 10 purposes,) in light of the potential ML, TF, fraud, and other illicit financing risks at stake, if there is a failure of identification/verification and/or identity authentication.

106. The first component of the RBA evaluation is objective and technical. For instance, as discussed below, it could involve an assessment of the reliability of each of the main processes involved in the digital ID system or solution—identity proofing, enrolment and binding; authentication and credential life cycle management; and (if relevant); federation and interoperability

107. The second component of the RBA evaluation builds on the first component, by considering whether the digital ID system or solution is adequate, *in the context of the relevant* illicit financing risks. Whether a digital ID system or solution complies with Recommendation 10 requirements thus requires considering reliability in relationship to the illicit financing risks associated with the type of customer; financial products and services; and the country or geographic area that will be involved in providing the financial services.

108. A more detailed discussion of the relationship of *identity risk management* to the RBA to *ML/TF risk* mitigation measures—including tiered CDD—is provided later in this Section.

[19] In the technical standards for digital identity, discussed below (cross ref. pages), the term "level of assurance (LoA) refers to the level of trustworthiness or reliability of a digital identity system or solution. As discussed below, the term has now been replaced with more granular assurance levels for each of the three main constituent steps or processes of a digital identity system.

Application of the RBA to digital identity systems provided by government or the private sector

109. The RBA to the use of digital ID systems is relevant for a broad range of actors in the digital ID ecosystem. Governments and financial institutions, as well as other private sector stakeholders, have very different roles and responsibilities in the digital ID space, and thus should use the digital ID RBA in ways tailored to their respective purposes and obligations.[20]

110. The application of the RBA by regulated entities will differ depending on two factors:

(1) whether the identity is provided by the government or by the private sector.

(2) whether the regulated entity has an opportunity to select digital ID products and services that have different levels of technical reliability.

111. The following table provides examples of when the RBA applies to digital ID systems and solutions.

Table 4. Examples of when to apply the RBA to digital ID systems

Actor	Situations where RBA should be applied
Governments	• To shape digital ID system architectures and legal frameworks, when developing and implementing national-level government-provided digital ID systems (universal or functional) and either permitting or requiring their use to conduct customer identification/verification at on-boarding and authentication of identity for account access/ongoing DD; and/or • To certify that a specific private sector-provided digital ID solution has a given level of technical reliability for each of its basic digital ID steps; and (depending on the digital ID ecosystem in the jurisdiction and the jurisdiction's legal framework) (i) to authorize government entities to use it for identifying and authenticating the identity of persons interacting with the government to e.g., obtain government benefits and services; and/or (ii) to authorize financial institutions to use it to conduct customer identification/verification and related CDD activities; and/or • As part of financial sector regulation and supervision, to determine whether a financial institution, DNFP, or VASP's use of a given private sector identity solution complies with the jurisdiction's national legal framework, implementing Recommendation 10 requirements for proving legal identity in the financial sector.
Regulated entities	• To decide whether a given private sector-provided digital ID solution complies with Recommendation 10's trustworthiness (reliable, independent) requirements, as implemented by national law in the jurisdiction; or • With respect to the required or permitted use of government-provided digital ID systems for on-boarding and account access, to decide whether the financial institution's own risk management policies and practices require a higher level of trustworthiness, such that the financial institution should o Adopt additional identity assurance measures (e.g., supplemental digital data or processes, such as additional digital device authenticators, geolocation data, or behavioural biometric data); o Adopt additional illicit financing mitigation measures to reduce the risks of ML, TF, and fraud associated with the types of customers; financial products and services; and/or the country or geographic area involved; and/or • To help assess the AML/CFT risks presented by a given country or financial institution, in deciding whether to engage in particular correspondent relationships, or to provide financial services in the country.
International Organisations and NGOs	• Creating or participating in major international initiatives or more limited, bi-lateral efforts to help developing countries establish trustworthy national-level digital ID systems, to ensure that the digital ID systems their projects are helping develop and implement can comply with Recommendation 10 requirements and are thus fit-for purpose to prove legal identity in the financial sector.

[20] In addition, as discussed in greater detail below, the application of the RBA by financial institutions may differ, depending upon whether a government-provided digital identity system or a private sector-provided digital identity solution is used for customer identification/ verification and related CDD activities.

Applying the RBA to government-provided or certified digital ID systems

112. As a general matter, in applying the RBA, when the appropriate authorities require or authorise (permit) the use of a government-provided digital ID system or private sector-provided digital ID solution to conduct CDD, regulated entities should be permitted to assume the technical reliability of the ID (and need not conduct their own evaluation of the first component of the RBA to digital ID).

113. In addition, if the government-provided digital ID system does not offer a range of ID products/services, with different levels of technical reliability, regulated entities should be permitted to rely on the appropriate authorities' decision that the system is appropriate for customer identification/verification, without conducting their own RBA evaluations of whether the digital ID system is appropriate for this purpose and complies with Recommendation 10 requirements (the second component of the RBA to digital ID). This is because the government stands behind the trustworthiness of the digital ID system, and the regulated entity does not have an opportunity to select different digital ID products and services.

114. The same is true for private sector-provided digital ID solutions that are authorised by the government for use in conducting CDD but are not differentiated by technical reliability. Financial institutions should not be required to conduct their own RBA determination of whether using a particular, government-certified digital ID solution is appropriate, when the government has effectively made that decision for the financial sector.

115. That said, even in the above circumstances, financial institutions are encouraged to consider whether they should adopt additional digital ID risk mitigation measures (if available), such as additional data points or additional authenticators, and/or ML/TF risk mitigation measures, given the financial institution's own AML/CFT and fraud risk management framework.

116. Importantly, in some jurisdictions,[21] the government certifies a broad range of private sector-provided digital solutions, with different levels of audited, publicly disclosed technical reliability, and leaves it up to regulated entities (and to different government entities, with different services and different ID-failure risks) to determine which of the various digital ID solutions are appropriate for them to use. When that is the case, regulated entities may rely on the solutions certified technical reliability and need not conduct their own evaluation (component one of the RBA to digital ID), but they must still conduct the RBA's second, broader trustworthiness evaluation, and select a digital ID solution for CDD that is appropriate, given its level of technical reliability, and the potential ML, TF, fraud and other ML/TF risks associated with the financial institution's customer; products and services; geographic area of operations, and other relevant ML/TF risk factors.

Leveraging the Digital ID Technical Standards to Implement the RBA

117. As discussed above, the RBA to the use of digital ID systems requires governments (as IDSPs and/or as regulators, supervisors, and policy makers) and financial institutions (as relying parties) to adequately consider the relevant ID risk factors, in relation to the relevant ML/TF risk factors and mitigating measures. Several jurisdictions have developed **digital ID technical standards** which provide a useful tool for applying the first component of the RBA to digital ID on technical reliability. The International Standards Organisation (ISO) is developing global digital ID technical standards based on these national standards.

[21] See, for example, the United States NIST 800-63-3 and USG ICAM Policy.

118. Governments and regulated entities are therefore encouraged, but not required, to consider the ID risk information provided by the technical standards when evaluating technical reliability. They are also encouraged to consider the reliability of each of its main digital ID processes separately. This is because, depending on the potential ML/TF risk factors and mitigating measures, the same degree of reliability may not be required for ID proofing as for authentication or (if applicable), federation.

119. The **process-by-process approach to reliability** is particularly relevant in the context of financial inclusion. The technical standards for UK Gov.Verify and the final version of the US NIST 800-63 Digital ID Guidelines retired the concept of level of assurance (LOA) as a single ordinal for a digital ID system or solution and replaced it with separate assurance levels for each of the ID system or solution's basic processes: ID assurance level (IAL); authentication and credential life cycle management level of assurance (ALA); and federation level of assurance (FAL).

120. This Guidance relies on the technical standards, as set forth in the United States Government NIST *Digital ID Guidelines* with adopts the process-by-process approach to reliability as this expected to be reflected in international standards that are currently in development. While other national digital ID technical standards may differ in certain ways, [22] they are in most part comparable to the NIST standard. Hereafter, when this Guidance uses the general terms, "the digital ID technical standards," or "technical standards," in reference to assurance levels and related requirements, it is referring to the framework set out in the NIST *Digital ID Guidelines*.[23]

121. Digital ID technology and architecture, and digital ID technical standards, are dynamic and evolving. The technical standards themselves are flexible and outcome-based. They permit different technologies and architectures to satisfy the requirements for the distinct levels of assurance at present, and are framed in ways intended to help make them as future-proof as possible. Jurisdictions should avoid adopting a fixed, prescriptive approach that locks in current assurance level requirements as a ceiling, rather than a floor, for reliability.

122. Similarly, regulated entities may consider any relevant information in applying the RBA to the use of digital ID systems and solutions for CDD. This includes other technical standards, such as the FIDO Alliance technical standards for hardware-based ID authentication, or the GMSA standards for identifying users of mobile communication devices; or the draft provisions of a UN instrument, currently under development by the United Nations Commission on International Trade Law (UNCITRAL) Working Group IV (Electronic Commerce), for the cross-border recognition of ID management systems and trust services used in international commercial transactions.

Using digital ID assurance levels to assess technical reliability

123. The technical standards set forth three, progressively more reliable, assurance levels with increasingly rigorous technical requirements, for each of the three main steps in a digital ID system:

[22] For example, some digital identity technical standards may not currently have process-by-process assurance levels, and instead apply the earlier, unitary LOA to the digital identity system or solution. Jurisdiction-level technical standards may also currently use different numbers of and/or names for the assurance levels —issues which the mapping exercise, noted in text above, is intended to resolve.

[23] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

- Identity Assurance Level (IAL) refers to the reliability of the ID proofing process, as determined by the technical digital ID requirements it requires. The assurance levels for ID proofing, in order of increasing reliability, are IAL1; IAL2; and IAL3;
- Authentication Assurance Level (AAL) refers to the reliability of the authentication process. The assurance levels for authentication (and credential life cycle management), in order of increasing reliability, are AAL1; AAL2; and AAL3; and
- Federation Assurance Level (FAL) (if applicable) refers to the reliability of the federated network—i.e., to the reliability (strength) of an assertion used to communicate authentication results and ID attribute information in a federated environment. The assurance levels for federation, in order of increasing reliability, are FAL1; FAL2; and FAL3.

124. Just as the Interpretative Note to Recommendation 10 provides examples of potentially higher-risk and lower-risk ML/TF factors, the technical standards provide ID *reliability* factors, in the form of assurance levels for the three basic constituent processes of a digital ID system or solution. Each assurance level reflects a specified level of certitude or confidence in the process at issue. A process with a higher assurance level is more reliable; a process with a lower assurance level presents a greater risk of failure and is less reliable. Authorities and regulated entities can use the assurance levels to evaluate the reliability of a given digital ID system or solution, as part of their RBA to digital ID.

125. The technical standards support a process-by-process evaluation of reliability, and contemplate that different digital ID processes may, but need not, all be at the same level of assurance. More fundamentally, the RBA requires a determination of what assurance levels for which processes are appropriate, given the ML, TF, fraud, and other illicit financing risks. That approach does not support a one-size-fits-all determination that, e.g., financial institutions must use digital ID systems or solutions with IAL2, AAL2, and FAL 2, in order to be compliant with Recommendation 10s trustworthiness requirements.

126. To illustrate both the type of ID reliability factors that appropriate authorities, financial institutions, and other stakeholders might leverage, and the flexibility allowed by the technical standards, the discussion below summarises the assurance levels and describes in broad terms, some of the technical requirements for ID Proofing. The discussion of the requirements for the various IALs is limited, and is presented by way of example. See Appendix B for more a more detailed description of the requirements in the technical standards.

Box 15. Leveraging the Digital ID Technical Standards to Evaluate the Reliability of ID Proofing

IAL1—There is no requirement to link the applicant to a specific real-life identity –i.e., there is no assurance that the applicant is who they claim to be, because no ID proofing is required. This means that:

- No identity attributes are required;
- The applicant may, but need not, self-assert identity attributes.
- If any attributes are provided or collected, they are either self-asserted or treated as self-asserted and are not validated or verified.

IAL2—There is high confidence that the identity evidence is genuine; the attribute information it contains is accurate; and that it relates to the applicant.

- Evidence of identity attributes is collected based on the quality of the evidence (weak, fair, strong and superior) and the number of documents or digital information relied upon.
- The identity evidence is validated as genuine.
- The identity evidence and the identity attributes it contains support the real-world existence of the claimed identity, and
- The identity evidence is verified, confirming that the validated identity relates to the individual (applicant), including address confirmation
- Either remote or in-person identity proofing is permitted.
- Biometrics are optional
- In instances where an individual cannot meet conventional identity proofing requirements, such as identity evidence requirements, a trusted referee may be used to assist in identity proofing the applicant.

IAL3—There is very high confidence that the identity evidence is genuine and accurate; that the identity attributes belong to a real-world person, and that the claimant is that person and is appropriately associated with this real world identity.

- Identity proofing must be in-person; NB: In-person identity proofing includes supervised remote identity proofing, as well as physically present identity proofing (i.e., physical interaction with the applicant). (See the discussion of Non-Face-to-Face On-boarding, below.)
- The identity evidence quality requirements are more rigorous
  - IAL requires providing additional identity evidence of superior strength
  - Biometrics are mandatory. Biometric identity attributes and biometric processes are required to detect fraudulent or duplicate enrolments and as a mechanism for binding the verified identity to a credential
- Identity attributes must be verified by an authorised and trained CSP representative.

Source: United States NIST standards

Special considerations for financial inclusion

The Relationship of the Digital ID RBA Identity Risk Management to AML/CFT RBA and ML/TF risk mitigation measures

127. As discussed above, under the RBA, whether the use of digital ID systems and solutions to conduct customer identification/verification complies with Recommendation 10 reliable, independent requirements depends on whether the digital ID system or solution is sufficiently trustworthy for these purpose, given the relevant ML/TF risk factors and mitigating measures involved.

128. The RBA to digital ID is dynamically related to the RBA to AML/CFT, because where the risks of ML or TF are lower, one or more of the digital ID system or solution's basic processes could be less reliable and still satisfy Recommendation 10 requirements. In other words, greater technical reliability is required for higher risk ML/TF situations and conversely; lower risk ML/TF situations may permit use of digital ID systems with lower levels of reliability for the processes that are most directly relevant for combating ML/TF risks.

129. For example, when the ML/TF risks of on-boarding a given potential customer are lower, because of the individual's risk profile, a digital ID system or solution with a lower IAL may be appropriate. Similarly, when the illicit financing risks associated with unauthorised account access are higher (e.g., because of the prevalence of ID theft in a jurisdiction), but a customer is low risk, an ID system or solution with lower IALs (for customer identification/verification at on-boarding) but greater reliability for its authentication processes may be used under Recommendation 10.

130. The interrelationship of digital ID trustworthiness and the RBA for AML/CFT has important implications for financial inclusion. For example, under tiered CDD, where a poor, formerly excluded or underserved individual would be provided an account with built-in AML/CFT risk mitigants, such as limitations on the account's total value and the value and number of transactions within a specified time frame, a lower level of reliability may be appropriate for ID proofing, enrolment and binding processes, than is appropriate for authentication. Authenticating the customer's identity to authorize the claimant to conduct transactions, even for low value accounts, is important to combat fraudulent transfers and to make sure that tiered CDD value, velocity and volume requirements are not circumvented.

Trusted Referees under the Technical Standards (IAL2)

131. As noted in the summary of identity assurance level requirements, above, when an individual cannot meet the conventional IAL2 identity evidence requirements, the technical standards permit the DISP (CSP) to use trusted referees—such as notaries, legal guardians, medical professionals, conservators, persons with power of attorney, or some other form of trained and approved or certified individual—to vouch for or act on behalf of the applicant,[24] in accordance with the jurisdiction's applicable laws, regulations, or agency policies.

132. Trusted referees may be used at IAL2 for both remote and in-person ID proofing. Use of trusted referees requires the CSP to:

[24] NIST 800-63A 4.4.2. IAL2 Trusted Referee Proofing Requirements.

- Establish written policies and procedures, addressing how a trusted referee is determined (selection criteria) and the lifecycle of the trusted referee's status as a valid referee, to include any restrictions, revocation and suspension requirements;
- Identity-proof the trusted referee at the same IAL as the applicant, and determine the minimum identity evidence required to establish the relationship between the trusted referee and the applicant.

Non-Face-to-Face On-boarding and Transactions

133. Digital ID systems may enable non-face-to-face business relationships and transactions—and their use for customer identification/verification at on-boarding, and to authenticate identity for account access, when the situation is lower-risk because it involves "financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes" (INR 10).

134. Moreover, INR 10 sets out examples where regulated entities may be allowed to conduct simplified CDD measures that take into account the nature of the lower risk. In the low-risk situation described above (e.g., tiered accounts for financial inclusion purposes), simplified CDD permits verifying the customer's identity until account transactions rise above a defined monetary threshold.

135. As noted above, the technical standards permit in-person identity proofing at IAL2, and **require in-person identity proofing at IAL3**. Importantly—particularly with respect to financial inclusion objectives—in-person identity proofing, enrolment and binding (henceforth in this section, identity proofing)—even at IAL3--can be conducted either by:

- A physical interaction with the applicant, supervised by an operator, where the applicant is in the same physical location as the DISP (CSP) (in-person/same location physical interaction); or
- A remote interaction with the applicant, supervised by an operator, based on specified requirements for remote in-person identity proofing, which achieves comparable levels of confidence and security to in-person/physical interaction identity proofing (in-person/supervised remote).

136. For either type of in-person identity proofing:

- The *operator* must inspect the biometric source (e.g., fingers, face) for presence of non-natural materials as part of the proofing process; and
- The *CSP* must collect biometrics in a way that ensures that the biometric is collected from the applicant and not another subject and that all biometric performance requirements set forth in the standards are applied.

137. The technical standards specify a range of requirements to establish that in-person/supervised remote identity proofing is comparable, in terms of trustworthiness, to in-person/same location physical interaction identity-proofing and enrolment.

Appendix

Appendixes to be inserted:

- Glossary
- Summary of technical standards
- Summary of ID4D Principles - id4d.worldbank.org/principles

Annex B. World Bank Proposal – categorisation of types of digital identity

Digital identity schemes can be provided through different models. As noted above, this can involve one or multiple actors playing different roles within the identity lifecycle, including as different types of IDSPs (RAs, CSPs, and Verifiers) and as relying parties. In addition to variation in the number of entities involved, digital ID systems also vary in their involvement of both public and/or private sector actors. Furthermore, these models are continuously evolving. Broadly speaking, however, we are able to categorize various types of digital ID systems into two groups:

a. **Government-recognized digital ID:** *A government-recognized digital ID system is one that provides proof of identity for official, government transactions* (i.e., "proof of legal identity"), such as in-person and online access to public services and rights. Generally speaking, this require a relatively high-level of assurance; as such, the identity proofing for these systems has often relied on "authoritative sources" [25] of identity information operated by the government, including by systems like national IDs and population registers or—in the absence of these systems—sectoral ID systems like social security numbers and voter lists. For certain groups—such as refugees—international organizations like UNHRC may instead serve as authoritative sources of identity information. While the authoritative sources for these systems are typically (though not necessarily) government-operated, the digital ID infrastructure itself—including credentials and authentication—may be provided through multiple arrangements (see diagram below), many of which involve private sector companies as IDSPs. This includes:

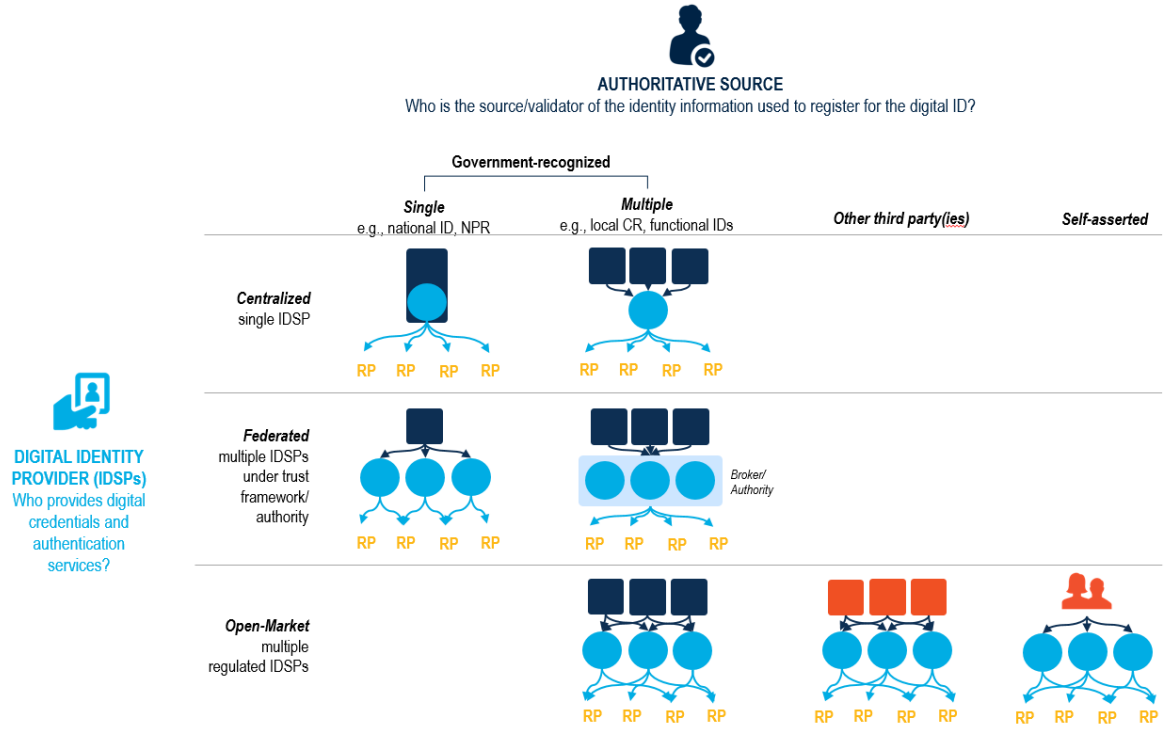
   i. **Centralized digital ID:** Under the centralized model, there is a single IDSP for a particular system that is typically—though not necessarily—a government agency. In some cases, the digital ID is provided by the same agency that manages the country's national ID or similar-type system (e.g., **Belgian eCard**, **Netherlands' DigiD**, **India's Aadhaar,** and eIDs in **Estonia**, **Singapore**, **Peru**, and many others). In other cases, the digital ID is provided centrally by an IDSP that relies on multiple functional or lower-tiered government ID systems as authoritative sources for identity proofing (e.g., the current myGovID system in **Australia**).

   ii. **Federated digital ID:** Other systems have *multiple* IDSPs that operate in a coordinated, certified/accredited manner—e.g., under a trust framework or federation authority—to provide government-recognized digital ID. These IDSPs may be public and/or private entities and may either leverage a single ID system as their authoritative source (e.g., **BankID in Sweden**, **NemID in Denmark, Itsme® in Belgium**), or draw from multiple functional systems as well as civil registers through a "broker" or federation authority (e.g., **UK.GOV Verify**, **Canada**).

[25] An **authoritative source** for identity information can be defined as "a repository or system that contains attributes about an individual and is considered to be the primary or most reliable source for this information. In the case that two or more systems have mismatched or have conflicting data, the data within the authoritative data source is considered the most accurate." See FICAM Playbook at: https://bnbuckler.github.io/ficam-identity/2_step-2/.

iii. **Open-market digital ID:** Finally, some countries have multiple regulated IDSPs that provided government-recognized digital ID based on multiple functional IDs and or civil registers as authoritative sources of identity information. In contrast to the federated system, however, these IDSPs operate based on bilateral agreements with RPs rather than a central scheme (e.g., **U.S.**).

b. **Other forms of digital ID:** In addition to the "legal" forms of digital identity discussed above, countries may have a host of other digital ID products and services operated by private sector entities. These systems may be (a) provided for a firm's internal use and/or (b) as a service offered to individuals and/or other businesses. In some cases, the private-sector-provided IDs may be **derived** directly from the government-recognized authoritative sources or digital IDs described above or may rely on these IDs as part of the identity proofing process. In other cases, identity proofing may be based on non-official, third-party sources (e.g., a credit score provider). Finally, some private-sector provided identities are self-asserted by the users themselves (e.g., social media, email accounts, commercial platforms, etc.) and undergo no identity proofing process. There are also emerging decentralized (also called "self-sovereign") models of digital identity.[26]



[26] To our knowledge, such models have not yet been accepted as "government-recognized" proof of identity for use in official (online or in-person) transactions.