DRAFT GUIDANCE ON DIGITAL IDENTITY

FOR PUBLIC CONSULTATION

For more information, including areas of focus:
www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html

Table of Contents

EXECUTIVE SUMMARY **2**
SECTION I: INTRODUCTION **8**
SECTION II: DIGITAL ID TERMINOLOGY AND KEY FEATURES **11**
SECTION III: FATF STANDARDS ON CUSTOMER DUE DILIGENCE **17**
SECTION IV: BENEFITS AND RISKS OF DIGITAL ID SYSTEMS FOR AML/CFT COMPLIANCE AND RELATED ISSUES **22**
SECTION V: ASSESSING WHETHER DIGITAL ID SYSTEMS ARE RELIABLE AND INDEPENDENT IN LINE WITH A RISK-BASED APPROACH TO CDD **32**
Appendix A: Description of a Basic Digital Identity System and its Participants **39**
Appendix B: Country case studies **50**
Appendix C: ID4D Principles on Identification for Sustainable Development **63**
Appendix D: Digital ID assurance framework and technical standard setting bodies **67**
Appendix E: Overview of US and EU digital ID assurance frameworks and technical standards **68**
Glossary **72**

EXECUTIVE SUMMARY

1. Digital payments are growing at an estimated 12.7% annually, and are forecast to reach 726 billion transactions annually by 2020.[1] By 2022, an estimated 60% of world GDP will be digitalised.[2] For the FATF, the growth in digital financial transactions requires a better understanding of how individuals are being identified and verified in the world of digital financial services. Digital identity (ID) technologies are evolving rapidly, giving rise to a variety of digital ID systems. This Guidance is intended to assist governments, regulated entities[3] and other relevant stakeholders determine how digital ID systems can be used to conduct certain elements of customer due diligence (CDD) under FATF Recommendation 10.

2. An understanding of how digital ID systems work is essential to apply the risk-based approach recommended in this Guidance. Section II of the Guidance briefly summarises the key features of digital ID systems that are explained in detail in Appendix A.

3. Section III summarises the main FATF requirements for customer identification and verification and ongoing due diligence addressed in this Guidance. It also clarifies that non-face-to-face customer-identification and transactions that rely on reliable, independent digital ID systems, may present a standard level of risk, and may even be lower-risk.

4. The risk-based approach recommended by this Guidance relies on a set of open source, consensus-driven assurance frameworks and technical standards for digital ID systems (referred to as 'digital ID assurance frameworks and standards') that have been developed in several jurisdictions. The International Organization for Standardization (ISO), together with the International Electrotechnical Commission (IEC), is standardising these digital ID assurance frameworks and updating a range of ISO/IEC technical standards relating to identity, information technology security and privacy to develop a comprehensive global standard for digital identity systems. An identity assurance framework sets requirements for different 'assurance levels' or 'levels of assurance'. Assurance levels measure the level of confidence in the reliability of a digital ID system and its components. While the assurance levels developed by various jurisdictions may vary in certain respects, for ease of reference, this Guidance primarily refers to the US National Institute of Standards and Technology (NIST) digital ID assurance framework

[1] Capgemini & BNP Paribas (2018), *World Payments Report 2018*, accessed online at: https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf.

[2] International Data Corportation (IDC), *IDC FutureScape: Worldwide IT Industry 2019 Predictions*

[3] For the purposes of this guidance, 'regulated entities' refers to financial institutions, virtual asset service providers (VASPs) and, designated non-financial businesses and professions (DNFBPs), as defined under the FATF Standards and to the extent DNFBPs are required to undertake CDD in the circumstances specified in R.22. In June 2019, the FATF revised Recommendation 15 (New Technologies) and INR 15 to, among other things, impose Recommendation 10 CDD obligations on VASPs.

and standards (NIST Digital ID Guidelines)[4] and the EU's e-IDAS regulation.[5] Jurisdictions should consider the approach set out in this guidance in line with their domestic digital ID assurance frameworks and other relevant technical standards.[6]

5. Digital ID assurance frameworks and standards and AML/CFT regulations have different origins and intended audiences. This Guidance draws links between digital ID assurance frameworks and standards and the FATF's CDD requirements, to demonstrate that the key components of digital ID systems align with specific CDD requirements under Recommendation 10. Accordingly, the digital ID assurance frameworks and technical standards provide a highly useful tool for assessing the reliability and independence of digital ID systems for AML/CFT purposes.

CDD requirements (natural persons)	Key components of Digital ID systems
Identification / verification – R.10 (a)	Identify proofing and enrolment (with binding)– who are you? Obtain identifiers (name, DoB, ID # etc.) and ID evidence for those attributes, validate, and verify ID evidence and resolve it to identity proofed person; Binding—issue credentials/authenticators linking the person in possession/control of the credentials to the identity proofed individual (i.e.,--linking the identity proofed individual to the onboarded customer /to the customer's ID); Authentication – Are you the identified/verified individual who has possession and control of the binding credentials? (applies to 10(a) if the regulated entity is conducting identification/verification of a pre-existing ID system)

6. The Guidance explains how, in a digital finance and digital ID context, effective authentication of customer identity for authorising account access supports AML/CFT efforts.

7. Section V is the crux of the Guidance and provides guidance for government, regulated entities and other relevant parties on how to apply a risk-based approach to using digital ID systems for customer identification and verification consistent with Recommendation 10(a) and to support ongoing due diligence in Recommendation 10(d). The recommended approach is technology neutral (i.e., it does not prefer any particular types of digital ID systems). There are two elements of this approach:

a. Understanding of the assurance levels of the digital ID system's technology main components (including its architecture and governance) to determine its reliability/independence; and

b. Making a broader, risk-based determination of whether, given its assurance levels, the particular digital ID system provides an appropriate level of reliability and independence in light of the potential ML, TF, fraud, and other illicit financing risks at stake.

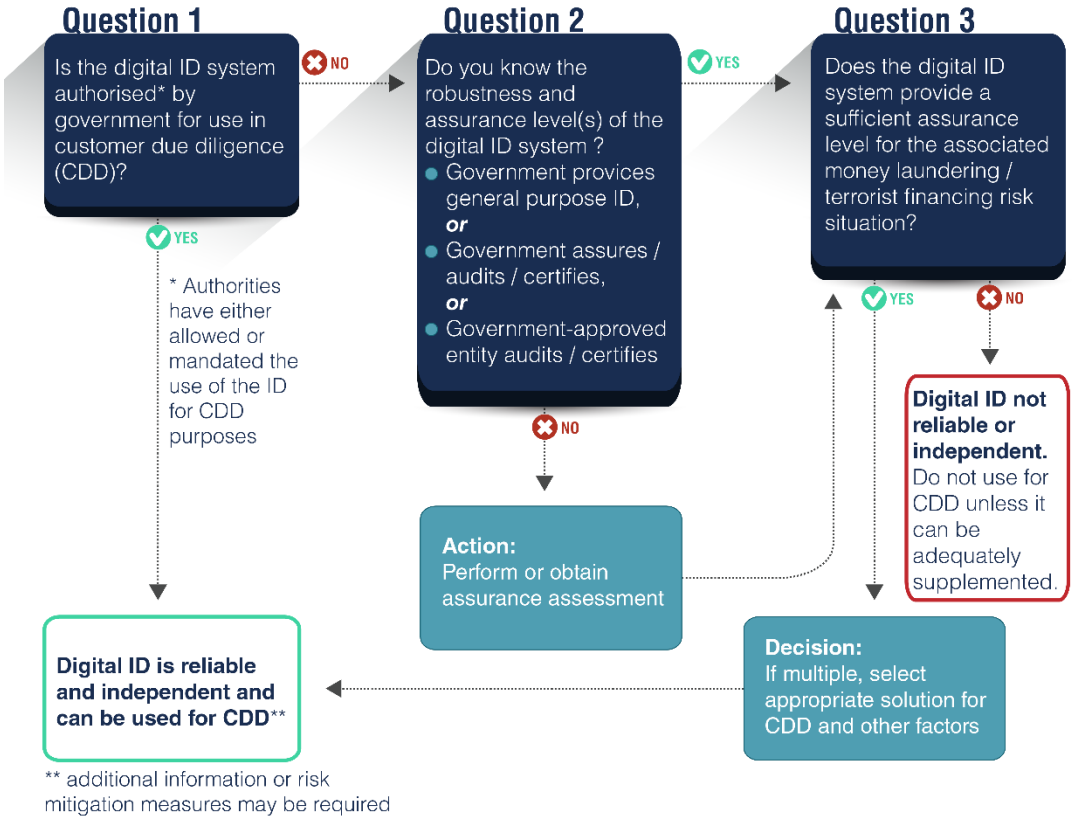
[4] The NIST 800-63 Digital Identity Guidelines consists of a suite of documents: NIST SP 800-63-3 Digital Identity Guidelines (Overview); NIST SP 800-63A: Digital Identity Guidelines: Enrollment and Identity Proofing; NIST SP 800-63B Digital Identity Guidelines: Authentication and Life Cycle Management; and NIST SP 800-63C, Digital Identity Guidelines: Federation and Assertions.

[5] Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market

[6] A jurisdiction may not have a digital ID assurance framework or technical standards specific to digital ID systems, but may have other technical standards (e.g., IT information security) standards that are highly relevant.

8. Section V explains how to leverage digital ID assurance frameworks and standards for assessing reliability/independence. It also sets out a decision process for regulated entities to guide determinations about whether the use of digital ID to conduct CDD is appropriate under Recommendation 10. Governments and regulated entities will need to adapt this decision process to the particular circumstances of the jurisdiction and of individual entities. Depending upon the digital identity system(s) and regulatory framework in a particular jurisdiction, governments and regulated entities may have different roles and responsibilities in assessing an identity system's assurance levels and its appropriateness for CDD, as reflected in the decision-making flow chart for regulated entities, below.

Figure 1. Decision process for regulated entities



9. Section IV of the Guidance explores some of the benefits of digital ID systems, as well as the risks they pose. Many risks associated with digital ID systems also exist in documentary IDs. However, identity proofing and authenticating individuals over an open communications network (the Internet) creates risks specific to digital ID systems – particularly in relation to cyberattacks and potential large-scale identity theft. On the other hand, digital ID systems that mitigate these risks in accordance with digital ID assurance frameworks and standards hold great promise for strengthening CDD and AML/CFT controls, increasing financial inclusion, improving customer experience, and reducing costs for regulated entities.

10. The Guidance highlights a number of ways in which the use of digital ID systems for CDD can support financial inclusion. First, digital ID systems may enable governments to take a more flexible, nuanced, and forward-leaning approach in establishing the required attributes, identity evidence and processes for proving official identity – including for the

purposes of conducting customer identification and verification at on-boarding in ways that facilitate financial inclusion objectives. Secondly, the digital ID assurance frameworks and standards themselves provide some flexibility in the process that can be used to identity proof and authenticate individuals, which can be tailored to meet financial inclusion objectives. Lastly, supervisors and regulated entities, in taking a risk-based approach to CDD can support financial inclusion, including via the use of digital ID systems, in line with the approach in the 2017 FATF supplement on CDD and financial inclusion.

Recommendations for authorities

11. Develop clear guidelines or regulations allowing the appropriate, risk-based use of reliable, independent digital ID systems by entities regulated for AML/CFT purposes. As a starting point, understand the digital identity systems available in the jurisdiction and how they fit into existing requirements or guidance on customer identification and verification and ongoing due diligence (and associated record keeping and third-party reliance requirements).

12. Assess whether existing regulations and guidance on CDD accommodate digital ID systems, and revise, as appropriate, in light of the jurisdictional context and the identity ecosystem. For example, authorities should consider clarifying that non-face-to-face on-boarding may be standard risk, or even low-risk for CDD purposes, when digital ID systems with robust assurance levels are used for remote customer identification/verification and authentication.

13. Adopt principles, performance, and/or outcomes-based criteria when establishing the required attributes, identity evidence and processes for proving official identity for the purposes of CDD. Given the rapid evolution of digital ID technology, this will help promote responsible innovation and future-proof the regulatory requirements.

14. Adopt policies, regulations, and supervision and examination procedures that encourage regulated entities to develop an efficient, integrated approach to digital ID streaming applicable digital processes across all relevant efforts.

15. Develop an integrated multi-stakeholder approach to understanding opportunities and risks relevant to digital ID and developing relevant regulations and guidance to mitigate the risks. Assess and leverage, where appropriate, existing digital ID assurance frameworks and technical standards adopted by the authorities responsible for identity, cybersecurity/data protection, and privacy (including technology, security, governance and resource considerations) for assessing the assurance levels of digital ID systems for use in CDD. In line with FATF Recommendation 2, co-operate and co-ordinate with relevant authorities to facilitate a comprehensive, coordinated approach to understanding and addressing risks in, the digital identity ecosystem and to ensure the compatibility of AML/CFT requirements on digital ID systems with Data Protection and Privacy rules.

16. AML/CFT authorities could consider adopting mechanisms to enhance dialogue and cooperation with relevant private sector stakeholders, including regulated entities and digital ID service providers, to help identify key identity-related opportunities, risks and mitigation measures. Mechanisms could include a regulatory ‘sandbox’ approach to provide a supervised environment to test how digital ID systems interact with national AML/CFT laws and regulations. Authorities could also consider developing mechanisms to promote cross-industry collaboration in identifying and addressing vulnerabilities in existing digital ID systems.

17. Consider supporting the development and implementation of reliable, independent digital ID systems by auditing and certifying them against transparent digital ID assurance

frameworks and technical standards, or by approving expert bodies to perform these functions.

18. Apply appropriate digital ID assurance frameworks and technical standards when developing and implementing government-provided digital identity, authorities should be transparent about how its digital ID system works and its levels of assurance.

19. Encourage a flexible, risk-based approach to using digital ID systems for CDD that supports financial inclusion. Consider providing guidance on how to use digital ID systems with different assurance levels for identity proofing/enrolment and authentication for tiered CDD.

20. Monitor developments in the digital ID space with a view to share knowledge, best practices, and to establish legal frameworks at both the domestic and international level that promote responsible innovation and allow for greater flexibility, efficiency and functionality of digital ID systems, both within and across borders.

Recommendations for regulated entities

21. Take an informed risk-based approach to relying on digital ID systems for CDD that includes:

a. understanding the digital ID system's assurance level/s, particularly for identity proofing and authentication, and

b. ensuring that the assurance level/s are appropriate for the ML/TF risks associated with the customer, product, jurisdiction, geographic reach, etc.

22. Understand the basic components of digital ID systems, particularly identity proofing and authentication, and how they map to required CDD elements (see section II and Appendix A).

23. Consider whether digital ID systems with lower assurance levels may be appropriate for simplified due diligence in cases of low ML/TF risk. For example, where permitted, adopting a tiered CDD approach that leverages digital ID systems with various assurance levels to support financial inclusion.

24. If as a matter of internal policy or practice, non-face-to-face customer identification is always classified as high-risk, review and revise those policies to take into account that customer identification/verification that relies on reliable, independent digital ID systems, with strong risk-mitigation measures in place, may be standard risk, and may even be lower-risk.

25. Where relevant, utilise anti-fraud and cyber-security processes to support digital identity proofing and/or authentication for AML/CFT efforts (customer identification/verification at on-boarding and ongoing due diligence and transaction monitoring). For example, regulated entities could utilise safeguards built into digital ID systems to prevent fraud (i.e., monitoring authentication events to detect systematic misuse of digital IDs to access accounts, including through lost, compromised, stolen, or sold digital ID credentials/authenticators) to feed into systems to conduct ongoing due diligence on the business relationship and to monitor, detect and report suspicious transactions to authorities.

26. Regulated entities should ensure that they have access to, or have a process for enabling authorities to obtain, the underlying identity information and evidence or digital information needed for identification and verification of individuals. Regulated entities are encouraged to engage with regulators and policy makers, as well as digital ID service

providers, to explore how this can be efficiently and effectively accomplished in a digital ID environment.

Recommendations for digital ID service providers

27. Understand the AML/CFT requirements for CDD (particularly customer identification/verification and ongoing due diligence) and other related regulations, including requirements for regulated entities to keep CDD records.

28. Seek assurance testing and certification by the government or an approved expert body, or where these are not available, another internationally reputable expert body.

29. Provide transparent information to AML/CFT regulated entities about the digital ID system's assurance levels for identity proofing, authentication, and, where applicable, federation/interoperability.

SECTION I: INTRODUCTION

30. The Financial Action Task Force (FATF) is committed to ensuring that the global standards encourage responsible financial innovation. In this regard, the FATF strongly supports the use of new technologies in the financial sector that align with, and strengthen, the implementation of anti-money laundering/counter financing of terrorism (AML/CFT) standards and financial inclusion goals.[7]

31. The rapid pace of innovation in the digital identity (ID) space has reached an inflection point. Digital ID standards, technology and processes, have evolved to a point where digital ID systems are, or could soon be, available at scale. Some of these relevant technologies include: a range of biometric technology; the near-ubiquity of the Internet and mobile phones (including the rapid evolution and uptake of "smart phones" with cameras, microphones and other "smart phone" technology); digital device identifiers and related information (e.g., MAC and IP addresses;[8], mobile phone numbers, SIM cards, global position system (GPS) geolocation); high-definition scanners (for scanning drivers licenses and other ID); high-resolution video transmission (allowing for remote identification and verification and proof of "liveness"); artificial intelligence/machine learning (e.g., for determining validity of government-issued ID); and distributed ledger technology (DLT).

Potential benefits

32. Digital ID systems that meet high technology, organisational and governance standards hold great promise for improving the trustworthiness, security, privacy and convenience of identifying natural persons in a wide variety of settings, such as banking, health, and e-government in the global economy of the digital age. These digital IDs are referred to as those with higher 'levels of assurance'.

33. In relation to the FATF Standards, digital ID systems could:

- improve customer identification and verification at on-boarding
- support ongoing due diligence and scrutiny of transactions throughout the course of the business relationship,
- facilitate other customer due diligence (CDD) measures, and
- aid transaction monitoring for the purposes of detecting and reporting suspicious transactions, as well as, general risk management and anti-fraud efforts.

34. They also have the potential to reduce costs and increase efficiencies for regulated entities, and allow for the re-allocation of resources to other AML/CFT functions.

35. Reliable, independent[9] digital ID systems can also contribute to financial inclusion by enabling unserved and underserved people to prove official identity in a wide range of circumstances, including remotely, in order to obtain regulated financial services. Bringing more people into the regulated financial sector further reinforces AML/CFT safeguards.

Potential risks

[7] 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.

[8] MAC addresses identify devices, IP addresses identify connections.

[9] To support readability, the term 'trustworthy' is used as a synonym for "reliable, independent" is some cases.

36. Digital ID systems also pose ML/TF risks that must be understood and mitigated. These risks are covered in detail in Section IV. Large scale digital ID systems that do not meet appropriate levels of assurance pose cybersecurity risks, including allowing cyberattacks aimed at disabling broad swaths of the financial sector, or at disabling the digital identity systems themselves. They also pose major privacy, fraud or other related financial crimes risks, since cybersecurity flaws can result in massive identity theft, which compromises individuals' identity information. Risks related to governance, data security and privacy also have an impact on AML/CFT measures. These risks vary in relation to the components of the digital ID system but they can be more devastating than breaches associated with traditional ID systems due to the potential scale of the attacks. Advances in technology and well-designed identity proofing and authentication processes can help mitigate these risks as set out in Section IV and discussed further in Section V.

37. Recognising the potential risks and benefits of digital ID systems, the FATF has developed this Guidance to clarify how digital ID systems can be used to comply with specific AML/CFT requirements under its standards.

Purpose and Target Audience

38. This Guidance aims to help government agencies develop a clearer understanding of how digital ID systems work and to clarify how they can be used under the global AML/CFT standards. This includes policymakers, regulators, supervisors and examiners of regulated entities; privacy, data protection and cybersecurity authorities (as relevant); as well as, other government authorities with related policy objectives (e.g., increasing financial inclusion).

39. The Guidance also aims to help private sector stakeholders, including regulated entities and digital ID service providers. It is also relevant to international organisations, non-governmental organisations (NGOs) and others involved in providing and using digital ID systems for financial services and humanitarian assistance.

Scope

40. This Guidance focuses on the application of Recommendation 10 (Customer Due Diligence) to the use of digital ID systems for identification/verification at on-boarding (account opening) and the potential to support ongoing due diligence (including transaction monitoring). It also addresses the application of Recommendation 17 (Third Party Reliance) to situations in which regulated entities provide digital ID systems for conducting customer identification/verification to other regulated entities. This guidance also focuses on the identification of individuals (natural persons) and does not cover the identification of legal persons.

41. Under the principle of technology neutrality, the requirements of Recommendation 11 (Record-keeping) apply equally to recordkeeping in digital and physical (documentary) form. As a practical matter, digital ID systems may present distinctive issues with respect to how required CDD information is retained and accessed in order to enable regulated entities to comply with Recommendation 11 requirements. Approaches to record keeping in the digital ID context will vary with the type of digital identity systems, the types and responsibilities of its constituent providers, and the relevant regulatory and contractual frameworks in the jurisdiction. For example, when governments provide digital ID systems, they collect the underlying identity evidence (source documents, information and data) for identity proofing/enrolment, and would therefore be expected to have access to this information for law enforcement purposes, thus satisfying

R. 11 objectives. Where regulated entities use digital ID systems provided by non-government providers, the underlying identity evidence may be retained in whole, or in part, by the digital ID service provider and/or other entities. These matters are appropriately addressed by jurisdictions, in their AML/CFT and digital ID regulatory frameworks, and by regulated entities, including through standard agency and financial services provider contractual relationships. Accordingly, recordkeeping and such requirements are not further addressed in the Guidance.

42. In relation to CDD, this Guidance only addresses the use of digital ID systems to: (1) conduct customer identification and verification for individuals (i.e. natural persons) when establishing business relations (onboarding) under Recommendation 10(a), and (2) potentially support ongoing due diligence under Recommendation 10(d).

43. The Guidance does not cover the use of digital ID systems to help conduct other elements of the CDD process. In particular, the Guidance does not address the use of digital ID systems to identify and verify the identity of a legal person's representative(s); to identify and verify the identity of beneficial owner(s); or to understand and obtain information on the purpose and intended nature of the business relationship—although reliable, independent digital ID systems are important for all of these CDD functions.

44. This Guidance covers digital ID systems provided by government, or on behalf of government, and by the private sector. With respect to government-provided digital ID systems, the Guidance focuses on general-purpose digital ID systems (i.e., ID valid for proving legal identity for all or various purposes in the jurisdiction), although it also discusses government-provided limited-purpose (i.e., ID valid for a specific purpose), such as voter registries or databases, when the government authorises their use for CDD purposes and makes them available to regulated entities and digital ID service providers. More information on the type of digital ID systems covered under this guidance is provided in Section II.

The Guidance does not establish assurance frameworks or technical standards for assessing the independence or reliability of digital ID systems in terms of its technology, processes and architecture. Instead, it relies on digital ID assurance frameworks and technical standards (referred to as digital ID assurance frameworks and standards) developed, or being developed, by other organisations and in different jurisdictions. See Section II for an explanation of the technical standards, and Section V and Appendix A for further information.

45. *Appendix C: ID4D Principles on Identification for Sustainable Development* highlights the governance/accountability, privacy, and other operational issues that are being addressed by various jurisdictions and organisations. [10]

46. This Guidance is non-binding. It clarifies rather than revises the current FATF Standards, which are technology-neutral.

[10] These Principles were developed through a collaborative process facilitated by the World Bank and have been endorsed by 25 development partners, international organisations, NGOs, private sector associations, and government entities.

SECTION II: DIGITAL ID TERMINOLOGY AND KEY FEATURES

What is 'identity' for the purposes of this Guidance?

Concept of official identity

47. Identity is a complex concept with many meanings. For FATF's purposes, identity refers to official identity, which is distinct from broader concepts of personal and social identity that may be relevant for unofficial purposes (e.g., unregulated commercial or social, peer-to-peer interactions in person or on the Internet). The Guidance covers the use of digital ID systems for proving "official identity" for access to financial services.

48. For purposes of this Guidance,[11] **official identity** is the specification of a unique natural person that:

a. is based on characteristics (identifiers or attributes) of the person that establish a person's uniqueness in the population or particular context(s), and

b. is recognised by the state for regulatory and other official purposes.

Proof of official identity

49. **Proof of official identity** generally depends on some form of government-provided or issued registration, documentation or certification (e.g., a birth certificate, identity card or digital ID credential) that constitutes evidence of core identifiers or attributes (e.g., name, date and place of birth) for establishing and verifying official identity.

50. The criteria for proving "official identity" can vary by jurisdiction. In the exercise of their sovereignty, governments establish the required attributes, identity evidence and processes for proving official identity. These factors can change over time and as technology evolves, governments may authorise various attributes. Governments 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 support responsible innovation and to better future-proof the requirements for proving official identity, given the rapid evolution of digital ID technology and related technical standards. In the EU, reliance on common assurance frameworks enables jurisdictions to accommodate jurisdiction-specific criteria, such as the acceptance of different types of nationally available official ID documentation.

51. In many countries, proof of official identity is provided through **general-purpose** ID systems (sometimes referred to as foundational ID systems), such as national ID and civil registration systems. Such systems typically provide documentary and/or digital credentials that are widely recognised and accepted by government agencies and private sector service providers as proof of official identity for a variety of purposes.

52. Jurisdictions also typically have a variety of "**limited-purpose**" ID systems (also referred to as functional ID systems) that are developed to provide identification, authentication, and authorisation for specific services or sectors, such as tax administration; access to specific government benefits and services; voting; authorisation to operate a motor vehicle; and (in some jurisdictions) access to financial services, etc. Examples of limited-purpose ID evidence include (but are not limited to): taxpayer identification numbers, driver's licenses, passports, voter registration cards, social security numbers and

[11] The FATF's use of this definition, for purposes of this Guidance, is not intended to limit alternative definitions by other SSBs.

refugee identity documents. In some cases—and particularly in countries without general-purpose ID systems—such functional systems and credentials may also be used to provide proof of official identity. For example, in Europe, the eIDAS Regulation offers the possibility to use limited-purpose IDs for different purposes under a digital ID.

53. Typically, proof of official identity has been provided by—or on behalf of—governments.[12] In the digital era, we have begun to see new models, with digital credentials provided by, or in partnership with, the private sector being recognised by the government as official proof of identity in an online environment (e.g., NemID in Denmark), alongside more traditional government-issued digital credentials (e.g., electronic national IDs).

54. In the case of refugees, proof of official identity may also be provided by an internationally recognised organisation with such mandate.[13] See Box 14.

What is a digital ID system for the purposes of this Guidance?

55. Digital ID systems use electronic means to assert and prove a person's official identity in online (digital) and/or in-person environments at various levels of assurance.

56. The focus of this Guidance is on end-to-end digital ID systems, i.e. systems that cover the process of identity proofing/enrolment and authentication. Digital ID systems can involve different operational models and may rely on various entities and types of technology, processes and architecture. References to digital ID systems in this Guidance refer to overarching system rather than its component parts.

57. Not all elements of a digital identity system are necessarily digital. In a digital ID system – identity proofing and enrolment can be either digital or physical (documentary), or a combination, but **binding, credentialing, authentication, and portability/federation (where applicable) must be digital.** These concepts are described further in the next section.

58. Digital ID systems may use digital technology in various ways, for example:

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

What are the key components of a digital ID system?

59. As reflected in the NIST digital ID Guidelines, **digital ID systems** involve two basic components, and an optional third component, as set out below. Different entities can be responsible for the operations of subcomponents including a mix of government entities and private sector entities. The terminology used by different jurisdictions and

[12] See 1951 Convention on the Status of Refugees, Article 25 and 27 and the 1950 Statute of the Office of the United Nations High Commissioner for Refugees.

[13] See 1951 Convention on the Status of Refugees, Article 25 and 27 and the 1950 Statute of the Office of the United Nations High Commissioner for Refugees.

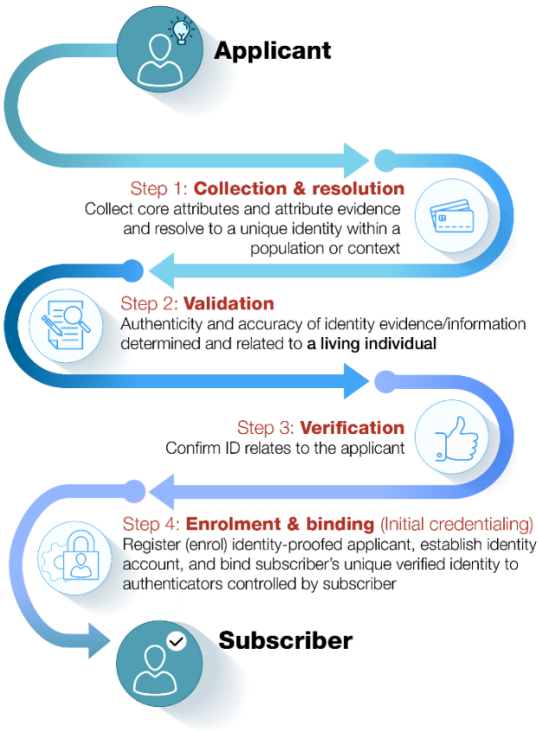
organisations may differ slightly depending on the system being described. A more detailed description of each of the stages is at *Appendix A*: ***Description of a Basic Digital Identity System and its Participants***.

Component One: Identity proofing and enrolment (with initial binding/credentialing) *(essential)*

60. This component answers the question: ***Who are you?*** and involves collecting, validating and verifying identity evidence and information about a person; establishing an identity account (enrolment) and binding the individual's unique identity to authenticators possessed and controlled by this person.

61. This component is directly and most immediately relevant to (overlaps with) R 10 (a)'s identification/verification requirement (see Section III).

Figure 2. Identity proofing and enrolment



Note: This diagram is for illustration only, the stages of identity proofing and enrolment could occur in a different order. The objective is to identify and verify the person and have the identity bound to an authenticator. See also Appendix A for a further explanations of key terms used in this diagram.

62. For the purposes of illustration only, some examples of actions taken within Component One could include:

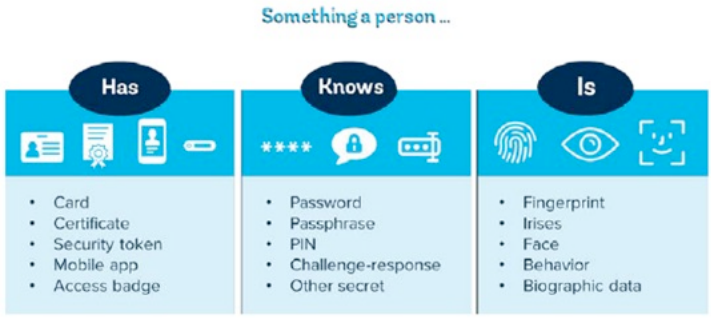
- Collection: in-person presentation of physical identity evidence; online submission of information relating to core attributes and other identifiers (e.g., by filling out an online form; sending a selfie photo for collection of facial recognition attributes) and online collection of identity evidence (e.g., by sending digital photo of driver's license or passport).

- Validation: electronic document verification to ensure that the document, data or information is reliable (for example, using physical security features, expiration dates, and verifying authenticity and attributes via other services).
- De-duplication: establishing the uniqueness of a person in the system using duplicate record searches, biographic deduplication algorithms, and/or biometric recognition.
- Verification: biometric solutions like facial recognition and liveness detection to link the individual to the identify evidence provided.
- Authenticator or credential issuance and delivery: binding one or more authenticators, (for example passwords, one time code generator on a smartphone, PKI smart cards, etc.) to the identity account.

Component Two: Authentication and identity lifecycle management (*essential*)

63. Authentication answers the question: ***Are you who you say you are?*** It establishes that the person seeking access to a service (the on-boarded customer or claimant) is the same person who has been identified and verified (e.g., identity proofed, enrolled, and has possession and control of the binding credentials). There are three types of factors that can be used to authenticate someone (see Figure 3 below): (1) knowledge factors (something you know, e.g., a password); (2) ownership factors (something you possess, e.g., cryptographic keys), (3) inherent factors, (something you are, e.g., biometrics).

Figure 3. Common authentication factors



Source: World Bank ID4D

64. Authentication can rely on various types of authentication factors and protocols or processes. An authentication process is usually more robust and reliable when it employs multiple types of authentication factors.

65. Authentication can be relevant to CDD measures in a number of ways:

- Authentication of identity during customer identification/verification for account opening (if using existing digital ID credentials/authenticators for on-boarding).
- Authentication of existing customers to authorise transactions and account access (this often involves credentials issues by the regulated entity, e.g. PINs, password, token, biometrics on smartphones).

66. Authentication linking existing customers to their account activities can be used to support ongoing due diligence. ***Identity lifecycle management*** refers to the actions that should be taken in response to events that can occur over the identity lifecycle and affect

the use, security and trustworthiness of authenticators, for example, loss, theft, unauthorised duplication, expiration, and revocation of **authenticators** and/or **credentials**.

Component Three: Portability and interoperability mechanisms (optional)

67. Digital ID systems can include a component that enables proof of identity to be portable. Portable identity means that an individual's digital identity credentials can be used to prove official identity for new customer relationships at unrelated private sector or government entities, without their having to obtain and verify personal data and conduct customer identification/verification each time. Portability can be supported by different digital ID architecture and protocols. In Europe, the eIDAS Regulation provides a framework for cross-recognition of digital ID systems.

68. Federation is one way of allowing official identity to be portable. Federation refers to the use of federated architecture and assertion protocols to convey identity and authentication information *across a set of networked systems*. It enables interoperability across separate networks. In the UK, GOV.UK Verify is an example of a federated digital ID – see Box 15.

Digital ID Assurance Frameworks and Technical Standards

69. Assurance frameworks and technical standards for the reliability of digital ID technology, processes, and architecture have been developed or are being developed by:

- various jurisdictions or supra-national jurisdictions (e.g. eIDAS Regulation by the European Union)
- independent, international standards organisations such as the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Faster Identity Online (FIDO) Alliance, and the OpenID Foundation (OIDF), and
- by industry-specific organisations such as the International Telecommunications Union (ITU) and GSMA.

70. See *Appendix D: Digital ID assurance framework and technical standard setting bodies* for a high-level summary of these organisations.

71. The digital ID assurance frameworks and standards developed at a jurisdictional level may currently use different numbers of and/or names for the assurance levels, but largely align in substance. Jurisdictions are currently mapping their respective digital ID technical standards to each other, to resolve any outstanding discrepancies. In 2018, the International Organisation for Standardization (ISO), together with the International Electrotechnical Commission (IEC), issued an international standard for identity proofing and enrolment of natural persons (ISO/IEC 29003:2018). The ISO is currently revising its entity authentication assurance framework (ISO/IEC 29115:2013) and addressing the application of its Risk Management Guidelines (ISO 3100:2018) to identity-related risks. In addition, the ISO is working to update, align and synchronize all other ISO standards to create a comprehensive international digital identity assurance framework.

72. In light of the evolving standards, this Guidance makes many references to the NIST digital ID Guidelines and the e-IDAS scheme. AML/CFT authorities should work closely with counterparts in digital ID, cyber-security and other relevant agencies to identify applicable digital ID assurance frameworks and standards.

73. As digital ID technology, architecture and processes evolve, the assurance frameworks and technical standards for digital ID systems themselves will need to evolve, and will likely lag behind the evolution of digital ID systems. Governments and the private sector are urged to closely track emerging digital ID technology/processes that offer more robust identity proofing or authentication and treat the frameworks and standards as a useful assessment tool, rather than using existing higher assurance levels to establish a ceiling.

SECTION III: FATF STANDARDS ON CUSTOMER DUE DILIGENCE

74. This Section requires a basic understanding of how digital ID systems work. Readers are encouraged to review the brief explanation of the basic steps in a generic digital ID systems in Section II and in Appendix A, which provides the basis for the discussion in this Section on how Recommendation 10—and in particular, its "reliable, independent" criteria — comes into play.

75. Recommendation 10 requires jurisdictions to impose customer due diligence (CDD) obligations on regulated entities. The discussion below clarifies the application of Recommendation 10 (a) in the context of digital ID systems. Regulated entities are required to determine the extent of CDD measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to Recommendation 10 and to Recommendation 1. It also briefly considers how reliable digital ID systems can support other AML/CFT requirements—including in particular ongoing due diligence on the business relationship under R. 10(d).

Customer identification/verification requirements (on-boarding)

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

Documentary or digital form of identity evidence and processes

77. 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/physical or digital) that identity evidence – "source documents, information or data" – can take.

78. Moreover, although Recommendation 10(a) 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 as part of identification/verification at on-boarding. Recommendation 10 thus does not impose limitations as to the use of digital ID systems for that purpose. The FATF standards leave the matter to each jurisdiction, as part of its national legal framework for proving official ID when conducting CDD.

"Reliable, independent" identity evidence

79. The key to determining how digital ID systems 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 digital context. Digital ID assurance frameworks and standards refer to the term "assurance" in describing the robustness of systems. Assurance levels are therefore useful for determining whether a given digital ID system is "reliable, independent" for AML/CFT purposes.

80. The following discussion explores the development of the global standards' current "reliable, independent" requirement, to flesh out its underlying meaning and objectives.

81. In the original FATF Forty Recommendations (July 1990), Recommendation 12 required regulated entities to identify their clients "on the basis of an official or other

reliable identifying document".[14] 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 was adopted in February 2012. In 2012, FATF added the "verification of identity" requirement and the requirement that identity evidence must be "independent" in addition to "reliable." At the same time, the 2012 revision 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. It also dropped the previous Recommendations' explicit reference to "official identifying documents."

82. 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.

83. Digital ID systems are more complex. In the digital ID context, the requirement that digital "source documents, data or information" must be "reliable, independent" means that the digital ID system used to conduct CDD relies upon technology and processes that provide an appropriate level of assurance or confidence that produce accurate results. This means that they have mitigation measures in place to prevent the types of risks set out in Section IV.

Risk-based approach to CDD

84. Recommendation 10 requires regulated entities to use a risk-based approach (RBA) to determine the extent of the CDD measures to be applied, including customer identification/verification. Under Recommendation 10 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. FATF has published Guidance on how jurisdictions/regulated entities could apply CDD measures using the risk-based approach to support financial inclusion objectives.[15]

---

[14] The original FATF Forty Recommendations (July 1990) imposed customer identification requirements on financial institutions to strengthen their role in combatting the ML of illicit drug-trafficking proceeds. Recommendation 12 (1990) provided, in relevant part (emphasis added; punctuation in original):
[F]inancial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they *should be required* (by law, by regulation, by agreements between supervisory authorities and financial institutions or by self-regulatory agreements among financial institutions) *to identify, on the basis of an official or other reliable identifying document*, and record the Identity of *their clients*, either occasional or usual, *when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe-deposit [sic] boxes, performing large cash transactions).*

[15] FATF (2013-2017), *Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence*, FATF, Paris www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.htmlhttps://www.fatf-gafi.org/fr/publications/inclusionfinanciere/documents/financial-inclusion-cdd-2017.html?hf=10&b=0&s=desc(fatf_releasedate)

85. As discussed in detail in Section V, under Recommendations 1 and 10 and their INRs, regulated entities should apply CDD measures that are commensurate with the type and level of ML/TF risks. The Interpretative Note to Recommendation 1 emphasises 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. Along with Recommendation 10 and INR10, INR1 specifically provides 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 business relationships and transactions

86. For the FATF's purposes, face-to-face identification/verification generally occurs in-person, and non-face-to-face identification/verification occurs remotely.

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

88. Given the evolution of digital ID technology, architecture, processes, and the emergence of consensus-based open-source digital ID technical standards, it is important to clarify that non-face-to-face customer identification and verification and non-face-to-face transactions, which rely on digital ID systems that meet appropriate assurance levels, may be standard risk. They may even be lower-risk where higher levels of assurance are achieved and/or appropriate ML/TF risk control measures, such as product functionality limits and other measures discussed in INR10 and FATF Guidance on Financial Inclusion, are present (see also the section on 'Special Considerations for Financial Inclusion, Remote Identity Proofing and Enrolment' later in this Guidance).

Ongoing due diligence on the business relationship

89. In addition, under Recommendation 10 (d), regulated entities must conduct "ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds."

90. With the accelerating transition to digital financial systems and accompanying reliance on the use of digital ID systems, regulated entities that use digital ID systems to confirm customer identity for account access are encouraged to consider ways to leverage the authentication component of digital ID systems to strengthen ongoing due diligence, in line with the risk-based approach to CDD.

91. As explained in Section II, above, and in further detail in Appendix A, **authentication** is the second component of a digital ID system and establishes that an individual (e.g., a customer of a regulated entity) is who the person that was identified and verified and is in possession of the binding credentials. This may aid the regulated entity (e.g., the relying party) with conducting ongoing due diligence and scrutiny of transactions. Authentication can rely on various types of authentication factors and processes, the type

and number of which determine the strength of authentication (See Appendix A on authentication factors).

92. For regulated entities, successful authentication of an onboarded customer provides reasonable, risk-based assurance (i.e., confidence) that the person asserting identity today is the same person who previously opened the account or other financial service, and is in fact the same individual who underwent "reliable, independent" identification and verification at on-boarding. Digital authentication of the customer's identity links that individual with their financial activity and can therefore facilitate ongoing due diligence on the customer relationship, including ongoing scrutiny of the customer's transactions, pursuant to Recommendation 10(d). Robust authentication enables regulated entities to reliably determine that the person seeking to access the customer's account and conduct transactions digitally, has the required authenticators and is in fact the identified and verified customer, strengthening the ability to conduct meaningful ongoing due diligence or transaction scrutiny throughout course of the business relationship.

93. When using the credentials of an existing identity system for identification/verification, regulated entities may issue their own authenticators for authorising account access, in support of ongoing due diligence. Authentication is one part of authorising account access. The regulated entity collects other complementary data (such as, geolocation, IP addresses, etc.) for the authorisation decision, which could also support ongoing due diligence.

Third Party Reliance Requirements

94. Under Recommendation 17, countries may permit regulated entities [16] to rely on third parties to perform customer identification/verification at on-boarding,[17] provided that the following conditions are met:

- The third party must be a regulated entity subject to CDD requirements in line with Recommendations 10, and regulated and supervised or monitored for compliance.
- Regulated entities should:
  - Immediately obtain the necessary information concerning customer identification/verification
  - Take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to Recommendation 10 (a) requirements will be made available from the third party upon request without delay;
  - Satisfy itself that the third party is regulated, supervised or monitored for; has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11; and
  - Consider country risk information, when determining in which countries the third party that meets the above conditions can be based.

95. When such reliance is permitted, the ultimate regulatory responsibility for CDD measures remains with the regulated entity that relies on the third party.

[16] Recommendation 22 provides that the reliance requirements in R.17 apply to DNFBPs.

[17] Recommendation 17 authorises third party reliance for elements (a)-(c) of the CDD measures set out in Recommendation 10, It does not authorise third party reliance for conducting ongoing due diligence on the business relationship. This Guidance discusses Recommendation 17 only as it relates to Recommendation 10 (a) identification/verification.

Third Party Reliance in the Digital ID Context (where regulated entities also act as a digital ID service provider)

96. If permitted by the jurisdiction, a regulated entity could rely on another such entity that satisfies the criteria described above to conduct customer identification/verification at on-boarding, using a digital ID system, provided the third party's digital ID system enables the relying regulating entity to:

- Immediately obtain the necessary information concerning the identity of the customer (including the level of assurance or confidence, where applicable). For example, the digital ID system could enable the prospective customer to assert identity to the relying regulated entity and the third party to authenticate the person's identity and provide information, such as the person's name, date of birth, a state-provided unique identity number, or other attributes required to prove official identity to establish business relationship in the jurisdiction.
- Take adequate steps to satisfy itself that the third party will make available copies or other appropriate forms of access to the identity evidence (documents, data and other relevant information) relating to Recommendation 10 (a) requirements upon request without delay. For example, the relying entity could take appropriate steps to (1) satisfy itself that, as part of identity proofing and enrolment, the third party established a digital ID account for the identified person that contains adequate attribute evidence and other identity data and information, and (2) that the third party's authentication processes enable it to provide that information to the relying party upon request without delay.

Regulated entities as Digital Identity Service Providers outside Recommendation 17

97. Regulated entities that have developed their own digital ID systems could seek to become digital ID service providers by acting as agents or outsource entities for other regulated entities. Where allowed, this would involve outsourcing of customer identification/verification at onboarding and authentication of customers. In this situation, third-party reliance under Recommendation 17 does not apply, as Recommendation 17 does not cover outsourcing or agency relationships.

98. Like other digital ID service providers acting as agents or outsourcing entities, regulated entities acting as a digital ID service provider would use its digital ID system to conduct customer identification/verification (and authentication) *on behalf of* the delegating regulated entity. Also like other digital ID service providers, it could seek certification, pursuant to jurisdiction's government-audit and certification frameworks, if available, or audit and certification from a reputable private sector certification organisation.

99. In any case, as principal, the designated entity would remain responsible for conducting *effective* customer identification/verification, and *effective* authentication, using the digital ID system provided by the digital ID service provider, and would need to apply the RBA to using digital ID systems for customer identification/verification and authentication, as discussed in Section V.

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

100. This section describes some of the potential benefits of digital ID systems for regulated entities, their customers, and government, as well as potential risks that need to be identified, understood, monitored, and adequately managed or mitigated. These benefits and risks relate to both the implementation of AML/CFT safeguards and to financial inclusion.

101. The section is intended to raise stakeholders' awareness of potential risks specific to digital identity technologies so they can be prevented or effectively managed by applying the RBA set out in Section V. The discussion of risk, below, is not intended to discourage the use of reliable, independent digital ID systems—i.e., those that meet an appropriate level of assurance framework (i.e. governance arrangements and technical standards) and do appropriately address the potential risks. Nor is it meant to suggest that the use of digital ID systems, especially for customer identification/verification, is necessarily more vulnerable to abuse than traditional documentary methods.

102. To the extent that digital ID systems rely on official identity documents for identity proofing, weaknesses in the reliability of documentary identity evidence can have a domino effect on the risks posed by digital ID systems. The "reliability, independence" of purely documentary approaches can be undermined by identity theft and the widespread counterfeiting of official identity documents—including where official identity documents either lack advanced security features to prevent tampering or counterfeiting or are issued without adequate identity proofing. Indeed, unprecedented levels of identity theft from online databases generate similar risks for both digital ID systems and documentary approaches.

103. While this section provides a general overview of some of the risks, the digital ID assurance frameworks and standards provide a framework for assessing a digital ID system's risk mitigation measures. Jurisdictions are encouraged to review these standards, which address a broad range of risks (in relation to technology, but also other relevant organisational and governance) that exist and how they should be mitigated.

Potential benefits of digital ID systems

Strengthening CDD

104. Digital ID systems have the potential to improve the reliability, security, privacy, convenience and efficiency of identifying individuals in the financial sector, to the benefit of both customers and regulated entities. Specifically, reliable, independent digital ID systems may offer significant benefits for improving customer identification/verification at on-boarding, and authenticating the identity of customers to authorise account access. Moreover, accurate customer identification could enable other CDD measures, including effective ongoing due diligence on the business relationship and transaction monitoring.

Minimise weaknesses in human control measures

105. In some jurisdictions, traditional documentary methods of conducting customer identification/verification largely rely on human control measures – e.g., comparing a photograph on an official identity document with the person seeking to open an account, and making a judgment call that the identity document is genuine and belongs to the person presenting it. Such front-line personnel may lack the tools, technology, training, skill sets and experience needed to reliably identify counterfeit, forged or stolen documents.

However, some types of fraud may be less likely to occur in-person or in processes requiring human intervention, including 'massive attack frauds' which are more likely to happen remotely.

106. The use of reliable, independent digital ID systems can potentially reduce the possibility of human error in identifying and verifying the identity of a person.

- First, even when a digital ID system relies on in-person,[18] documentary identity proofing, that process may often be conducted by identity experts, with adequate levels of training and expertise, and access to advanced technical tools for detecting fraudulent and stolen ID documents. Remote identity proofing—at least at higher assurance levels for this stage—typically employs increasingly sophisticated and effective digital identity technologies to determine that documentary identity evidence is genuine, not counterfeit, as well as additional data and information that help reliably identity proof the individual. In the absence of some electronically verifiable content (e.g. a chip), there is a risk that remote checking of documents that require an ultraviolet (UV) light source or are intrinsic to the construction of the document (such as security stitching, etching or punches that go through multiple pages etc.) may be more difficult or impossible to check remotely. However, in practice, for the reasons stated above, the checks on the features that are useable remotely are more robust.
- Second, digital identity authentication largely eliminates the role of subjective human judgement in determining that customers are who they claim to be. Digital ID systems with multiple factor authentication and secure processes can be consistently reliable in determining that the person seeking to open or access an account is in fact the same individual to whom the identity credentials were originally issued. They therefore could not only strengthen CDD and other AML/CFT compliance measures, such as transaction monitoring and identification and reporting of suspicious transactions; they may also improve anti-fraud measures and general risk management, generating additional cost savings while reinforcing broader integrity.

Box 1. Nigeria Bank Verification Numbers (BVN)

In 2015, Nigeria began a biometric verification pilot for all civil servants in an effort to improve the accuracy of personnel records and reduce payments of 'ghost' salaries. 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, and that number has since doubled – saving the taxpayer equivalent of USD $74 million.

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

Improve customer experience and generate cost savings

107. Reliable, independent digital ID systems can also provide more efficient, user-friendly experiences for potential customers at onboarding, and thereafter, for customers seeking to access their accounts. In the UK, an estimated 25% of financial services

[18] As set out in Section II and Appendix A, under a digital ID system, identity proofing is one component that can occur in-person (i.e. it does not have to occur remotely to be considered a digital ID system).

applications are abandoned, for example, due to difficulties in the KYC process.[19] Ease of use for customers, combined with potential efficiency gains for regulated entities, can help lower on-boarding costs. One report suggests that institutions using digital ID at high-levels of assurance could see up to 90 percent cost reduction in customer "on-boarding" with the time taken for these interactions reduced from days or weeks to minutes. [20] These cost savings could facilitate financial inclusion for otherwise excluded or under-served individuals by reducing on-boarding costs. It can also help to redistribute savings towards other AML/CFT compliance functions.

Transaction monitoring

108. As noted above, robust digital authentication of customer ID for ongoing account access may facilitate the identification and reporting of suspicious transactions, because it ensures that the person accessing an account and conducting transactions today is the same person who accessed the account previously, and is in fact, the identified/verified customer who holds that account. In addition, depending on the operational model and other factors, such as user consent and data protection/privacy laws, digital ID authentication and authorisation for account access may enable regulated entities to capture additional information, such as geolocation, IP address, or the identity of the digital device used to conduct transactions. This information can help regulated entities develop a more detailed understanding of the client's behaviour as a basis for determining when its financial transactions appear to be unusual or suspicious. For example, Internet and cell phone data associated with particular financial transactions may be very useful for determining who is controlling an account; whether they are controlling multiple accounts; and the network of individuals and entities involved in the financial transactions conducted, using those accounts.

Financial inclusion

109. The rapid digitisation of financial services has greatly increased the importance of reliable, independent digital ID systems for financial inclusion, especially in developing countries,[21] where digital ID systems and digital financial services have emerged as core drivers of financial inclusion.[22] The development of digital ID standards based on outcomes can allow financial excluded people who do not have access to evidence documents, such as passports and driving licences, to develop robust digital IDs using, for example, a collection of secondary evidence as well as a guarantee from trusted bodies in the public or third sector who have established relationships with these individuals.

---

[19] World Bank (2018), Private sector economic impacts from identification systems, http://documents.worldbank.org/curated/en/219201522848336907/Private-Sector-Economic-Impacts-from-Identification-Systems.pdf

[20] McKinsey Global Institute (2019), Digital Identification, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx.

[21] In the 2017 Global Findex Survey, 26 percent of unbanked individuals in low-income countries cited lack of official identity documentation as the primary barrier to obtaining financial services.

[22] FATF (2013-2017), *Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence*, FATF, Paris www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html.

110. In developing countries, government-to-person (G2P) payments, including social benefit transfers (e.g., conditional cash transfers, child support payments and student allowances), payment of government salaries and pensions, and tax refunds are increasingly digital, as are commercial activities and retail consumer payments. In humanitarian contexts, life-saving assistance is increasingly delivered in the form of digitally delivered cash-based assistance. All these activities require access to a transaction account.

111. Using reliable, independent digital ID systems could reduce the costs of CDD and enable many more unserved and underserved persons to use regulated financial services (see Box 5 on India's Aadhaar). This facilitates financial inclusion and with it, improves the reach and effectiveness of AML/CFT regimes.

Box 2. Peru

The National Registry of Identification and Civil Status (Registro Nacional de Identificación y Estado Civil, or RENIEC) is the national digital ID system in Peru. RENEIC has been used as a form of identification for a wide range of public and private services. For example, RENIEC serves as the core verification database for e-money platform called 'Modelo Peru' serving millions of customers across Peru for e-money transactions. In addition, a new service using RENIEC known as Billetera Movil (BiM), was launched in February 2016, which provides services such as cash in/cash out at agents, the ability to check balances, conduct P2P payments and top-up credit.

Source: Wold Bank (2018), *Digital ID On-boarding*

Risks and challenges presented by digital ID systems

112. Digital ID systems present a variety of technical challenges and risks of failure, because they often involve identity proofing and authenticating individuals over an open communications network (the Internet). As a result, the processes and technologies employed by digital ID systems present multiple opportunities for cyberattacks at any point of communication between the parties (IDSP, customer and relying party). Without careful consideration of relevant risk factors and implementation of appropriate, technology-based safeguards, as well as effective governance and accountability measures to address them, criminals, money launderers, terrorists, and other bad actors may be able to abuse digital ID systems to create false identities or exploit (hack) authenticators linked to a legitimate identity.

113. The digital ID assurance frameworks and standards provide a key tool for identifying and assessing some of these risks, and mitigating them with digital identity technologies and processes that offer appropriate, assurance for each of the components of digital ID.[23] The following risk discussion applies to digital ID systems that are *not* sufficiently reliable, in terms of digital ID risk management frameworks. It also touches on broader connectivity and privacy challenges in the digital space that may impact the integrity or availability of digital ID systems to conduct CDD.

[23] See Appendix E for a more detailed discussion of Identity Assurance Levels (IALs); Authentication Assurance Levels (AALs); Federation Assurance Levels (FALs), used to assess and mitigate risks at each of these basic stages.

114. As described below, the outcome of identity proofing/enrolment risks is that the digital ID obtained is "fake"—i.e., obtained under false premises through an intentionally malicious act. These risks are mitigated through having a higher identity assurance level. It is distinguished from the risks listed under authentication where a legitimately issued digital ID has been compromised and is no longer under the control of the person to whom it was originally issued. These risks are mitigated by having a higher authentication assurance level.

Identity proofing and enrolment risks

115. There are two general categories of threats to the enrolment process: (1) cyberattacks and security breaches leading to the presentation of false evidence either by impersonating another person's identity or creation of a synthetic ID, and (2) compromise of, or misconduct by, the IDSP or compromise of the broader digital identity infrastructure. This section focuses on the first category as IDSP compromise/misconduct, cybersecurity and broader infrastructure threats are addressed by broader governance/organisational requirements in digital ID assurance frameworks and standards and traditional computer security controls (e.g., intrusion protection, record keeping, independent audits) and are outside the scope of this guidance.

Impersonation risks and synthetic IDs (involving cyberattacks, data protection and/or security breaches)

116. In certain respects, the risks arising from the presentation of false evidence (which is either stolen or counterfeit) in digital identity systems, mirror the risks posed by counterfeit, forged or stolen official ID documents for documentary customer identification/verification at onboarding. However, in the digital identity world, these risks can be actualised at much greater scale. **Impersonation** involves a person pretending to have the identity of another genuine person, this might be through simply using a stolen document of someone that looks similar, but may also be combined with counterfeit or forged evidence (e.g. photo substitution on a person's genuine passport with the impostor's image). **Synthetic identities** are developed by criminals by combining real (usually stolen) and fake information to create a new (synthetic) identity, which can be used to open fraudulent accounts and make fraudulent purchases. Unlike impersonation, the criminal is pretending to be someone who does not exist in the real world rather than impersonating an existing identity. For example, criminal groups can engage in identity theft, generating large numbers of synthetic digital IDs that are based in part on a real-individuals' identity attributes and other data that have been stolen from online transactions or by hacking Internet databases, and in part on entirely fake information. The synthetic IDs can be used to obtain credit cards or online loans and withdraw funds, with the account abandoned shortly thereafter. According to digital ID experts, the use of synthetic identities pose the greatest risk in the identity proofing and enrolment stage of digital ID systems in the US.

117. For the purposes of illustration, the table below sets out these risks and presents some strategies for mitigating threats to identity proofing and enrolment processes under the NIST Guidelines.

Table 1. NIST - Identity Proofing/Enrolment Risk Mitigation Strategies

Type of risk	Description	Potential risk mitigation strategies
Falsified identity proofing evidence	An applicant claims an incorrect identity by using a forged driver's license.	IDSP (CSP) validates physical security features of presented evidence. IDSP (CSP) validates personal details in the evidence with the issuer or other authoritative source.
Fraudulent use of another's identity	An applicant uses a passport associated with a different individual	IDSP (CSP) verifies identity evidence and biometric of applicant against information obtained from issuer or other authoritative source.

Source: NIST 800-63A

Authentication and identity life cycle management risks

118. Vulnerabilities associated with the types and numbers of different authentication factors may give rise to unidentified and unintended risks that can allow bad actors to assert an individual's (e.g., customer's) legitimate identity to a relying party to open an account or obtain unauthorised access to products, services, and data.

119. For the purposes of illustration only, some of these vulnerabilities may include:

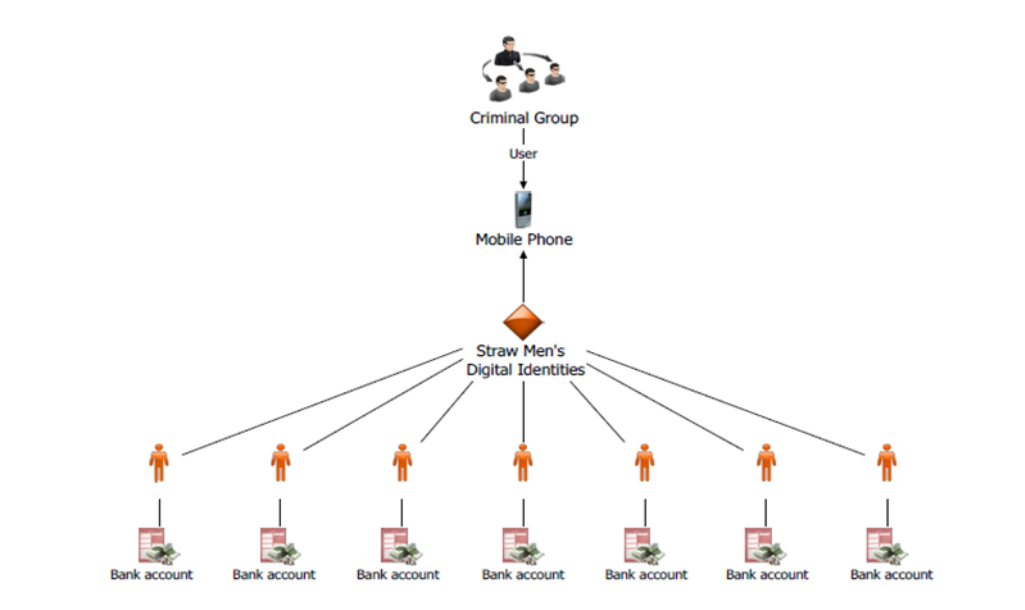
- Credential stuffing (also referred to as breach replay or list cleaning): Type of cyberattack where stolen account credentials (often from a data breach) are tested for matches on other systems. This type of account can be successful if the victim has used the same password (that was stolen in the data breach) for another account.
- Phishing: Is a fraudulent attempt to gather credentials from unknowing victims using deceptive emails and websites. For example, a criminal attempts to trick its victim into supplying names, passwords, government ID numbers or credentials to a seemingly trustworthy source.
- Man-in-the-middle or credential interception: Attempts to achieve the same goal as phishing and can be tool to commit phishing, but does so by intercepting communications between the victim and the service provider.
- PIN code capture and replay: this involves capturing a PIN code entered on the keyboard of a PC in with a key logger and, without the user noticing, using the captured PIN when the smartcard is present in the reader to access services).

120. Most authentication vulnerabilities are exploited without the identity owner's knowledge, but abuse can also involve the witting participation of subscribers or IDSPs. For example, shared-secret authenticators, such as passwords, may be stolen and exploited by bad actors, but they can also be deliberately shared by the owner of the identity credentials for illicit purposes.

121. For example, criminal organisations can purchase digital ID credentials from individuals that enable them to access to the individuals' accounts at regulated entities, in effect turning them into digital mules for the organisation. The individuals may either already have an account, or agree to open one in connection with selling the identity credentials (see the case study below).

Box 3. 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. This is a risk that could also exist in face-to-face transactions but is provided to illustrate how these attacks could take place in the digital world. 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 above). The bank accounts are then controlled by the criminal group. It is important to note that the overwhelming majority of digital IDs that are misused by criminal groups, are issued on this basis of legitimate identity evidence (i.e. proof of identification).

Source: Sweden

122. Some of the primary known risks associated with specific types of authenticators/processes are described below.

123. **Multi-Factor Authentication (MFA) Vulnerabilities:** Passwords or passcodes, which are supposed to be "shared secret" knowledge authenticators, are vulnerable to brute-force login attacks, phishing attacks, and massive online data breaches, and are very easily defeated. Stolen, weak or default passwords are behind 81 percent of data breaches.[24] Multi-factor authentication (MFA) solutions, such as SMS one-time codes texted to the subscriber's phone, add another layer of security to passwords/passcodes but they can also be vulnerable to attack.

124. **Biometric Authenticators:** Biological or biological-based biometric authenticators, such as fingerprints and iris scans, are more difficult to defeat than traditional authenticators and are increasingly ubiquitous (most smartphones have built-in fingerprint scanners; some next-generation smart phones have built-in iris scanners; and facial recognition capabilities are built into many personal computer systems and advanced smart phones). There is the potential that they can be spoofed or fraudulently validated,

[24] Source to be included.

however currently these types of attacks are difficult and/or highly resource intensive and are therefore not scalable. In contrast to knowledge or possession based authenticators, stolen biometric authenticators are difficult to revoke or replace.[25] Biometric characteristics could be stolen in bulk from central databases.[26] They could also be obtained online or by taking a picture of someone with a cell phone, capturing their facial images with or without their knowledge; lifted from objects the individual touches (e.g., latent fingerprints); or captured with high resolution images (e.g., iris patterns). However, the risk of spoofing attacks in relation to on-device matching, while possible, is fairly low and does not easily scale because it requires physical access to the device.

125. In addition to spoofing attack vulnerabilities, biometrics have a variety of other weaknesses that give rise to reliability concerns when used for authentication purposes. Fingerprints may not be read, or read incorrectly. Facial recognition factors can be rendered unreliable by facial expressions of different moods, changes in facial hair, makeup; and varying lighting conditions. Due to incomplete data sets, facial recognition has been less reliable for persons with darker skin pigmentation and certain ethnic features, although this is improving.

126. **Identity life cycle risks:** Poor identity life cycle and access management can, wittingly or unwittingly, compromise the integrity of authenticators and 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.

127. **Unknown risks:** Digital ID systems develop and evolve. In many cases, technical design changes introduce operational improvements but bring with them vulnerabilities that are not apparent until they are exploited by bad actors in ways that disclose how the digital ID system has been compromised.

Potential obstacles to accessing identity information for ongoing due diligence and transaction monitoring

128. Authentication in the digital ID environment can contribute to ongoing CDD and transaction monitoring. Where the regulated entity adopts third-party digital ID system and does not itself collect information such as transaction patterns, locations, device access etc., it may not have access to information that is important to analyse the customers' behaviour and transaction patterns for the purpose of determining whether transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds. Where this information is collected for anti-fraud purposes, it could also be useful for AML/CFT purposes. To the extent such information is accessible to them, regulated entities should consider using authentication data to enable the detection of systematic misuse of digital IDs, including compromised, stolen or sold digital IDs. This information could be considered in identifying and determining whether to report suspicious activities. One possible benefit of the federated identity model is that identity fraud detection can be shared across a network of identity providers and relying parties.

[25] While methods for revoking biometric credentials exist, at present, their availability is limited, and the technical standards for testing them are still under development.

[26] In an attack on the U.S. Office of Personnel Management (OPM) in 2015, 5.6 million sets of fingerprint images were stolen.

Connectivity issues

129. Digital ID systems also present challenges with respect to connectivity and resilience in the face of unreliable electrical grids and internet access, as well as access challenges where 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 involving digital ID systems in a jurisdiction or in particular areas of a country.

130. Connectivity issues exist predominantly in instances where digital transactions occur. However, digital ID systems can be designed to support both offline and online transactions, in which case they can function with or without access to the electrical grid.

Domestic frameworks for official identity

131. While the FATF does not require jurisdictions to adopt any specific type of identity framework, it is important to note that the risks associated with identity documents and digital ID may be different depending on whether a country has a general-purpose identity system or a range of limited-purpose identities. A digital ID, which has been developed for a limited or specific purpose, may not be able to cope with the demand for applications in other situations and may create high costs for regulated entities.

132. Digital ID schemes rely on a backbone of connected systems, databases, and civil or population registries. The meaning of Digital ID changes significantly depending on the existence or not of general-purpose identification infrastructure in the country. In developed countries, moving to digital identification might mean enhancing existing infrastructure and making it more efficient to serve other purposes (e.g. France, South Korea or Singapore). In many emerging markets the lack of robust civil identification registries or physical identification means that they build digital systems without building on general-purpose identification systems (e.g. Guinea, Kenya, Uganda) serving a specific function or purpose or even multipurpose or several functions. In some countries, some of these identification systems become de-facto a general-purpose identification systems (e.g. Mexico's INE).

Data Protection and Privacy Challenges

133. Digital ID involves the collection and processing of personal data. Digital databases that contain identity attributes used for identity proofing may include personally identifiable information (PII) and attributes, such as an individual's name, age, height, date of birth, ID numbers, as well as fingerprints or other biometric information.

134. Importantly, the assurance frameworks and standards for digital ID incorporate data protection and privacy (DPP) requirements, which may be based on separate standards established by a jurisdiction's and/or an international standards organisations' standards in these areas.

135. 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, accuracy and integrity of the data, which are primary responsibility of the data controller (aka digital ID service 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. In countries with limited data protection laws in place, without adequate mitigation

measures in place, there could be greater risk of identity theft and cybersecurity risks, and trust in the system may consequently be lower.

136. In accordance with Recommendation 2, AML/CFT and DPP authorities should seek to co-operate and co-ordinate to ensure compatibility of requirements and rules. In order to mitigate privacy and data protection and privacy related risks, Digital ID service providers could conduct a data-protection impact assessment (DPIA) to identify potential challenges and appropriate risk control measures. New technologies may assist in mitigating some of the risks associated with DPP, but, in turn, may also give rise to new risks.

Financial exclusion considerations

137. To the extent that digital ID systems do not cover all, or most, persons in a jurisdiction, or exclude certain populations, they may drive —or at least fail to mitigate— financial exclusion. In this way, the mandatory use of a particular digital ID that is not universal for account opening presents similar challenges for inclusion as the prescriptive use of particular non-digital IDs or other substantiating documents required for CDD but not accessible to the entire population. A lack of access to digital technology or low levels of technology literacy, however, may compound some of these exclusion risks. For example, lack of access to mobile phones, smartphones, or other digital access devices, or lack of coverage and/or unreliable connectivity, may exclude poor and rural populations or women as well as those living in fragile and conflict affected areas such as refugees and displaced people. Digital ID systems may also contribute to financial exclusion to the extent that they use biometric authentication without providing alternative mechanisms for authentication. This is due to the fact that certain biometric modalities have greater failure rates for some vulnerable groups such as manual labourers' inability to read worn fingerprints; the elderly (match failure due to altered facial characteristics, hair loss, or other signs of aging, illness, or other factors); or certain ethnic groups and individuals with certain physical characteristics (disproportionate facial recognition failures, related to darker pigmentation, eye shape, or facial hair).

SECTION V: ASSESSING WHETHER DIGITAL ID SYSTEMS ARE RELIABLE AND INDEPENDENT IN LINE WITH A RISK-BASED APPROACH TO CDD

138. As noted in Section III, in the digital ID context, the requirement that customer identification/verification must be conducted, using reliable, independent "source documents, data or information" means that digital ID systems should rely upon technology, processes, governance and other safeguards, that provide an *appropriate* level of trustworthiness. This means that there is an appropriate level of confidence (assurance) that the digital ID system works as it is supposed to and produces accurate results. It should also be adequately protected against internal or external manipulation or falsification, to fabricate and credential false identities or authenticate unauthorised users, including by cyberattack or insider malfeasance.

139. To determine whether the use of a digital ID system is consistent with Recommendation 10 (a) and (d) requirements, governments, financial institutions, and other stakeholders should conduct the following assessments:

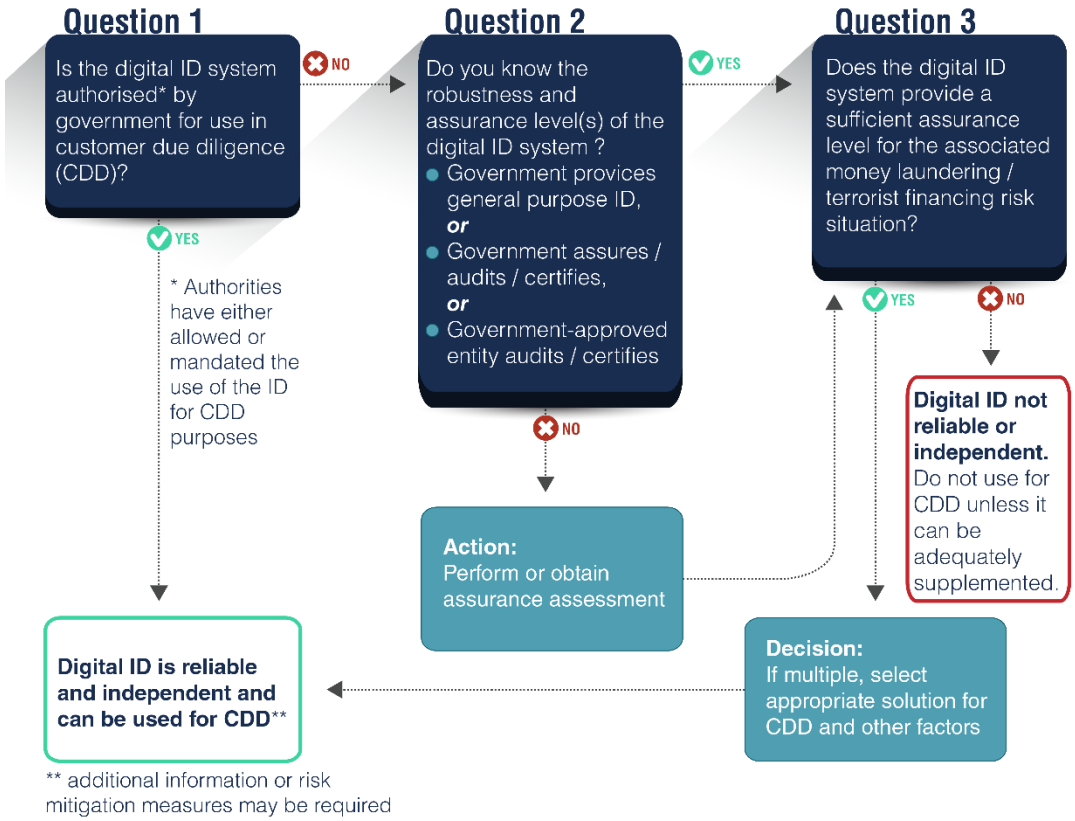
a. Understand the level of assurance of the digital ID system's technology, architecture and governance to determine its reliability/independence; and

b. Make a risk-based determination of whether the particular digital ID system, given its level of assurance, provides an appropriate level of reliability and independence in light of the potential ML, TF, fraud, and other illicit financing risks.

140. Depending upon the digital ID system(s) and regulatory framework in a particular jurisdiction, governments and regulated entities may have different roles and responsibilities in assessing an identity system's assurance levels and its appropriateness for CDD, as reflected in the decision flow chart for regulated entities, below.

141. The flow chart decision process sets out a path for regulated entities in deciding whether to use a digital ID system for customer identification and verification and ongoing due diligence purposes. The two assessments set out above are reflected in questions two and three, respectively.

Figure 4. Decision process for regulated entities



Question One: Is the digital ID system authorised by government for use in CDD?

142. Under Question One, where the government "stands behind" a digital ID system *and* has deemed it appropriate for use in CDD, regulated entities can use the digital ID system without performing the assessments under Question Two and Three. The government has in effect conducted both steps of the recommended assessment—at least for standard CDD risks—for the regulated entities. However, depending on AML/CFT laws and the digital ID ecosystem in the jurisdiction, regulated entities may be required to take additional measures (see paragraphs 147 and 148 below). Where this is not the case, the remaining parts of the decision process do not apply.

143. Governments may explicitly deem a digital ID system to be appropriate for use in CDD by issuing regulations or providing guidance to regulated entities, *either permitting or requiring* regulated entities to use the digital ID system(s) for certain aspects of CDD. Explicit authorisation may occur, for example, when the government developed and operates the digital ID system(s) and therefor has confidence in them, or when the government has a mechanism for obtaining audited, certified information on the assurance levels of another provider's digital ID system.

144. Governments may also implicitly "stand behind" and deem a digital ID system appropriate for regulated entities to use in CDD. That could be the case, for example, when the government provides a general-purpose digital ID system that is used to prove official identity, whenever required in the jurisdiction. Governments should be transparent about

how its digital ID system works and its relevant assurance levels. The same is true for its limited-purpose identity systems, authorised for use in the financial sector.

145. Depending on domestic AML/CFT laws and regulations, regulated entities may need to supplement the use of authorised digital ID systems in certain circumstances, including for example, higher risk situations and to collect information on other aspects of CDD not covered for the purposes of this guidance (i.e. understanding the purpose and intended nature of the business relationship). Some jurisdictions may have regulations only authorising the use of digital ID systems only for lower risk situations.

146. Apart from their jurisdiction's regulatory requirements, regulated entities are encouraged to consider whether they should adopt additional digital ID risk mitigation measures (if available), such as additional identity attribute data points or additional authenticators, and/or ML/TF risk mitigation measures, given the financial institution's own AML/CFT, anti-fraud, and general risk management policies.

Question Two: Do you know the relevant assurance level/s of the digital ID system?

147. Where the government has not explicitly or implicitly authorised the use of specific digital ID systems for CDD, the regulated entity must first determine, for any digital ID system it is considering adopting, the system's assurance levels. [27]

148. If the government assures, audits or certifies digital ID systems (either directly, or by designating organisations to act on its behalf[28]), regulated entities may rely on these assessments to answer Question Two of the decision process. Similarly, the government may also approve an expert body, domestic or foreign, to test/audit and certify the assurance levels of digital ID systems on which regulated entities may rely. See Appendix D for an overview of some of these expert bodies. The digital ID systems may be certified as meeting a minimum level of assurance, or may have different, increasingly robust (reliable/independent) assurance levels (either unitary or for each of its components), but the authoritative information should be publically available.

149. If the government has neither authorised a digital ID system(s) for use in CDD, nor provided a mechanism to obtain authoritative information on a digital ID system's assurance level/s, regulated entities must determine the reliability, independence of the system themselves by either:

a. performing the assurance assessment themselves, or

b. using audit or certification information on assurance levels from by an expert body (albeit not officially government-approved).

150. Where the regulated entity performs the assurance assessment themselves, they should conduct appropriate due diligence on the digital ID system provider, including the governance systems in place, and exercise additional caution.

---

[27] As set out previously in this Guidance, the term "**assurance level**" refers to the level of trustworthiness, or confidence in the reliability of each of the components of the digital ID process.

[28] These activities may not be undertaken by the jurisdiction's AML/CFT regulators, because the capacity to determine whether an entity applies appropriate, publicly-disclosed assurance frameworks and technical standards, is likely to reside in another part of government. The choice of competent authorities for performing this function is a matter for each jurisdiction to determine. By way of example, in the US, the General Services Administration (GSA) has approved a number of Trust Framework Providers to certify ID systems for government use.

151. A regulated entity should only use information from another expert body if it has a reasonable basis for concluding that the entity accurately applies appropriate, publicly-disclosed digital ID assurance frameworks and standards. For example, the entity may be approved for similar purposes by another government or may be widely recognized as reliable by appropriate experts in the jurisdiction, region, or internationally.

Question Three: Is the digital ID system appropriate for the ML/TF risk situation?

152. Once, the regulated entity is satisfied that it knows the assurance levels of the digital ID system (via the processes described under Question Two), it should analyse whether the digital ID system is adequate, in the context of the relevant illicit financing risks. In other words, given the assurance level/s, is the digital ID system appropriate for use in customer identification/verification and ongoing due diligence in light of the potential ML/TF risks associated with the customer, products and services, geographic area of operations, etc.? Regulated entities should analyse whether, given its assurance levels, the digital ID system is adequate, in the context of the relevant illicit financing risks. Depending on the jurisdiction's AML/CFT requirements and available digital ID systems, regulated entities may have the option to select from multiple digital ID systems that have different assurance levels for identity proofing and authentication. In this situation, regulated entities should match the robustness of the system's identity proofing and/or authentication to the type of potential illicit activities and the level of ML/TF risks.

153. In some countries, the government has stipulated a required (unitary) level of assurance for standard and or high ML/TF risk situations. Regulated entities may still be able to choose within a range of digital ID system(s) with the required assurance level, or to select varying levels of identity proofing and/ or particular credentials and authenticators offered by the same system. Where this is the case, they should consider the specificities of their ML/TF risks as they relate to identity proofing and authentication in deciding on an option(s). Regulated entities may also have the option to choose appropriate digital ID for lower risk scenarios (see also section on financial inclusion later in this section).

Leveraging the Digital ID Assurance Frameworks and Technical Standards to Implement the RBA

154. As discussed above, governments (as IDSPs and/or as regulators, supervisors, and policy makers) and regulated entities (as relying parties) should adequately consider the relevant digital ID risk factors, in relation to the relevant ML/TF risk factors and mitigating AML/CFT measures. As explained in greater detail below, the **digital ID assurance frameworks and standards** provide a useful tool in undertaking this assessment.

155. Governments and regulated entities are therefore encouraged, to consider the digital ID risk information provided by the assurance frameworks and standards when assessing the assurance level of the digital ID system. They are also encouraged to consider the reliability of each of the system's main digital ID components 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 each component of the digital ID system (identity proofing/enrolment, authentication, or, if applicable, federation.

156. Understanding the levels of assurance of each component of the digital ID system can help regulated entities take a more nuanced risk-based approach to CDD when relying on digital ID. The **process-by-process approach to assessing assurance** is particularly relevant in the context of financial inclusion. The technical standards for GOV.UK Verify and the final version of the US NIST 800-63-3 Digital ID Guidelines have adopted separate

"assurance levels" for each of the ID system's basic processes.[29] For those assurance frameworks / technical standards that foresee a global assurance level for the whole digital ID system (like the eIDAS Regulation) the process-by-process approach can be implemented by examining how the individual requirements for each level of assurance relevant for every process are met.

157. Digital ID technology and architecture, and digital ID standards, are dynamic and evolving. The 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.

Using digital ID assurance standards and frameworks

158. The digital ID assurance frameworks and standards usually set out various, progressively more reliable, assurance levels with increasingly rigorous technical requirements, for each of the three main steps in a digital ID system.

159. 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 basic constituent processes of a digital ID system. 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. This Guidance does not require or recommend any particular assurance levels.

160. Some 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 assurance level (AL). 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. Even with frameworks that assign a single level of assurance, entities can examine how the individual requirements for each level of assurance relevant for every process are met.

161. 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 digital ID assurance frameworks and standards, *Appendix E: Overview of US and EU digital ID assurance frameworks and technical standards* sets out, by way of example, the NIST assurance levels and describes in broad terms, some of the technical requirements for Identity Proofing (the first stage of a digital ID system).

Special considerations for financial inclusion

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

162. Ideally, the take up digital ID systems, particularly in countries with weaker identity frameworks, will increase individual's access to identity at higher levels of assurance.

[29] For example, under the NIST Guidelines, there are assurance levels (1-3) for each of the stages of the digital ID process: ID assurance level (IAL); authentication and credential life cycle management level of assurance (ALA); and federation level of assurance (FAL).

However, as digital ID is often based on documentary identity evidence, there continues to be parts of the population in some countries that may not be able to access digital ID at higher levels of assurance due to difficulties in identity proofing. As highlighted earlier in this paper, jurisdictions facing issues in relation to financial inclusion should adopt a flexible approach in establishing the required attributes, identity evidence and processes for proving official identity, to ensure that financial excluded people can be captured under the identity proofing requirements (for example, a permanent residential address may be an optional attribute). As part of broader international, government or NGO initiatives to address these issues, including by increasing access to identity evidence, AML/CFT authorities and regulated entities should consider how a risk-based approach to CDD applies in relation to digital ID systems particularly in jurisdictions, or within particular populations, where financial exclusion has been identified as a risk.

163. In 2017, the FATF provided a specific supplement to the 2013 Guidance on AML/CFT Measures and Financial Inclusion, focusing specifically on CDD and financial inclusion.[30] The paper highlights risk mitigation measures that regulated entities should apply commensurate with the nature and level of risks identified. It also presents different CDD approaches which can be implemented to facilitate financial inclusion and remove obstacles linked to the verification of the customer's identity, either a broad understanding of the reliable and independent source of information, or simplified due diligence measures. The Guidance also notes that in a number of countries, the expansion of digital financial services has been supported by the implementation of a tiered approach to CDD. 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 assurance for the purposes of simplified due diligence.

164. 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 with a lower assurance level for identity proofing 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, a digital ID system with a lower assurance level for identity proofing (for customer identification/verification at on-boarding) but greater reliability for its authentication processes may be used. In this situation, the regulated entity may have a lower level of assurance regarding who their customer is, but will have a higher assurance that the account is only being accessed by the person that was identified. In this case, there is less risk that a number of account are being created and ultimately controlled by a bad actor. Additional measures may be required to ensure ML/TF risk is mitigated, including for example, putting restrictions on the use of the account.

165. The ability to adopt a flexible approach 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 (a) limitations on the account's total value and/or the value and number of transactions within a specified time frame, and (b) verification of the customer's identity is delayed until specified thresholds are reached, a lower level of reliability may be appropriate for the digital ID system's ID proofing component than is appropriate for authentication. Authenticating the customer's identity to authorise account access to conduct transactions, even for low value accounts, is important to combat fraudulent transfers and to make sure

[30] FATF (2013-2017), Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence, FATF, Paris www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

that tiered CDD value, velocity and volume requirements are not circumvented. These measures will not be appropriate where TF risks apply as even small amounts of funds can be a significant TF risk.

166. As set out in the FATF Customer Due Diligence (CDD) and Financial Inclusion Guidance (2017), the consistency of these sorts of measures with the FATF requirements depends on the availability of a sound risk assessment and whether they are risk-based and proportionate given the ML/TF risk situation. It is also important to note that CDD is not a static exercise. While individuals with digital IDs of lower levels of assurance may be on-boarded but have restricted access to financial services, regulated entities may over time, develop stronger confidence in the identity of their customers.

Digital ID standards and frameworks can support financial inclusion – e.g. the case of 'Trusted Referees'

167. One example, in which the some digital ID assurance frameworks and standards allow for those without traditional identity evidence is to permit the use of 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 the applicant as a form of identity evidence,[31] in accordance with the jurisdiction's applicable laws, regulations, or agency policies.

168. For example, under the NIST, the use of trusted referees requires the IDSP to:

- 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 level as the applicant, and determine the minimum identity evidence required to establish the relationship between the trusted referee and the applicant.

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

Appendix A: Description of a Basic Digital Identity System and its Participants

169. This Appendix provides a more detailed explanation of the basic components of a generic digital ID system, expanding on the brief summary set out in Section III. The description is presented at a high level of generality. It provides some examples of technology or process that may be applied for the purposes of illustration for the reader only – it does not encourage or approve the use of any any particular identity technology, architecture, or processes, such as biometrics or mobile phone technology. Thus, it applies to a broad range of digital ID systems. This Appendix focuses on the first two components of a digital ID system, because they are most directly relevant to the application of Recommendation 10 requirements for customer identification/verification at on-boarding, and for authenticating customer identity for account access.

Summary of the digital ID process

170. As reflected in the NIST digital ID standards, the digital ID process involves two basic components and a third optional component:

> **Component One: Identity proofing and enrolment (with initial binding/credentialing)** (essential);
>
> **Component Two: Authentication and identity lifecycle management** (essential); and
>
> **Component Three: Portability and interoperability mechanisms** (optional).

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

172. The terminology used by different jurisdictions and organisations may differ slightly, depending on the system being described. A more detailed description of each of the stages follows.

Component 1: Identity proofing and enrolment

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

174. **Identity proofing** answers the question, "Who are you?" and refers to the process by which an identity service provider (IDSP) collects, validates and verifies information about a person and resolves it to a unique individual within a given population or context. The following discussion describes the process flow of identity proofing in three actions: (1) collection/resolution, (2) validation, and (3) verification.

- ***(1) Collection and Resolution*** 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). The process of resolving identity evidence and attributes to a single unique identity within a given population or context(s) is called **de-duplication.** Some government-provided digital identity solutions include a de-duplication process as part of identity proofing, which may involve checking specific the applicant's biographic attributes (e.g., name, age, and gender); biometrics (e.g., fingerprints, iris scans, or facial recognition images); and government-assigned identifiers (e.g., driver's license and/or passport numbers or taxpayer identification number) against the identity system's database of enrolled

individuals and their associated attributes and identity evidence to prevent duplicate enrolment.

- **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). Traditionally, identity evidence has taken a physical form, such as (for natural persons) a government-issued document (preferably, for reliability, bearing a photograph and hologram or similar safeguards)—e.g., a birth certificate; national identity card; driver's license; or passport. Also, traditionally, documentary identity evidence has been physically presented by the claimant to the IDSP. 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 inherent—i.e., based on an individual's personal biometric (biological or behavioural) characteristics. Biometrics has rapidly evolved, from static to dynamic, giving rise to distinct types of biometric identity technology, with varying reliability and privacy risks. In order of technological maturity and scale of commercial adoption—as well as the severity of potential privacy threats—digital identity systems may include the use of:
  - Biophysical biometric attributes, such as fingerprints, iris patterns, voiceprints, and facial recognition—all of which are static.
  - 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, based on the new computational social science discipline of social physics, 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.[32]
- The required (core) official identity attributes vary by jurisdiction but could include: full official name; date of birth; place of birth; home address and a unique government-issued identity number. However, governments have considerable flexibility in determining the attributes and evidence required to prove official identity in the jurisdiction. A government's approach to determining required identity attributes may change over time, with the evolution of technology and the related confidence in the trustworthiness of various types of identity attributes.[33] In addition, governments may consider

[32] See D. Shrier, T. Hardjono and A. Pentland, "Behavioral Biometrics," Chapter 12, *New Solutions for Cybersecurity* (ed. By H. Shrobe; D. Shrier; and A. Pentland (MIT Connection Science and Engineering, MIT Press 2017).

[33] For instance, the evolution of Human-Computer Interface (HCI) technology (e.g., combing eye movement and mouse usage) or haptic interfaces may lead some governments eventually to replace reliance on traditional r identifiers with l reliance on biomechanical attributes. See Section V for a

country context and financial inclusion goals in establishing required identity attributes. For example, especially in developing countries with significant itinerate or homeless populations, the government may decide to not require address as a core identifier for proving official identity.

- ***(2) Validation*** involves determining that the evidence is genuine (not counterfeit, forged or misappropriated) and the information the evidence contains is accurate by checking the identity information/evidence against an acceptable (authoritative/reliable) source to establish that the information matches reliable, independent source data/records. For instance, the IDSP could (1) 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 (a) determine that there are no alterations;; the identification numbers follow standard formats; and the physical and digital security features are valid and intact; and (b) query the government issuing sources for the license and/or passport and validate (confirm) that the information matches.
- ***(3) Verification*** involves confirming that the validated identity relates to *the* individual (applicant) being identity-proofed. 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 passport identity evidence or the photo on file in the government's passport or license database; 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 which is tied to the identity; 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 identity proofed.

175. **Enrolment** is the process by which an IDSP registers (enrols) an identity-proofed applicant as a 'subscriber' 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 also referred to as 'credentialing'.

176. An **authenticator** is something the claimant possess and controls—typically, a cryptographic module, one time code generator or password—that is used to authenticate (confirm) the claimant. More precisely, an **authenticator** is something the claimant possess and controls that is used to authenticate (confirm) that the claimant is the individual to whom a credential was issued, and therefore (depending on the strength of the authentication component of the digital identity system) is (to varying degrees of likelihood, specified by the authentication assurance level) the actual subscriber and account holder. A **credential** is a physical object or digital structure that authoritatively binds a subscriber's proofed identity, via an identifier/s, to at least one authenticator possessed and controlled by the subscriber. When a digital IDSP (acting as a credential service provider (CSP) issues the authenticator/s and authoritatively binds the authenticator/s to the subscriber's identity, the physical object or digital structure that results is a credential.

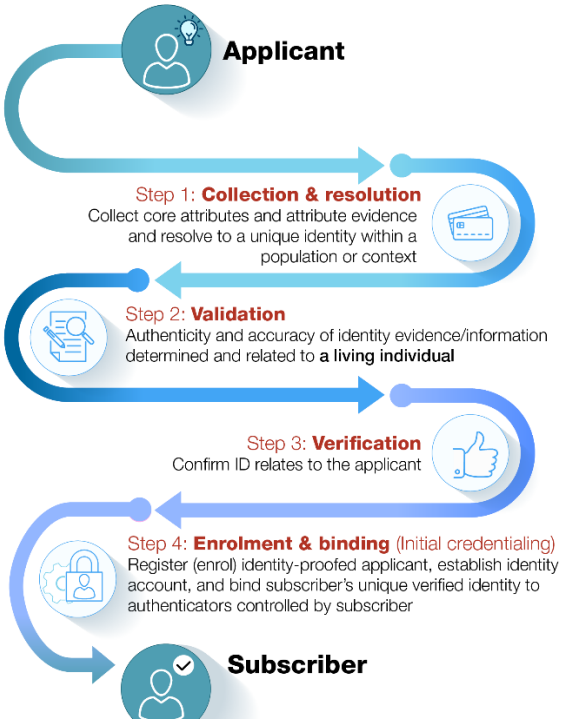
---

discussion of the evolving role of behavioural biometric attributes in digital identification/verification and authentication.

177. 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 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.

178. Identity proofing 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 processes. Similarly, binding the proofed identity during enrolment can be accomplished by a single service provider or by a separate service provider that does not also perform identity proofing.

Figure 5. Identity Proofing and Enrolment



Component 2: Authentication

179. Authentication answers the question, "***Are you who you say you are?"*** It establishes that the individual seeking access to an account (or other services or resources)--the claimant—is the same person who has been identity proofed, enrolled, and credentialed (e.g., is the on-boarded customer). Authentication can rely on various types of authentication factors and processes, as described below. The trustworthiness of the authentication depends on the type of authentication factors used and the security of the authentication processes.

Authentication factors

180. 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, 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).

181. Knowledge authentication factors (something you know) may not actually be 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 NIST standards. Similarly, a biophysical biometric inherence factor does not constitute a secret, and the NIST standards allow the use of biophysical biometrics for authentication only when strongly bound to a physical authenticator.

182. Importantly, new kinds of technology-based ownership and inherence authenticators (including advanced digital device authenticators, biomechanical biometrics, 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.

183. Traditionally (and as reflected in the NIST digital ID standards), digital ID authentication is conducted at a particular point in time: when the claimant asserts the customer's/subscriber's identity and seeks authorisation to begin a digital (online session) or in-person interaction to access the customer's account or other financial services or resources. Today, however, many regulated entities, particularly larger financial institutions in developed countries, augment traditional authentication at the beginning of an online interaction with "continuous authentication" solutions that leverage **biomechanical biometrics, behavioural biometric patterns**, and/or dynamic **Transaction Risk Analysis**. Instead of relying on a combination of something the claimant has/knows/is to establish at the beginning of the interaction that the claimant is the on-boarded customer and is in control of the authenticators/credentials issued to that customer, continuous authentication focuses on ensuring that certain data points collected throughout the course of an online interaction, such as geolocation, MAC and IP addresses, typing cadence and mobile device angle—match "what should be expected" during the entire session.

184. Ways to measure the impact (effectiveness) of continuous authentication technology in mitigating authentication risks have not reached maturity, and the digital ID technical standards, such as the NIST, do not currently address them. The European Commission Delegated Regulation (EU) 2018/389 (RTS on Strong customer authentication and secure communication) under the second Payment Services Directive (PSD2) requires all payment service providers (PSPs) to have transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions for the purpose of implementing the SCA requirements in PSD2 (Art. 2 Regulatory Technical Standards (RTS)). In addition, PSPs that wish to benefit from the "Transaction Risk Analysis" exemption to SCA under Art. 18 RTS need to have in place

real time risk monitoring mechanisms in accordance with Art 18 RTS and demonstrate that their fraud rates are below certain thresholds defined in the RTS.[34]

The following discussion applies to static, single-point of time identity authentication methods, addressed by the NIST standards for digital ID.

Authentication processes

185. 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 usually 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 authenticate. 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 authentication factor, from a different authentication factor category. An online banking customer might use an ownership authentication factor, such as a private key generated in the FIDO-certified authenticator that came embedded in their mobile phone.
- **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.

186. Under the NIST standards, 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. Under the EU PSD2, and as reiterated in the RTS, strong customer authentication is defined as an 'authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.

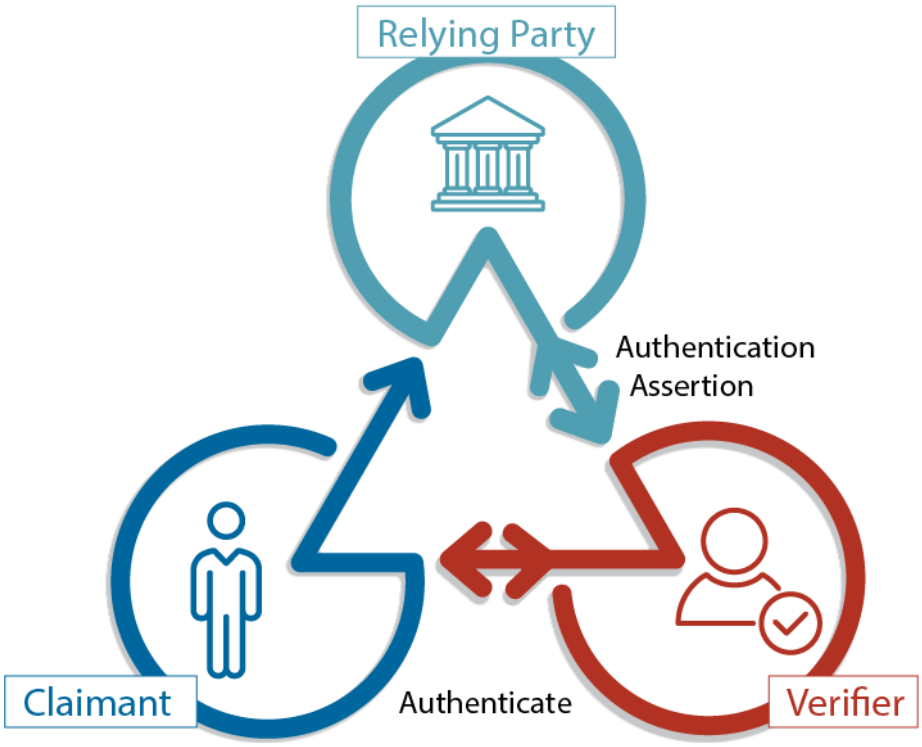
187. The figure below illustrates the authentication process, using the example of a typical financial transaction. In this diagram, an existing customer wants to initiate a financial transaction and must first prove, via one or more authenticators, that he/she is who he/she claims to be—i.e., is the 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. NB: the CSP, verifier, and RP may be the same entity (simple, two-party authentication, consisting

[34] The text of the RTS is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389.

only of claimant and RP). [**Note**: this diagram may be amended in response to expert comments.]

Figure 6. Digital authentication

NB: the CSP, verifier, and RP may be the same entity (simple, two-party authentication, consisting only of claimant and RP



188. Traditionally, and as reflected in the NIST standards, digital ID authentication is conducted at a particular point in time – when the claimant asserts an identity and seeks authorisation to begin a digital (online session) or in-person interaction and access an s account or other financial services. Today, however, many regulated entities, particularly larger financial institutions in developed countries, augment traditional authentication at the beginning of an online interaction with "continuous authentication" solutions that leverage biomechanical biometrics, behavioural biometric patterns and/or "Transaction Risk Analysis".

189. The European Commission and the European Banking Authority (EBA) have specifically recognised and permitted the use of "Transaction Risk Analysis" as part of their Regulatory Technical Standards (RTS) for Strong Customer Authentication (SCA) under the second Payment Services Directive (PSD2).[35]

Identity Lifecycle management

[35] The EC and the EBA allow Transaction Risk Analysis to be used in lieu of traditional SCA, provided that banks can demonstrate that their use of this continuous authentication technology meets appropriate fraud detection rates at different payment levels. See RTS, Articles 8-21 at https://hyperlink.services.treasury.gov/agency.do?origin=https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN

190. **Identity 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 and binding authenticators to credentials, either at enrolment or post-enrolment, loss, theft, unauthorised duplication, expiration, and revocation of authenticators and/or credentials.

191. 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.

Component Three: Portability and interoperability mechanisms (optional)

192. Digital ID systems can—but need not--include a component that allows proof of official identity to be portable. Portable identity means that an individual's digital identity credentials can be used to prove official identity for new customer relationships at unrelated private sector or government entities, without their having to obtain and verify personally identifiable information (PII) and conduct customer identification/verification each time. Portability requires developing interoperable digital identification products, systems, and processes. Portability/interoperability can be supported by different digital ID architecture and protocols.

193. Federation is one way of allowing official identity to be portable. Federation refers to the use of federated digital architecture and assertion protocols to convey identity and authentication information across a set of networked systems. Federated identity architecture provides interoperability across separate networks—i.e., it provides the infrastructure that links separate systems into an interoperable network. APIs that do not use federated architecture and assertion protocols are another way of achieving portability.

194. 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 limited-purpose identity systems.

195. Trustworthy federation and other approaches to enabling portable private sector digital ID systems could provide many significant benefits. For example, portability/interoperability 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 authorising customer account access. Federation or API-based portability solutions could also potentially save customers the inconvenience of having to prove identity for each unrelated financial institution or government service, and reduce the risk of identity-theft stemming from the repeated exposure of PII.

196. For example, the interoperability framework under the eIDAS Regulation ensures cross-border cooperation and interoperability of national digital ID systems. The interoperability infrastructure set by the eIDAS framework created technical interfaces relying on eIDAS nodes that play a central role in the interconnection between the relying parties and different national digital ID schemes connected to the nodes.

Participants in a digital ID system

197. As noted above, digital ID systems can involve different operational models, with different roles for the government and private sector in developing and operating the system and/or providing specific components or sub-components or processes.

198. The following table describes the basic participants and their roles in a generic digital ID system. Although the table describes each type of participant by its specific function, it should be understood that in government-provided general-purpose or limited-purpose digital ID systems, the government directly conducts (or has another entity(ies) undertake on its behalf) all of the fundamental provider/operator functions. Similarly, for private-sector digital ID systems, a single entity or multiple entities may play all or some of the provider/operator roles.

Table 2. Participants in digital ID systems

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. IDSPs provide digital ID systems 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 and uses it to prove his/her (legal) identity. Users are typically referred to by different names at different stages in a digital ID system, depending on their activities-based role with respect to each of the three components of a digital ID system, 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 authorisation decision. Typical RPs include financial institutions and government departments and agencies.
Trust Framework Provider / Trust Authority	Trusted entity that certifies and/or 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) 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).

Appendix B: Country case studies

[**Note for public consultation:** Please note that these case studies are being reviewed alongside the public consultation.]

Box 4. eIDAS interoperability and mutual recognition

Under the eIDAS framework are member states free to use or to introduce means for the purposes of electronic identification for accessing online services. They should also be able to decide whether to involve the private sector in the provision of those means. Member states should not be obliged to notify their electronic identification schemes to the European Commission. Under the principle of mutual recognition member states are obliged to accept notified electronic identification means of other member states. This obligation applies if they allow the use of electronic identification means for online access to their public services, and if the assurance level of the notified means is equal or higher than the one necessary to access the service. The eIDAS Regulation defines three different assurance levels (low, substantial and high) depending on the degree of confidence in the claimed or asserted identity of a person.

The security of electronic identification schemes is key to trustworthy cross-border mutual recognition of electronic identification means. In this context, EU member states cooperate with regard to the security and interoperability of the electronic identification schemes at EU level. Whenever electronic identification schemes require specific hardware or software to be used by relying parties at the national level, cross-border interoperability calls for those member states not to impose such requirements and related costs on relying parties established outside of their territory. In that case appropriate systems should be discussed and developed within the scope of the interoperability framework.

Source: European Commission

Box 5. India's Universal ID (UID) number

India's Universal ID (UID) number—or Aapka Aadhaar (henceforth, Aadhaar) identity program uses 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

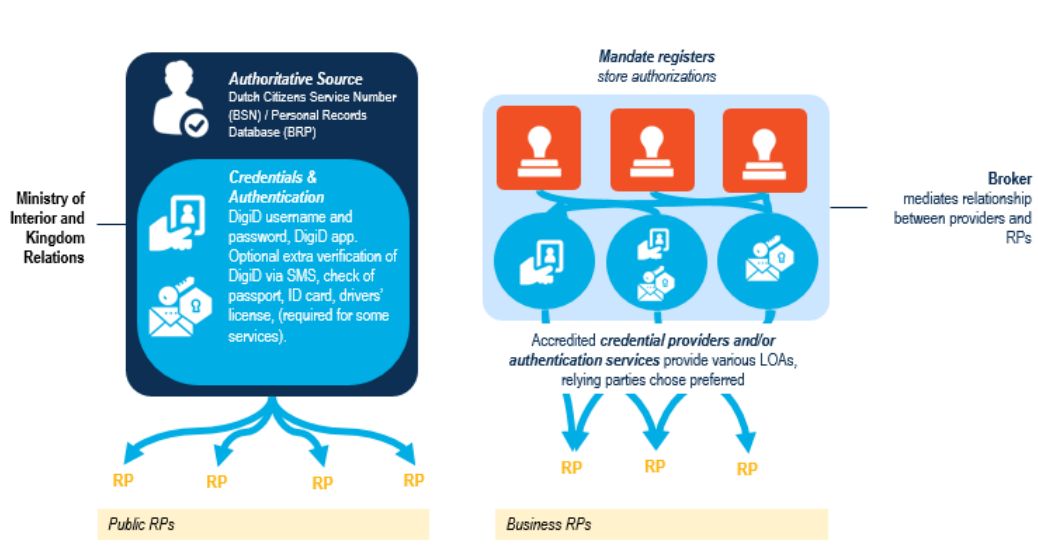
entitlement document enrols in Aaahar, using valid Proof-of-Identity and Proof-of-Address documents. The head of the household can then introduce other members in the family while they are enrolling. UIDAI accepts eight document types as Proof of Relationship. Where no documents are available, a resident may also use Introducers notified by the Registrar, who are available at the enrolment centre.

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

Source: World Bank

Box 6. 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 organisations 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/.



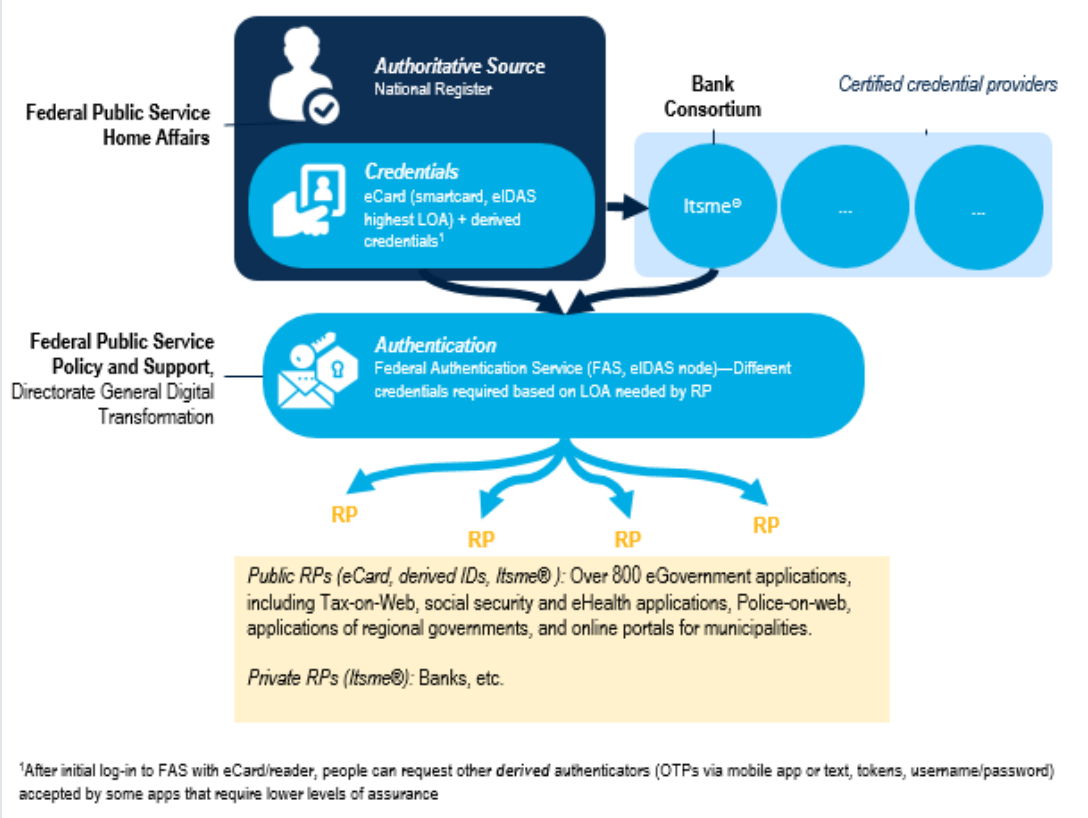
Source: Netherlands and World Bank

Box 7. Belgium – eCards & ItsMe ®

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.



ItsMe ®

Since January 2018, Belgian citizens have the option to use a mobile identification mean to authenticate themselves on public applications. "ItsMe ®" (created by BMID, a privately

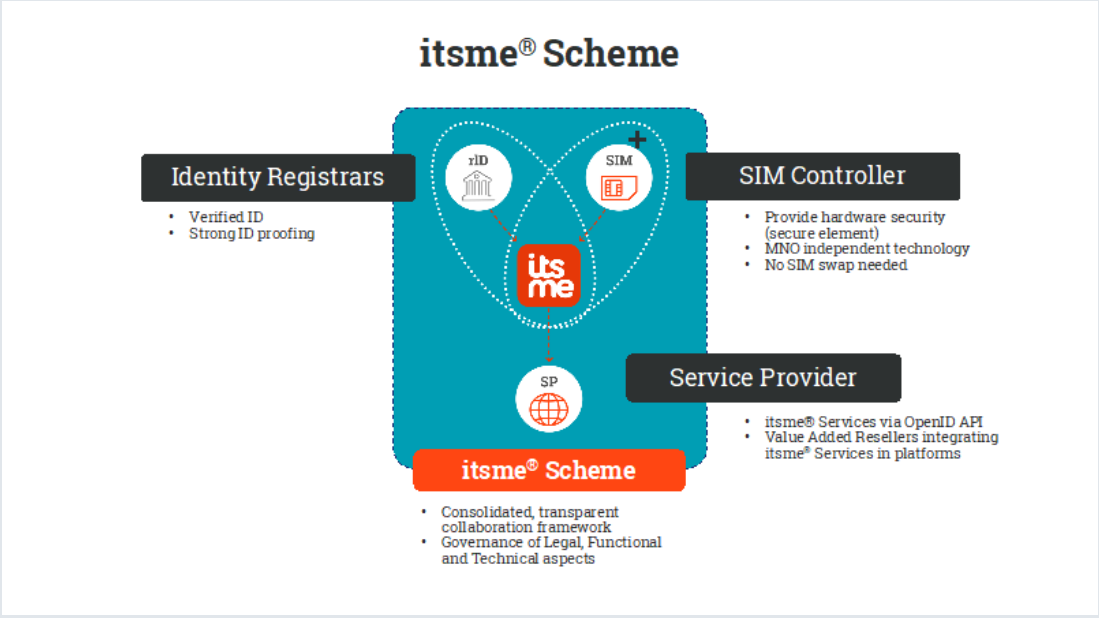
owned company) has been recognized by the Belgian government as a valid authentication mean, with a Level of Assurance 'high'.

Activation of this service on the mobile device is directly or indirectly bootstrapped with the Belgian eID card, to assure proof of identity.

The authentication flow between the itsme® user and the FAS, using the itsme® App, is based on the OpenID Connect standard (Doc Ref. 1.2.4).

During the itsme® authentication flow, the browser redirects the itsme® users' browser to the itsme® login page with the authentication context (https://merchant.itsme.be/oidc/authorization/phone/confirmation), where it requests the mobile phone number (MSISDN) from the itsme® user. The MSISDN is the unique identifier for this itsme® user, the itsme® app instance as well as the device on which it is installed (1 Unique itsme® user = 1 MSISDN = 1 Device = 1 App). The central itsme® service will request the itsme® app to answer a challenge for which the user enters the correct itsme® PIN (or uses the correct fingerprint if that was configured by the user).

The itsme® PIN is only known to the user. Based on the response received, including the device and/or SIM fingerprint information, the login transaction will be validated and approved.



Source: Belgium and World Bank

Box 8. Sweden – BankID

Sweden has a long history of robust federal identity ecosystem with a general-purpose 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 a digital ID 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 minimise 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

Box 9. 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 Computerised 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 onboarding 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

Box 10. Italy - Public System of Digital ID

The Italian Public System of Digital Identity (SPID) is the Italian solution developed under the EU eIDAS Regulation.

It is a public open system allowing public and private entities (Identity Providers), accredited by the Agency for Digital Italy (AGID), to offer registration services and the digital ID verification for access to services for citizens and businesses.

The acceptance of SPID is mandatory for the public sector and is optional for private and financial sectors. SPID envisages different levels of authentication, consistent with standard ISO-IEC 29115, according to the level of security of the services required by the users. Launched in 2016, SPID reached about 2.5 million digital identities by March 2018.

Opportunities of the adoption of SPID are commonly envisaged in the identification of (potential) customers in the CDD process. The Italian legislation allows financial institutions to use digital identity for the identification and verification of customers (as long as they are natural persons). Indeed, obliged entities can identify and verify customers through digital identities that are EIDAS compliant, like SPID.

Source: World Bank and Banca d'Italia

Box 11. China - Private sector provided digital ID

In China, Ant Financial has created digital ID, based on the CDD information which has been verified against China's Ministry of Public Security (MPS) as well as other data collected, including face recognition. The customer's name and ID number are verified by the authoritative database held by the MPS to ensure the accuracy of the identity information. Face recognition (matching with avatars on valid documents), multi-channel cross-validation and black list screening is combined with business scenarios to complete customer due diligence. Each verification is based on the user's explicit authorisation and confirms the use of the verification service.

Ant Financial Digital Identity has been widely accepted in various financial service scenarios, providing more than 3 billion face verification services to hundreds of millions of Alipay users. In addition to the implementation of the world's first face verification payment in KFC, it is also used in pension inquiry, pension collection, tax declaration and other public services, verifying faces for delivery collection, hotel check-in, public transport, and other daily life scenarios. In the financial scenario, Ant Financial and financial institutions cooperate to provide financial services such as insurance, fund, and microfinance to customers, and also fully use Digital Identity to provide financial institutions with services such as customer identification and customer risk assessment.

Source: China

Box 12. China – eID and Tencent E Pass

What is eID?

Derived from the citizen ID number, eID is a network electronic identity generated for Chinese citizens, unified by the Ministry of Public Security's Citizen Network Identification System based on cryptographic algorithm. While ensuring each eID is unique, it reduces the spread of plaintext information of citizen identity through the Internet and allows remote online identification without disclosing the identity information.

What are the key features of eID?

- Authority: Issued by the Ministry of Public Security's Citizen Network Identification System, eID can effectively prevent identity fraud and ensure unique consistency with the holder's true identity;
- Security: After issuance, the consistency of eID with the real-name information is only held by the public security system. The platform obtains appeidcode derived from eID, thus ensuring that eID cannot be illegally read, copied, tampered with, or used through high-intensity security mechanisms;
- Universality: eID serves as the network identity across regions and industries, not subject to the physical form of the carrier, as long as the security verification means in the carrier meets the eID related standards;
- Privacy: The unique identifier of eID is generated by the national commercial cryptographic algorithm and contains no personal identity information, which can effectively protect citizen identity information.

What are the functions of eID?

- To protect personal information, eID aims to prevent the disclosure of citizens' personal information and the accurate portrait of big data by transforming the citizenship information into de-identified and fragmented personal marks, so as to ensure property and personal safety for citizens.
- On the basis of comprehensive study and analysis of China' s mainstream identity authentication technology and application, eID helps build a national unified digital identity system, to integrate various digital identity authentication technologies and achieve interoperability of authentication;
- By classifying the security and reliability of eID issuance and authentication process, it builds the framework of eID system.
- It is committed to promoting the opening and circulation of China's data, facilitating the development of China's digital government and digital economy, and building China into an Internet leader.

Tencent E Pass

A carrier is needed to apply and promote the eID. Cooperating with the Third Research Institute of the Ministry of Public Security, Tencent FIT launched Tencent E Pass. Supported by the eID technology of the Third Research Institute, Tencent E Pass has enhanced the financial risk control and the safety in eID use, offering digital identity-based

solutions for various industries. Currently, Tencent E Pass is available for online and offline identity verification:

(1) Online: Switching from the merchant side (applet /APP/official account) to Tencent E Pass, users authorize Tencent E Pass to verify their identities;

(2) Offline: After creating a Tencent E Pass, you can scan the QR Code for face recognition through camera to verify your identity.

Risk Control Measures of Tencent E Pass

Scenario-based hierarchical authentication

(1) Weak authentication scenario: Based on the WeChat risk control system, we only need to verify users' WeChat accounts and obtain users' eID codes;

(2) General authentication scenario: In addition to WeChat risk control system, we need to check the verification code of users' mobile phone number and obtain users' eID code and information comparison result (Y/N);

(3) Strong authentication scenario: In addition to WeChat risk control system, we need to verify users' face information, and obtain users' eID code and real-name information.

Multi-identity verification to ensure authentic operation

(1) WeChat account system security, related to WeChat account system;

(2) Mobile phone number verification to verify the consistency of mobile phone number and real-name information;

(3) Face detection in vivo, including anti-remake detection to confirm that the operation is authentic and authorized.

Prevention of unauthorized/repeated use

(1) Uniqueness: eID only works on one WeChat account and device at the same time. If you change the account or device, re-authentication is required.

(2) Reliability: The issued eID identification code changes every 10 seconds, and the screen shot is invalid. The QR code is only available on this device and cannot be reused.

(3) Security: The identity will be verified according to different scenarios during use to ensure that the operation is authentic and authorized.

Privacy Protection Measures

(1) Issuing process of eID: Tencent E Pass is only used for collection and transmission in the process of issuing eID. The user information is not stored. The eID is issued by Ministry of Public Security's Citizen Network Identification System;

(2) Scenario application: The QR code of Tencent E Pass is used as a carrier and does not display any plaintext information of identity in case of information disclosure;

(3) Information transmission: Upon the request of the merchant, the user information will be encrypted by the Third Research Institute of the Ministry of Public Security and sent by Tencent to the merchant, and then decrypted by the merchant. As the private key is only held by the merchant, no intermediary party can decrypt the plaintext information of users during the transmission.

Problems facing e ID

(1) Lack of legislative support: Currently, there is no national legislation to support eID. It is only used as a research result for pilot application and is an identity certificate without legal effects. It cannot be applied in some scenarios where the use of identity certificate is explicitly stipulated by laws.

(2) Lack of regulation: Most merchants do not need the plaintext of user real-name information. They only need a user mark and verification result. However, they have to obtain user information in order to adapt to the original system since eID is currently not recognized by the regulator.

Box 13. Singapore – National Digital Identity (NDI)

In 2003, Singapore launched an authentication system, known as SingPass, for residents to access digital Government services. Two-factor authentication (2FA) is required for digital transactions involving sensitive information such as filing taxes. It has since been used by more than 3.3 million residents.

Under the Smart Nation initiative, Singapore has identified key strategic national projects to drive pervasive adoption of digital and smart technologies throughout Singapore. A key initiative is the National Digital Identity (NDI), which is to develop a digital identity service stack for Singapore residents and businesses to transact digitally with the Government and private sector in a convenient and secure manner. The NDI services have been gradually deployed since 2017 and are expected to be fully operational by 2020.

MyInfo forms the trusted identity data service of NDI and was launched in early 2017, with SingPass users auto-enrolled into MyInfo from late 2017. MyInfo includes government-verified data retrieved from various Government agencies and contains more than 100 personal data items. It helps the public to auto-fill their government-verified personal information on public and private sector e-services via a reliable and independent channel upon the individual's consent. Where MyInfo is used, financial institutions will not be required to obtain physical documents to verify a customer's identity and will also not be expected to separately obtain a photograph of the customer. Today, more than 30 financial institutions in Singapore leverage MyInfo for over 120 digital services. This feature allows banks and other financial institutions to develop integrated services with straight-through processing (such as account opening).

In late 2018, SingPass Mobile was launched as the trusted identity authentication service of NDI. This new 2FA mode enables users to be authenticated with their fingerprint, facial recognition or a 6-digit passcode.

Source: Singapore

Box 14. UNHCR – digital ID for refugees

At the end of 2018, the United Nations Refugee Agency (UNHCR) estimated that there were 25.9 million refugees and 3.5 million asylum seekers globally. Countries in developed

regions hosted 16 per cent of refugees, while one third of the global refugee population (6.7 million people) were in the World's Least Developed Countries.

Host countries are primarily responsible for issuing proof of general-purpose official identity to refugees, although this process may be administered by an internationally recognised and mandated authority.

The identity challenges that refugees face are in many ways unique. Many refugees do not possess identity credentials when they arrive in a host State because their credentials were left behind, lost or destroyed during flight. Some refugees may never have been registered in their country of origin's general-purpose official identity system because they came from fragile or conflict affected areas or faced discrimination. At the same time, there is a general rule against the authorities of the country of origin being contacted to verify a refugee's identity, without the refugees' consent and if there is any risk of harm. International standards therefore indicate that the identity proofing of refugees requires greater reliance on evidence collected during in person applications and interviews, as well as knowledge of the applicant's country of origin, local culture and other local information. Identity assurance increases through regular contact and validation over time to monitor consistency, manage risk and build the refugee's identity in the new context.

Host States use varying approaches to providing refugees with general-purpose official identity. Refugees are rarely included as a category in the host State's general-purpose official identity system aimed primarily at citizens. Most commonly refugees are issued with a specific "general-purpose official identity" by the host State's designated government authority, which administers a refugee-specific registry. In many instances this authority receives support and technical assistance from UNHCR and uses UNHCR's Population Registration and Identity Management Ecosystem (PRIMES) as its digital identity management system. In some situations UNHCR will undertake this role on behalf of the Host State. By September 2018 over 8 million refugees in 63 countries had been biometrically enrolled in UNHCR's PRIMES systems. PRIMES tools aim to comply with international digital identity standards and guidance on evidence of identity for refugees is promoted.

Refugees' ability to access to financial services is increasingly important because it facilitates the delivery of humanitarian assistance through cash grants (known as "cash-based interventions") and provides a basis for their greater self-reliance and contributions to the host community. For example, at the end of 2018 Iraq hosted over 283,200 refugees and asylum seekers, with the vast majority coming from Syria. UNHCR and its partners have provided humanitarian assistance to Syrian refugees in Iraq since the crisis began in 2011, aiming to provide as much as possible through cash grants. In the early part of the response the limited coverage of banking services and regulatory concerns were limiting. However, with the introduction of mobile "e-wallets" to the country in around 2016 the position changed. The Central Bank of Iraq supported flexible terms of registration requirements and creation of "humanitarian wallets" or "temporary wallets" using simplified Customer Due Diligence (CDD) processes. The simplified CDD processes recognizes UNHCR's registration credentials as official identity to open an e–wallet, alongside government issued credentials. As a result, UNHCR could provide the full "Survival Minimum Expenditure Basket" for vulnerable refugees living outside camps. The amount is fixed at 292,500 IQD (250 USD) per month, per family, with family size having already been taken into account. In 2019, these arrangements are being enhanced by the biometric authentication of identity for low value transactions, strengthening risk mitigation measures.

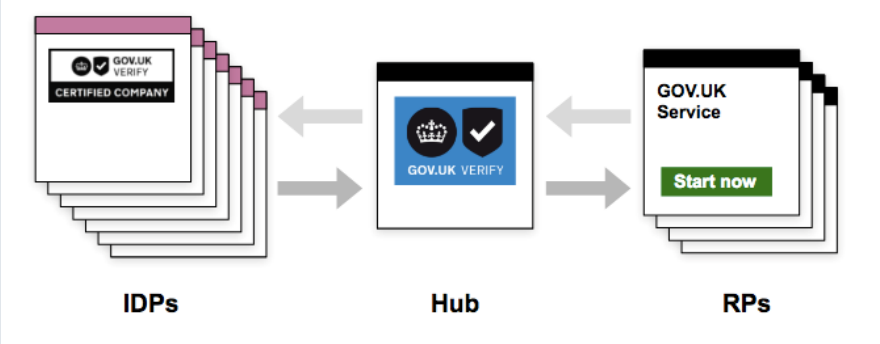
By way of further example, refugees returning to their home country often lack official identity documents, which can limit access to financial services that can contribute to their dignified and durable return. However, interim solutions have been found. Refugees who have been biometrically enrolled in UNHCR's PRIMES system in Kenya and whose identities have been regularly authenticated are able to access return assistance through financial service providers if they choose to return to Somalia. In these circumstances, the identity credential issued by UNHCR to facilitate the refugee's voluntary return, when accompanied by biometric authentication against UNHCR's PRIMES system, can be considered proof of official identity to onboard for financial services by the Somali Central Bank.

Source: UNHCR

Box 15. UK – GOV.UK Verify

In 2012, the UK Government published a Government Digital Strategy, that introduced the concept of 'Digital by default' i.e. providing services online and allowing wide access to those who wish to access these services, while not excluding those who cannot or do not wish to access these services in an online channel. As a part of this 'Digital by default' policy, it was recognised that there was a need for a strong identity verification solution that enabled users to prove their identity online, and Government to trust those users are who they say they are.

GOV.UK Verify is a federated digital identity scheme that enables UK citizens and UK residents to prove their identity in an online channel. It uses private sector Identity Providers (IDPs) to verify the identity of the individual to a set of requirements and specifications under which the scheme operates. IDPs are on a government framework, and have met government and industry standards to provide identity assurance services as part of the GOV.UK Verify scheme.



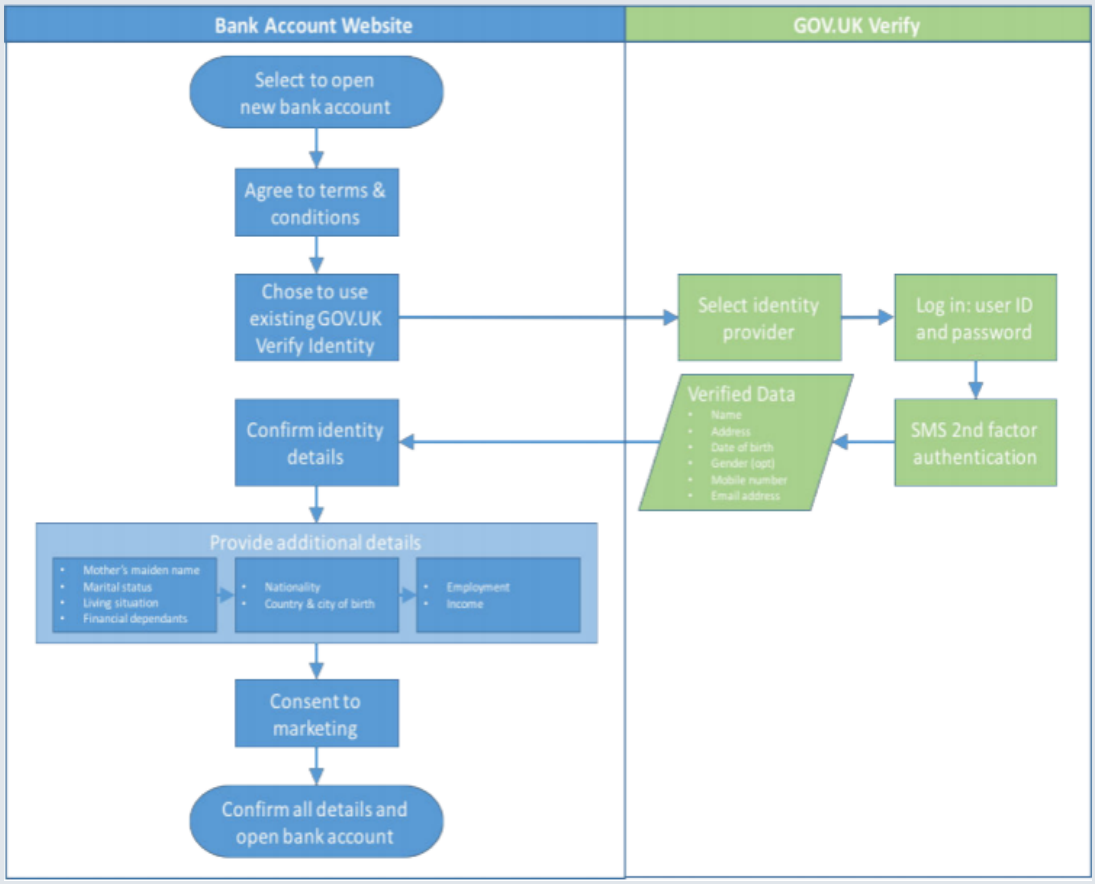
The GOV.UK Verify Hub is the centrally provided infrastructure that manages interactions between users, government services, IDPs, and matching services for the purpose of

authenticating a user to a government service. It also ensures that the required level of identity assurance is requested from an IDP.

A product called the Document Checking Service (DCS) is an API endpoint that allows identity providers to run checks on UK government issued documents against government databases, in support of identity proofing for GOV.UK Verify.

All accounts in GOV.UK Verify require as a minimum 2FA.

The diagram below developed by Open Identity Exchange displays a prototype journey of using GOV.UK Verify for opening a bank account.



Source: OIX (2017), https://openidentityexchange.org/wp-content/uploads/2017/01/The-value-of-digital-identity-to-the-financial-service-sector-Full.pdf p.13

Source: United Kingdom

Other potential examples:

- Switzerland[36]

[36] 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)

- UAE – Emirates ID
- Germany – EID
- Canada – Treasury Board Standard on Identity and Credential assurance and the Pan-Canadian Trust Framework
- Slovakia – national eID card
- Portugal – citizens card and CMD
- Estonia

Appendix C: ID4D Principles on Identification for Sustainable Development

1. This Guidance highlights several concrete ways that countries can digital identity ecosystems that allow them to reap the benefits of these systems while mitigating the risks described in Section IV. To begin, countries should follow the ten *Principles on Identification for Sustainable Development*, which have now been endorsed by over 25 international organisations, development agencies, and other partners.[37] Although these *Principles* were developed to support the creation of "good" government-recognized ID systems, they apply more broadly and can be adopted by both public- and privately provided and used identity systems and services.

Table 3. Principles on Identification for Sustainable Development

	PRINCIPLES
INCLUSION: UNIVERSAL COVERAGE AND ACCESSIBILITY	1. Ensuring universal coverage for individuals from birth to death, free from discrimination. 2. Removing barriers to access and usage and disparities in the availability of information and technology.
DESIGN: ROBUST, SECURE, RESPONSIVE AND SUSTAINABLE	3. Establishing a robust—unique, secure, and accurate—identity. 4. Creating a platform that is interoperable and responsive to the needs of various users. 5. Using open standards and ensuring vendor and technology neutrality. 6. Protecting user privacy and control through system design 7. Planning for financial and operational sustainability without compromising accessibility
GOVERNANCE: BUILDING TRUST BY PROTECTING PRIVACY AND USER RIGHTS	8. Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework. 9. Establishing clear institutional mandates and accountability. 10. Enforcing legal and trust frameworks through independent oversight and adjudication of grievances.

Goal 1. Ensure inclusion

2. The first two principles are intended to ensure that no one is left behind by ID systems, in support of SDG 16.9. *Principle 1* requires countries to fulfil their obligations to provide legal identification to all residents—not just citizens—from birth to death and free from discrimination, as set out in international law and conventions and their own legislative frameworks. This includes the commitment to universal birth registration for those born on in their territory or jurisdiction, but also extend to digital ID systems, particularly when these are a pre-requisite for accessing basic public and private sector services, such as banking, SIM cards, and cash transfers.

3. In recognition of the fact that certain groups will face disproportionate difficulties in accessing identity services—and digital services in particular—*Principle 2* requires practitioners to identify and mitigate legal, procedural, and social barriers to enrol in and use digital ID systems, with special attention to poor people and groups who may be at risk of exclusion for cultural, political or other reasons (such as women and gender minorities, children, rural populations, ethnic minorities, linguistic and religious groups, persons with disabilities, migrants, the forcibly displaced, and stateless persons). Furthermore, digital ID

[37] World Bank. 2017. *Principles on Identification for Sustainable Development: Toward the Digital Age*. Washington, DC: World Bank Group. id4d.worldbank.org/principles.

systems and identity data should not be used as a tool for discrimination or infringe on individual or collective rights.

Goal 2. Design robust, secure, responsive, and sustainable ID systems

4. In addition to providing universal coverage, digital ID systems should be robust to fraud and error, useful for a variety of stakeholders, and sustainable, while also protecting user privacy and adopting open standards to facilitate innovation and avoid vendor and technology lock-in.

5. Specifically, *Principle 3* states that accurate, up-to-date identity information is essential for ensuring the trustworthiness of identities and attributes used in transactions. In addition, identities must be unique to the context, avoiding duplicate identities or using identifiers that could be attributed to multiple people. Furthermore, digital ID systems must have safeguards against tampering (alteration or other unauthorized changes to data or credentials), identity theft, data misuse, and other errors occurring throughout the identity lifecycle.

6. *Principle 4* highlights the need for identification and authentication services to be flexible, scalable, and meet the needs and concerns of people (users) and relying parties (e.g., public agencies and private companies). To ensure that identity-related systems and services meet specific user needs, practitioners should engage the public and important stakeholders throughout planning and implementation. The value of digital ID systems to relying parties is highly depended on their portability and interoperability with multiple entities—subject to appropriate privacy and security safeguards—both within a country and across borders.

7. For government-recognized digital identity in particular, *Principle 5* further emphasizes the need for vendor and technology neutrality to increase flexibility and avoid system design that is not fit for purpose or suitable to meet policy and development objectives. This requires robust procurement guidelines to facilitate competition and innovation and prevent possible technology and vendor "lock-in," which can increase costs and reduce flexibility to accommodate changes over time. In addition, open design principles enable market-based competition and innovation. They are essential for greater efficiency and improved functionality of digital ID systems, and for enduring interoperability. Similarly, open APIs also support efficient data exchange and portability by ensuring that a component of the digital ID system—e.g., a particular type of credential—can be replaced with minimal disruption.

8. In addition to architecture that is responsive and flexible, *Principle 6* emphasizes that digital ID systems must protect people's privacy and control over their data through system design. This is crucial for mitigating many of the risks to privacy and data protection identified in Section IV of this Guidance. Designing with people's privacy in mind means that no action should be required on the part of the individual to protect his or her personal data. Information should be protected from improper and unauthorized use by default, through both technical standards and preventative business practices. These measures should be complemented by a strong legal framework (as emphasised below in *Principle 8*).

9. For example, data collected and used for identification and authentication should be fit for purpose, proportional to the use case and managed in accordance with global norms for data protection, such as the OECD's Fair Information Practices (FIPs) and with reference to emerging international best practices, such as the European Union's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act. Authentication protocols should only provide "yes or no" confirmation of a claimed

identity or—if mandated by an AML or CCC-related law—only disclose the minimal data necessary for the transaction. The method of authentication should reflect an assessment of the level of risk in the transactions and can be based on recognized international standards and frameworks for levels of assurance. Furthermore, credentials and identifier numbering systems should not unnecessarily disclose sensitive personal information (e.g., reference numbers should be random).

10. *Principle 7* recognizes the importance of designing public-sector systems that are financially and operationally sustainable while still maintaining accessibility for people and relying parties. This may involve different business models including reasonable and appropriate service fees for identity verification services, offering enhanced or expedited services to users, carefully designed and managed public-private partnerships (PPPs), recuperating costs through efficiency and productivity gains and reduced leakages, and other funding sources.

Goal 3. Build trust by protecting privacy and user rights

11. The final group of principles addresses how digital ID systems should be governed to protect user privacy and rights, system security, and clear accountability and oversight.

12. *Principle 8* sets out the requirements for a comprehensive legal framework. Digital ID systems must be underpinned by policies, laws and regulations that promote trust in the system, ensure data privacy and security, mitigate abuse such as unauthorized surveillance in violation of due process, and ensure provider accountability. This typically includes an enabling law and regulations for the digital ID system itself as well as laws and regulations on data protection, digital or e-government, electronic transactions and commerce, AML, civil registration, limited-purpose ID systems, and freedom of information, among others.

13. The enabling law and regulations for a digital ID system should clearly describe the purpose of the system, its components, the roles and responsibilities of different stakeholders, how and what data is to be collected, liability and recourse for digital ID holders (subjects) and relying parties, the circumstances in which data can be shared, correction of inaccurate data attributes, and how inclusion and non-discrimination will be maintained. Laws and regulations on data protection and privacy should also include oversight from an independent oversight body (e.g. a national privacy commission) with appropriate powers to protect subjects against inappropriate access and use of their data by third parties for commercial surveillance or profiling without informed consent or legitimate purpose. Frameworks require the right balance between regulatory and self-regulatory models that does not stifle competition, innovation, or investment.

14. In addition, *Principle 9* highlights the need for clear institutional mandates and accountability in the governance of digital ID systems. Ecosystem-wide trust frameworks must establish and regulate governance arrangements for ID systems. This should include specifying the terms and conditions governing the institutional relations among participating parties, so that the rights and responsibilities of each are clear to all. There should be clear accountability and transparency around the roles and responsibilities of identification system providers.

15. Finally, *Principle 10* emphasizes that the ID system should include clear arrangements for the oversight of these legal and regulatory requirements. The use of ID systems should be independently monitored (for efficiency, transparency, exclusion, misuse, etc.) to ensure that all stakeholders appropriately use identification systems to fulfil their intended purposes, monitor and respond to potential data breaches, and receive individual complaints or concerns regarding the processing of personal data. Furthermore, disputes regarding identification and the use of personal data that are not satisfactorily

resolved by the providers—for example, refusal to register a person or to correct data, or an unfavourable determination of a person's legal status—should be subject to rapid and low-cost review by independent administrative and judicial authorities with authority to provide suitable redress.

Appendix D: Digital ID assurance framework and technical standard setting bodies

1. This list does not include national or regional bodies such as eIDAS and NIST that have also developed national/regional level frameworks and standards – see Appendix E.

2. The **International Organization for Standardization (ISO)** is a Geneva-based, independent international organisation, with a membership of 164 national standards entities (one per country), that develops voluntary, consensus-based, market relevant international standards that provide specifications for products, services and systems, to ensure quality, safety and efficiency and support innovation.

3. The **International Telecommunication Union (ITU)** is the United Nations specialised agency for information and communication technologies (ICTs), founded to facilitate international connectivity in communications networks. ITU allocates global radio spectrum and satellite orbits and develops technical standards intended to ensure that ICT networks and technologies seamlessly interconnect, worldwide.

4. **W3C** is an international organisation that develops and promotes a broad range of voluntary, consensus-based open technical standards and protocols for the Internet to support interoperability, scalability, stability, and resiliency. In the digital identity space, W3C developed the Web Authentication browser/platform standard for MFA, using biometrics, mobile devices, and FIDO security keys, and is developing standards for verified identity claims in decentralised identity systems.

5. The **FIDO Alliance** is an industry association that promotes effective, easy-to-use strong authentication solutions by developing technical specifications that define an open, scalable, interoperable set of mechanisms to authenticate users; operating industry certification programs to help ensure successful worldwide adoption of the specifications; and submitting mature technical specification(s) to recognised standards development organisation(s) (e.g., ISO, ITU X.1277 and X.1278) for formal standardisation. FIDO is also involved in verification through its Identity Verification and Binding Working Group (IDWG).

6. The **OpenID Foundation (OIDF)** is a technology agnostic, non-profit trade organisation that focuses on promoting the adoption of digital ID services based on open standards.

7. **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.

8. **ETSI** (European Telecommunications Standards Institute) is one of the 3 primary European standards bodies alongside CEN and CENELEC. ETSI provides members with an open and inclusive environment to support the development, ratification and testing of globally applicable standards for ICT systems and services across all sectors of industry and society. ETSI has been working on identity proofing, primarily aimed at trust services as defined by eIDAS, with potential application in other areas such as issuing of eID and CDD processes. ETSI developed a set of standards for implementing the requirements of the RTS under PSD2 for use of qualified certificates as defined in eIDAS to identify third parties (TPPs) in payment transactions.

Appendix E: Overview of US and EU digital ID assurance frameworks and technical standards

NIST – United States

- 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.

Leveraging the NIST 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 interactions with the applicant, as well as interactions where the applicant and identity service provider are physically present in the same location. (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

eIDAS – European Union

1. The eIDAS framework provides for three levels of assurance for electronic identification means delivered in the framework of a notified electronic identification scheme: low, substantial and high. Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 sets the minimal security specifications for each of these levels. International standard ISO/IEC 29115 has been taken into account for the specifications and procedures set out in this implementing act as being the principle international standard available in the domain of assurance levels for electronic identification means. However, the content of the eIDAS Regulation differs from that international standard, in particular in relation to identity proofing and verification requirements, as well as to the way in which the differences between Member State identity arrangements and the existing tools in the EU for the same purpose are taken into account. If, in an EU/EEA country, a public sector body requires, to access one of its online services, an electronic identification with a substantial or high level or assurance, it also has to accept, to access this online service, all the electronic identification means with the same or a superior level of assurance and relating to a notified identification scheme to the Commission and published on the OJ (Official Journal of the European Union). Furthermore, public sector bodies can decide, on a voluntary basis, to recognise electronic identification schemes with a low level of assurance.
2. For the purposes of eIDAS, the components of a digital ID system are:
   - **Enrolment** insures identification uniquely representing either a natural or legal person, or a natural person representing a legal person. Enrolment involves different steps:
     - Application and registration: (1) Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means. (2).Ensure the applicant is aware of recommended security precautions related to the electronic identification means. (3) Collect the relevant identity data required for identity proofing and verification.

  - Identity proofing and verification, consisting in ID document authenticity and validity verification, and relates to a real person, and verification that that person's identity is the claimed identity.

- **Electronic identification** means management, deals with number and nature of authentication factors, whether the electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs, revocation and renewal of it.
- **Authentication** sets out the requirements per assurance level with respect to the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party.
- **Management and organisation**, all participants providing a service related to electronic identification in a cross-border context shall have in place documented information security management practices, policies, approaches to risk management, and other recognised controls so as to provide assurance to the appropriate governance bodies for electronic identification schemes in the respective Member States that effective practices are in place.

3. For each of these four stages, three assurance levels are defined, low, substantial and high according to following criteria:

- **Low** – provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;
- **Substantial** – provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;
- **High** – provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

4. It is presumed that when the electronic identification means issued under a notified electronic identification scheme meets a requirement listed in a higher assurance level then fulfil the equivalent requirement of a lower assurance level.

Table 4. Requirements for authentication under eIDAS Levels of Assurance

ASSURANCE LEVEL	ELEMENTS NEEDED
LOW	• The release of person identification data is preceded by reliable verification of the electronic identification means and its validity. • Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline. • The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.
SUBSTANTIAL	Level low, plus: • The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication. • The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker **with moderate attack potential** can subvert the authentication mechanisms.
HIGH	Level substantial, plus: • The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker **with high attack potential** can subvert the authentication mechanisms.

Glossary

Assurance levels or levels of assurance: refers to the level of trustworthiness, or confidence in the reliability of each of the three stages of the digital ID process. See the overview of technical standards in Section II of the report and 'Leveraging the Digital ID Technical Standards to Implement the RBA' under Section V of the report.

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).

Authentication establishes that the claimant (customer) who asserts his or her identity to obtain access to the customer's account is the same person whose identity was obtained, verified, and credentialed during on-boarding.

An **authenticator** is something the claimant possess and controls that is used to authenticate (confirm) that the claimant is the individual to whom a credential was issued, and therefore (depending on the strength of the authentication component of the digital identity system) is (to varying degrees of likelihood, specified by the authentication assurance level) the actual subscriber and account holder.

Biometrics

- biophysical biometrics: attributes, such as fingerprints, iris patterns, voiceprints, and facial recognition—all of which are static
- biomechanical biometrics: attributes, such as keystroke mechanics, are the product of unique interactions of an individual's muscles, skeletal system, and nervous system.
- behavioural biometric patterns: attributes, based on the new computational social science discipline of social physics, 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.

Collection and resolution is part of identity proofing and involves obtaining attributes (identifiers), collecting attribute evidence; and resolving identity evidence and attributes to a single unique identity within a given population or context.

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). A Claimant can also be described as a Subscriber who asserts ownership of an identity to a Relying Party (RP) and seeks to have it verified, using authentication protocols.

A **credential** is a physical object or digital structure that authoritatively binds a subscriber's proofed identity, via an identifier/s, to at least one authenticator possessed and controlled by the subscriber.

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.

Credential Stuffing (also referred to as breach replay or list cleaning): Type of cyberattack where stolen account credentials (often from a data breach) are tested for matches on other systems. This type of account can be successful if the victim has used the same password (that was stolen in the data breach) for another account.

De-duplication: The process of resolving identity evidence and attributes to a single unique identity within a given population or context(s).

Digital ID systems, for the purposes of this Guidance, are systems that cover the process of identity proofing/enrolment and authentication. Identity proofing and enrolment can be either digital or physical (documentary), or a combination, but binding, credentialing, authentication, and portability/federation must be digital.

Digital ID assurance frameworks and technical standards are a set of open source, consensus-driven assurance frameworks and technical standards for digital ID systems that have been developed in several jurisdictions and also by international organisations and industry bodies See *Appendix D: Digital ID assurance framework and technical standard setting bodies*. See for example NIST standards and eIDAS Regulation at *Appendix E: Overview of US and EU digital ID assurance frameworks and technical standards*.

eIDAS Regulation: (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market.

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 also referred to as '**credentialing'**.

Federation refers to the use of federated digital architecture and assertion protocols to convey identity and authentication information across a set of networked systems.

General-purpose identity systems (or foundational identity systems) typically provide documentary and/or digital credentials that are widely recognised and accepted by government agencies and private sector service providers as proof of official identity for a variety of purposes (for example, national ID systems and civil registration).

Identity evidence – see attribute evidence.

Identity lifecycle management refers to the actions that should be taken in response to events that can occur over the identity lifecycle and affect the use, security and trustworthiness of authenticators, for example, loss, theft, unauthorised duplication, expiration, and revocation of authenticators and/or credentials.

Identity proofing answers the question, "Who are you?" and refers to the process by which an identity service provider (IDSP) collects, validates and verifies information about a person and resolves it to a unique individual within a given population or context. It involves three actions: (1) collection/resolution, (2) validation, and (3) verification.

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 digital ID solutions to users and relying parties. A single entity can undertake the functional roles of one or more IDSPs – see *Appendix A: Description of a Basic Digital Identity System and its Participants* for a summary of all the relevant entities including – identity provider, credential service provider (CSP), registration authority (RA) (or identity manager), verifier, user/Individual,

applicant, subscriber, claimant, relying party and Trust Framework Provider / Trust Authority.

Impersonation involves a person pretending to have the identity of another genuine person, this might be through simply using a stolen document of someone that looks similar, but may also be combined with counterfeit or forged evidence (e.g. photo substitution on a passport with the impostor's image).

Limited-purpose identity systems (or functional identity systems) provide identification, authentication, and authorisation for specific services or sectors, such as tax administration; access to specific government benefits and services; voting; authorisation to operate a motor vehicle; and (in some jurisdictions) access to financial services, etc. Examples of functional ID evidence include (but are not limited to): taxpayer identification numbers, driver's licenses, passports, voter registration cards, social security numbers and refugee identity documents.

Man-in-the-middle attack: Attempts to achieve the same goal as phishing and can be a tool to commit phishing, but does so by intercepting communications between the victim and the service provider.

Multi-Factor Authentication (MFA) combines use of two or more authentication factors for enhanced security.

NIST Standard/Guidelines: US National Institute of Standards and Technology 800-63 Digital ID Guidelines.

Official identity, for the purposes of this guidance, is the specification of a unique natural person that (1) is based on characteristics (identifiers or attributes) of the person that establish a person's uniqueness in the population or particular context(s), and (2) is recognised by the state for regulatory and other official purposes.

Phishing (also referred to as man-in-the-middle or credential interception) is a fraudulent attempt to gather credentials from unknowing victims using deceptive emails and websites. For example, a criminal attempts to trick its victim into supplying names, passwords, government ID numbers or credentials to a seemingly trustworthy source.

PIN code capture and replay involves capturing a PIN code entered on the keyboard of a PC in with a key logger and, without the user noticing, using the captured PIN when the smartcard is present in the reader to access services).

Portability / Interoperability: Portable identity means that an individual's digital identity credentials can be used to prove official identity for new customer relationships at unrelated private sector or government entities, without their having to obtain and verify personally identifiable information (PII) and conduct customer identification/verification each time. Portability requires developing interoperable digital identification products, systems, and processes. Portability/interoperability can be supported by different digital ID architecture and protocols.

Proof of official identity generally depends on some form of government-provided or issued registration, documentation or certification (e.g., a birth certificate, identity card or digital ID credential) that sets out evidence of core identifiers or attributes (e.g., name, sex, date and place of birth) for establishing and verifying official identity.

Regulated entities, for the purposes of this guidance, 'regulated entities' refers to financial institutions, virtual asset service providers (VASPs) and, Designated Non-Financial Businesses and Professions (DNFBPs), to the extent DNFBPs are required to undertake CDD in the circumstances specified in R.22. In June 2019, the FATF revised

Recommendation 15 (New Technologies) and INR 15 to, among other things, impose Recommendation 10 CDD obligations on VASPs.

Validation is part of identity proofing and involves determining that the evidence is genuine (not counterfeit or misappropriated) and the information the evidence contains is accurate by checking the identity information/evidence against an acceptable (authoritative/reliable) source to establish that the information matches reliable, independent source data/records.

Verification is part of identity proofing and involves confirming that the validated identity relates to the individual (applicant) being identity-proofed.

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.

Relying Party (RP): A 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. Typical RPs include financial institutions and government departments and agencies.

Subscriber: 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.

Synthetic identities are developed by criminals by combining real (usually stolen) and fake information to create a new (synthetic) identity, which can be used to open fraudulent accounts and make fraudulent purchases. Unlike impersonation, the criminal is pretending to be someone who does not exist in the real world rather than impersonating an existing identity.

Two-factor authentication (2FA) uses a combination of two independent authenticators from two different factor categories to confirm the individual's identity.