FATF

DIGITAL IDENTITY

MARCH 2020

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

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

Citing reference:

FATF (2020), *Guidance on Digital Identity,* FATF, Paris,
www.fatf-gafi.org/publications/documents/digital-identity-guidance.html

Table of Contents

ACRONYMS

AAL 1/2/3	Authentication Assurance Level (under NIST)
AL	Assurance Level
AML/CFT	Anti-money laundering/Countering the financing of terrorism
API	Application Programming Interface
ASP	Authentication Service Provider
CDD	Customer Due Diligence
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CSP	Credential Service Provider
DCS	Document Checking Service
DLT	Distributed Ledger Technology
DNFBP	Designated Non-Financial Businesses and Professions
ETSI	European Telecommunications Standards Institute
eIDAS	Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market
FAL 1/2/3	Federation Assurance Level (under NIST)
FIDO	Fast Identity Online
GDPR	General Data Protection Regulation
GPS	Global Position System
GSMA	Global System for Mobile Communications
ICT	Information and communications technology
IAL 1/2/3	Identity Assurance Level (under NIST)
ID	Identity
IDSP	Identity Service Provider
IEC	International Electrotechnical Commission
INR.	Interpretive Note to Recommendation
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunications Union
IVSP	Identity Verification Service Provider
LoA	Level of Assurance
MAC	Media Access Control
ML	Money laundering
MFA	Multi-factor authentication
NGO	Non-governmental organisations
NIST	National Institute of Standards and Technology
OIDF	OpenID Foundation
PII	Personally Identifiable Information
PIN	Personal Identification Number
R.	Recommendation
RBA	Risk-based approach

SAG	Standards Advisory Group
SCA	Strong Customer Authentication
TF	Terrorist financing
VASP	Virtual Asset Service Providers
W3C	World Wide Web Consortium
UNHCR	United Nations High Commissioner for Refugees

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 in determining 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 addressed in this Guidance, including the requirement to identify and verify customers' identities using 'reliable, independent' source documents, data or information (Recommendation 10(a)). 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, adequate governance, processes and procedures that provide appropriate levels of confidence that the system produces accurate results. The Guidance clarifies that non-face-to-face customer-identification and transactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place, may present a standard level of risk, and may even be lower-risk.

Reliable, independent digital ID systems with appropriate risk mitigation measures in place may be standard 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

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 Corporation (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.

(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 ID 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 and independence 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 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. As illustrated in the table below, key components of digital ID systems are relevant to specific identification and verification requirements under Recommendation 10(a). Accordingly, the digital ID assurance frameworks and technical standards which define these components and set requirements for each assurance level, provide a highly useful tool for assessing the reliability and independence of digital ID systems for AML/CFT purposes.

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.

CDD requirements (natural persons)	Key components of Digital ID systems
Identification / verification – R.10 (a)	Identity proofing and enrolment (with binding) – Who are you? Obtain attributes (name, DoB, ID # etc.) and evidence for those attributes; validate and verify ID evidence and resolve it to a unique identity-proofed person. Binding—issue credentials/authenticators linking the person in possession/control of the credentials to the identity proofed individual Authentication – Are you the identified/verified individual? Establish that the claimant has possession and control of the binding credentials. Authentication applies to 10(a) if the regulated entity conducts identification/verification by confirming the potential customer's possession of pre-existing digital ID credentials.

6. The Guidance explains that (1) authentication is relevant to R.10(a) where the regulated entity opens an account for a customer with pre-existing digital ID credentials – i.e., not an in-house digital ID solution, and (2) that, in a digital finance and digital ID context, effective authentication of customer identity for authorising account access can support AML/CFT efforts.

7. Section V is the crux of the Guidance and provides guidance for government authorities, 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:

Apply a **risk-based approach** to using digital ID for CDD: (1) understand the assurance levels of the digital ID system and (2) assess whether, given the assurance levels, the ID system is appropriately reliable, independent in light of the ML/TF risks

   a. Understanding of the assurance levels of the digital ID system's main components (including its technology, architecture and governance) to determine it is a reliable, independent source of information; and

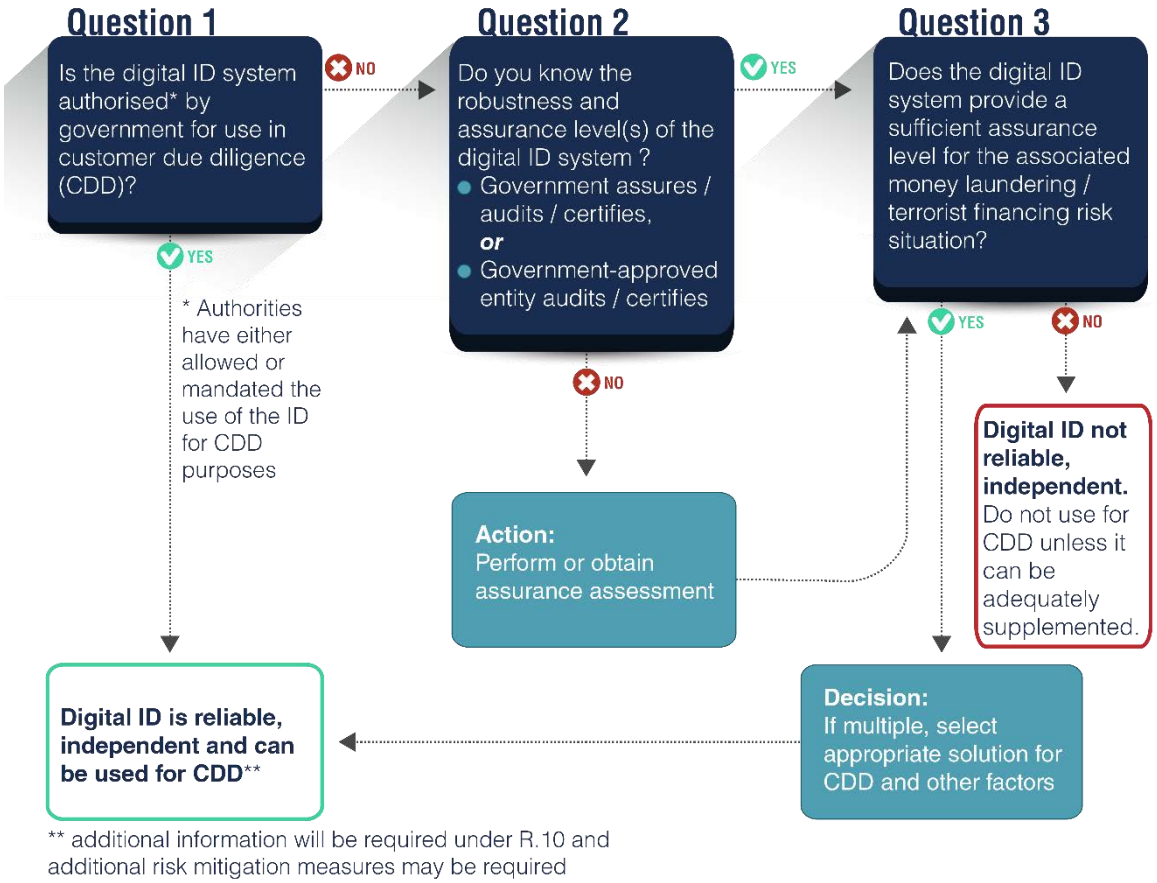
   b. Making a broader, risk-based determination of whether, given its assurance levels, the particular digital ID system provides an appropriate

level of reliability and independence in light of the potential ML, TF, fraud, and other illicit financing risks at stake.

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 decisions about whether the use of digital ID to meet some elements of CDD is appropriate under FATF 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 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-making flow chart for regulated entities, below.

9. This Guidance is non-binding. It clarifies the current FATF Standards, which are technology-neutral.

Figure 1. Decision process for regulated entities



10. 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/or 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.

Digital ID systems can support financial inclusion

11. 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 government authorities

12. 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 ID 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).

13. Assess whether existing regulations and guidance on CDD across all relevant authorities 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 appropriate assurance levels are used for remote customer identification/verification and authentication.

14. Adopt principles, performance, and/or outcomes-based criteria when establishing the required attributes, 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.

15. Adopt policies, regulations, and supervision and examination procedures that enable regulated entities to develop an effective, integrated "risk-based" approach that leverages data flows, technology architecture and processes across all relevant digital ID, AML-CFT, anti-fraud and general risk management activities to strengthen all risk-related functions.

16. 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 ID ecosystem and to ensure the compatibility of AML/CFT requirements on digital ID systems with Data Protection and Privacy rules.

17. 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.

18. 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. Where authorities do not audit or provide certification for IDSPs themselves, they are encouraged to support assurance testing and certification by appropriate expert bodies[7] so that trustworthy certification is available in the jurisdiction. Authorities are encouraged to support efforts to harmonise digital ID assurance frameworks and standards to develop a common understanding of what constitutes a "reliable, independent" digital ID system.

19. Apply appropriate digital ID assurance frameworks and technical standards when developing and implementing government-provided digital ID.

[7] These expert certification bodies can provide services for a particular jurisdiction or region, or offer their services internationally.

Authorities should be transparent about how the jurisdiction's digital ID system works and its assurance levels.

20. 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.

21. 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

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

23. 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.

24. Consider whether digital ID systems with lower assurance levels may be sufficient 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.

25. If, as a matter of internal policy or practice, non-face-to-face business relationships or transactions are always classified as high-risk, consider reviewing and revising those policies to take into account that customer identification/verification measures that rely on reliable, independent digital ID systems, with appropriate risk-mitigation measures in place, may be standard risk, and may even be lower-risk.

26. 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.

27. 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[8]

28. 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.

29. Seek assurance testing and certification by the government or an approved expert body, or where these are not available, another internationally reputable expert body. Where available, participate in public sector regulatory 'sandboxes' (or other relevant mechanisms) to assess the digital ID system's assurance levels.

30. 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.

8 While the FATF Standards are only applicable to regulated entities (i.e. financial institutions, virtual asset service providers and designated non-financial businesses and professions), this Guidance is relevant background for digital ID service providers who provide service to regulated entities (for FATF purposes). Ultimately, the regulated entity is responsible for the meeting the FATF requirements.

SECTION I: INTRODUCTION

31. The Financial Action Task Force (FATF) is committed to ensuring that the global anti-money laundering/counter financing of terrorism (AML/CFT) 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 AML/CFT standards and financial inclusion goals.[9]

32. 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;[10] mobile phone numbers, SIM cards, global position system (GPS) geolocation); high-definition scanners (for scanning ID cards, drivers licenses and other documents); 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).

The rapid pace of innovation has reached an inflection point... Digital ID systems are, or could soon be, available at scale.

Potential benefits

33. 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 financial services, health, and e-government in the global economy of the digital age. These digital IDs are referred to as those with higher assurance levels.

34. In relation to the FATF Standards, appropriately reliable, independent digital ID systems could:

- facilitate 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.

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

10 MAC addresses identify devices, IP addresses identify connections.

35. 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.

36. Reliable, independent[11] 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

37. Digital ID systems also pose ML/TF risks that must be understood and mitigated. Regulated entities that fail to do so, will also fail to meet the requirements set out in Recommendation 10(a) and requirements under the FATF standards that require regulated entities to identify, assess and mitigate the money laundering or terrorist financing risks that may arise in relation to the use of new or developing technologies for both new and pre-existing products.[12]

38. These risks are covered in detail in Section IV. Large scale digital ID systems that do not meet appropriate assurance levels pose cybersecurity risks, including allowing cyberattacks aimed at disabling broad swaths of the financial sector, or at disabling the digital ID systems themselves. They also pose major privacy, fraud or other related financial crimes risks, because cybersecurity flaws can result in massive identity theft, compromising individuals' personally identifiable information (PII).[13] 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 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.

39. 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

40. 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).

---

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

12 R.15 (for financial institutions and VASPs) and R.22 (for DNFBPs).

13 **PII** includes any information that by itself or in combination with other information can identify a specific individual.

41. 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

42. 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) under Recommendation 10(a). It also looks at the potential for digital ID to support ongoing due diligence (including transaction monitoring) under Recommendation 10(d). It 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.

43. 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 and design of digital ID 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 or generate 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 regulatory or law enforcement purposes, thus satisfying R.11's 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 (IDSP) and/or other entities. In addition, a private sector digital ID service provider may obtain/confirm some or all of the underlying identity data directly from the digital source (e.g., a government database or private sector utility records). In that case, it is possible that digital records specifying the types of identity evidence used for specific evidence, including data source, date/time and means of accessing it, might align with Recommendation 11. These matters are appropriately addressed by authorities in their AML/CFT and digital ID regulatory frameworks and by regulated entities through standard agency and financial services provider contractual relationships. Accordingly, recordkeeping and such requirements are not further addressed in the Guidance.

44. This guidance focuses on the identification of customers that are individuals (natural persons). The Guidance does not examine the use of digital ID systems to help identify and verify the identity of a legal person's representative(s) as part of the identification/verification of customers that are legal persons, or to help conduct other elements of the CDD process – in particular, to identify and verify the identity of beneficial owner(s) under Recommendation 10(b) or to understand and obtain information on the purpose and intended nature of the business relationship under

Recommendation 10(c)—although reliable, independent digital ID systems are important for all of these CDD functions.

45. This Guidance covers digital ID systems provided by government, or on behalf of government,[14] 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 official identity for all or most purposes in the jurisdiction), although it also discusses limited-purpose ID (i.e., ID valid for a specific purpose), such as social security registration or other 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.

46. 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 E for further information.

47. The Guidance includes five appendixes and a glossary with relevant further reading:

- *Appendix A: Description of a Basic Digital Identity System and its Participants:* provides a more detailed overview of the concepts set out in Section V regarding the components of a digital ID system.
- *Appendix B: Case studies* – provides examples of digital IDs in use in various jurisdictions, including for CDD and access to financial services.
- *Appendix C: Principles on Identification for Sustainable Development* – highlights the governance/accountability, privacy, and other operational issues that are being addressed by various jurisdictions and organisations. [15]
- *Appendix D: Digital ID assurance framework and technical standard setting bodies* – lists a number of standard setting bodies (not including national or regional bodies) that have developed relevant digital ID assurance frameworks or standards.
- *Appendix E: Overview of US and EU digital ID assurance frameworks and technical standards* – provides, as an example, the detail on national and regional digital ID assurance frameworks in the US and EU.
- *Glossary* – explanations of digital ID terminology used in this Guidance.

[14] A digital ID system is provided "on behalf of the government" when the government contracts with or otherwise arranges with or authorises an international organisation, such as the UNHCR, or another entity to provide and operate the digital identity system. The non-government actor stands in place of the government with respect to these identity functions.

[15] These Principles were developed through a collaborative process 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

48. Identity is a complex concept with many meanings. For FATF's purposes, in relation to Recommendation 10(a)—i.e., "identifying the customer and verifying that customer's identity"—"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.

49. For purposes of this Guidance,[16] **official identity** is the specification of a unique natural person that:

    a. is based on characteristics (attributes or identifiers) 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

50. **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 attributes (e.g., name, date and place of birth) for establishing and verifying official identity.

51. The criteria for proving "official identity" can vary by jurisdiction. In the exercise of their sovereignty, governments establish the required attributes, evidence and processes for proving official identity. These factors can change over time. As technology and cultural concepts of identity evolve, governments may authorise various attributes. In establishing the criteria for proving official identity, governments can use either a fixed, prescriptive, rules-based approach or one that is principles, performance, and/or outcomes-based. The latter approach is more flexible. Given, the rapid evolution of digital ID technology and standards, it enables jurisdictions to future-proof the requirements for proving official identity and support responsible innovation.

Using an outcomes-based approach for establishing identity attributes, enables jurisdictions to future-proof the requirements for proving official identity

52. In the EU, reliance on common assurance frameworks enables EU member states to accommodate different national requirements, such as the acceptance of different types of nationally available official ID documentation and procedures, provided that the outcome is compliant with the requirements in the eIDAS framework. Depending on the context in which an aspect of identity evidence needs to be verified, authoritative sources can take many forms, such as registries, documents and relevant bodies among other things. Authoritative sources may be different in the various EU member states even in a similar context, but the eIDAS framework allows for harmonisation and cross-recognition. The International Organisation for Standardization (ISO)[17] is currently working on developing global standards for the identification of natural persons for financial services, including in digital context.

53. 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

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

17 ISO Standards Advisory Group (SAG) of Technical Committee 68, Working Group 7

private sector service providers as proof of official identity for a variety of purposes. Not all jurisdictions have general-purpose ID systems.

54. 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 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.

55. Typically, proof of official identity has been provided by—or on behalf of—governments. 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).

56. In the case of refugees, proof of official identity may also be provided by an internationally recognised organisation with such mandate.[18] See Box 8.

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

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

58. 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.

59. Not all elements of a digital ID system are necessarily digital. Some elements of identity proofing and enrolment component 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.

60. Digital ID systems may use digital technology in various ways, for example but not limited to:

- Electronic databases, including distributed ledgers, to obtain, confirm, store and/or manage identity evidence

[18] 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.

- Digital credentials to authenticate identity for accessing mobile, online, and offline applications
- Biometrics to help identify and/or authenticate individuals, and
- Digital application program interfaces (APIs), platforms and protocols that facilitate online identification/verification and authentication of identity.

What are the key components of a digital ID system?

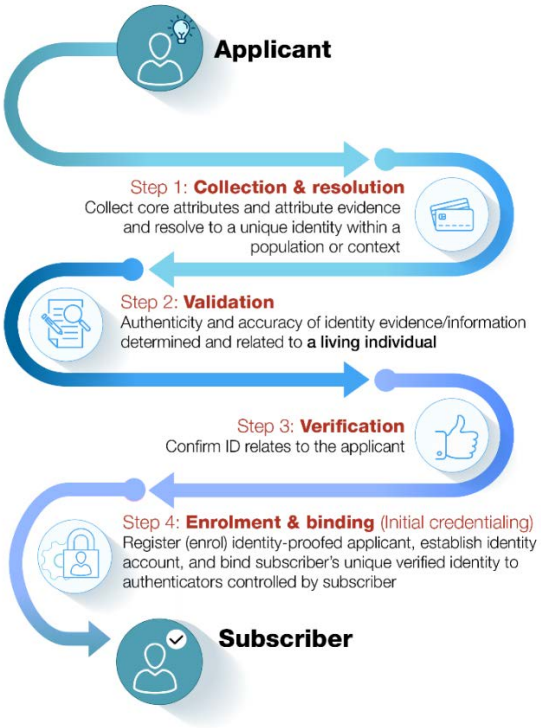
61. As reflected in the NIST digital ID Guidelines, **digital ID systems** involve two basic components, and an optional third component, as set out below. Different entities can be responsible for the operations of subcomponents including a mix of government entities and private sector entities. The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

62. 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.

63. 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.

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

- Collection: Present and collect identity attributes and evidence, either in person and/or online (e.g., by filling out an online form, sending a selfie photo, uploading photos of documents such as passport or driver's license, etc.).
- Validation: Digital or physical inspection to ensure the document is authentic and its data or information is accurate (for example, checking physical security features, expiration dates, and verifying attributes via other services).
- De-duplication: Establish that the identity attributes and evidence relate to a unique person in the ID system (e.g., via duplicate record searches, biometric recognition and/or deduplication algorithms).
- Verification: Link the individual to the identity evidence provided (e.g., using biometric solutions like facial recognition and liveness detection).
- Enrolment in identity account and binding: Create the identity account and issue and link one or more authenticators with the identity account (e.g., passwords, one time code (OTC) generator on a smartphone, PKI[19] smart cards, FIDO certificates, etc.). This process enables authentication (see below).

19 Public Key Infrastructure

Component Two: Authentication and identity lifecycle management (essential)

65. Authentication answers the question: ***Are you the person who has been identified and verified?*** It establishes, based on possession and control of authenticators, that the person asserting an identity (the on-boarded customer or claimant) is the same person who was identity proofed and enrolled

66. There are three types of factors that can be used to authenticate someone (see Figure 3 below): (1) ownership factors (something you possess, e.g., cryptographic keys) (2) knowledge factors (something you know, e.g., a password); (3) inherent factors, (something you are, e.g., biometrics).[20]

67. Authentication can rely on various types of authentication factors and protocols or processes. These authentication factors have different levels of security – see the discussion authentication risks in Section V. A single authentication factor is generally not considered sufficiently trustworthy. An authentication process is usually considered more robust and reliable when it employs multiple types of authentication factors.[21]

[20] When the Guidance describes components of authentication, those are not the same as 'strong customer authentication (SCA)' under the EU's legal framework. What constitutes or does not constitute a valid SCA factor for the purpose of Directive (EU) 2015/2366 (PSDII) has to be assessed in accordance with the PSDII and the Regulatory Technical Standards on strong customer authentication and secure communication under PSDII (RTS on SCA & CSC), rather than FATF guidance.

[21] As digital ID systems evolve this understanding is becoming more nuanced. Where authentication is active and continuous, authentication strength is sometimes assessed, not in terms of the number of different authentication factors and types, but in terms of overall robustness resulting from the use of multiple sources of dynamic, digital customer data, including expected log-in channels, geolocation, frequency of usage, type of usage, IP addresses and biomechanical metric behavioural patterns

Figure 3. Common authentication factors

Source: World Bank ID4D

Box 1. Role of Authentication in Customer Due Diligence and Other AML/CFT measures

- Once a person has been identity proofed and enrolled in a digital ID system, they can then use the credentials and authenticators bound to their identity to "assert" this identity to a third, "relying party" (e.g., a regulated entity). While the strength of the identity proofing and enrolment process provides the relying party with a level of confidence of the veracity of the identity information (e.g., that attributes like name and age are correct and relate to a real person), the authentication process assures the relying party that the person presenting the credential is really the person to whom it belongs, and not a thief or imposter. The ability of digital ID systems to authenticate a person is therefore an important component of

their functionality, and can be used by regulated entities as part of the CDD identification/verification process during account opening.

- Note that "authentication" of existing customers is also an important security measure for ongoing due diligence and authorising account access. In some cases, regulated entities may use the same digital ID credentials and authentication services used during account opening for authorising account access, however this need not be the case. For example, many regulated entities issue their own credentials/authenticators (e.g., PINs and tokens, for logging in to online accounts) and/or link these to on-device authenticators integrated into mobile phones or browsers (e.g., using FIDO standards).

68. ***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)

69. Digital ID systems can include a component that enables proof of identity to be portable. Portable identity means that an individual's digital ID 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.

70. 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 16

Digital ID Assurance Frameworks and Technical Standards

71. 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. European Union, Canada and Australia)
- international standards organisations or industry-specific organisations such as the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Fast Identity Online (FIDO) Alliance, the OpenID Foundation (OIDF), the International Telecommunications Union (ITU) and GSMA.

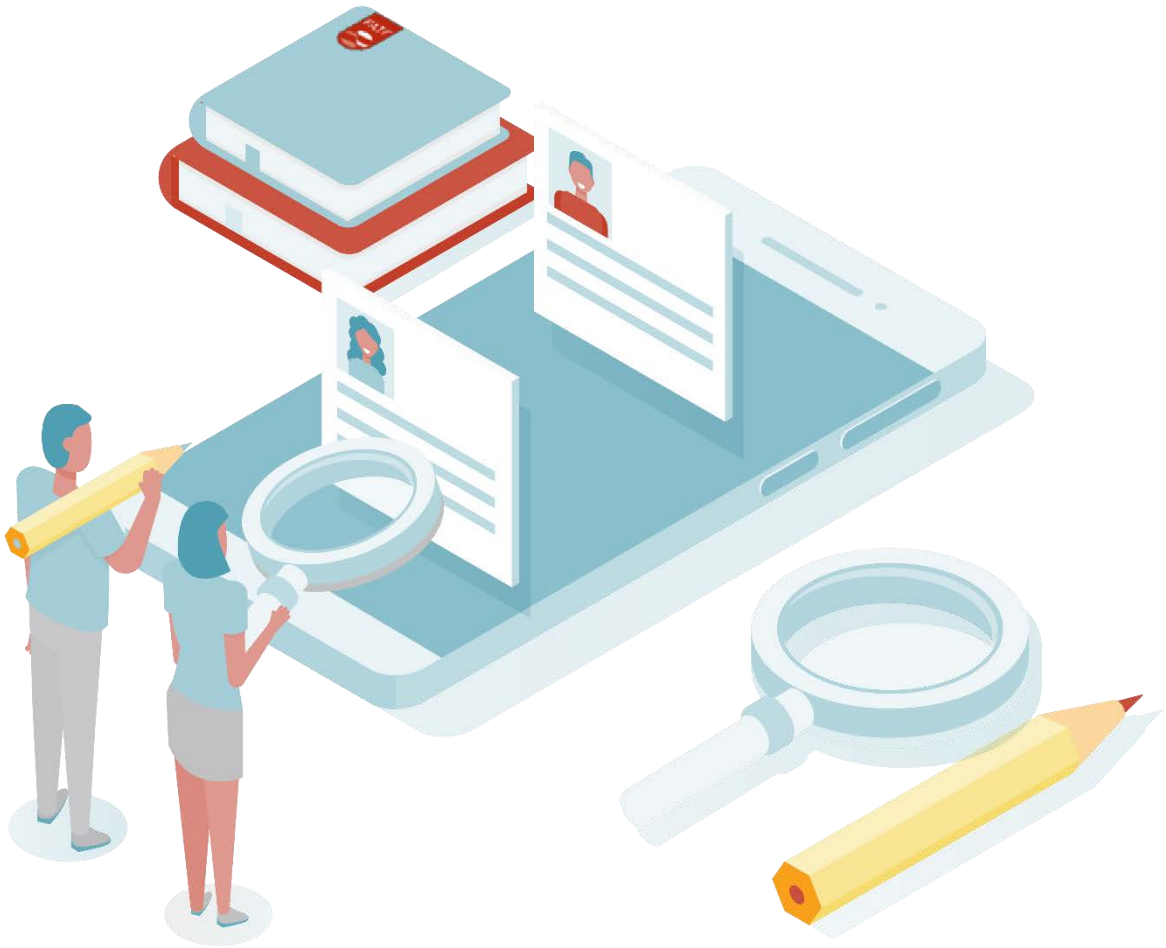
72. See ***Appendix D: Digital ID assurance framework and technical standard setting bodies*** for a high-level summary of these organisations.

73. The digital ID assurance frameworks and standards developed at a jurisdictional level 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 ISO, together with the International 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 31000:2018) to identity-related risks. In addition, the ISO is working to update, align and synchronise all other ISO standards to create a comprehensive international digital ID assurance framework.

74. In light of the evolving standards, this Guidance makes many references to the NIST digital ID Guidelines and the eIDAS framework. 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.

75. 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



76. 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.

77. 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 under R. 10(d).

Customer identification/verification requirements (on-boarding)

78. 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

79. 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.

80. 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

81. 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.

82. The following discussion explores the development of the FATF's current "reliable, independent" requirement, to flesh out its underlying meaning and objectives.

83. 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".[22] This language was carried forward unchanged

[22] 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

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."

84. 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, adequate governance, processes and procedures that provide appropriate level of confidence that the system produces 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

85. 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.[23]

Apply a risk-based approach to CDD measures to support financial inclusion objectives

86. 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).

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).*

23 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/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf

Non face-to-face business relationships and transactions

87. The FATF uses the terms, face-to-face and **non-face-to-face** in categorising business relationships (including onboarding) and transactions. For the FATF's purposes, face-to-face interactions are considered to occur in-person—meaning the parties to the interaction/transaction are in the same physical location and conduct their activities by physical interaction. **Non-face-to-face interactions** are considered to occur remotely—meaning the parties are not in the same physical location and conduct activities by digital or other non-physically-present means, such as mail or telephone.[24]

88. 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.

89. 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 transactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place, may present a standard level of risk, and may even be lower-risk where higher assurance levels are implemented 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

90. 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."

91. As explained in Section II, above, and in further detail in Appendix A, **authentication** using a digital ID system and establishes confidence that an individual is the person who was identity proofed and issued with the relevant credentials. Regulated entities that use digital ID systems to authenticate the identity of their existing customers as part of account authorisation are encouraged to leverage the data generated by

[24] The definition of face-to-face and non-face-to-face interactions may differ according to national regulations. For example, some jurisdictions consider video identification to be face-to-face interaction.

authentication and related information,[25] to support ongoing due diligence and transaction monitoring. This information is traditionally obtained for the purpose of protection the regulated entity from fraud. However, with the accelerating transition to digital financial systems and accompanying reliance on the use of digital ID authentication to authorise account access, it can also be relevant for AML/CFT purposes.

92. For regulated entities, ongoing 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. Ongoing digital authentication of the customer's identity links that individual with their financial activity. It can therefore facilitate strengthen the ability to conduct meaningful ongoing due diligence and transaction monitoring pursuant to R.10(d).

Third Party Reliance Requirements

93. This Section explains how an entity regulated for AML/CFT purposes can (1) rely on customer identification/verification undertaken by another regulated entity in the context of digital ID (under the scope out Recommendation 17), and (2) act as an agent for, or as outsourced entity, for another regulated entity (outside of the scope of Recommendation 17).

94. Under Recommendation 17, countries may permit regulated entities [26] to rely on third parties to perform customer identification/verification at on-boarding,[27] provided that the following conditions are met:

- The third party must also 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;

25 Authentication is one part of authorising account access. The regulated entity may also collect other complementary data (such as, geolocation, IP addresses, etc.) for the authorisation decisions.

26 Recommendation 22 provides that the reliance requirements in R.17 apply to DNFBPs.

27 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.

- 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.

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 assurance (confidence) levels, 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 ID 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. This section is intended to raise stakeholders' awareness of potential risks specific to digital ID 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 appropriate assurance levels (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. This section also highlights a number of broader challenges presented by digital ID systems. Responding to these challenges usually will not fall under the direct purview

of AML/CFT authorities, but these challenges may have an indirect impact on AML/CFT efforts.

103. While this section provides a general overview of some of the risks and challenges, 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 provision of financial services, to the benefit of customers, regulated entities, and the integrity of the financial sector. As discussed below, 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. 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 that the identity document is genuine. The front-line personnel may lack the tools, technology, training, skill sets and experience needed to reliably identify counterfeit, altered or stolen documents.

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 the identity proofing component of a digital ID system is conducted in-person[28] and relies on human judgement, that process will often be conducted by specialists with access to advanced technical tools for detecting fraudulent and stolen ID documents. For example, remote identity proofing—at least at higher assurance levels—typically employs increasingly sophisticated and effective digital ID technologies to determine that documentary identity evidence is genuine, not counterfeit, as well as

[28] 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).

additional data and information that help reliably identity proof the individual.[29]

- Second, the authentication component of a digital ID system 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.

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. Customer acceptance and convenience are important drivers in completing applications and transactions and customer retention. Ease of use for customers, combined with potential efficiency gains for regulated entities, can help lower on-boarding costs. One report suggests that regulated entities using digital ID systems could see up to 90 percent cost reduction in customer onboarding with the time taken for identification/verification and other CDD elements reduced from days or weeks to minutes.[30] These cost savings could enable regulated entities to allocate compliance resources to other AML/CFT compliance functions, and also facilitate financial inclusion for otherwise excluded or under-served individuals by reducing on-boarding costs.

Transaction monitoring

108. As noted above, robust digital authentication of customer ID for authorising ongoing account access may facilitate the identification and reporting of suspicious transactions, because it helps the regulated entity establish 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 for authorising 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, and may assist law enforcement in investigating crimes. For example, complementary data where

[29] At present, security features that are readable only by ultraviolet (UV) light or are an element of the document's physical construction, such as security stitching, etching or punched holes that go through multiple pages, may be more difficult or impossible to validate remotely, but most identity documents have robust security features that can be effectively checked remotely.

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

captured by regulated entities through different means and channels (including internet and mobile phone), in accordance with local regulations including data protection and privacy rules, 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,[31] where digital ID systems and digital financial services have emerged as core drivers of financial inclusion.[32] The development of flexible, outcomes-based digital ID assurance frameworks and standards can allow financially excluded people who lack access to traditional official identity documents, such as passports and drivers licences, obtain digital IDs at a lower identity assurance level (which requires less stringent identity evidence and verification) and use them to obtain financial services in appropriate low risk situations. The assurance frameworks and standards also enable financially excluded individuals to obtain digital IDs by using alternative identity evidence (e.g., the use of 'trusted referees' to vouch for the applicant as a form of identity evidence). In addition, digital ID systems can reach excluded populations in remote areas to support secure non-face-to-face identity proofing/enrolment for customer identification/verification. These issues are discussed in greater detail in the section on 'Special considerations for financial inclusion' later in this Guidance.

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, which can be facilitated by the use of digital ID systems.

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 4 on India's Aadhaar and Box 5 on Peru's National Registry of Identification and Civil Status). This facilitates financial inclusion and with it, improves the reach and effectiveness of AML/CFT regimes.

---

31. 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.

32 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.

Risks and challenges presented by digital ID systems

112. This Guidance focuses on digital ID systems for conducting certain elements of CDD, not on the use of traditional documentary identity systems. The discussion of risk below is not intended to suggest either that the risks of digital ID systems outweigh their benefits, or that they are more risky as a general matter than traditional documentary identity systems.

113. Like any ID system, reliability of digital ID systems depends on the strength of documents, processes, technologies, and security measures used for identity proofing, credentialing, and authentication, as well as ongoing identity management. In both documentary and digital ID systems, for example, reliability can be undermined by identity theft and source documents that can be easily forged or tampered with. 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. While digital ID systems provide security features—e.g., secure authentication—that mitigates some issues with paper-based systems, they also increase some risks, such as data loss, data corruption or misuse of data due to unauthorised access.

114. Digital ID systems present a variety of technical challenges and risks, 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 a 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 or spoof) authenticators linked to a legitimate identity.

115. The digital ID assurance frameworks and standards provide a key tool for identifying and assessing some of these risks, and mitigating them with digital ID technologies and processes that offer appropriate, assurance for each of the components of digital ID.[33] The following risk discussion applies to digital ID systems that are *not* sufficiently reliable, in terms of the risk management frameworks set out in digital ID assurance frameworks and standards. It also touches on broader connectivity, cybersecurity and privacy challenges in the digital space that may impact the integrity or availability of digital ID systems to conduct CDD.

116. The discussion below covers both identity proofing/enrolment risks and authentication risks. Risks at the identity proofing stage may result in digital ID's that are "fake" (i.e., obtained under false premises through an intentionally malicious act) and can be used to facilitate illicit activities. These risks are mitigated by having an appropriate identity assurance level. Identity proofing risks are distinguished from authentication risks, where a legitimately issued digital ID has been compromised and

[33] 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.

its credentials or authenticators are under the control of an unauthorised person. These risks are mitigated by having an appropriate authentication assurance level.

Identity proofing and enrolment risks

117. There are two general sources of threats to the enrolment process: (1) cyberattacks and security breaches leading to the compromise of personally identifiable information (PII) and presentation of false evidence either by stealing a real person's identity (impersonation) or creating a synthetic ID, and (2) compromise of, or misconduct by, the IDSP or compromise of the broader digital ID infrastructure. This section focuses on the first category as IDSP compromise/misconduct, cybersecurity and broader infrastructure threats are more directly 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) that are outside the scope of this Guidance.

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

118. In certain respects, the risks arising from the presentation of false evidence (which is either stolen or counterfeit) in digital ID systems, can be actualised at much greater scale.[34] **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.[35]

119. 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.

---

34 Searches on the internet for "fake IDs" reveal hundreds of websites promising counterfeit drivers' license, passports, birth certificates, immigration papers and other official documents that can be indistinguishable from the legitimate versions.

35 FATF project team meeting with Digital ID experts, September 2019.

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

120. 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.

121. 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 social engineering attacks such as deceptive emails, phone calls, text messages or 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).

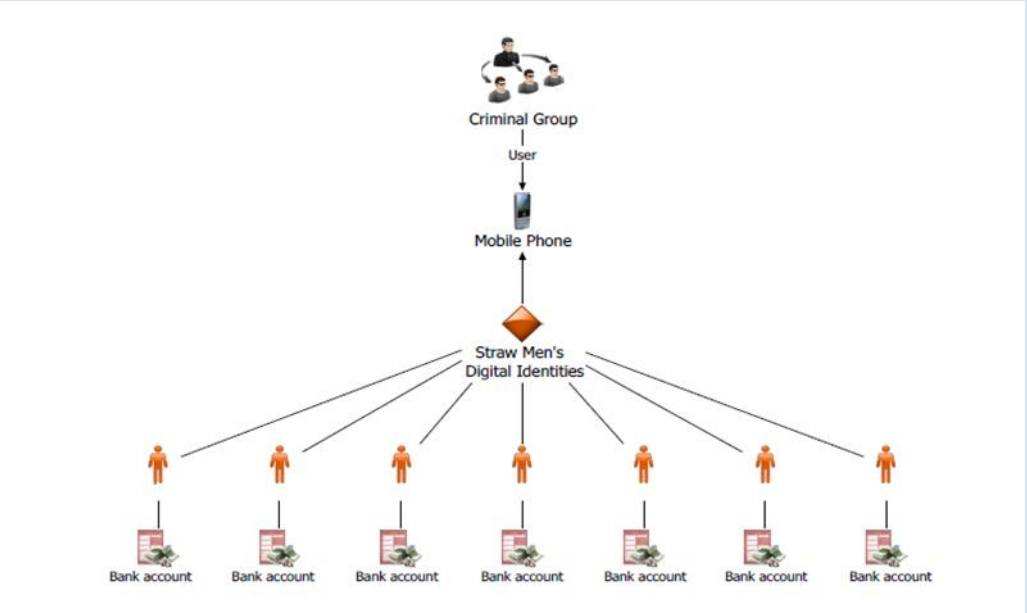
122. Most authentication vulnerabilities are exploited without the identity owner's knowledge, but abuse can also involve the witting participation of subscribers or IDSPs. For example, shared-secret authenticators, such as passwords, may be stolen and exploited by bad actors, but they can also be deliberately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

123. 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 2. 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

124. Some of the primary known risks associated with specific types of authenticators/processes that are particularly relevant to AML/CFT efforts are described below.

125. **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.[36] 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 phishing and other attacks. Phishing-resistant authenticators where at least one factor relies on public key encryption[37] (e.g., authenticators built off PKI certificates or the FIDO standards) can help combat these vulnerabilities.

126. **Biometric Authenticators:** Bio-physical 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 smart phones have built-in iris scanners; and facial recognition capabilities are built into many personal computer systems and advanced smart phones.

127. Biometric characteristics could be stolen in bulk from central databases.[38] They could also be obtained by taking high resolution images (photos); lifted from objects the individual touches (e.g., latent fingerprints); or captured with high resolution images (e.g., iris patterns), and thereafter spoofed. Currently, however, these types of attacks are difficult and/or highly resource intensive and are therefore not scalable. For instance, biometric authenticators that require on-device matching cannot be fraudulently used at scale because they require physical access to the device of the customer.

128. Biometrics have a variety of other weaknesses that give rise to reliability concerns when used for authentication purposes, and have lead some technical standards to restrict their use for authentication (vs. identity-proofing).[39] 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. In contrast to knowledge or possession based authenticators, stolen biometric authenticators are difficult to revoke or replace.[40]

129. **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 and transaction monitoring requirements in protecting the financial system from abuse.

---

36 Verizon 2018 Data Breach Investigation Report (DBIR), available at https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf.

37 In **public-key encryption**, a pair of keys are generated for an entity—a person, system, or device—and that entity holds the private key securely, while freely distributing the public key to other entities. Anyone with the public key can then use it to encrypt a message to send to the private-key holder, knowing that only they will be able to open it.

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

39 See NIST 800-63-3, NIST 800-63 (b) and Appendix E.

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

130. **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

131. 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. Regulated entities may wish to consider obtaining access to (or third party analysis of) their account access authentication data to enable the detection of systematic misuse of digital IDs, including compromised, stolen or sold digital IDs. This information could be used in identifying and determining whether to report suspicious activities. One important benefit of the federated identity model is that identity fraud detection can be shared across a network of identity providers and relying parties.

Broader issues presented by digital ID systems which may impact AML/CFT efforts

Connectivity issues

132. Lack of reliable infrastructure can undermine the digital ID systems in a jurisdiction or in particular geographic areas for meaningful periods of time. However, digital ID systems can be designed to support both offline and online transactions, allowing them to function with or without access to the Internet or a mobile network. Regulated entities should take into account resilience when deciding whether to use a digital ID system for CDD.

Domestic frameworks for official identity

133. 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. Identity theft from online databases generate similar risks for both digital ID systems and documentary approaches.

134. A digital ID, which has been developed for a limited or specific purpose unrelated to financial-sector CDD may not be able to cope with the demand for applications in other situations or face limitations and may create high costs for regulated entities or prove unfeasible to use for CDD purposes (see for example Box 7 in Appendix II) .

Data Protection and Privacy Challenges

135. Digital ID involves the collection and processing of personal data (PII), including biometrics. 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 and/or an international standards organisation. In addition, innovative, technology based solutions (for example, decentralised digital identity) are being developed to give the individual more control over how PII is shared with others and for what purpose to further address privacy and data protection issues.

136. Government has primary responsibility to establish the DPP regime in the jurisdiction. These requirements, which protect the confidentiality, accuracy and integrity of the data, would typically apply to Digital ID Service Providers and require them to, for example, conduct a data-protection impact assessment (DPIA) to identify potential challenges and appropriate risk control measures. DPP safeguards are important for reducing the risk of identity theft and cybersecurity risks that could undermine the reliability of the digital ID system. Therefore, in accordance with FATF Recommendation 2, AML/CFT and DPP authorities should seek to co-operate and co-ordinate to ensure compatibility of requirements and rules.

Financial exclusion considerations

137. Where 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, which is an AML/CFT risk. The mandatory use of a specific digital ID that is not universally available for CDD presents similar challenges as the prescriptive use of a documentary ID that is not accessible to the entire population. Lack of access to digital technology or low levels of technology literacy, may compound 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 if they use biometric authentication without providing alternative mechanisms for authentication, because certain biometric modalities have greater failure rates for some vulnerable groups. Manual labourers' typically have worn fingerprints, which often cannot be read by biometric readers; the elderly may experience frequent match failure, due to altered facial characteristics, hair loss, or other signs of aging, illness, or other factors; and certain ethnic groups and individuals with certain physical characteristics related to darker pigmentation, eye shape, or facial hair experience disproportionate facial recognition failures.

SECTION V: ASSESSING WHETHER DIGITAL ID SYSTEMS ARE SUFFICIENTLY RELIABLE AND INDEPENDENT UNDER 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:

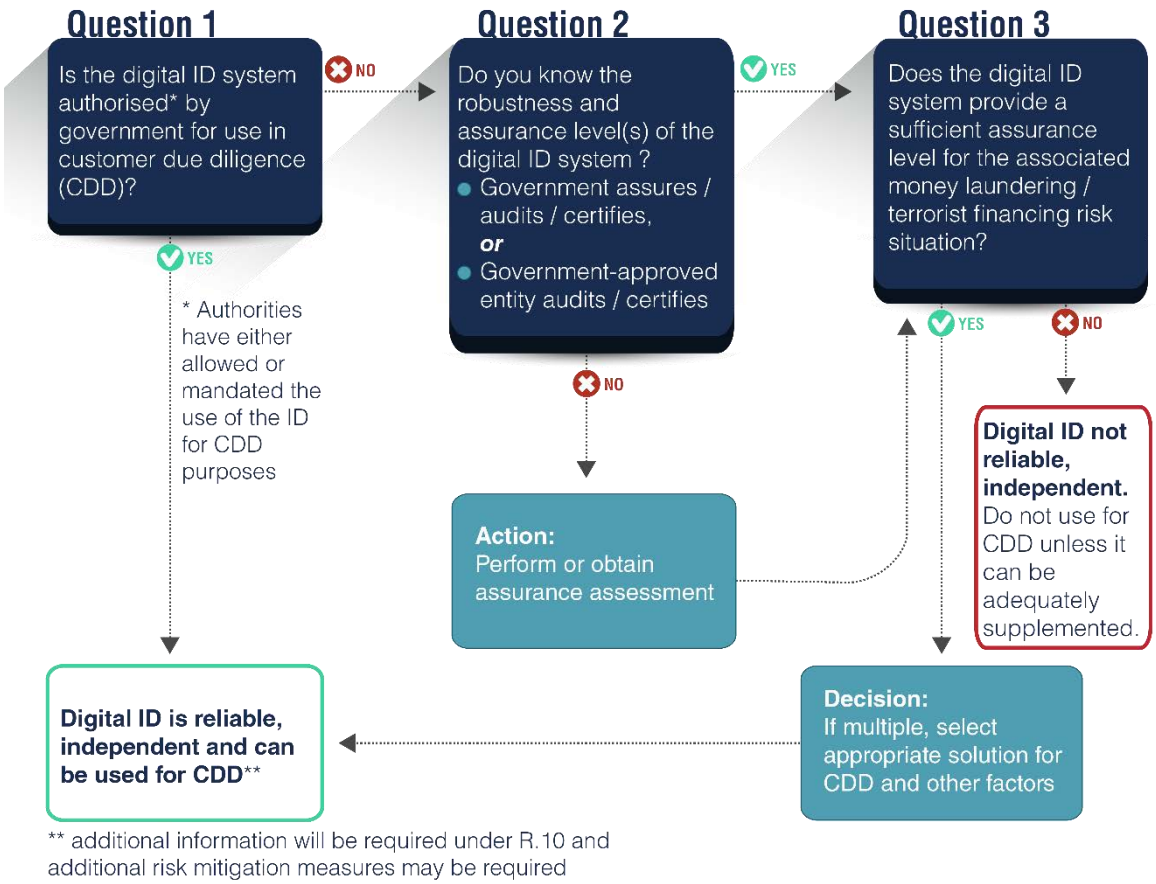
    a. Understand the assurance levels of the digital ID system provides based on its technology, architecture and governance to determine its reliability/independence; and

b. Given the digital ID's assurance levels, make a risk-based determination of whether the digital ID system is appropriately reliable, independent 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 and the remaining parts of the decision process do not apply. 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).

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 will 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. [41]

148. If the government assures, audits or certifies digital ID systems (either directly, or by designating organisations to act on its behalf[42]), 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 assurance level, or may have different, increasingly robust assurance levels (either unitary or for each of its components), but the authoritative information should be publicly 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 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.

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 recognised as reliable by appropriate experts in the jurisdiction, region, or internationally.

---

41 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.

42 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.

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, under the FATF's risk-based approach to CDD. 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) assurance level 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 discussion 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 and assurance levels, 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 information provided by the assurance frameworks and standards when assessing whether a digital ID system satisfies the "reliable, independent" criteria of Recommendation 10 (a). 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 assurance level 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.[43] For those assurance frameworks and standards that adopt a single assurance level for the whole digital ID system (like the eIDAS Regulation), the process-by-process approach can be implemented by examining how each component of the process meets the requirements for each assurance level .

157. Digital ID technology and architecture, and digital ID assurance frameworks and standards, are dynamic and evolving.[44] The standards themselves are flexible and outcome-based in order to facilitate innovation. They permit different technologies and architectures to satisfy the requirements for the distinct assurance levels 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

---

43 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).

44 It should be acknowledged that the digital ID standards have not always kept up with evolving technology. For example, at the time this Guidance was finalised, the digital ID assurance frameworks and standards did not yet address continuous authentication. Nor did they address the notion of progressive identity as it relates to ongoing, dynamic identity proofing.

assurance, entities can examine how each component of the process meets the individual requirements for each assurance level.

161. To illustrate both the type of factors that appropriate authorities, financial institutions, and other stakeholders might leverage in assessing if digital ID is reliable, independent, 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 US and EU assurance levels. It describes in broad terms, some of the technical requirements for identity proofing (the first stage of a digital ID system). It also briefly flags some of the key considerations associated with authentication assurance levels.

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 adoption of digital ID systems will enable individuals to prove official identity at higher assurance levels—particularly in countries that do not yet provide robust official identity to most of the population. However, as digital ID is often based on documentary identity evidence, in countries where there is low coverage by an official ID system, parts of the population may continue to be unable to obtain digital ID at higher assurance levels due to difficulties in identity proofing.

163. As highlighted earlier in this paper, jurisdictions facing financial inclusion challenges should adopt a flexible approach in establishing the required identity attributes, evidence and processes for proving official identity. This will ensure that financially excluded people can be captured under the identity proofing requirements (e.g., making a permanent residential address an optional attribute and allowing for trusted individuals to attest to a person's identity). 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 ML/TF risk.

164. In 2017, the FATF published a supplement to the 2013 Guidance on AML/CFT Measures and Financial Inclusion, focusing specifically on CDD and financial inclusion.[45] The paper highlights risk mitigation measures that regulated entities should apply, commensurate with the nature and level of identified risks. It also presents different CDD approaches that can remove obstacles to financial inclusion linked to the verification of the customer's identity, such as a broad understanding of the reliable and independent source of information, or simplified due diligence measures. The Guidance notes that in a number of countries, the expansion of digital financial services has been supported by a tiered approach to CDD. Under this

45 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

approach, for example, a formerly excluded or underserved individual is provided an account with built-in AML/CFT risk mitigants, such as limitations on the account's total value and/or the value and number of transactions within a specified time frame, and verification of the customer's identity is delayed until specified thresholds are reached.

165. Applying the lessons of the 2017 Financial Inclusion Guidance to the use of digital ID systems means that, when the ML/TF risks of on-boarding a given potential customer are lower, a digital ID system with a lower assurance level for identity proofing may be appropriate. Additional measures may be required to ensure ML/TF risk is mitigated, including for example, putting restrictions on the use of the account, as described above. Similarly, when the illicit financing risks associated with unauthorised account access are higher (e.g., because of the prevalence of stolen usernames and passwords in a jurisdiction), but the 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 assurance for its authentication component may be used to prevent the account from being used by an unauthorised person. 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 that tiered CDD value, velocity and volume requirements are not circumvented.

166. The ability to adopt a flexible approach to the use of digital ID systems under the FATF standards has important implications for financial inclusion. It can facilitate the implementation of tiered CDD and delayed identity verification, because under digital ID assurance frameworks and standards, digital ID systems with a lower assurance level for identity proofing/enrolment require less stringent identity evidence or verification of the person's identity (see Appendix E). This means that a formerly excluded or underserved individual (who lacks certain documents to provide proof of official identity for onboarding) can still be enrolled in a digital ID system. The individual can then use the digital ID's authenticators for customer identification to open an account without verification, subject to specified controls and thresholds.

167. In addition, digital ID systems can enable formerly underserved or excluded individuals to develop a more robust digital footprint and risk profile over time that allows them to access a broader range of financial services. Depending on the jurisdiction's approach to the requirements for proving official identity, digital ID systems can potentially transform the concept of official identity itself, from something that is fixed to something that can strengthen over time—i.e., progressive identity. With progressive identity, as an individual (e.g., the customer) engages in digital financial and other online activities and builds a digital presence, additional identity attributes and authentication factors become available and can strengthen the individual's digital ID, thereby increasing the confidence level in a customer's identity.

168. Progressive identity supports financial inclusion, even when digital ID systems are not interoperable and digital ID is not portable, because it allows a particular regulated entity to gain a better understanding of the individual customer and build confidence in the business relationship to provide a broader range of financial

services. However, its value is greatly increased—including for financial inclusion purposes—when progressive identity is portable, because it allows the more robust identity created by the individual's behavioural patterns, transaction data and associated authentication information collected by one regulated entity to travel with the individual and be used for customer identification/verification at unrelated regulated entity. Absent portability, customers would have to re-establish their progressive identity at each regulated entity over a period of time, during which they could only access low value/low risk products and services.

Box 3. Illustration of how the use of digital ID in tiered and progressive CDD can support financial inclusion

A financially excluded individual applies for a basic bank account, using a digital ID obtained without presenting identity evidence. The digital ID has a lower assurance level for identity proofing but an authentication assurance level that provides confidence that the claimant controls authenticator(s) bound to the identified individual.

The regulated entity onboards the customer and provides a low risk bank account, with a very low threshold for value, transaction volume, and velocity and no cross-border transactions (these risk mitigation measures are based on risk analysis). The customer uses this account to obtain a mobile phone under a contract and receives digital wage payments directly into the bank account among other activities.

The regulated entity uses data associated with the direct deposit of wages, social transfers or benefits, to verify employment, occupation, and source of funds, and regular payments from the account for mobile phone and utility services to establish a pattern of responsible financial behaviour. The regulated entity also collects other transaction and associated authentication information to verify the customer's address. Over time, the regulated entity uses the customer's consistent financial activities and behavioural patterns (e.g., transaction times, typical amounts, purposes/counterparties and geolocation) to strengthen authentication for account access and anti-fraud measures.

The jurisdiction's AML/CFT legal framework is principles-, performance-, and outcomes-based. Its customer identification/verification regulations require regulated entities to have a reasonable basis to believe they know who their customers are, but do not rigidly prescribe how they are to achieve this objective. The regulated entity treats the data generated by the customer's activities over time as identity evidence and uses it to build confidence that it knows who its customer is and the customer's risk profile. When that confidence satisfies the regulated entity that it has complied with its customer identification/verification obligations and satisfied its own risk appetite and risk management practices and procedures for other financial services, the regulated entity offers a standard bank account with higher thresholds and greater functionality and later, provides a small loan, which the customer uses to start a business.

This approach for digital ID mirrors the same process which is set out in the FATF's 2017 Guidance on CDD and Financial Inclusion, where persons without adequate identity documents can undergo tiered CDD and progressively expand their level of access to financial services, beginning from a restricted, low-risk form of account.

Source: US Treasury

Digital ID standards and frameworks can support financial inclusion

'Trusted Referees'

169. One example, in which some digital ID assurance frameworks and standards allow for those without traditional identity evidence is to permit the use of trusted referees—such as village heads, local government authorities, judges/magistrates, employers; persons with good standing in the community (e.g. businessmen, lawyers, notaries); or some other form of trained and approved or certified individual—to vouch for the applicant as a form of identity evidence,[46] in accordance with the jurisdiction's applicable laws, regulations, or agency policies.

170. 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.

Remote Identity Proofing and Non-Face-to-face Onboarding

171. As noted previously, digital ID systems can enable remote customer identification/verification and support remote financial transactions at standard or even low levels of risk. The technical standards permit remote identity proofing and enrolment, even at higher assurance levels. See Appendix E.

[46] NIST 800-63A 4.4.2. IAL2 Trusted Referee Pr4oofing Requirements.

APPENDIX A: DESCRIPTION OF A BASIC DIGITAL IDENTITY SYSTEM AND ITS PARTICIPANTS

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 II. 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 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. This appendix is provided to provide context and does not intend to stipulate the technical or organisational requirements for an eligible digital identity within the AML & CTF framework.

Summary of the digital ID process

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).

Identity proofing and enrolment may be either digital or documentary, and face-to-face (in-person) or non-face-to-face (remote).[47] In a digital ID system, binding/credentialing, authentication and portability/federation are always, and necessarily, digital.

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

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

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.

47 See further explanation of these terms in the Guidance.

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, 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 ID 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 attributes (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).*
  - Attributes may also be inherent—i.e., based on an individual's personal biometric (biological or behavioural) characteristics.[48] 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 ID 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 —all of which are dynamic.

[48] It is important to distinguish the use of biometrics as identity attributes from biometrics for identification or deduplication (i.e., as used to establish an individual's identity and uniqueness) versus their use as authenticators. The digital identity technical standards (e.g. NIST standards) support only limited use of biometrics for authentication purposes and impose rigorous requirements and guidelines for this use to address a variety of concerns.

  - 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, mobile phone usage, geolocation patterns, and file access log (including expected log-in channels, geolocation, timing; frequency and type of usage (account balance and activity review vs. transaction).[49]

- 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.[50] In addition, governments may consider country context and financial inclusion goals in establishing required identity attributes. For example, especially in developing countries with significant itinerate or homeless populations and people without formal addresses, 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 or 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

49 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).

50 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 identifiers with reliance on biomechanical attributes. See Section V for a discussion of the evolving role of behavioural biometric attributes in digital identification/verification and authentication.

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.

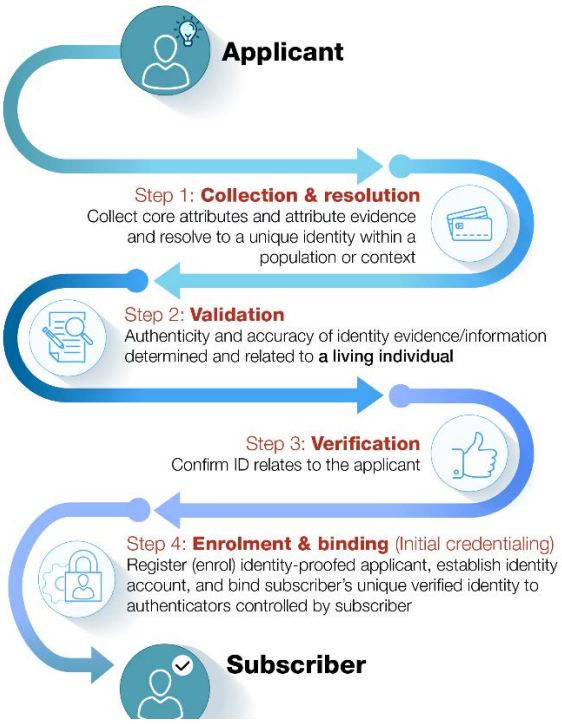
Enrolment is the process by which an IDSP registers (enrols) an identity-proofed applicant as a 'subscriber' establishes their identity account. This process authoritatively binds the subscriber's unique verified identity (i.e., the subscriber's attributes) to one or more authenticators possessed and 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'.

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 ID 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.

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.

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

Authentication answers the question, "***Are you the identified/verified individual?"*** It establishes that the individual seeking to access an account (or other services or resources)--the claimant—is the same person who has been identity proofed, enrolled, and credentialed and has possession and control of the binding credentials and other authenticators, if applicable (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.[51]

Authentication factors

Traditionally, there are three basic categories of authentication factors:

- Knowledge factors: Something you know such as: a shared secret (e.g., username, 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 USB-dongle) or software that the subscriber controls; a one-time password (OTP) generated

51 When the Guidance describes components of authentication, those are not the same as 'strong customer authentication (SCA)' under the EU's legal framework. What constitutes or does not constitute a valid SCA factor for the purpose of PSDII has to be assessed in accordance with the PSDII and the RTS on SCA+ CSC, rather than FATF guidance.

by a hardware device; or a software OTP generator installed on a digital device, such as a mobile phone.

- Inherence factors: Something you are (biophysical biometrics, such as facial recognition and fingerprint or retinal pattern biometrics; biomechanical 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; and advanced behavioural biometrics).

As discussed below, a given digital ID system will not necessarily use each of these types of factors. For example, although many current digital ID systems use biometrics, it should not be assumed that all digital ID systems do so.

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 therefore allow the use of biophysical biometrics for authentication only when strongly bound to a physical authenticator.

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.[52]

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.

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

[52] As noted in the Guidance itself, digital ID systems also present significant risks (including privacy risks) and opportunities for abuse (e.g., bias or human rights abuse), which are outside the scope of this Guidance but should be effectively addressed.

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 2 RTS and demonstrate that their fraud rates are below certain thresholds defined in the RTS.[53]

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

Authentication processes

Authentication processes are generally categorised by the number and type of authentication factors the process requires, on the understanding that the more factors an authentication process employs, the more robust and trustworthy the authentication system is likely to be. As authentication technology/processes have evolved, that notion is being revised and augmented by a more modern, outcomes-based approach, in which multi-factor authentication is assumed, but the strength of the authentication component does not depend on *how many* factors and types of factors it uses, but rather, on whether its authentication processes are resistant to comprise by commonly executed and evolving attacks, such as phishing and man-in-the-middle attack vectors. (This more holistic, outcomes-based approach should better accommodate the emergence of continuous authentication.)

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.
- **Multi-factor authentication (MFA)** uses two or more independent authenticators from at least two different authentication factor categories (knowledge/possession/inherence) to authenticate the claimant's identity. For example, when a claimant seeks to log into an online bank account, using a knowledge-based authenticator (e.g., username and password), the claimant would also need to enter an additional authentication factor from a different authentication factor category in order to successfully access the account. The claimant might use an ownership authentication factor, such as a private key generated in the FIDO-certified authenticator embedded in their mobile phone for this purpose. MFA may be implemented by using either multiple authenticators that in combination present authentication factors from a different categories directly to the verifier, or a single authenticator that provides more than one type of factor, as is the case when an authenticator

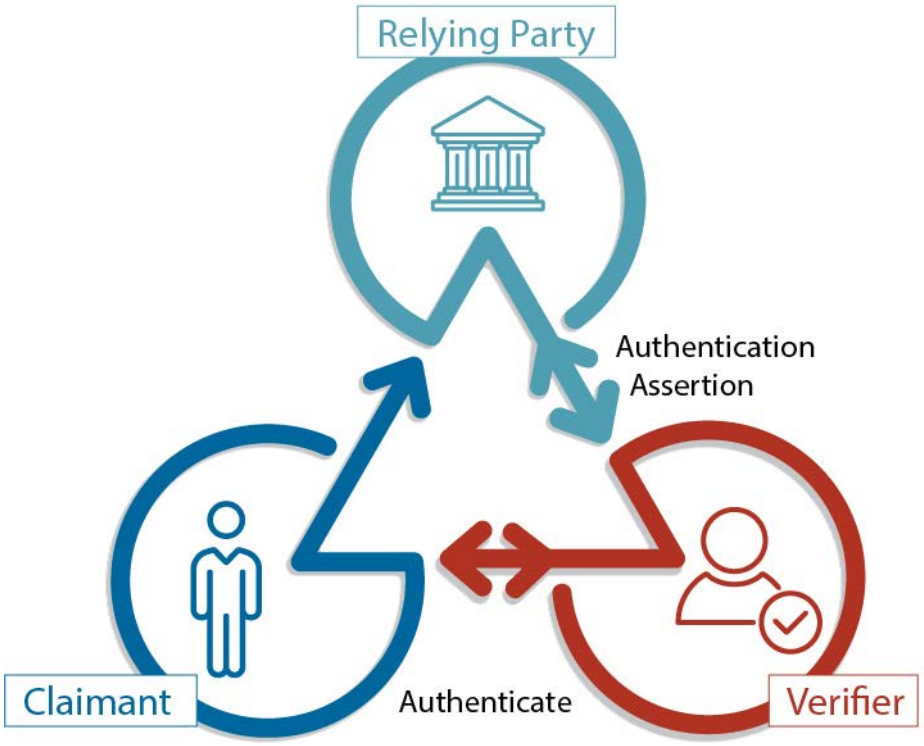
[53] The text of the RTS is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389.

uses one or more factors to protect another type of factor, which in turn is presented directly to the verifier. [54]

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 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 only of claimant and RP).

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



54 Under the NIST standards, strong authentication requires either two factor authentication 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. See Appendix E for a more detailed discussion of the technical standards.

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 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".

Identity Lifecycle management

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.

The attributes associated with an identity may change from year to year. Analytics systems may uncover risk signals suggesting an identity is being used in a manner consistent with fraud or account compromise (as noted previously, in the discussion of "continuous authentication"). Some commercial identity management systems are building in capabilities that analyse whether and how an identity evolves over the course of its lifecycle.

The discussion below uses the function-based term, 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)

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 ID 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.

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.

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.

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.

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

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.

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 Verification Service Provider (IVSP)	Entity that conducts identity proofing (validation of evidence and verification linking validated evidence to the applicant).
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.

IDENTITY SERVICE PROVIDERS	
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 assurance levels. Trust Framework Providers may be government entities (e.g. EU/ eIDAS) or a trusted industry organization, such as Open Identity Exchange (OIX); FIDO (Fast 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: CASE STUDIES

Box 4. India's Unique ID (UID) number

Features of the digital ID system: India's Unique ID (UID) number—or Aadhaar—identity program uses multiple biometrics and biographic information, as well as official identity documentation where it is available, to provide a digital ID to all residents in India, regardless of age or nationality.

The Unique Identification Authority of India (UIDAI) has released a mobile app, m-Aadhaar, which generates a "virtual ID" number, linked to but different than the Aadhaar number, to increase privacy and security. Both the Aadhaar number and Virtual ID can be authenticated online, against the Aadhaar database, or offline, using a QR code.

Financial inclusion measures: The UIDAI Aadhaar enrolment process has flexible identity evidence requirements in order to achieve comprehensive coverage in a jurisdiction where many people lack basic identity documents, and relies on biometrics to establish uniqueness. Enrolment must be in-person but is conducted at authorized registrars located throughout the country (primarily state governments, central ministries, banks and public sector organizations), using software and biometric capture and other equipment prescribed by UIDAI by MOU. Registrars are required to take special measures to enrol women, children, senior citizens, persons with disability, unskilled and unorganised workers, nomadic tribes and all other marginalised/vulnerable groups of individuals who do not have any permanent dwelling.

UIDAI accepts numerous different types of identity documents to verify core attributes at enrolment — 32 types of identity documents containing name and photo; 14 proof of relationship (PoR) documents; 10 date of birth documents; 45 proof of address documents. (see https://uidai.gov.in/images/commdoc/valid_documents_list.pdf).

If an individual does not have any of the "notified" identity documents, the individual can enrol in Aadhaar if a family entitlement document includes his/her name and the Head of Family in the entitlement document enrols in Aaadhar, using required identity Proof-of-Identity and Proof-of-Address documents and introduces the family member while they are enrolling. Where no PoR or other required documents are available, a resident may use Introducers or certifiers, who are individuals notified by the Registrar or regional UIDAI office, who are available at the enrolment centre

Use for CDD: Importantly, under the Amending Aadhaar Act, adopted in July 2019 to comply with the Supreme Court's 26 September 2018 decision that struck down certain provisions of the original Aadhaar Act on privacy grounds, use of Aadhaar remains mandatory for tax purposes and to receive government benefits, subsidies and services financed from the Consolidated Fund of India, but is no longer mandatory to open a bank account (or obtain a mobile phone number). Instead, use of Aadhaar for CDD is strictly voluntary and must be based on the customer's informed consent. Regulated entities may verify the identity of their customers by: (i) authentication or offline verification of Aadhaar, (ii) passport, or (iii) any other documents notified by the central government.

Source: World Bank

Box 5. Peru

Peru's national digital ID system, the National Registry of Identification and Civil Status (Registro Nacional de Identificación y Estado Civil (RENIEC) provides digital ID services to wide range of public and private entities across numerous sectors, enabling them to streamline identity verification and authentication and improve service delivery. In the financial sector, RENIEC serves as the core system for conducting customer identification/verification in compliance with CDD requirements for Peru's e-money and mobile money platform—Billetera Movil (BiM), which was launched in February 2016 and provides services such as cash in/cash out at agents, the ability to check balances, conduct P2P payments and top-up credit to millions of customers.

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

Box 6. Nigeria Bank Verification Numbers (BVN)

Each Nigerian with a bank account is registered in the Bank Verification Number (BVN) system which consists of a biometric-enabled ID database and the e-KYC infrastructure managed by the Nigerian Inter-bank Settlement System (NIBSS). Over 36 Million adults are covered in the BVN database and can use the BVN number to open a new account with another bank, open an online wallet, or apply for a loan. This has lowered onboarding costs and contributes to more robust competition in the financial services market. Customer identification and verification with the BVN is instantaneous and also allows for remote (non-face-to-face) verification through mobile devices. NIBSS has provided Application Programming Interfaces (APIs) allowing for BVN integration to banks and non-bank digital financial service providers, including FinTechs across the country.

Source: World Bank

Box 7. Mexico - High costs in the use of an ID system for CDD purposes

In Mexico, the foundational identification system for individuals is the *Clave Única de Registro Nacional de Población* (CURP), while targeting the entire population and having the potential to use biometrics, is not unique and does not meet the necessary assurance levels for CDD regulatory requirements in Mexico.

On the contrary, the voters card issued by the Instituto Nacional Electoral every ten years includes two forms of biometrics since 2016 (facial recognition and fingerprints) which presents lesser risks of duplications than the CURP. The "general-purpose" nature of the INE for adults in Mexico was created under a temporary legal provision included under the *Ley General de Población* to be used as the primary source of identity for Mexicans until the CURP could provide similar assurance levels to those of INE.

The INE developed a service to allow third parties to verify credentials against the database but the cost of this service – although necessary – is impacting small and medium sized financial institutions as well as Fintech companies willing to operate in the country.

In 2018, the Fintech Law was issued and, conscious at the time of the increasing cases of ID theft in the country, authorities issued measures to mitigate such concerns while meeting FATF recommendations on CDD. Measures issued included the use of the INE as primary source for verification credential for regulated entities and detailed rules regarding the use of biometrics prompting regulated entities to seek adequate Digital ID market solutions to meet the CDD regulatory requirements.

However, the INE was developed to serve as a voters' card and not as a general-purpose identification verifying services and therefore authorities have initiated, in a coordinated manner, an integral reform with regards to digital ID with the objective of having a an official digital ID that can also be used for CDD related purposes .

Source: World Bank

Box 8. UNHCR – Digital ID for refugees

As of the end of 2018, the United Nations Refugee Agency (UNHCR) estimated there were 25.9 million refugees and 3.5 million asylum seekers globally. Countries in developed regions hosted 16% 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 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 had been issued with official identity cards or other credentials, often because they came from fragile or conflict affected areas or faced discrimination preventing registration. At the same time, there is a general principle that prevents contact with the authorities of the country of origin to verify a refugee's identity without the refugee's 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.

UNHCR's digital ID system is used by many host Governments and UNHCR for the registration and identity management of asylum seekers and refugees. By March

2020 over 9 million refugees in 72 countries had been biometrically enrolled in the system.

Features of the digital ID system:

- UNHCR is in the process of strengthening its digital ID system for asylum seekers and refugees. UNHCR's process of identity proofing and enrolment for these individuals is described in UNHCR's Guidance on Registration and Identity Management,[55] Chapter 5.3 "Ascertaining an individual's identity: document review and data collection" and 5.6 "Biometric enrolment and photographs".
- The means of identity authentication provided by UNHCR's digital ID system varies, depending on the country context and the use-cases. The identity credentials issued by the system are mainly used in face-to-face environments. Both asylum seekers' and refugees' identity credentials vary according to host government requirements, but contain facial image and biographic information, which includes a minimum data set and additional attributes that uniquely identify a person. The identity credentials also have a printed bar code or QR code and a unique reference number for the holder.
- UNHCR's digital ID system can support authentication using biometrics, which was initially used for the distribution of humanitarian assistance, including cash transfers (which are termed cash-based interventions). For example, in a number of countries in the Middle East, including Jordan, cash-based interventions are delivered through ATMs with iris scanning equipment to authenticate a user's identity.
- In Malaysia and Indonesia, an Android application is used by the authorities to check the validity of the identity card issued to a refugee by UNHCR and to facilitate verification of the identity of the holder through comparison to a photograph displayed in the application.
- In Uganda, the Office of the Prime Minister (which is responsible for refugee registration and identity and uses UNHCR's digital identification system) in cooperation with the Uganda Communications Commission and UNHCR is establishing a system that will allow for biometric authentication at point of sale by SIM Card vendors. At the time of writing the process was in testing. In Somalia, biometric authentication has been put in place for onboarding for financial services for returning refugees (see below for further details).

Participants in the digital ID system: The roles of participants in UNHCR's digital ID system vary, depending on the country context.

- Where UNHCR is undertaking refugee registration and identity management on behalf of the host Government or in the context of return and resettlement, UNHCR is the sole data controller.
- In other contexts, a hybrid solution is adopted—most commonly where the host State uses UNHCR's system for the registration and identity management of refugees. In these circumstances, UNHCR provides the

55. UNHCR, "Registration and Identity Management Guidance" https://www.unhcr.org/registration-guidancehapter5/registration/

system and the host Government and UNHCR are the joint data controllers, regulated through data sharing agreements.

- In the case of the biometrics system used in Egypt, Iraq, Jordan, Lebanon and Syria, UNHCR works with a private-sector supplier within the context of a data protection protocol.

Use for CDD and relevant regulations: UNHCR's digital ID system and credentials issued by it are allowed to be used for customer identifcation/verification at onboarding in various countries including: Burundi, Malawi, Jordan, Niger and Zambia.[56]

The Central Bank of Somalia has agreed to adopt an approach to CDD for returning refugees who have been biometrically enrolled in UNHCR's system in Kenya and other neighbouring countries. The Voluntary Return Form issued by UNHCR to the returnee prior to departure in the country of asylum, together with biometric authentication of identity using UNHCR's system will be allowed for customer identification/verificationto open a bank account. This solution was tested in December 2018 with accounts opened for two individuals and is expected to be implemented on a wider scale with a Financial Service Provider in 2020.

System's assurance level: The assurance level of UNHCR's system has not been audited against the digital ID trust frameworks and technical standards discussed in this Guidance however at time of writing UNHCR has commissioned external assessments by expert consultants and is evaluating the conclusions.

Financial inclusion: Financial inclusion of refugees is an important component of refugees' protection, self-reliance and resilience. UNHCR distributed 2.4 Billion USD in humanitarian cash-based interventions from 2016-19. To promote financial inclusion, UNHCR aims to deliver cash-based interventions through beneficiaries' bank or mobile money accounts (respecting local regulations), and to give priority to "open loop" systems that leverage local markets and ecosystems, rather than investing in "closed-loop" systems, which only make a limited contribution to financial inclusion. By leveraging digital technology and mobile platforms specifically, UNHCR aims to promote the financial inclusion, which has demonstrated a positive andt tangible impact on the lives of refugees.

Source: UNHCR

Box 9. China - Private sector provided digital ID

Features of, and participants in, the digital ID system: Ant Financial has created a digital ID system, 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

[56] UNHCR, "Displaced and Disconnected" (2019) https://www.unhcr.org/innovation/displaced-and-disconnected/

scenarios to complete customer due diligence. Each verification is based on the user's explicit authorisation and confirms the use of the verification service.

Use for financial services: Ant Financial and financial institutions cooperate to provide financial services such as insurance, fund, and microfinance to customers, and also fully use digital ID to provide financial institutions with services such as customer identification and customer risk assessment. Ant Financial's digital ID has been widely accepted in various financial service scenarios, providing more than 3 billion face verification services to hundreds of millions of Alipay users. It is also used in pension inquiry, pension collection, tax declaration and other public services. In addition, Ant Financial provides digital IDs for short term tourists in China who do not have a Chinese bank account but want to make mobile payments. Ant Financial takes special identity verification measures with the Immigration Office to confirm that the passport information is authentic.

System's assurance level: There are no transparent digital ID assurance frameworks and technical standards in China, but it has been suggested that if assessed against the NIST standards, the Ant Financial digital ID system might have identity assurance level 2 (IAL2), authentication assurance level 1(AAL1) and Federation assurance level 2 (FAL2).

Financial inclusion measures:

(1) For residents in rural or remote underdeveloped areas without access to bank accounts or where camera technology is not advanced enough to support facial recognition technologies, Ant Fianncial can verify customer information via the Citizen Identity Information Verification Platform. Limitations are placed on the account (payments cannot exceed 1000 yuan) and cross-border payments are not permitted.

(2) For college students without access to bank accounts, Ant Financial can verify student identities via the China Higher Education Student Information Network, including the student's education status.

Source: China

Box 10. Singapore – National Digital Identity (NDI)

Under the National Digital Identity (NDI), the Singaporean Government is developing 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. NDI is built on public key infrastructure (PKI) cryptographic security techniques, and the services have been gradually deployed since 2017 and are expected to be fully operational by 2020.

Features of the digital ID system: There are 4 distinct layers in the NDI stack.

- Trusted data: MyInfo forms the trusted identity data service of NDI and was launched in early 2017. MyInfo includes government-verified data retrieved from various Government agencies and contains more than 100 personal data items. It provides citizens and residents access to and be in control over the sharing of their data. The public are able 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.

- Trusted identity: A National Certificate Authority (NCA) will be put in place by the Government to issue each resident with a cryptography-based digital identity securely generated and residing within a mobile phone. A digital identity that can be universally trusted by both government and private sector companies. It will supports a multi-tiered identity assurance model, allowing users to conduct more sensitive transactions as their identity assurance level increases.
- Trusted access: NDI will support an open and federated ecosystem of authentication service providers (ASPs). The Government will operate one of the ASPs, but other ASPs may be operated by the private sector, all referencing the same digital identity issued by the Government. In late 2018, SingPass Mobile was launched to enable secure authentication without the need for hardware tokens or SMS-OTPs, which provides greater digital inclusion and ease of access for both public and private sector.
- Trusted services: These are digital services built on NDI's layers. An example is digital signing. Financial institutions can rely on NDI to provide more trusted and high assurance services as well as streamline customer journeys regardless of the boundaries of systems or organisations.

Participants in the Digital ID system: The trusted data and trusted identity layers are provided by the Government. The trusted access layer will support an open and federated ecosystem of authentication and digital signing service providers (ASPs and DSAPs). The Government will operate one of the ASPs.

Use for CDD: Today, more than 60 financial institutions in Singapore leverage MyInfo for over 220 digital services to on-board and perform CDD on customers.

Relevant digital ID-specific AML/CFT regulations: The Monetary Authority of Singapore has issued Guidance on the 'Use of MyInfo and CDD Measures for Non Face-to-Face Business Relations' (AMLD 01/2018).[57] 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. MAS has clarified that it considers MyInfo to be a reliable and independent source for the purposes of verifying the customer's name, unique identification number, date of birth, nationality and residential address. Financial institutions are required to maintain proper records of data, including data obtained from MyInfo, in accordance with regulatory requirements in Singapore.

System's assurance level: The NDI has used US NIST and EU e-IDAS as reference examples. NDI will be assessing its assurance level against other countries' assurance level as Singapore embarks on bilateral cooperation opportunities. For authentication assurance, it is based on Common Criteria (CC) Evaluation Assurance Level (EAL), with the use of AVA: Vulnerability Assessment (AVA_VAN, from 1 to 5) class.

57. www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Circular-on-MyInfo-and-CDD-on-NFTF-business-relations.pdf

Financial inclusion: The NDI is provided free to all Singapore citizens and residents, and is part of the inclusion programme of the relevant government agencies.

Source: Singapore

Box 11. South Africa

In order to respond to increasing need to mitigate fraud and ID theft, as well as to meet CDD requirements, the South African Banking Risk Information Centre (SABRIC) was established in 2002. Initially composed of the four largest banks, SABRIC now also includes other banks, three Cash-In-Transit and one ATM service provider. In 2007, SABRIC and Department of Home Affairs (DHA) began collaborating to fight identity-related crime. Initially, banks verified customer identity on the basis of a visual inspection of the barcoded green ID book and visual comparison of the photo in it to the appearance of the (prospective) customer. However, the 'manual' method of identity verification had weaknesses. To address them, SABRIC members and the DHA collaborated to enable the verification of customers' identities by matching their fingerprints directly against the DHA's biometric HANIS database, which sends back a 'verified' or 'not verified' response. A secure connection for accessing the DHA database was established in participating bank offices via South Africa's State Information Technology Agency (SITA). The banks pay DHA for verification. The verification process generates an audit trail and the system provides reliable management information. By the end of 2018, seven banks and 4,000 branches were participating in the project. Currently, the number of verifications is about 3 million per month. Queries of the DHA database last typically between 4 and 16 seconds. Between 2 percent to 3.8 percent of e-verifications have been unsuccessful, because the person whose identity was verified lacked a biometric record in HANIS.

Source: World Bank

Box 12. eIDAS interoperability and mutual recognition

Under the eIDAS framework member states can use digital ID for accessing online services. They can also decide to involve the private sector in providing digital ID solutions (means). Under the principle of mutual recognition, member states are obliged to accept notified digital ID means of other member states if they allow the use of digital ID for online access to their public services, and 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.

Source: European Commission

Box 13. Belgium – eCards & ItsMe ®

Belgium's digital ID system includes both public and private-sector components. As explained in greater detail below the government provides general-purpose digital identity credentials, the Belgian Citizen eCard and the Foreigner eCard (together referred to as the Belgian eCards). It also provides the digital identity authentication platform for e-government services. 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. In addition, a private-sector digital identity authentication service, Itsme®, provides mobile-phone based authentication of identities that are linked to an eCard and a specific mobile phone and SIM card for participating banks and mobile network operators (MNOs). Existing customers can use Itsme® to authenticate their identity in order to log in to their accounts and conduct transactions.

Features of the digital ID system and key participants:

eCards

- Registration for the Belgian e-cards occurs in-person. Municipalities / consulates and embassies are responsible for identity proofing, enrolment, issuance, and delivery of the eCard.
- The Belgian Government provides the Federal Authentication Service (FAS) to authenticate identities for accessing online government services. The FAS platform supports both Internet browser and mobile-phone access, and relies on the IETF TLS standard which provides end-to-end cryptgraphic communications security over networks. FAS authentication involves the following steps:
    - The citizen or foreigner seeks to log into an eGovernment service by entering the PIN code for the individual's eCARD online.
    - The internet browser sends an authentication certificate to the FAS which perhaps the necessary certificate verifications to ensure the integrity, validity and authenticity of the presented TLS client authentication certificate.
    - FAS authenticates the certificate, allowing the individual to complete log-in and access the requested government application.

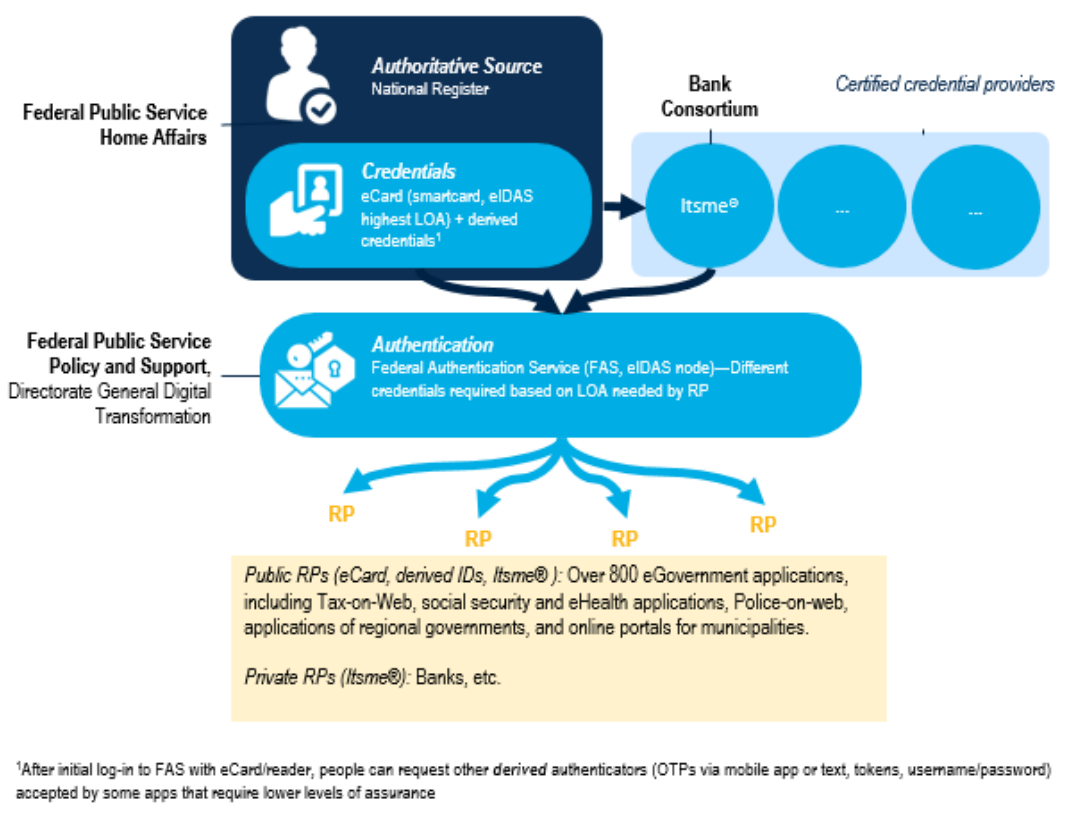
Itsme®

- Itsme® is an initiative of Belgian Mobile iD, a consortium of four leading Belgian banks (Belfius, BNP Paribas Fortis, ING, KBC) and mobile network operators (Orange, Proximus, Telenet). Activation of Itsme® on a mobile device is tied to 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).

Use in financial services: The Belgian FAS platform is only available to access public services, no financial services are possible at this moment. The itsme® solution is used to authenticate transactions.

Systems' assurance level:

- Belgian eCards provide a High Level of Assurance under eIDAS specifications as confirmed by the eIDAS cooperation network after an in-depth peer review by the Member States.
- Itsme® has undergone a thorough security and governance audit and is recognised by the Belgian government as a valid means of authentication with a 'high' Level of Assurance.



Source: Belgium

Box 14. Sweden – eID Framework and BankID

The Swedish Govenrment, which maintains a central database of the identities of all Swedish citizens and residents, facilitaties digital ID through a public-private partnership. The government provides the federated digital ID architecture (the eID framework - Sweden Connect Technical Framework) and private entities, including banks, act as digital ID service providers, issuing digital ID credentials and providing authentication services.

Features of the digital ID system and key participants: The federation includes both digital ID service providers and relying parties that provide commercial goods or services or government services online. There are currently four digital ID service providers: (1) AB Svenska Pass, (2) BankID, (3) Freja eID, and (4) Telia E-identification—although Telia stopped enrolling individuals for e-idetification in autumn 2017, the e-identification credentials it had issued are valid until they expire.

First launched in 2003 and managed by a consortium of 10 Swedish banks, BankID provides customers with a free digital ID, which can be used to authenticate identity to conduct transactions across the private and public sector. Companies looking to integrate BankID with their services contract with a bank in the BankID network and pay fees for BankID services, which generates a revenue stream for the participating banks. Identity credentials are available in "hard" form—encoded on a smart chip—or "soft" form—available as software on a user's personal computer, tablet, cell phone or other digital device.

Use in financial services: Bank ID can be used for onboarding customers. To obtain a bank ID in the first instance, the individual must undergo documentary CDD by the bank issuing the digital ID. Once obtained, Bank ID can be used to open account with other financial institutions. As at 2016, BankID facilitated 2 billion transactions per year and was used by more than 80 percent of Swedish citizens.

Relevant digital ID-specific AML/CFT regulations: The use of digital ID for customer identification/verification is explicitly provided for in the AML/CFT Act (Ch. 3, s. 7):

"An obliged entity should identify the customer and verify the customer's identity through identity documents or extracts from registers or through other information and documents from an independent and reliable source.

In the application of the first sub-section, instruments for electronic identification and trusted services pursuant to the eIDAS Regulation may be used. Other secure remote or electronic identification processes that are regulated, recognised, approved or accepted by relevant authorities may also be used."

System's assurance level: The Swedish E-Identification Board undertakes checkes of e-identification issuers in accordance with Svensk e-legitimation. Four assurance levels (1 to 4) are defined in the Swedish eID Assurance Framework.[58]

Source: Sweden
References:
https://elegitimation.se/inenglish/howeidentificationworks.4.769a0b711614b669f2953f.html

58 https://docs.swedenconnect.se/technical-framework/mirror/digg/Tillitsramverk-for-Svensk-e-legitimation-2018-158.pdf (in Swedish)

Box 15. Italy - Public System of Digital ID

Features of, and participants in, the digital ID system: Developed under the EU eIDAS Regulation and launched in 2016, the Italian Public System of Digital Identity (SPID),, is a public open digital ID system that allows public and private entities (Identity Providers) accredited by the Agency for Digital Italy (AgID) to offer digital identity registration services to natural persons (citizens and or individuals with residence permits) 18 and older, and to authenticate the SPID digital ID credentials, enabling the identified individual to access public and private services. SPID had about 2.5 million digital identities by March 2018. SPID registration can take place in person, online, or using a mobile device with webcam, depending on the registration procedures offered by a given Identity Provider. To obtain SPID ID credentials, an individual can provide an Identity Provider with a valid identity document (identity card or passport), health card, email address and mobile phone number, or use their digital signature, electronic identity card (CIE), or national service card (CNS).

Use in financial services: The acceptance of SPID is mandatory for the public sector and optional for private sectors (commercial and financial). According to an ABI Lab (Italian Banking Association) survey of Italian banks, 38% of the sample banks planned to use the SPID system for onboarding mobile banking customers and 18% planned to use it for internet banking onboarding by the end of 2019.

Relevant digital ID-specific AML/CFT regulations: The Italian legislation allows obliged entities to use eIDAS compliant digital IDs, like SPID, for customer identification and verification of customers who are natural persons. .

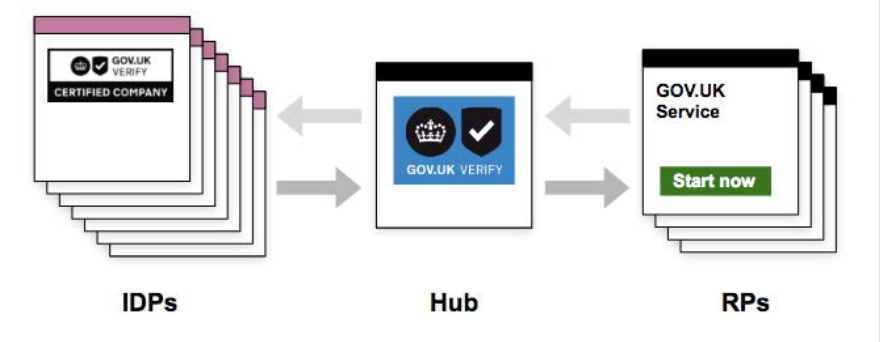
System's assurance level: SPID offers three assurance levels for identity authentication, consistent with standard ISO-IEC 29115. Level 1 allows access to online services, using a user name and password chosen by the user. Level 2, for services that require a higher degree of security, allows access through a user name and password chosen by the user, plus the generation of a temporary access code (one time password), usable through a digital device (e.g., smartphone). Level 3 provides additional security measures, including the use of physical devices (e.g., smart cards) provided by the identity manager. The assurance level required for SPID identity authentication depends on the level of security required by the online service providers.

Source: World Bank, Banca d'Italia and the European Banking Federation

Box 16. 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 digital ID 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 ID system that enables UK citizens and UK residents to prove their identity online. It uses private sector Identity Providers (IDPs) to identity proof and authenticate the identity of the individual to a specified set of requirements and specifications. IDPs have met government and industry standards to provide identity assurance services as part of GOV.UK Verify.



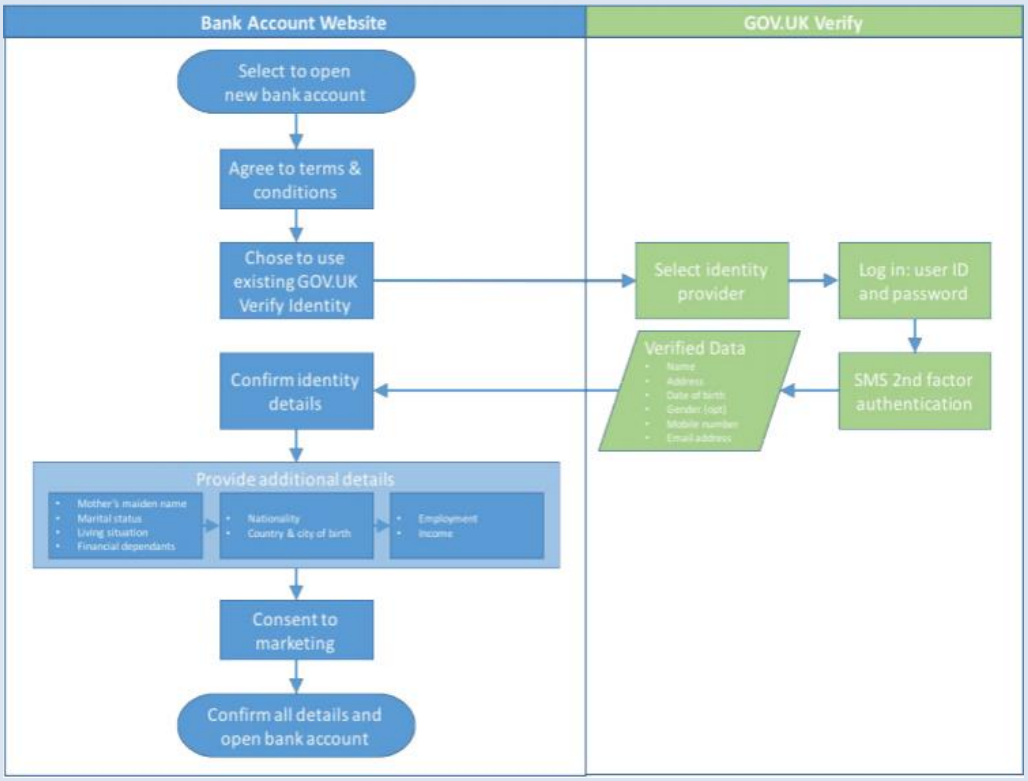
The GOV.UK Verify Hub is the centrally provided infrastructure that manages interactions between users, government services, IDPs, and matching services for the

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 IDPs 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 using GOV.UK Verify to open 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

Box 17. Estonia

Features of the digital ID system: There are a range of digital ID systems available in Estonia, including:

- ID-cards – the primary identification document in Estonia, are compulsory for all citizens and residents and are the most widely used digital ID option. The ID-card has a photograph and a chip that securely stores personal identity data and digital signature certificates, using public key infrastructure (PKI).
- Mobile-ID is a private sector digital ID service, which can be used via a person's mobile phone. Mobile-ID is issued by a telecom provider in connection to a person's SIM and ID-card. The service needs to be activated on the Police and Border Guard Board's (PPA) website.
- Smart-ID is a private-sector digital ID service that uses the Smart-ID API on a person's mobile phone and the Smart-ID key management server service. Smart-ID can be issued to persons with an Estonian personal identification code. It functions similarly to the ID-card and Mobile-ID in identifying and verifying a customer.

Participants in the digital ID system:

- The Estonian Information System Authority (RIA) coordinates the digital ID authentication solutions. The Police and Border Guard Board issues identity credentials (ID-card, residence card, Digi-ID, and e-resident's Digi-ID) in accordance with the Identity Documents Act. Ministry of Foreign Affairs is responsible for the e-residency programme.
- Two private companies provide technical solutions - Tieto Estonia AS offers user support for the ID-card's basic software and SK ID Solutions AS issues and validates eID certificates.

Use for CDD: Estonian digital ID solutions are used for customer identification/verification at onboarding, as well as for strong customer authentication in compliance with Directive (EU) 2015/2366 (the second Payment Services Directive) and its regulatory technical standards to authorise payment transactions.

Relevant digital ID-specific AML/CFT regulations: In Estonia, a customer can be onboarded face-to-face, via information technology means (video onboarding) and by using two different sources of identity verification. Legislation does not specify what the two verification means should be but the Estonian Financial Supervisory Authority has issued relevant guidance[59] saying that digital ID solutions (i.e. information obtained through authenticating with digital ID) can be one of those sources (point 4.3.1.22), but there should be one additional source of information (point 4.3.1.23) to verify the identity of the customer.

System's assurance level: All the notified Estonian eID schemes have high level of assurance under the eIDAS scheme

Source: Estonia

59. www.fi.ee/sites/default/files/2019-01/FI%20rahapesu%20t%C3%B5kestamise%20juhend%202018%20%28EN%29_pdf.pdf

APPENDIX C: PRINCIPLES ON IDENTIFICATION FOR SUSTAINABLE DEVELOPMENT

This Guidance highlights several concrete ways that countries can develop digital ID 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.[60] 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

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.

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

60 World Bank. 2017. *Principles on Identification for Sustainable Development: Toward the Digital Age*. Washington, DC: World Bank Group. id4d.worldbank.org/principles. A list of endorsing organisations can be found on the website.

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 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

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.

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.

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.

For government-recognized digital ID in particular, *Principle 5* further emphasizes the need for vendor 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.

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*).

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).

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 that do not compromise the goal of providing proof of identity that is accessible for all and meets the needs of people and relying parties.

Goal 3. Build trust by protecting privacy and user rights

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.

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.

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.

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.

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

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.

The **International Organization for Standardization (ISO)** is a Geneva-based, independent international organisation, with a membership of 163 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. Some of the relevant standards include: identity proofing and enrolment of natural persons (ISO/IEC 29003:2018); entity authentication assurance framework (ISO/IEC 29115:2013 – under revision) and application of Risk Management Guidelines (ISO 31000:2018) to identity-related risks. Through its newly convened TC68[61] Working Group 7, ISO is currently working on global standards for natural persons' identification, including in digital context.

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.

The **World Wide Web Consortium (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 ID 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.

The **Fast Identity Online (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).

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.

61 ISO/TC68 is the Technical Committee within ISO tasked with developing and maintaining international standards covering the areas of banking, securities, and other financial services.

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.

The **European Telecommunications Standards Institute (ETSI)** is one of the three 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 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.

Identity proofing

Box 18. 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. NB: In the NIST Digital ID Standards, "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 discussion below).
- 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.
- Evidence of identity attributes must meet specified evidence quality requirements, permitting various combinations of required numbers of pieces of evidence at given strengths, determined by specified characteristics.

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 in Section III)
- The identity evidence quality requirements are more rigorous
  - Requires more additional identity evidence at higher 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 credential service provider (CSP) representative.

Source: United States NIST standards

Table 4. Summary of Identity Proofing Requirements for IAL 1, IAL2, and IAL 3

Requirement	IAL1	IAL2	IAL3
Presence	No Requirements	In-person and unsupervised remote.	In-person and supervised remote.
Resolution	No Requirements	• The minimum attributes necessary to accomplish identity resolution. • KBV may be used for added confidence.	Same as IAL2
Evidence	No identity evidence is collected.	• One piece of SUPERIOR or STRONG evidence depending on strength of original proof and validation occurs with issuing source, OR • Two pieces of STRONG evidence, OR • One piece of STRONG evidence plus two (2) pieces of FAIR evidence.	• Two pieces of SUPERIOR evidence, OR • One piece of SUPERIOR evidence and one piece of STRONG evidence depending on strength of original proof and validation occurs with issuing source, OR • Two pieces of STRONG evidence plus one piece of FAIR evidence.
Validation	No validation	Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented.	Same as IAL2
Verification	No verification	Verified by a process that is able to achieve a strength of STRONG.	Verified by a process that is able to achieve a strength of SUPERIOR.
Address Confirmation	No requirements for address confirmation	Required. Enrollment code sent to any address of record. Notification sent by means different from enrollment code.	Required. Notification of proofing to postal address.
Biometric Collection	No	Optional	Mandatory
Security Controls	N/A	• Moderate Baseline (or equivalent federal or industry standard).	• High Baseline (or equivalent federal or industry standard).

Box 19. In-person identity proofing and enrolment

As noted above, the technical standards permit in-person identity proofing at IAL2 and *require* it at IAL3. Importantly—including with respect to financial inclusion objectives—in-person identity proofing and enrolment can be conducted either by:

- A physical interaction with the applicant, supervised by an operator; or
- A *remote interaction* with the applicant*, supervised by an operator*, based on specified requirements for remote in-person identity proofing, that achieves comparable levels of confidence and security to in-person (physical interaction) identity proofing.

For either type of in-person identity proofing, the technical standards require that (1) The operator must inspect the biometric source (e.g., fingers, face) for presence of non-natural materials as part of the proofing process; (2) the CSP must collect biometrics in a way that ensures that the biometric is collected from the applicant and not another subject and that all biometric performance requirements set forth in the standards are applied.

Comparability Requirements for Supervised Remote In-Person Identity-Proofing and Enrolment

To establish comparability between supervised remote in-person identity proofing and enrollment, and identity-proofing and enrollment where the applicant is in the same physical location as the CSP, the following requirements must be met (in addition to the IAL3 validation and verification requirements, discussed above):

The CSP must:

- Monitor the entire identity proofing session (e.g., by a continuous high-resolution video transmission of the applicant).
- Have a live operator participate remotely with the applicant for the entirety of the identity proofing session. Operators must have undergone a training program to detect potential fraud and to properly perform a virtual in-process proofing session.
- Have all digital verification of evidence (e.g., via chip or wireless technologies) performed by integrated scanners and sensors.
- Ensure that all communications occur over a mutually authenticated protected channel.
- Employ physical tamper detection and resistance features appropriate for the environment in which the identity-proofing session occurs (e.g., a kiosk located in a restricted area or monitored by a trusted individual requires less physical tamper detection than one located in a semi-public area, such as a shopping mall concourse).

The applicant must remain continuously in (cannot depart from) the monitored identity proofing session and all actions taken by the applicant during the identity proofing session must be clearly visible to the remote operator.

Box 20. Authentication and Life Cycle Management

AUTHENTICATION ASSURANCE LEVELS (AALs) set the technical requirements for (1) authentication protocols and processes (including credential and authenticator issuance and binding) and (2) authenticator lifecycle management (including revocation in the event of loss or theft, and expiration/re-proofing and re-binding). Stronger authentication (a higher AAL) requires malicious actors to have better capabilities and expend greater resources to successfully subvert the authentication process. Authentication at higher AALs can effectively reduce the risk of impersonation, replay, and other attacks that can lead to fraudulent claims of a subject's digital ID attacks. AALs include technical requirements for authenticator types; approved cryptography and secure authentication channels (including compromise detection, impersonation and replay resistance requirements); re-authentication of (extended) subscriber sessions; record retention; cyber-security; and privacy. The AALs also establish requirements for binding authenticators to a proofed identity and for actions to be taken in response to events that can occur over the lifecycle of a subscriber's authenticator that that go to the authenticator's trustworthiness after binding, including loss, theft, unauthorized duplication, expiration, and revocation. Many of these requirements are highly technical and incorporate by reference other highly technical information security standards.

The following summary describes at a high level of generality only some of the requirements for authentication at various AALs. See NIST 800-63(b) for a detailed discussion.

- AAL1: Provides *some assurance* that the claimant (the individual asserting (claiming) identity for account authorization) controls an authenticator(s) bound to the subscriber's account. AAL1 permits a wide range of authentication technologies and authenticator types and information security controls at a *low* baseline. MFA is optional). Biometrics alone may be used as a single-factor authenticator at AAL1.

- AAL2: Provides *high confidence* the claimant controls authenticator(s) bound to the customer/subscriber's account. It requires MFA (either a multi-factor authenticator or two single-factor authenticators), using secure authentication protocol(s) that incorporate specified approved cryptographic techniques, and information security controls at a *moderate* baseline. AAL2 imposes more stringent requirements on authenticator types than AAL1.[62] Biometrics may be used as one authentication *factor*

[62] AAL2 permits use of any of the following multi-factor authenticators: multi-factor OTP device; multi-factor cryptographic software; or multi-factor cryptographic device. When a combination of two single-factor authenticators is used, one authenticator must be a memorized secret authenticator and the other must be possession-based (i.e., "something you have") and use any of the following: look-up secret; out-of-band device; single-factor OTP device; single-factor cryptographic software; or single-factor cryptographic device.

(something you are), with the device authenticated as a second factor (something you have), but cannot serve as the only authenticator type.

- AAL3: Provides *very high confidence* that the claimant controls authenticator(s) bound to the subscriber's account. AAL3 requires MFA that uses both a hardware-based authenticator and an authenticator that provides verifier impersonation resistance (VIR), based on proof of possession of a key through an approved cryptographic protocol.[63] Claimants must prove possession and control of two distinct authentication factors through secure authentication protocol(s), using approved cryptographic techniques. The authenticators must be verifier impersonation resistant, replay resistant and resist relevant side-channel attacks. When a biometric factor is used, the identity service provider (verifier) must make its own determination that the biometric sensor and subsequent processing meet specified performance requirements. The CSP must employ appropriately-tailored security controls at a *high* baseline.

eIDAS – European Union

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., 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.

63 The claimant uses a private key stored on the authenticator to prove possession and control of the authenticator. An IDSP (verifier), knowing the claimant's public key through some credential (typically, a public key certificate) uses an approved cryptographic authentication protocol to verify that the claimant has possession and control of the associated private key authenticator, and asserts the person's verified identity to the RP.

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.

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.

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 5. 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

Application: computer software designed to help a user perform specific tasks.

Application Programming Interface (API): a set of definitions and protocols for building and integrating application software. APIs let digital products or services readily communicate with other products and services.

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 who asserts his or her identity 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 ID 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.

Continuous authentication is a dynamic form of authentication. It can leverage biomechanical biometrics, behavioural biometric patterns, and/or dynamic Transaction Risk Analysis to focus on ensuring that certain data points collected throughout the course of an online interaction with an individual (such as geolocation, MAC and IP addresses, typing cadence and mobile device angle) match "what should be expected" during the entire session.

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 systems 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.

Personally Identifiable Information (PII) includes any information that by itself or in combination with other information can identify a specific individual.

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 ID 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.

Progressive identity: Official identity that can change over time as the identified individual develops a progressively more robust digital footprint that provides an increasing number of attributes and/or authenticators that can be verified against an increasing number and range of sources.

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. The criteria for proving "official identity" can vary by jurisdiction.

Public-key encryption (used in Public Key Infrastructure (PKI) Certificates): Where a pair of keys are generated for an entity—a person, system, or device—and that entity holds the private key securely, while freely distributing the public key to other entities. Anyone with the public key can then use it to encrypt a message to send to the private-key holder, knowing that only they will be able to open it.

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.

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.

Tiered CDD (sometimes called tiered accounts or progressive CDD): access to a range of different account functionalities depending on the extent of identification/verification conducted by the regulated entity. Access to the basic, 1st level set of services is provided upon minimum identification. Access to the subsequent account levels and additional services (e.g., higher transaction limits or account balances, diversified access and delivery channels) is allowed only if/when the customer provides the required additional identification/verification information. In the meantime, the accounts have limited services (e.g., caps on daily/monthly withdrawals, deposit limits based on the level of CDD conducted and the customer's risk profile). See the FATF (2013-2017), Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence.

Trusted Referees (also referred to as 'introducers') can be nominated individuals or organisations (e.g., notaries, legal guardians, medical professionals, conservators, persons with power of attorney, or some other form of trained and approved or certified individual) that can vouch for the applicant as a form of identity evidence, in accordance with the jurisdiction's applicable laws, regulations, or agency policies. This is a term used in the US NIST standards: see NIST 800-63A 4.4.2. IAL2 Trusted Referee Proofing Requirements.

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.