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.

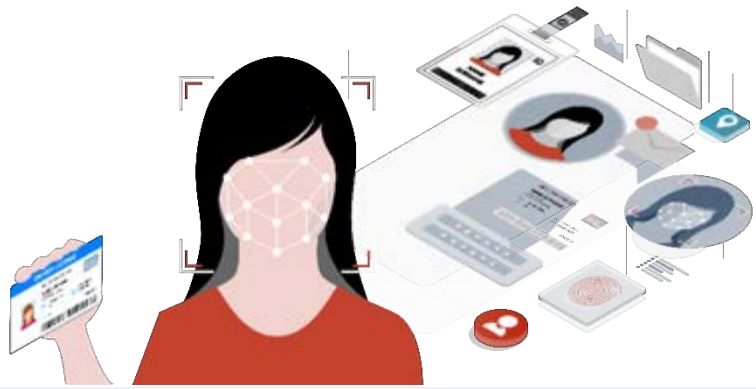
(IEC), is standardising these digital ID assurance frameworks and updating a range of ISO/IEC technical standards relating to identity, information technology security and privacy to develop a comprehensive global standard for digital ID systems. An identity assurance framework sets requirements for 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

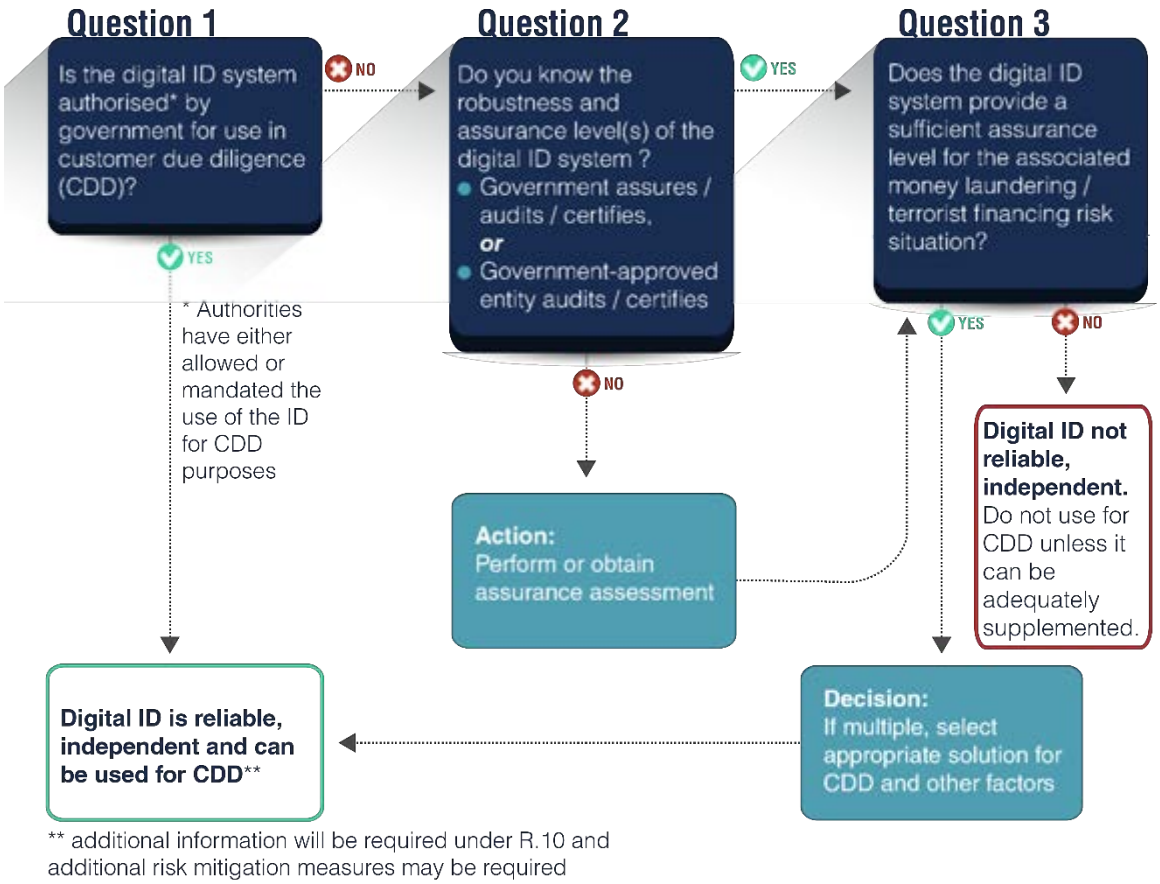
   b. Making a broader, risk-based determination of whether, given its assurance levels, the particular digital ID system provides an appropriate

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).

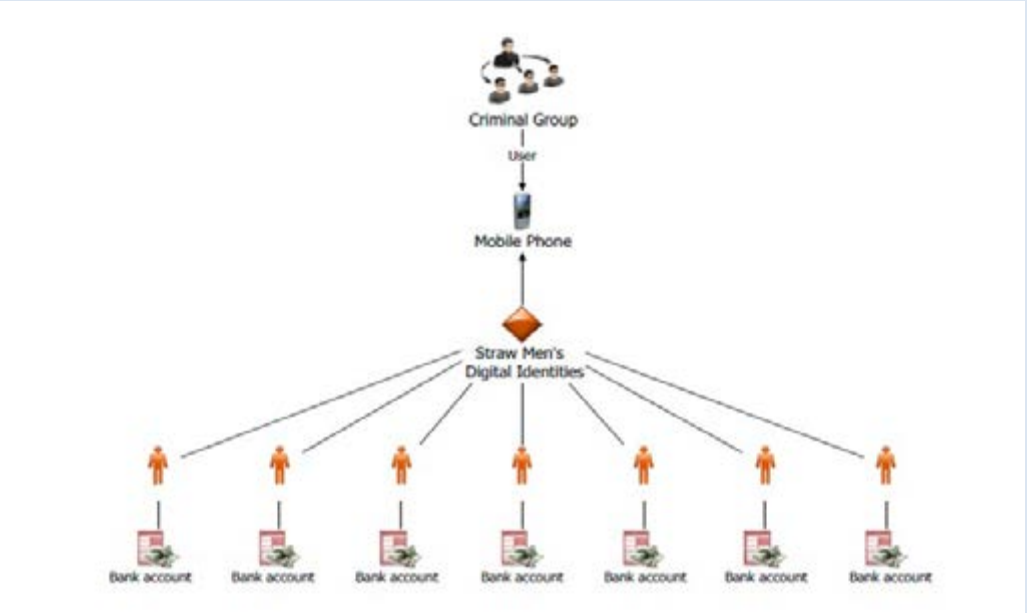
122. Most authentication vulnerabilities are exploited without the identity owner's knowledge, but abuse can also involve the witting participation of subscribers or IDSPs. For example, shared-secret authenticators, such as passwords, may be stolen and exploited by bad actors, but they can also be deliberately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

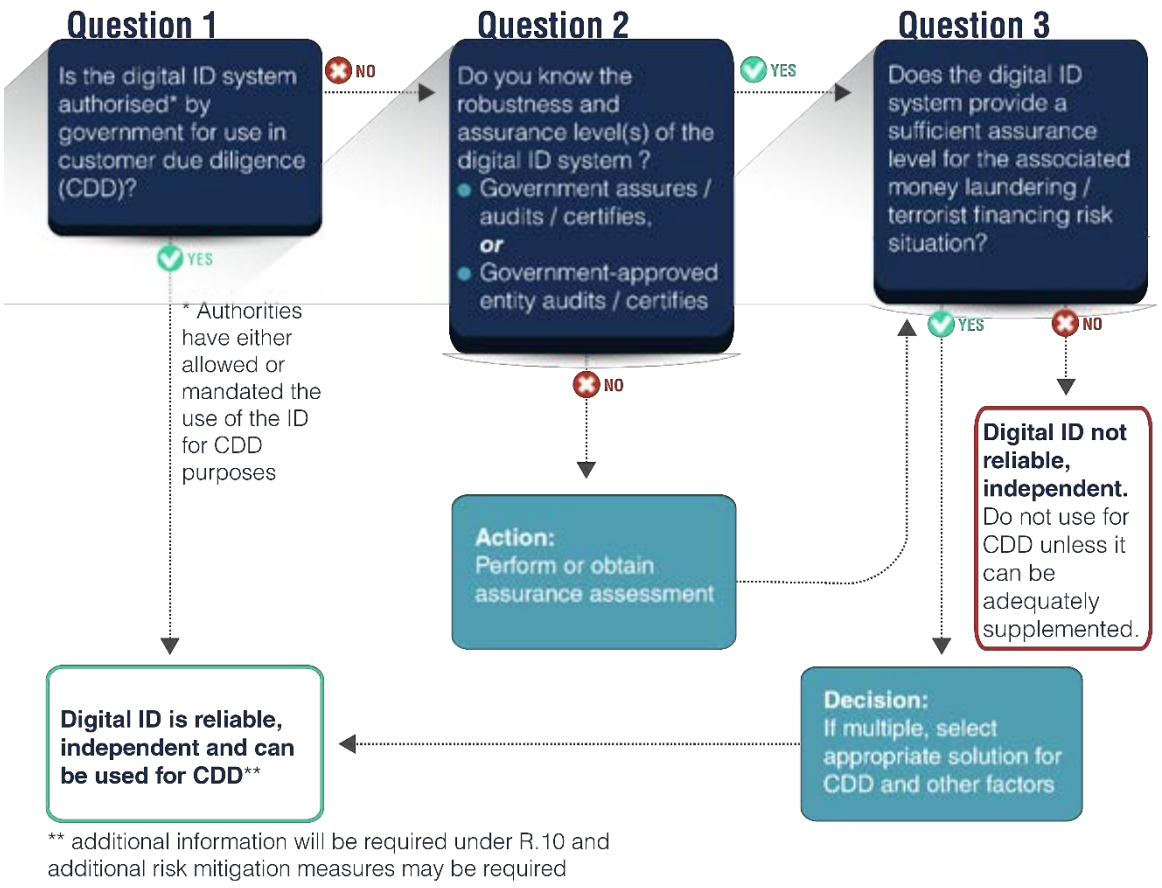
    a. Understand the assurance levels of the digital ID system provides based on its technology, architecture and governance to determine its reliability/independence; and

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.