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.

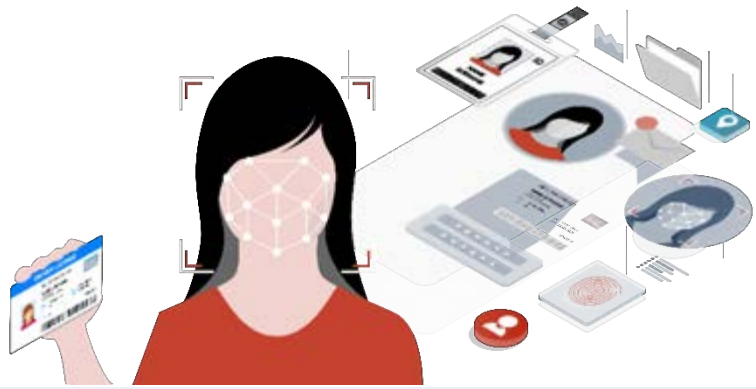
(IEC), is standardising these digital ID assurance frameworks and updating a range of ISO/IEC technical standards relating to identity, information technology security and privacy to develop a comprehensive global standard for digital ID systems. An identity assurance framework sets requirements for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

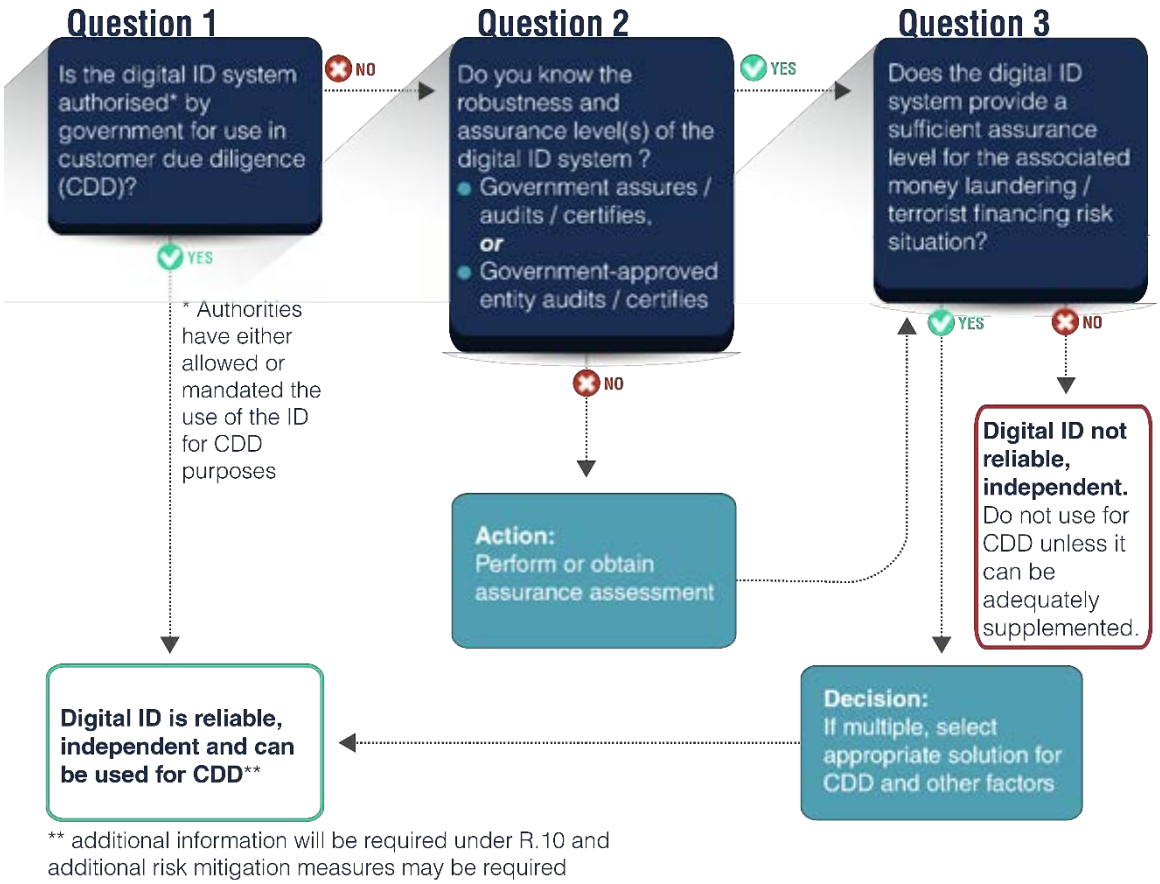
   b. Making a broader, risk-based determination of whether, given its assurance levels, the particular digital ID system provides an appropriate

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.