مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM AND ILLEGAL ORGANISATIONS

GUIDANCE FOR LICENSED FINANCIAL INSTITUTIONS ON DIGITAL IDENTIFICATION FOR CUSTOMER DUE DILIGENCE

31 October 2022

Contents

1. Introduction

1.1. Purpose

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019), *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 3090/2021 dated 29/06/2021), and the *Guidelines for Financial Institutions adopting Enabling Technologies* (dated 11/07/2021), and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices and red flag indicators. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

1.2. Applicability

Unless otherwise noted, this guidance applies to all natural and legal persons, which are licensed and/or supervised by CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, issuers and providers of stored value facilities, licensed retail payment service providers, card schemes, registered hawala providers, and other LFIs; and
- Insurance companies, agencies and brokers.

[1] Available at https://www.centralbank.ae/en/cbuae-amlcft and https://centralbank.ae/en/fintech-office.

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

(i) Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and Financing Illegal Organisations (as amended by Federal Decree Law No. (26) of 2021) ("AML-CFT Law"); and

(ii) Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations ("AML-CFT Decision").

This Guidance also builds on global standards and best practices issued by the Financial Action Task Force ("FATF")[2] and the Wolfsberg Group, as well as on industry standards and best practices.

1.4. Acronyms

Terms	Description
AML	Anti-money laundering
API	Application program interface
CBUAE	Central Bank of the United Arab Emirates
CDD	Customer due diligence
CFT	Combating the financing of terrorism
CSP	Credential service provider
DNFBP	Designated non-financial business or profession
DPP	Data protection and privacy
FATF	Financial Action Task Force
FIDO	Fast Identity Online
ID	Identity
IDSP	Identity service provider
IP	Internet Protocol
LFI	Licensed financial institution
MAC	Media Access Control
MFA	Multifactor authentication
ML	Money laundering
NIST	National Institute of Standards and Technology
OTP	One-time password
PKI	Public key infrastructure
PII	Personally identifiable information

[2] Including FATF Guidance on Digital ID, available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html.

PIN	Personal identification number
SIM	Subscriber identity module
TF	Terrorist financing

2. Overview of Digital ID Systems and Participants

2.1. Terminology and Definitions

For the purposes of this Guidance, in relation to identifying and verifying the identity of a customer as part of the customer due diligence ("CDD") process, **identity** ("ID") refers to the specification of a unique natural person that is:

- Based on characteristics (attributes or identifiers) of the person that establish a person's uniqueness in the population or particular context(s); and
- Recognized by the state for regulatory and other official purposes.

Proof of identity generally depends on some form of government-provided or issued registration, documentation, or certification (such as a birth certificate, identity card, or digital ID credential) that constitutes evidence of core attributes (such as name and date and place of birth) for establishing and verifying identity. Proof of identity may be provided through general-purpose ID systems (such as national ID and civil registration systems) or various limited-purpose ID systems (such as taxpayer identification numbers, driver's licenses, passports, voter registration cards, social security numbers, and refugee identity documents).

Digital ID systems use electronic means to assert and prove a person's identity online and/or in in-person environments, including through the use of:

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

Identification Systems in the UAE

LFIs should understand and utilize national-level identification systems and processes currently in place or under development in the UAE, including but not limited to:

- **UAE Pass**, the UAE's first national digital identity and signature solution that enables users to identify themselves to government service providers in all emirates through a smartphone-based authentication protocol and to sign documents digitally with a high level of security. The UAE Pass app uses biometric facial recognition software to verify and register users without requiring an in-person visit to a government services center. The UAE Pass also includes a "digital vault" for storing users' digital documents and sharing them with government departments, as well as a "digital signature" function to complete official transactions without the need for paper documents or physical signatures.
- **Emirates ID**, the mandatory, government-issued identity card for all UAE citizens and residents. While issued as a physical card, the Emirates ID card uses public key infrastructure to attach individual identities to digital certificates that can be used to sign and encrypt data, as well as fingerprint biometrics. When verifying an Emirates ID card, LFIs should use the online validation gateway of the Federal Authority for Identity and Citizenship and should keep a copy of the Emirates ID and its digital verification in their records.
- **Emirates Facial Recognition**, an initiative launched by the UAE Ministry of Interior and Federal Authority for Identity, Citizenship, Customs & Port Security, together with private sector partners. The facial recognition initiative includes a "face fingerprint" system for digital verification of digital transactions and remote identities.

Digital ID systems involve two basic components and an optional third component:

- **Identity proofing and enrollment** answers the question: *Who are you?* It involves collecting, validating, and verifying identity evidence and information about a person, establishing an identity account, and binding the individual's unique identity to authenticators possessed and controlled by this person.
- **Authentication and identity lifecycle management** 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 the identity is the same person who was identity proofed and enrolled, and ensures that adequate controls are in place to manage events that can occur over the identity lifecycle that affect the use, security, and trustworthiness of authenticators.
- **Portability and interoperability mechanisms**, where used, enable proof of identity to be portable, so that an individual's digital ID credentials can be used to prove identity for new customer relationships at unrelated private-sector or governmental entities, without their having to obtain and verify personal data and conduct customer identification and verification each time. Portability and interoperability are optional components of any digital ID system.

Not all elements of a digital ID system are necessarily digital. Some elements of identity proofing and enrollment can be either digital or physical, or a combination; however, binding, credentialing, authentication, and portability/federation (where applicable) are always and necessarily digital. These concepts are explained further in the following sections.

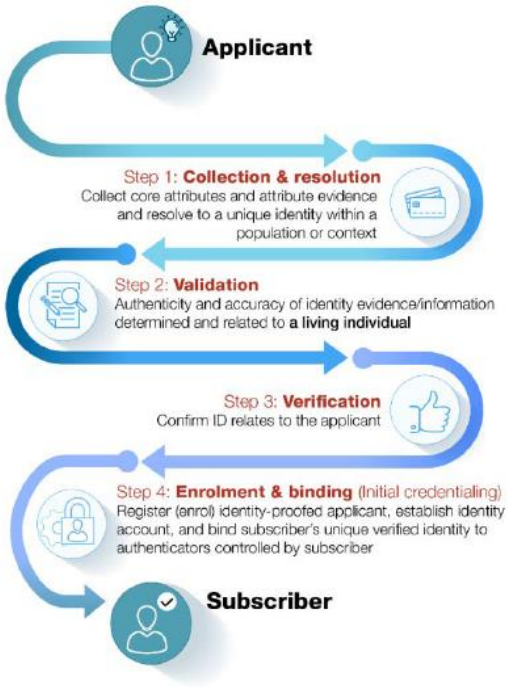
Digital ID systems can enable remote customer identification and verification, support remote financial transactions, and otherwise facilitate **non-face-to-face business relationships and transactions**, defined as interactions in which the parties are not in the same physical location and conduct activities by digital or other non-physically present means, such as mail or telephone. Under international standards, non-face-to-face business relationships and transactions are included as an example of a potentially higher-risk situation in undertaking CDD.[3] However, given the evolution of digital ID technology, architecture, and processes, and the emergence of consensus-based open-source digital ID technical standards, non-face-to-face interactions 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 present a lower level of risk where higher assurance levels are implemented and/or appropriate control measures are present.[4] See section 4 below for specific risk mitigation measures and strategies that can help ensure that a digital ID system is suitably "reliable" and "independent" in this sense.

2.2. Identity Proofing and Enrollment

Identity proofing and enrollment (with initial binding/credentialing) constitute the first stage of a digital ID system. This component is directly and most immediately relevant to LFIs' customer identification and verification obligations under Article 8 of the AML-CFT Decision. For illustrative purposes only, Figure 1 below presents a sample process flow for identity proofing and enrollment; the discussion that follows explains each step in greater detail.

[3] See *The FATF Recommendations*, Interpretive Note to Recommendation 10, at 68, available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.
[4] FATF, *Guidance on Digital Identity*, at 30, available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf.

Figure 1. Identity Proofing and Enrollment



Source: The Financial Action Task Force[5]

Identity proofing comprises three actions: (1) collection and resolution, (2) validation, and (3) verification. Examples of each of these actions are included in the discussion below for illustrative purposes only; there is no expectation that LFIs employing a digital ID system for CDD use any particular method of identity proofing unless otherwise required.

1. **Collection and resolution** involves obtaining attributes, collecting attribute evidence, and resolving identity evidence and attributes to a single unique identity within a given population or context (a process known as "de-duplication").[6]
    - Attribute evidence may be either physical (documentary) or purely digital, or a digital representation of physical attribute evidence (such as a digital representation of a paper or plastic driver's license). Identity evidence has traditionally taken a physical form and been physically presented by the person seeking to prove his or her identity (known as a "claimant") to an identity service provider ("IDSP"). However, with the development of digital technology, identity evidence may now be generated digitally (or converted from physical to digital form) and stored in electronic databases, allowing the identity evidence

[5] Available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf.
[6] Some government-provided ID solutions include a de-duplication process as part of identity proofing, which may involve checking the applicant's specific biographical attributes (such as name, age, or gender), biometrics (such as fingerprints, iris scans, or facial recognition images), and/or government-assigned attributes (such as driver's license, passport, or taxpayer identification numbers) against the identity system's database of enrolled individuals and their associated attributes and identity evidence to prevent duplicate enrollment.

to be *obtained remotely* and/or identity evidence to be *remotely verified and validated* against a digital database.

- Attributes may also be inherent, that is, based on an individual's personal biometric characteristics, including:
  - Biophysical biometrics, such as fingerprints, iris patterns, voiceprints, and facial recognition—all of which are static;
  - Biomechanical biometrics, such as keystroke mechanics, which are the product of unique interactions of an individual's muscles, skeletal system, and nervous system—all of which are dynamic; and
  - Behavioral biometrics, such as email or text message patterns, mobile phone usage, geolocation patterns, and file access log, which are based on an individual's patterns of movement and usage in what are known as "geospatial temporal data streams."
- Under Article 8.1 of the AML-CFT Decision and section 6.3.1 of the *AML/CFT Guidelines for Financial Institutions*, required identity attributes for CDD under UAE regulations and guidance include, for a natural person, the name (as in the passport or identity card, number, country of issuance, date of issuance and expiration date of the identity card or passport), the nationality, the address (i.e., the permanent residential address), the date and place of birth, and the name and address of employer (if applicable).

  When verifying the Emirates ID card, either physically or by way of digital or electronic Know Your Customer ("e-KYC") solutions, LFIs should use the online validation gateway of the Federal Authority for Identity, Citizenship, Customs & Port Security, the UAE Pass Application, or other UAE Government-supported solutions, and keep a copy of the Emirates ID and its digital verification record. Where passports, other than Emirates IDs, are used in the KYC process, a copy should be physically obtained from the original passport, which should be certified as "Original Sighted and Verified" under the signature of the employee who carries out the CDD process and retained.

2. **Validation** involves determining that the evidence is *genuine* (i.e., not counterfeit, forged, or misappropriated) and that the information the evidence contains is *accurate*. Validation is performed by checking the identity information and evidence against an authoritative and reliable source to establish that the information matched reliable, independent source data or records.
   - For instance, in order to assess whether an individual's physical identity evidence (such as a driver's license or passport), or the digital images thereof, is *genuine*, an IDSP may review the evidence to determine that there have been no alterations, that the identification numbers follow standard formats, and that the physical and digital security features are valid and intact.
     - When utilizing a physical or digital copy of identity evidence such as an Emirates ID card for purposes of validation, LFIs are expected to review the evidence for physical or digital abnormalities or possible alterations and to make a determination as to whether the evidence has been altered or forged.

- In order to assess whether such evidence is *accurate*, the IDSP may query the government issuing sources for the license or passport and confirm that the information matches.
    - As noted above, LFIs should use the online validation gateway of the Federal Authority for Identity, Citizenship, Customs & Port Security, the UAE Pass Application, or other UAE Government-supported solutions, to ensure that the information presented for validation purposes matches the information included in reliable databases or other sources.

3. **Verification** involves confirming that the validated identity relates to the specific individual being identity-proofed, including (but not limited to) through the use of biometric solutions like facial recognition or liveliness detection.
    - For example, if performing verification remotely, an LFI or other IDSP could ask the applicant to take and send a mobile phone video or photo with other liveliness checks, compare the submitted photos to the photos on the applicant's Emirates ID, passport, or other valid documents, and determine that they match to a given level of certainty.
    - To tie this identity evidence to the actual (real-person) applicant, the IDSP could then send an enrollment code to the applicant's validated phone number, email address, or another address that is tied to the identity, require the applicant to provide the enrollment code to the IDSP, and confirm that the submitted code matches the code sent. Such measures would verify that the applicant is a real person, in possession and control of the validated phone number. At this point, the applicant will have been identity proofed.

The fourth and final action in the first stage of a digital ID system is **enrollment and binding**.

4. **Enrollment** is the process by which an IDSP registers (or "enrolls") an identity-proofed applicant as a "subscriber" and establishes their identity account. This process authoritatively **binds** the subscriber's unique verified identity (i.e., the subscriber's attributes/identifiers) to one or more authenticators possessed and controlled by the subscriber, using an appropriate binding protocol. The process of binding the subscriber's identity to authenticator(s) is also referred to as "credentialing."
    - An **authenticator** is something the claimant possesses and controls—typically, a cryptographic module, one-time code generator, or password—that is used to confirm or "authenticate" that the claimant is the individual to whom a credential was issued and therefore is (to a given degree of likelihood) the actual subscriber and accountholder. The likelihood that the claimant to whom a credential was issued is in fact the actual subscriber is a function, in part, of the strength of the authentication component; stronger authenticators, such as longer and more complex passwords, can increase an IDSP's confidence that the claimant is in fact the actual subscriber.
    - A **credential** is a physical object or digital structure, such as a physical or electronic ID card, that authoritatively binds a subscriber's proofed identity (via one or more identifiers) to at least one authenticator possessed and controlled by the subscriber. When a digital IDSP issues an authenticator (such as a password or PIN) and authoritatively binds the authenticator to the subscriber's identity, the physical object or digital structure that results (such as an ID card) is a credential.

Typically, an IDSP issues one or more authenticators (such as a password or auto-generated code) *to the subscriber* and registers the authenticators in a way that ties them to the subscriber's proofed identity at enrollment. However, the IDSP can also bind the subscriber's account to authenticators provided *by the subscriber* that are acceptable to the IDSP. For example, users of the UAE Pass app are prompted to create a signing password while completing the verification step at a UAE Pass kiosk or through the mobile app. The IDSP can also bind a subscriber's credentials to additional or alternative authenticators at a later point in time, as part of identity lifecycle management (discussed immediately below).

2.3. Authentication and Identity Lifecycle Management

Authentication and identity lifecycle management constitute the second stage of a digital ID system. **Authentication** answers the question: *Are you the person who has been identified and verified?* It establishes the individual seeking to access an account (or other services or resources) is the same person who has been identity proofed, enrolled, and credentialed and has possession and control of the binding credentials and other authenticators, if applicable. In other words, it establishes that the *claimant* is the *onboarded customer*. Authentication can rely on various types of authentication factors and processes, with the trustworthiness of the authentication depending on the type of authentication factors used and the security of the authentication processes:

- **Authentication factors** fall into three basic categories:
    - **Knowledge factors**, that is, something you *know*, such as a shared secret (e.g., username, password, or passphrase), a personal identification number ("PIN"), or a response to a pre-selected security question;
    - **Ownership factors**, that is, something you *have*, such as a cryptographic key stored in hardware (e.g., in a mobile phone, tablet, computer, or USB-dongle) or software that the subscriber controls; a one-time password ("OTP") generated by a hardware device; or a software OTP generator installed on a digital device, such as a mobile phone; and
    - **Inherence factors**, i.e., something you *are*, including biophysical biometrics, biomechanical biometrics, and behavioral biometrics (as discussed in section 2.2 above).
- **Authentication processes** have historically been assessed by the number and type of authentication factors the process requires, on the assumption that the more factors an authentication process employs, the more robust and trustworthy the authentication system is likely to be. As authentication technology and processes have evolved, however, this assumption has been revised, and the strength of the authentication component is no longer assumed to depend on *how many* factors (or types of factors) it uses but rather on whether its authentication processes are *secure*: that is, resistant to compromise by commonly executed and evolving attacks, such as phishing and man-in-the-middle attack vectors. In this revised paradigm, multifactor authentication ("MFA")—where an IDSP uses two or more independent authenticators from at least two different authentication factor categories (knowledge/possession/inherence) to authenticate the claimant's identity—is typically assumed.
    - As detailed in the *Guidance for Financial Institutions adopting Enabling Technologies*, LFIs should implement MFA using a biometric factor where possible to authorize high-risk

activities and protect the integrity of customer account data and transaction details. High-risk activities include changes to personal data (e.g., customer office or home address, email address, or telephone contact details), registration of third-party payee details, high-value funds transfers, and revisions to funds transfer limits.

- LFIs deploying MFA at login that includes a biometric factor should consider employing phishing-resistant authenticators where at least one factor relies on public key encryption to secure the customer authentication process.

- Digital ID authentication has traditionally been conducted at a particular point in time: namely, when the claimant asserts the customer's/subscriber's identity and seeks authorization to begin a digital or in-person interaction to access his or her account or other financial services or resources. Today, however, many regulated entities augment traditional authentication at the beginning of an online interaction with **continuous authentication** solutions that leverage biomechanical biometrics, behavioral biometrics, and/or dynamic transaction risk analysis.

  - Instead of relying on something the claimant has/knows/is to establish at the beginning of the interaction that the claimant is the onboarded customer and is in control of the authenticators issued to that customer, continuous authentication focuses on ensuring that certain data points collected throughout the course of an online interaction—such as geolocation, Media Access Control ("MAC") and Internet Protocol ("IP") addresses, typing cadence, and mobile device angle—match what should be expected during the entire session.

  - However, ways of measuring the effectiveness of continuous authentication technology in mitigating authentication risks have not reached maturity, and the digital ID technical standards, such as the U.S. National Institute of Standards and Technology ("NIST") Digital Identity Guidelines, do not currently address them.

- Finally, **identity lifecycle management** refers to the actions IDSPs should take in response to events that can occur over the lifecycle of a subscriber's authenticator that affect the use, security, and trustworthiness of the authenticator. The attributes associated with an identity may change from year to year, and analytics systems may uncover risk signals suggesting an identity is being used in a manner consistent with fraud or account compromise. Key identity lifecycle events may include:

  - **Issuing and recording credentials:** At customer onboarding, the IDSP issues the credential and records and maintains the credential and associated enrollment data in the subscriber's identity account throughout the credential's lifecycle.

  - **Binding:** Throughout the digital ID lifecycle, the IDSP should also maintain a record of all authenticators that are, or have been, associated with the identity account of each of its subscribers, as well as the information required to control authentication attempts. When an IDSP binds a new authenticator to the subscriber's account post-enrollment, it should require the subscriber to first authenticate at the assurance level (or higher) at which the new authenticator will be used.

- **Compromised authenticators:** If a subscriber loses or otherwise experiences compromise of all authenticators of a factor required for MFA, the subscriber should repeat the identity proofing process, confirming the binding of the authentication claimant to previously proofed evidence, before the IDSP binds a replacement for the lost authenticator to the subscriber's identity account. If the subscriber has MFA and loses one authenticator, the IDSP should require the claimant to authenticate, using the remaining authentication factors.
- **Expiration and renewal:** Where an IDSP has issued an authenticator that expires, the IDSP should bind an updated authenticator prior to expiration, using a process that conforms to the initial authenticator binding process and protocol, and then revoke the expiring authenticator.
- **Revocation or termination:** IDSPs should promptly revoke the binding of authenticators when an identity ceases to exist (e.g.., because the subscriber has died or is discovered to be fraudulent); when requested by the subscriber; or when the IDSP determines that the subscriber no longer meets its eligibility requirements.

2.4. Portability and Interoperability Mechanisms

Digital ID systems can—but need not—include a component that allows proof of identity to be portable. An individual's identity is **portable** when his or her digital ID credentials can be used to prove identity for new customer relationships at unrelated private sector or government entities, without their having to obtain and verify personally identifiable information ("PII") and conduct customer identification and verification each time. Portability requires developing **interoperable** digital identification products, systems, and processes, including through the use of federated digital architecture and assertion protocols to convey identity and authentication information across a set of networked systems or through APIs that do not use federated architecture and protocols.

Portability and interoperability can potentially save relying parties (e.g., financial institutions and government entities) time and resources in identifying, verifying, and managing customer identities, including for account opening and authorizing customer account access, and may reduce the risk of identity theft stemming from the repeated exposure of PII. However, as discussed below, portability and interoperability are optional components of a digital ID system and will not be a focus of this Guidance.

2.5. Focus of this Guidance

This Guidance focuses on the **use of digital ID systems for CDD**, specifically for customer identification and verification at onboarding or account opening and for ongoing CDD monitoring, thus enabling LFIs to fulfill their obligations under Articles 8 and 7, respectively, of the AML-CFT Decision. The Guidance emphasizes, however, that **customer identification and verification and ongoing monitoring of the business relationship are only two components of LFIs' wider CDD obligations**, which include identifying and verifying the identities of a legal entity customer's beneficial owners and understanding the nature of the customer's business and the nature and purpose of the customer's business relationship with the LFI. LFIs are also separately required under Article 24 of the AML-CFT Decision to maintain all records and documents obtained through CDD measures for a period of no less than five years from the date of termination of the business relationship with the customer; under FATF standards and UAE regulation, such

recordkeeping requirements are technology neutral, meaning they apply equally to records kept in digital and physical (documentary) form.

The Guidance focuses primarily on **identity proofing and enrollment** and secondarily on **authentication**; it does not address portability and interoperability, as these components are regarded as optional under international AML/CFT standards and are less directly relevant to the application of CDD measures by LFIs. Particular emphasis will be placed on the use of third-party sources or providers to verify and authenticate customer identity through digital means.

Finally, the Guidance focuses on the use of digital ID systems to identify and verify the identity of customers that are **individuals (natural persons)**. It does not examine the use of digital ID systems to help identify and verify the identity of a legal person's representative(s) or beneficial owner(s) or to understand and obtain information on the nature and intended purpose of the business relationship—although reliable, independent digital ID systems are important for all of these CDD functions.

3. Use of Digital ID Systems for CDD

3.1. Customer Identification and Verification

Under Article 8 of the AML-CFT Decision, LFIs are required to identify each customer and verify the customer's identity using documents, data, or any other identification information from a reliable and independent source. This requirement is technology neutral and expressly permits LFIs to use documentary as well as non-documentary sources (i.e., information or data) when performing identification and verification; it does not impose any restrictions on the form—physical or digital—that identity evidence must take, nor does it impose limitations as to the use of digital ID systems for the purpose of linking a customer's verified identity to a unique, real-life individual, provided this is done using a "reliable" and "independent" source. As such, LFIs are permitted to utilize digital ID systems as well as physical forms to perform customer identification and verification, consistent with the expectations set forth in this Guidance.

In the digital ID context, the requirement that digital source documents, data, or information must be "reliable" and "independent" means that the digital ID system used to conduct CDD relies upon technology, adequate governance, processes, and procedures that provide an appropriate level of confidence that the system produces accurate results. Reliability and independence in this sense depends specifically on the effective application of mitigation measures to prevent and manage risks related to **identity proofing and enrollment**, such as the risks of an applicant using falsified identity evidence or another individual's identity, as well as risks related to **authentication and identity lifecycle management**, including various risks that bad actors will illicitly obtain an individual's legitimate identity credentials and assert them to open an account or obtain unauthorized access to products, services, and data. These risks and the corresponding mitigating measures that LFIs should consider implementing are discussed in greater detail in section 4 below.

3.2. Ongoing Due Diligence on the Business Relationship

Under Article 7 of the AML-CFT Decision, all customers must be subject to ongoing monitoring throughout the business relationship. Ongoing monitoring ensures that the account or other financial service is being

used in accordance with the customer profile developed through CDD during onboarding, and that transactions are normal, reasonable, and legitimate.

As discussed in section 2 above, authentication using a digital ID system establishes 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 onboarding. In other words, ongoing digital authentication of the customer's identity links that individual with their financial activity. LFIs that use digital ID systems to authenticate the identity of their existing customers as part of account authorization should leverage the data generated by authentication and related information (such as geolocation or IP addresses) to support ongoing due diligence and transaction monitoring, such as to assess whether a customer's actual activity conforms to the LFI's expectations of normal or typical activity and to identify cases in which a customer may be transacting from a sanctioned, otherwise prohibited, or high-risk jurisdiction.

3.3. Third-Party Reliance and Provision of Digital ID Services

Per Article 19 of the AML-CFT Decision, LFIs are permitted to rely on customer identification and verification undertaken by a third party at onboarding, provided the relying LFI:

1. Immediately obtains the necessary information concerning customer identification and verification from the third party, including the assurance levels, where applicable;
    - For example, the digital ID system could enable the prospective customer to assert identity to the relying LFI and the third party to authenticate the person's identity and provide additional needed information, such as the person's name, date of birth, government-provided unique identity number, or other attributes required to prove official identity.
2. Takes adequate steps to satisfy itself that the third party will make available copies of or other appropriate forms of access to identification data and other relevant CDD information and documentation without delay;
    - For example, the relying LFI could take appropriate steps to satisfy itself: (a) that, as part of identity proofing and enrollment, the third party established a digital ID account for the identified person that contains adequate attribute evidence and other identity data and information; and (b) that the third party's authentication processes enable it to provide that information to the relying party upon request without delay.
3. Satisfies itself that the third party adheres to the CDD and recordkeeping requirements set forth in the AML-CFT Decision and is regulated and supervised for compliance with these requirements. **In practice, this means that the third party should either be another LFI, a designated non-financial business and profession ("DNFBP"), or another regulated entity**, as defined in UAE regulation and guidance; and
4. Considers country risk information when determining in which countries a third party meeting the above conditions can be based.

Unlike **outsourcing** relationships, in which an LFI engages a third-party provider to perform certain control functions on the LFI's behalf and in conformity with the LFI's AML/CFT policies and procedures,[7] **third-party reliance** relationships typically involve an LFI relying the customer identification and verification measures already undertaken by another regulated entity on an existing customer of that entity in accordance with the entity's own AML/CFT policies and procedures. In reliance relationships, that is, the third party will usually already have a business relationship with the customer that is independent of the relationship to be formed by the customer with the relying institution. The third party will therefore have onboarded the customer in accordance with its own AML/CFT policies and procedures. In a typical reliance scenario, a prospective customer will assert identity to the relying LFI using a digital ID system, at which point the third party will be prompted by the system to authenticate the person's identity and (per condition 1 above) immediately provide relevant identification and verification information to the relying LFI. In all reliance relationships, the ultimate responsibility for CDD measures remains with the LFI that relies on the third party.

4. Risks and Challenges Presented by Digital ID Systems

Like any ID system, the reliability of digital ID systems depends on the strength of the 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, reliability can be undermined by identity theft and source documents that can be easily forged or tampered with. Some types of fraud, such as "massive attack" frauds, may be less likely to occur in-person or in processes requiring human intervention. While digital ID systems provide security features that mitigate some issues with paper-based systems, they also increase some risks, such as data loss, data corruption, or misuse of data due to unauthorized access.

Digital ID systems also present a variety of technical challenges and risks due to their reliance on open communications networks (i.e., the Internet) for identity proofing and authentication, and the involvement of multiple parties (such as the IDSP, the customer, and the relying LFI), which together can present multiple opportunities for cyberattacks. Without careful consideration of relevant risk factors and the implementation of appropriate, technology-based safeguards and effective governance and accountability measures to address these risks, criminals, money launderers, terrorists, and other illicit actors may be able to abuse digital ID systems to create false identities or exploit (e.g., hack or spoof) authenticators linked to a legitimate identity.

The discussion below covers both identity proofing and enrollment risks and authentication risks. Risks at the identity proofing stage include the risk that proofing and enrollment processes result in digital IDs that are fake—that is, obtained under false pretenses through an intentionally malicious act—and can be used to facilitate illicit activities. These risks are mitigated by having an appropriate identity assurance level. Risks at the authentication stage include the risk that a legitimately issued digital ID has been compromised and that its credentials or authenticators are under the control of an unauthorized person. These risks are mitigated by having an appropriate authentication assurance level. This section concludes with a discussion

[7] See also *Guidance for Financial Institutions adopting Enabling Technologies*, section 3.90 for additional detail related specifically to the outsourcing of biometric activities.

of broader connectivity, cybersecurity, and privacy challenges in the digital space that may impact the integrity or availability of digital ID systems to conduct CDD.

4.1. Identity Proofing and Enrollment Risks

This section focuses on threats to the identity proofing and enrollment process presented by cyberattacks, security breaches, and the production and presentation of false identity evidence, either by stealing a real person's identity or by combining real and fake information to create a new identity. The enrollment process may also be threatened through the compromise of, or misconduct by, an IDSP or through the compromise of the broader digital ID infrastructure. The latter type of threat is outside the scope of this Guidance and should be directly addressed by traditional computer security controls (such as intrusion protection, recordkeeping, and independent audits) and by broader governance and organizational requirements and digital ID assurance frameworks and standards.

In certain respects, the risks arising from the presentation of stolen or counterfeit identity evidence can be even greater in digital ID systems, as online counterfeiters and cybercriminals may be able to obtain or produce false identity evidence at far greater scale than illicit actors trading solely in physical documents. **Impersonation** involves a person pretending to have the identity of another genuine person, including by using a stolen document of someone with a similar appearance or by combining stolen identity evidence with counterfeit or forged evidence (as when an imposter places his or her photo onto a stolen passport or ID card). By contrast, a **synthetic ID** is created 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 using a synthetic ID is pretending to be someone who does not exist in the real world, rather than impersonating an existing identity.

For example, criminal groups have been known to produce synthetic digital IDs at large scale by stealing real individuals' identity attributes and other data from online transactions or by hacking Internet databases, and combining these attributes with entirely fake information. The resulting synthetic IDs have been used to obtain credit cards or online loans and to withdraw funds, with the account abandoned shortly thereafter.

The table below sets out these risks and presents some strategies for mitigating threats to the identity proofing and enrollment process, based on the U.S. National Institute of Standards and Technology ("NIST") Digital Identity Guidelines (also incorporated into the FATF's *Guidance on Digital Identity*). FATF further advises regulated entities to utilize safeguards built into digital ID systems to prevent fraud, such as monitoring authentication events to detect systemic misuse of digital IDs to access accounts, including through lost, compromised, stolen, or sold digital ID credentials/authenticators, to feed into suspicious activity monitoring and reporting systems.

Type of Risk	Description	Potential Risk Mitigation Strategy
Falsified identity proofing evidence	An applicant claims an incorrect identity by using a forged driver's license	• IDSP validates physical security features of presented evidence • IDSP 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 verified identity evidence and biometric of applicant against information obtained from issuer or other authoritative source

4.2. Authentication and Identity Lifecycle Management Risks

Risks at the authentication stage involve the possibility of bad actors asserting an individual's legitimate identity to a relying party to open an account or obtain unauthorized access to products, services, and data. Key authentication vulnerabilities include:

- **Credential stuffing** (also referred to as breach replay or list cleaning): a type of cyberattack where stolen account credentials, often from a data breach, are tested for matches on other systems. This type of attack can be successful if the victim has used the same password that was stolen in the data breach for another account.
- **Phishing**: 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 may attempt to trick his or her victim into supplying names, passwords, government ID numbers, or credentials to a seemingly trustworthy source that is in fact controlled by the criminal.
- **Man-in-the-middle** (also known as credential interception): an attack that attempts to achieve the same goal as phishing and can be a tool to commit phishing, but does so by intercepting communications between the victim and the service provider.
- **PIN code capture and replay**: an attack in which a criminal uses a key logger to capture a PIN code entered on a computer keyboard or other device and, without the user noticing, uses the captured PIN to access services (e.g., when a smartcard is present in the reader).

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, as in the case study below.

Misuse of Digital ID by Straw Men

Criminal organizations can purchase digital ID credentials from individuals that enable them to access the individuals' accounts at LFIs or other regulated entities, in effect turning them into digital mules for the organization. The individuals may either already have an account or agree to open one in connection with selling the identity credentials.

In one case highlighted by the FATF, criminal groups opened bank accounts using straw men, who established the account, obtained a digital ID and a security code, and provided their credentials to the criminal group, in exchange for money. In many cases, multiple digital IDs were used on a single mobile phone or tablet. Access to these accounts afforded the criminal groups access to real-time transactions, making it possible for them to quickly transfer money between various accounts. As the FATF notes, the overwhelming majority of digital IDs that are misused by criminal groups are issued on the basis of legitimate identity evidence.

Some of the primary known risks at the authentication stage are associated with specific types of authenticators or authentication processes, including:

- **Multifactor authentication 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 believed to be behind the vast majority of data breaches. MFA solutions, such as SMS one-time codes texted to the subscriber's phone, add another layer of security to passwords and passcodes, but they can also be vulnerable to phishing, subscriber identity module ("SIM") card swapping, mobile device compromise, and other attacks.
    - **Phishing-resistant authenticators**, where at least one factor relies on **public key encryption**, can help combat these vulnerabilities. In public-key encryption, a pair of keys are generated for an entity (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. Examples of phishing-resistant authenticators include authenticators built off public key infrastructure ("PKI") certificates or the Fast Identity Online ("FIDO") Alliance standards.
    - Per the *Guidance for Financial Institutions adopting Enabling Technologies*, LFIs should implement MFA using a biometric factor (discussed immediately below) where possible to authorize high-risk activities (including changes to personal, registration of third-party payee details, high-value funds transfers, and revisions to funds transfer limits) and to protect the integrity of customer account data and transaction details. Moreover, LFIs deploying MFA at login that includes a biometric factor should consider employing phishing-resistant authenticators where at least one factor relies on public key encryption to secure the customer authentication process.
- **Biometric authenticators:** Biophysical authenticators, such as fingerprints and iris scans, are more difficult to defeat than traditional authenticators and are increasingly ubiquitous. Most smart

phones have built-in fingerprint scanners, some have built-in iris scanners, and facial recognition capabilities are built into many personal computer systems and advanced smart phones. Biometric characteristics can be stolen in bulk from central databases, obtained by taking high-resolution photos, lifted from objects the individual touches, or captured with high-resolution images and then spoofed. Currently, however, these types of attacks are difficult and/or highly resource intensive and therefore not scalable. For example, biometric authenticators that require on-device matching cannot be fraudulently used at scale because they require physical access to the device of the customer.

    - Biometrics have a variety of other weaknesses that give rise to *reliability concerns* when used for authentication purposes and have led some technical standards to restrict their use for authentication (although not for identity proofing). Fingerprints may not be read or may be read incorrectly; and facial recognition factors can be rendered unreliable by changes in facial expressions, facial hair, makeup, or 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.

- **Identity life cycle risks:** Poor identity life cycle and access management can, wittingly or unwittingly, compromise the integrity of authenticators and enable unauthorized persons to access and misuse customer accounts, undermining the purpose of customer identification and verification, ongoing due diligence, and transaction monitoring requirements in protecting the financial system from abuse.
- **Compromised MFA workflow bypass:** Attackers have also been known to identify loopholes in MFA protocols, for example by initiating a denial-of-service attack that causes the MFA workflow to break or its security to degrade.
- **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.

4.3. Broader Issues Presented by Digital ID Systems

Beyond specific risks associated with identity proofing/enrollment and authentication, there are a number of broader issues in the digital space that may impact the integrity or availability of digital ID systems to conduct CDD. These include but are not limited to:

- **Connectivity issues:** The lack of a reliable network infrastructure can undermine digital ID systems at particular customer touchpoints or across larger 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. LFIs should consider the resilience of available networks and systems, including the geographic

locations from which customers may be utilizing a digital ID system for authentication, when deciding whether to use a digital ID system for CDD.

- **UAE frameworks for official identity:** The reliability and 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. Such weaknesses in the reliability of documentary identity evidence can have a cascading effect on the risks posed by digital ID systems, and identity theft from online databases can generate similar risks for both digital ID systems and documentary approaches.
    - The Emirates ID utilizes ultraviolet ink, public key infrastructure, and fingerprint biometrics to prevent tampering or counterfeiting of the card.
    - To further mitigate the risks associated with tampering or counterfeiting of official identity documents, LFIs should use the online validation gateway of the Federal Authority for Identity and Citizenship when verifying the Emirates ID card, and should keep a copy of the Emirates ID and its digital verification in their records.[8]
- **Data protection and privacy challenges:** Digital ID involves the collection and processing of PII, potentially including biometrics. As such, digital ID systems are subject to local data protection and privacy ("DPP") requirements, including Federal Decree-Law No .34 of 2021 Concerning the Fight Against Rumors and Cybercrime; Federal Decree-Law No. 46 of 2021 On Electronic Transactions and Trust Services; the Internet Access Management (IAM) policy; relevant Emirate-level requirements such as the Dubai Data Law; and Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data, where relevant.
    - Under the UAE's DPP framework, LFIs and DISPs are not permitted to transfer or store personal data, including digital or physical copies of Emirates IDs, outside of the UAE, except as permitted by Articles 22 and 23 of the Federal Decree-Law No. 45 of 2021.
    - LFIs should also consult the *Principles on Identification for Sustainable Development*, including Principle 8 regarding the protection of personal data and the maintenance of cyber security,[9] as well as guidance from global standard-setting bodies in their respective sub-sectors.
- **Financial exclusion considerations:** Where digital ID systems do not cover all, or most, persons within a jurisdiction, or where they exclude certain populations, they may drive (or at least fail to mitigate) financial exclusion. The mandatory use of a specific digital ID that is not universally available for CDD presents challenges similar to 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 technological 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

[8] See https://ica.gov.ae/en/ica-validation-gateway/.
[9] See https://id4d.worldbank.org/principles. Although developed to support the creation of "good" government-recognized ID systems, FATF's *Guidance on Digital ID* notes that they apply more broadly and can be adopted by both public- and privately-provided and used identity systems and services.

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, as certain biometric modalities have greater failure rates for some vulnerable groups. For example, manual laborers may have worn fingerprints, which 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.
- Special considerations for LFIs related to financial inclusion are discussed in section 5.2 below.

5. Assessing the Reliability and Independence of Digital ID Systems for CDD

Unless otherwise specified,[10] the UAE permits LFIs to adopt digital ID systems of their choosing, provided that they "rely upon technology, adequate governance, processes, and procedures that provide appropriate levels of confidence that the system produces accurate results."[11] This means that there is an appropriate level of confidence (or "assurance," in the FATF's terminology) that the digital ID system works as it is supposed to and produces accurate results. The digital ID system should also be adequately protected against internal or external manipulation or falsification designed to fabricate and credential false identities or authenticate unauthorized users, including by cyberattack or insider malfeasance.

To this end, LFIs should conduct:

- An **assurance level assessment**, through which the LFI can understand the assurance levels that the digital ID system provides based on its technology, architecture, and governance and determine its reliability and independence; and
- An **appropriateness assessment**, through which the LFI can make a risk-based determination—given the digital ID system's assurance levels—of whether the digital ID system is appropriately reliable and independent for CDD in light of potential ML, TF, fraud, and other illicit financing risks.

As explained in greater detail below, these assessments should be performed sequentially. If an LFI cannot assess a digital ID system's assurance level or determines that it is not sufficiently reliable and independent for its purposes, it should not proceed with using the system for CDD unless it can be adequately strengthened or supplemented; in such a case, it is therefore not necessary to perform an appropriateness assessment until assurance concerns have been resolved.

[10] For example, as noted above, when verifying the Emirates ID card, LFIs should use the online validation gateway of the Federal Authority for Identity and Citizenship and keep a copy of the Emirates ID and its digital verification in their records; see https://ica.gov.ae/en/ica-validation-gateway/.
[11] Available at https://www.centralbank.ae/en/cbuae-amlcft; see p. 49.

Both an LFI's assurance assessment of a digital ID system and its determination of the system's appropriateness for CDD given its business and risk profile should be documented—whether as part of the institution's enterprise risk assessment or through a separate process—and updated on a periodic and event-driven basis. LFIs may determine which functional unit or team within the institution is best suited to carry out the assurance and appropriateness assessments; there is no requirement that these assessments be performed by a specific unit, such as an internal audit department.

5.1. Understanding the System's Assurance Levels

Where UAE law, regulation, or supervisory guidance has not mandated or prohibited the use of a specific digital ID system for CDD, LFIs should first determine, for any digital ID system it is considering adopting, the system's assurance levels.[12] In determining the reliability and independence of a given system, LFIs may either:

- Perform the assurance assessment themselves; or
- Obtain audit or certification information on assurance levels from an expert body.

Where an LFI performs the assurance assessment itself, it should conduct appropriate due diligence on the digital ID system provider, including the governance systems in place, and exercise additional caution. An LFI should only use information from an expert body, including another member of the same financial group or an independent third party, if it has a reasonable basis for concluding that the entity accurately applies appropriate, publicly disclosed assurance frameworks and standards.

Digital ID assurance frameworks and technical standards are a set of open source, consensus-driven assurance guidelines and best practices for digital ID systems that have been developed in several jurisdictions and by international organizations and industry bodies, and provide a useful tool for informing an LFI's or expert body's assurance assessment.[13] LFIs are encouraged to consider the reliability of each of the system's main digital ID components separately, as the same degree of reliability may not be required for each component of the digital ID system (identity proofing/enrollment, authentication, or, if applicable, federation), depending on the relevant risk factors and mitigating measures in place.

Digital ID technology and architecture, and digital ID assurance frameworks and standards, are dynamic and evolving. The standards themselves are flexible and outcome-based in order to facilitate innovation. They permit different technologies and architectures to satisfy the requirements for different assurance levels and are framed in ways intended to help make them as future-proof as possible (e.g., by providing a floor, rather than a ceiling, for reliability).

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. 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 or certitude or confidence in the process at issue; a process with a higher assurance level is more reliable,

[12] Where the government of the UAE has mandated a specific digital ID system for CDD, as in the case of verifying the Emirates ID card via the online validation gateway of the Federal Authority for Identity and Citizenship, LFIs may rely on the government's assessment of such system's assurance levels.

[13] See, for example, FATF, *Guidance on Digital Identity*, Appendix D (Digital ID Assurance Framework and Technical Standard-Setting Bodies) and Appendix E (Overview of U.S. and EU Digital Assurance Frameworks and Technical Standards), available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf.

while a process with a lower assurance level presents a greater risk of failure and is less reliable. This Guidance does not require or recommend any particular assurance level; rather, LFIs are expected to perform an assurance assessment and to determine what assurance levels for which processes are appropriate, given their ML, TF, fraud, and other illicit financing risks.

For illustrative purposes only, the following table summarizes and adapts some of the technical requirements from the NIST Digital ID Guidelines[14] for the **identity proofing and enrollment** stage of a digital ID system, which LFIs might leverage in assessing the degree to which a digital ID system is reliable and independent.

Reliability Factor	No Assurance	High Assurance	Very High Assurance
Presence	No requirements	In-person or remote proofing is permitted	Either in-person or supervised[15] remote proofing is required
Resolution	No requirements	Collection of as many identity attributes as necessary to achieve resolution into a single unique identity (i.e., to achieve de-duplication) is required; knowledge-based verification may be used for added confidence	Same as "High"
Evidence	No identity evidence is collected	Evidence of identity attributes is collected based on the **quality** of the evidence (classified as weak, fair, strong, or superior) and the **number** of documents or **quantity** of digital information relied upon	Same as "High," albeit with higher thresholds for evidence quality and quantity; use of biometrics is mandatory (noted below)
Validation	No validation	Each piece of evidence is validated as genuine and accurate against independent and reliable sources	Same as "High"
Verification	No verification	The identity evidence is verified, confirming that the validated identity relates to the individual applicant[16]	Identity evidence is verified by an authorized and trained credential service provider ("CSP") representative

[14] 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. For additional context, see Appendix E of the FATF *Guidance on Digital Identity*.

[15] Supervised remote proofing involves a remote interaction with the applicant that is supervised by an operator in accordance with specified requirements so as to achieve comparable levels of confidence and security to in-person identity proofing. NIST comparability requirements, are provided in Box 19 of Appendix E of the FATF *Guidance on Digital Identity*, at 96.

[16] As noted above, an LFI need not verify the accuracy of every element of identifying information obtained at the collection and resolution stage but should do so for enough information to form a reasonable belief it knows the true identity of the customer.

Address Confirmation	No requirements for address confirmation	Required	Required
Biometric Collection	None	Optional	Mandatory
Security Controls	Not applicable	Moderate Baseline (per NIST Digital ID Guidelines)[17] or equivalent jurisdictional or industry standard	High Baseline (per NIST Digital ID Guidelines)[18] or equivalent jurisdictional or industry standard

Likewise, the NIST Digital ID Guidelines set forth technical requirements for authentication protocols and processes (including credential and authenticator issuance and binding) and authenticator lifecycle management (including revocation in the event of loss or theft, and expiration/re-proofing and re-binding). For illustrative purposes only, the following table describes at a high level of generality some of the NIST requirements for **authentication** at various authentication assurance levels.[19]

Assurance Level	General Requirements
Some Assurance	• This assurance level can be achieved through a wide range of authentication technologies and authenticator types, and information security controls at a *low* baseline • Biometrics alone may be used as a single-factor authenticator at this level
High Assurance	• MFA is required (i.e., either a multi-factor authenticator or two single-factor authenticators), using secure authentication protocols that incorporate specified approved cryptographic techniques, and information security controls at a *moderate* baseline • More stringent requirements are imposed on authenticator types at this level[20] • Biometrics may be used as one authentication factor (something you are), with the device authenticated as a second factor (something you have), but cannot serve as the only authenticator type
Very High Assurance	• Requires MFA that uses both a hardware-based authenticator and an authenticator that provides verifier impersonation resistance, based on proof of

[17] See FATF, Guidance on Digital Identity, pp. 97-98.
[18] See FATF, Guidance on Digital Identity, pp. 97-98.
[19] Appendix E of the FATF *Guidance on Digital Identity* also presents summary of authentication assurance levels under EU Regulation No. 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market.
[20] Under NIST standards, a "High" assurance level permits the use of any of the following multi-factor authenticators: multi-factor OTP device; multi-factor cryptographic software; or multi-factor cryptographic device. When a combination of two single-factor authenticators is used, one authenticator must be a memorized secret authenticator and the other must be possession-based (i.e., "something you have") and use any of the following: look-up secret; out-of-band device; single-factor OTP device; single-factor cryptographic software; or single-factor cryptographic device.

	possession of a key through an approved cryptographic protocol[21] • Claimants prove possession and control of two distinct authentication factors through secure authentication protocols, using approved cryptographic techniques • The authenticators are verifier impersonation resistant, replay resistant, and resist relevant side-channel attacks • When a biometric factor is used, the identity service provider (verifier) makes its own determination that the biometric sensor and subsequent processing meet specified performance requirements • The CSP employs appropriately tailored security controls at a *high* baseline

5.2. Determining Appropriate Usage in Context of Risk

Once the LFI is satisfied that it knows the assurance levels of the digital ID system, it should analyze whether the digital ID system is adequate for the purposes of performing CDD in the context of the relevant illicit financing risks associated with the LFI's customers, products and services, geographic areas of operations, and other relevant factors. Depending on the availability of digital ID systems, LFIs may have the option to select from multiple digital ID systems that have different assurance levels for identity proofing and authentication. In such circumstances, LFIs should match the robustness of the system's identity proofing and/or authentication processes to the type of potential illicit activities and level of ML/TF risks.

In choosing among digital ID systems providing the same assurance level, or selecting among varying levels of identity proofing and/or particular credentials and authenticators offered by a single system, LFIs should consider their specific ML/TF risks as they relate to identity proofing and authentication in selecting an option. LFIs may also have the option to choose appropriate digital ID systems for lower-risk scenarios.

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