What is Digital Identity (ID)?

CFATF Secretariat Research Desk
November 3rd, 2021.

Official Identity is the specification of a unique natural person that is:

- Based on characteristics of the person that establish a person's uniqueness in the population or particular context(s).
- Recognised by a country for regulatory and other official purposes.
- Generally dependent on some form of government-provided or issued registration, documentation or certification that constitutes evidence of core attributes for establishing and verifying official identity

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

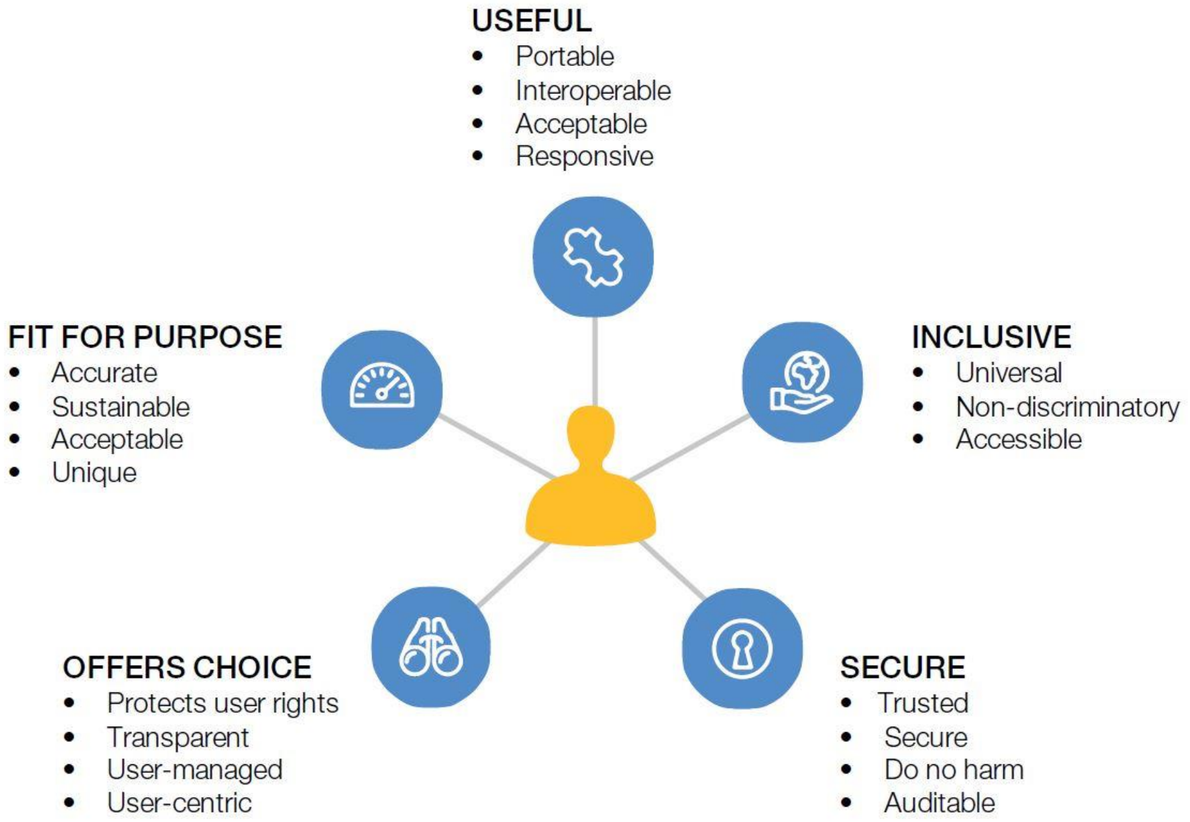
What is Digital Identity (ID)?

- A digital identity can be defined as a set of digital records that verify that an individual is who they say they are and allow them to engage in transactions in the modern, digital world. (1)

- A digital ID can be authenticated remotely over digital channels, which can be done regardless of the ID-issuing entity. Digital ID can also be applied irrespective of the specific technology used to perform digital authentication, which could range from the use of biometric data to passwords, PINs, or smart devices and security tokens. (2)

Source: 1. Commonwealth Secretariat. 2020, "Commonwealth FinTech Toolkit: Helping Governments to Leverage Financial Innovation" https://thecommonwealth.org/sites/default/files/inline/Commonwealth%20Fintech%20Toolkit.pdf; 2. McKinsey Global Institute. 2019. "Digital identification: A key to inclusive growth" https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

Five Elements of a Good Digital ID



Source: World Economic Forum (WEF). 2018, “Identity in a Digital World: A new chapter in the social contract.”

What is a digital ID system?

- The FATF Guidance on Digital ID notes that digital ID systems use electronic means to assert and prove a person's official identity online (digital) and/or in-person environments at various assurance levels. (1)
- Assurance levels measure the level of confidence in the reliability and independence of a digital ID system and its components.
- The World Bank Guide of ID Systems also described digital ID systems are those that use digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication. (2)

Sources: (1) FATF (2020), Guidance on Digital Identity, FATF, Paris, www.fatf-gafi.org/publications/documents/digital-identity-guidance.html; (2) The World Bank (2019), "ID4D Practitioner's Guide:" https://id4d.worldbank.org/guide/types-id-systems

Application of FATF Standards to CDD (R. 10) and digital ID systems

Identification and verification

- R. 10 (a) requires entities to identify the customer and verify that customer's identity, using "reliable, independent source documents, data or information."
- R. 10 does not impose any restrictions on the form (documentary/physical or digital) that identity evidence ,"source documents, information or data" can take.
- Entities must link a customer's verified identity to the individual in some "reliable" way but *how* this is done relies on each jurisdiction's legal framework for CDD.
- The requirement that digital "source documents, data or information" must be "reliable, independent" means that the digital ID system used to conduct CDD relies upon technology, adequate governance, processes and procedures that provide appropriate level of confidence that the system produces accurate results.

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

Application of FATF Standards to CDD (R. 10) and digital ID systems

Risk-Based Approach (RBA)

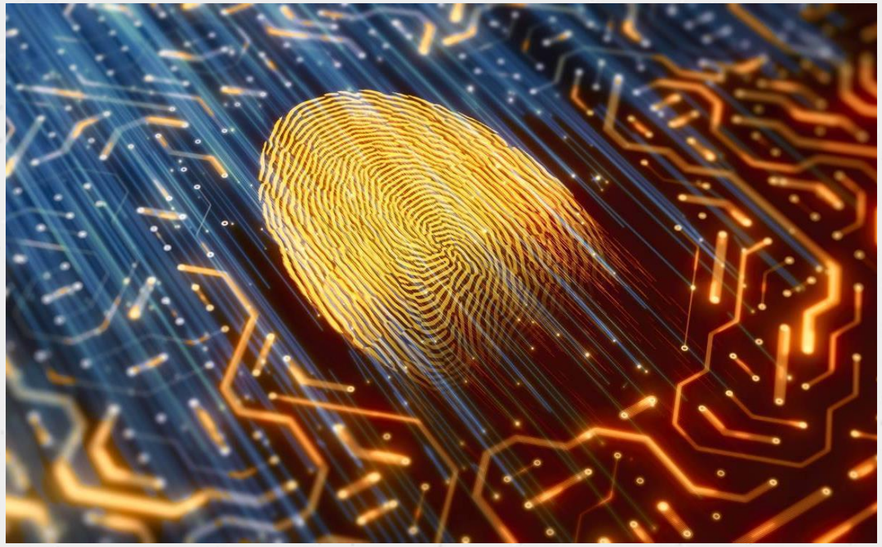
- Regulated entities must apply a RBA to determine the extent of the CDD measures to use for customer identification/verification. These must be commensurate with the type and level of ML/TF risks.

Ongoing due diligence on the business relationship

- R. 10 (d) requires ongoing due diligence and scrutiny of transactions conducted throughout the course of the business relationship.
- Authentication using a digital ID system establishes confidence that an individual is the same person who was identity proofed and issued with the relevant credentials.
- Ongoing digital authentication of the customer's identity links that individual with their financial activity and can strengthen the ability to conduct meaningful ongoing due diligence and transaction monitoring.

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

Benefits of Digital ID Systems for AML/CFT Compliance

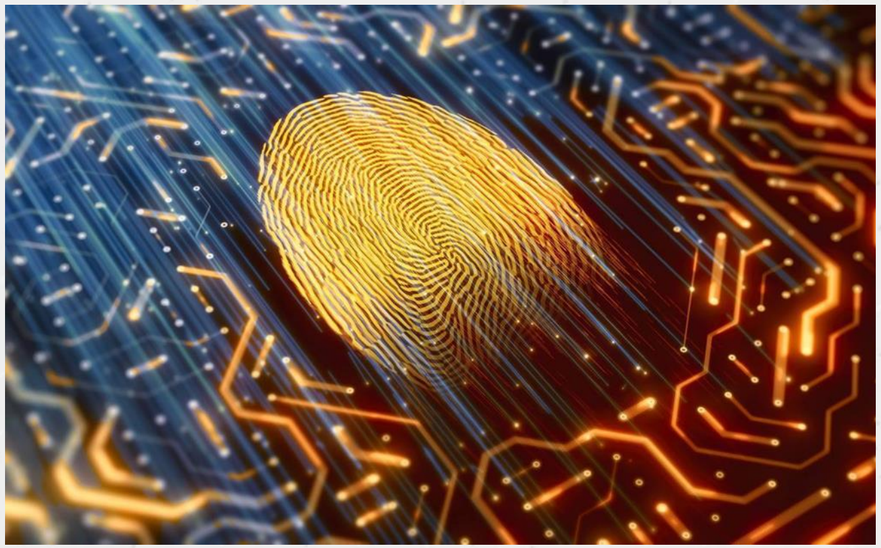


Strengthen Customer Due Diligence (CDD)

- Digital ID systems can improve the reliability, security, privacy, convenience and efficiency of identifying individuals of financial services, to the benefit of customers, regulated entities, and the integrity of the financial sector.
- Minimise weaknesses in human control measures: reduce human error and subjective judgement.
- Improve customer experience and generate cost savings: more efficient, user-friendly experiences for potential customers and lower costs for regulated entities.
- Transaction monitoring: May facilitate the identification and reporting of suspicious transactions, because it helps the regulated entity establish that the person accessing an account.
- Can enable regulated entities to capture additional information to get a detailed understanding of the client's behaviour.

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

Benefits of Digital ID Systems for AML/CFT Compliance



Financial Inclusion

- Allows financially excluded people who lack access to traditional official identity documents and use them to obtain financial services in appropriate low risk situations.
- Digital ID systems can reach excluded populations in remote areas to support secure non-face-to-face identity proofing/enrolment for customer identification/verification.
- Digital ID systems can facilitate government-to-person (G2P) payments, payment of government salaries and pensions and life-saving assistance in humanitarian contexts.

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

Challenges of Digital ID Systems for AML/CFT Compliance

Identity proofing and enrolment risks

- May result in digital ID's that are "fake" (i.e., obtained under false premises through an intentionally malicious act).
- Stolen and/or counterfeit identity information can be used to facilitate illicit activities, such as fraud and theft.
- Identity proofing and/or authenticating individuals over the Internet can create risks related to cyberattacks and potential large-scale identity theft.
- These risks are mitigated by having an appropriate identity assurance level.

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

Challenges of Digital ID Systems for AML/CFT Compliance

Authentication and identity life cycle management risks

- Different types of authenticators/processes may be vulnerable to risks that enable bad actors to use an individual's legitimate identity to a relying party to access goods and services.
- Most authentication vulnerabilities are exploited without the owner's knowledge, but abuse can also involve deliberate sharing of identity credentials for illicit purposes.
- Risks related to AML/CFT efforts include password authenticators, biometric authenticators and unknown risks through changes in technical design.

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

Challenges of Digital ID Systems for AML/CFT Compliance

- Connectivity issues: Lack of reliable infrastructure can undermine the digital ID systems. However, digital ID systems can be designed to support both offline and online transactions.
- Domestic frameworks for official identity: Weaknesses in the reliability of documentary identity evidence that digital ID systems rely on can affect the risks these systems are exposed to.
- Data Protection and Privacy (DPP) Challenges: DPP safeguards are important for reducing the risk of identity theft and cybersecurity risks that could undermine the reliability of the digital ID system.
- The FATF Recommendation 2 propose that AML/CFT and DPP authorities should seek to co-operate and co-ordinate to ensure compatibility of DPP requirements and rules.

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

Thank you!

CFATF Secretariat Research Desk

cfatf@cfatf.org

http://www.cfatf-gafic.org