FATF GUIDANCE ON DIGITAL IDENTITY

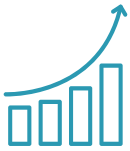
IN BRIEF

March 2020

FATF GUIDANCE ON

DIGITAL IDENTITY

summary



12.7%
growth in digital transactions every year

60%
of world GDP
will be digitised by 2022

In any financial transaction, knowing your customer is essential to ensure that the funds involved are not linked with crime and terrorism. However, in a digital context, traditional verification tools do not apply. The FATF has developed guidance that will help governments, financial institutions, virtual asset service providers and other regulated entities determine whether a digital identity (ID) is appropriate for use for customer due diligence (CDD).

Reliable digital ID can make it easier, cheaper and more secure to identify individuals in the financial sector. It can also help with transaction monitoring requirements and minimise weaknesses in human control measures.

Digital ID systems are evolving rapidly. Digital ID assurance frameworks and standards provide a risk-mitigation framework and help the private sector and governments to determine the level of confidence (or assurance) a digital ID system provides. To determine whether a digital ID is suitable, governments, financial institutions and other stakeholders should:

- Understand the assurance levels of the digital ID system's technology, architecture and governance
- Given its assurance levels, determine whether it is appropriately reliable, independent in light of potential risks that it is used to facilitate illicit finance

With 1.7 billion unbanked adults worldwide and 26% of them citing lack of documentation as the primary barrier, digital ID offers another important benefit. A robust digital ID can allow individuals without a traditional identification to nonetheless have a sound form of identification to access financial services and improve financial inclusion.

This guidance is technology-neutral, and has benefitted from a public consultation with the private sector.

What is digital ID?

Digital ID is the use of technology in asserting and proving identity.

See paragraph 57 to 60 of the Guidance for a more precise definition.

What are some common examples of digital ID?

There are a range of technologies and systems employed around the world. These systems may use digital technology in various ways, for example but not limited to:

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

The cases studies at Appendix B provide an example of some of the systems in place – from India, Peru and Nigeria to Sweden, Singapore and Estonia.

Why did the FATF look at digital ID?

The number of digital transactions are growing by almost 13% a year. By 2022, an estimated 60% of global GDP will be digitised. There is great demand from the private sector to be able to confidently identify people in the digital era. Currently, there are no comprehensive, internationally-agreed standards for developing digital ID. This guidance draws on a number of digital ID assurance frameworks and standards, especially those in place in the United States and the European Union, to draw links between the very technical world of digital ID and those developing policies to combat money laundering and terrorist financing.

Who does the Guidance apply to?

Government authorities and regulated entities. While the FATF Standards are only applicable to governments and 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.

Regulated entities' use of digital identity is voluntary and they have the choice to also use traditional documentary identification.

What are the benefits of digital ID?

Digital ID systems that meet high technology, organisational and governance standards hold great promise for improving the trustworthiness, security, privacy and convenience of identifying natural persons in a wide variety of settings, such as financial services, health, and e-government in the global economy of the digital age. In relation to the FATF Standards, appropriately reliable, independent digital ID systems could:

- facilitate customer identification and verification at on boarding
- support ongoing due diligence and scrutiny of transactions throughout the course of the business relationship,
- facilitate other customer due diligence measures, and
- aid transaction monitoring for the purposes of detecting and reporting suspicious transactions, as well as, general risk management and anti-fraud efforts.

See section IV for further details of the opportunities presented by digital ID.

1.7 Billion

unbanked adults worldwide in 2017
26% because of lack of official documentation

How does digital ID support financial inclusion?

Reliable, independent digital ID systems can contribute to financial inclusion by enabling unserved and underserved people to prove official identity in order to obtain financial services. Bringing more people into the regulated financial sector further reinforces anti-money laundering and counter-terrorist financing (AML/CFT) safeguards.

The Guidance highlights a number of ways digital ID systems can support financial inclusion:

- By harnessing new technologies, governments can take a more flexible, nuanced, and forward-leaning approach in establishing the requirements for proving official identity.

  For example, India's Aadhaar digital ID system has flexible identity evidence requirements in order to achieve comprehensive coverage in a jurisdiction where many people lack basic identity documents, and relies on biometrics to establish uniqueness.)

- The technical standards for digital ID provide some flexibility in processes used to identify and authenticate individuals.

  For example, under the US National Institute of Standards and Technology (NIST) standards, 'trusted referees'—such as village heads, local government authorities, judges/magistrates and employers can vouch for the applicant as a form of identity evidence.

- 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.

  Digital ID systems can enable formerly excluded individuals to develop a more robust digital footprint and risk profile over time that allows them to access a broader range of financial services (see hypothetical example at Box 3).

  See Potential Benefits of Digital ID Systems (Section IV: para 109 – 111); Special considerations for financial inclusion (Section V: para 162 – 171) and relevant case studies (Box - hypothetical example, Box 4 – India, Box 5 – Peru, Box 8 – UNHCR, Box 9 – China).

What are the risks of using digital ID for CDD?

Many risks associated with digital ID systems also exist with the use of documentary IDs. Whereas criminals may have used cash mules, they can now use digital mules to move their money either with or without the knowledge of the owner of the identity. Criminal organisations can purchase digital ID credentials from individuals that enable them to access to the individuals' accounts at regulated entities, in effect turning them into digital mules for the organisation.

The use of the internet for creates risks specific to digital ID systems. In certain respects, the risks arising from the presentation of false evidence (which is either stolen or counterfeit) in digital ID systems, can be actualised at much greater scale. Large scale digital ID systems that do not meet appropriate assurance levels pose cybersecurity risks, including allowing cyberattacks. They also pose major privacy, fraud or other related financial crimes risks, because cybersecurity flaws can result in massive identity theft, compromising individuals' personal data.

The discussion of risks in the Guidance is not intended to discourage the use of reliable, independent digital ID systems—i.e., those that meet appropriate assurance levels (i.e. governance arrangements and technical standards). Nor is it meant to suggest that the use of digital ID systems, especially for customer identification/verification, is necessarily more vulnerable to abuse than traditional documentary methods.

See section IV for further details of the risks and broader contextual issues presented by digital ID.

Are non-face-to-face customer identification and transactions high-risk?

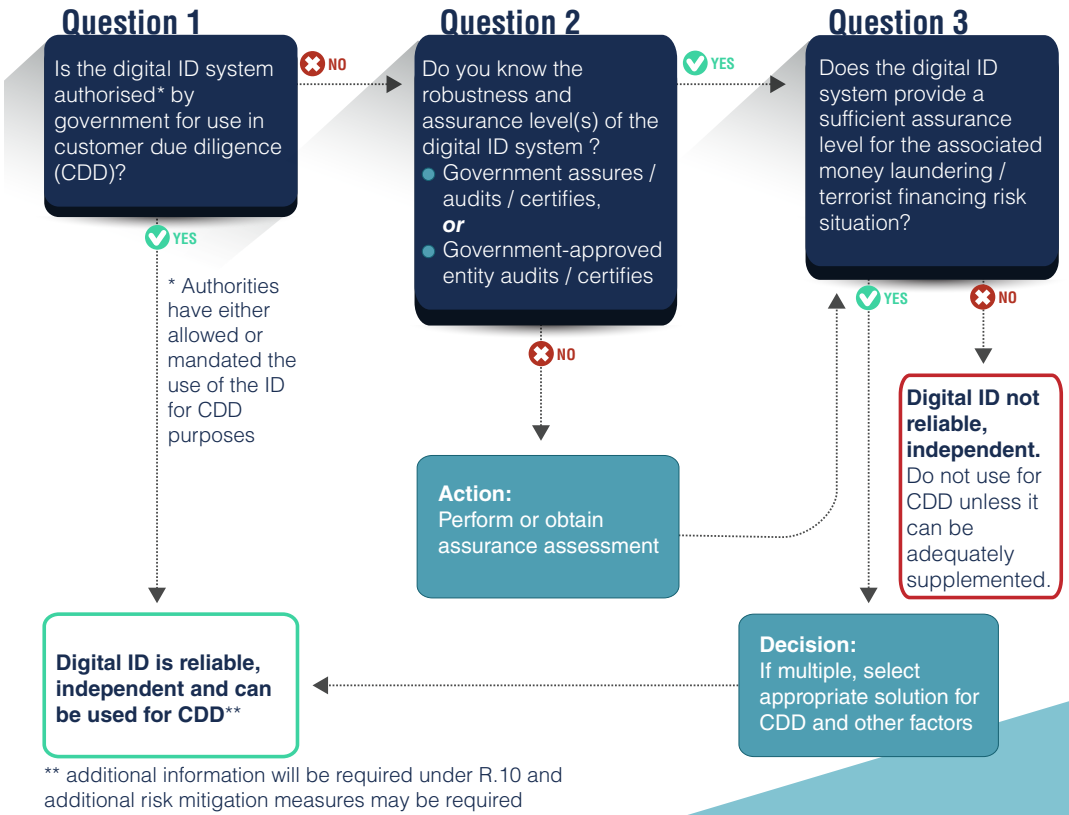
The Guidance clarifies that non-face-to-face customer-identification and transactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place, may present a standard level of risk, and may even be lower-risk.

When is a digital ID suitable for conducting CDD?

The FATF recommends a risk-based approach to applying digital ID for customer identification and verification. The decision process flowchart in the Guidance (below) will help regulated entities navigate this process although this will need to be adapted to each jurisdiction. In terms of AML/CFT considerations, there are two main things to do:

- Identity the assurance levels of the digital ID system based on its technology, architecture and governance – this will help you determine its reliability, independence; and
- Given the digital ID's assurance levels, make a risk-based determination of whether the digital ID system is appropriately reliable, independent in light of the potential ML, TF, fraud, and other illicit financing risks.

See Section V for more information on assessing whether digital ID systems are sufficiently reliable and independent undr a risk-based approach to customer due diligence



** additional information will be required under R.10 and additional risk mitigation measures may be required

What is the FATF's preferred digital ID technology or solution?

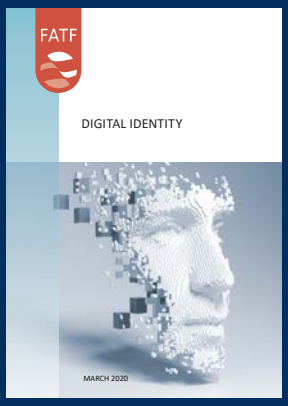
The FATF Standards remain technology-neutral. We highlight examples but do not favour any technology or specific requirements for digital identity to be used for AML/CFT purposes.

How is the FATF responding to data protection and privacy concerns associated with digital ID?

The FATF recommends to governments that they develop an integrated multi-stakeholder approach to understanding opportunities and risks relevant to digital ID and developing regulations and guidance to mitigate those risks. This includes co-operation with relevant authorities to ensure the compatibility of AML/CFT requirements on digital ID systems with Data Protection and Privacy rules (in line with FATF Recommendation 2).

Data protection and privacy 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 notes that the digital ID standards and frameworks relied on in this Guidance include technology, security, governance and resource considerations relevant to data protection and privacy. The Guidance notes that innovative, technology based solutions (for example, decentralised digital identity) are being developed to give the individual more control over how personal data is shared with others and for what purpose to further address privacy and data protection issues.

> *Appendix C includes the Principles on Identification for Sustainable Development, which have been endorsed by over 25 international organisations, development agencies, and other partners and describe how countries can develop digital ID ecosystems that allow them to reap the benefits of these systems while mitigating the risks described in Section IV of the Guidance. Principle 6 of this Guidance refers to "protecting user privacy and control through system design" and Principle 8 to "safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.*



Download the complete

FATF Guidance on **Digital Identity**

from the FATF website.

www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html