FATF

March 2020

Recommendations for **regulated entities**

Taking the money out of crime and terrorism

www.fatf-gafi.org

Recommendations for
regulated entities

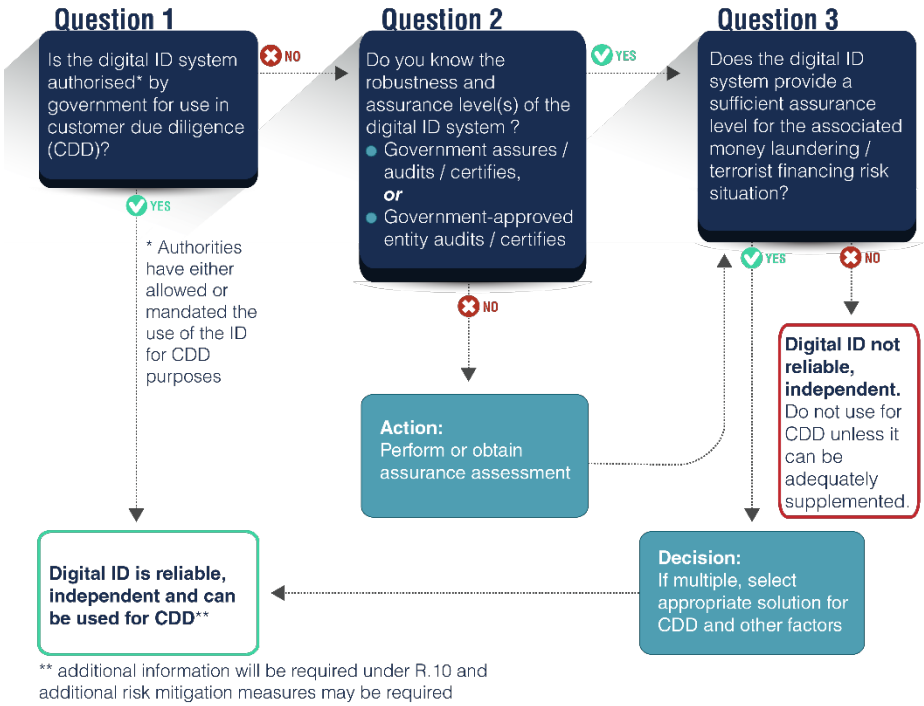
- **Understand the basic components of digital ID systems,** particularly identity proofing and authentication, and how they apply to required CDD elements (see Section II and Appendix A of the Guidance).

- **Take an informed risk-based approach to relying on digital ID** systems for CDD that includes:

    a. understanding the digital ID system's assurance level/s, particularly for identity proofing and authentication, and

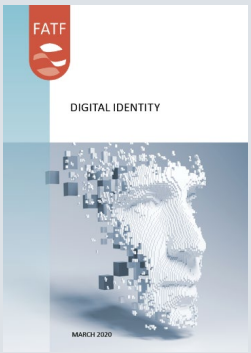
    b. ensuring that the assurance level/s are appropriate for the ML/TF risks associated with the customer, product, jurisdiction, geographic reach, etc.

Decision process for regulated entities



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

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



Recommendations for regulated entities

- **Consider whether digital ID systems with lower assurance levels may be sufficient for simplified due diligence in cases of low ML/TF risk.** For example, where permitted, adopting a tiered CDD approach that leverages digital ID systems with various assurance levels to support financial inclusion.

- If, as a matter of internal policy or practice, **non-face-to-face business relationships or transactions are always classified as high-risk, consider reviewing and revising those policies** to take into account that customer identification/verification measures that rely on reliable, independent digital ID systems, with appropriate risk-mitigation measures in place, may be standard risk, and may even be lower-risk.

- Where relevant, **utilise anti-fraud and cyber-security processes to support digital identity proofing and/or authentication for AML/CFT efforts** (customer identification/verification at on-boarding and ongoing due diligence and transaction monitoring). For example, regulated entities could utilise safeguards built into digital ID systems to prevent fraud (i.e., monitoring authentication events to detect systematic misuse of digital IDs to access accounts, including through lost, compromised, stolen, or sold digital ID credentials/authenticators) to feed into systems to conduct ongoing due diligence on the business relationship and to monitor, detect and report suspicious transactions to authorities.

- **Regulated entities should ensure that they have access to, or have a process for enabling authorities to obtain, the underlying identity information and evidence or digital information needed for identification and verification of individuals.** Regulated entities are encouraged to engage with regulators and policy makers, as well as digital ID service providers, to explore how this can be efficiently and effectively accomplished in a digital ID environment.

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