FATF

March 2020

Recommendations for **government authorities**

Taking the money out of crime and terrorism

www.fatf-gafi.org

Recommendations for
government authorities

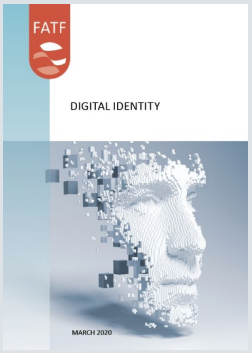
- **Develop clear guidelines or regulations allowing the appropriate, risk-based use of reliable, independent digital ID systems by entities regulated for AML/CFT purposes.** As a starting point, understand the digital ID systems available in the jurisdiction and how they fit into existing requirements or guidance on customer identification and verification and ongoing due diligence (and associated record keeping and third-party reliance requirements).

- **Assess whether existing regulations and guidance on CDD across all relevant authorities accommodate digital ID systems, and revise, as appropriate, in light of the jurisdictional context and the identity ecosystem.** For example, authorities should consider clarifying that non-face-to-face on-boarding may be standard risk, or even low-risk for CDD purposes, when digital ID systems with appropriate assurance levels are used for remote customer identification/verification and authentication.

- **Adopt principles, performance, and/or outcomes-based criteria when establishing the required attributes, evidence and processes for proving official identity for the purposes of CDD.** Given the rapid evolution of digital ID technology, this will help promote responsible innovation and future-proof the regulatory requirements.

- **Adopt policies, regulations, and supervision and examination procedures that enable regulated entities to develop an effective, integrated "risk-based" approach** that leverages data flows, technology architecture and processes across all relevant digital ID, AML-CFT, anti-fraud and general risk management activities to strengthen all risk-related functions.

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

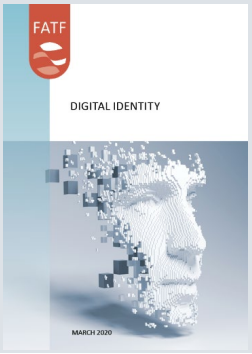


Recommendations for
government authorities

- **Develop an integrated multi-stakeholder approach to understanding opportunities and risks relevant to digital ID** and **developing relevant regulations and guidance to mitigate the risks**. Assess and leverage, where appropriate, existing digital ID assurance frameworks and technical standards adopted by the authorities responsible for identity, cybersecurity/data protection, and privacy (including technology, security, governance and resource considerations) for assessing the assurance levels of digital ID systems for use in CDD. In line with FATF Recommendation 2, co-operate and co-ordinate with relevant authorities to facilitate a comprehensive, coordinated approach to understanding and addressing risks in, the digital ID ecosystem and to ensure the compatibility of AML/CFT requirements on digital ID systems with Data Protection and Privacy rules.

- AML/CFT authorities could consider **adopting mechanisms to enhance dialogue and cooperation with relevant private sector stakeholders**, including regulated entities and digital ID service providers, to help identify key identity-related opportunities, risks and mitigation measures. Mechanisms could include a regulatory 'sandbox' approach to provide a supervised environment to test how digital ID systems interact with national AML/CFT laws and regulations. Authorities could also consider developing mechanisms to promote cross-industry collaboration in identifying and addressing vulnerabilities in existing digital ID systems.

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



Recommendations for government authorities

- **Consider supporting the development and implementation of reliable, independent digital ID systems** by auditing and certifying them against transparent digital ID assurance frameworks and technical standards, or by approving expert bodies to perform these functions. Where authorities do not audit or provide certification for IDSPs themselves, they are encouraged to support assurance testing and certification by appropriate expert bodies [1] so that trustworthy certification is available in the jurisdiction. Authorities are encouraged to support efforts to harmonise digital ID assurance frameworks and standards to develop a common understanding of what constitutes a "reliable, independent" digital ID system.

- **Apply appropriate digital ID assurance frameworks and technical standards when developing and implementing government-provided digital ID.** Authorities should be transparent about how the jurisdiction's digital ID system works and its assurance levels.

- **Encourage a flexible, risk-based approach to using digital ID systems for CDD that supports financial inclusion**. Consider providing guidance on how to use digital ID systems with different assurance levels for identity proofing/enrolment and authentication for tiered CDD.

- **Monitor developments in the digital ID space** with a view to share knowledge, best practices, and to establish legal frameworks at both the domestic and international level that promote responsible innovation and allow for greater flexibility, efficiency and functionality of digital ID systems, both within and across borders.

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