Navigating the digital frontier

A guide to understanding CBUAE's guidance surrounding digital identity systems by Kabir Hastir Kumar of KARM Legal Consultants.

INTRODUCTION

Digital ID systems have seen significant advancements in recent years. These systems use various technologies such as biometrics, blockchain, and cryptography to provide secure and convenient ways for individuals to prove their identity and access services. Financial service players are increasingly leveraging digital ID systems as an efficient, cost-effective and seamless way of onboarding customers and facilitating non-face-to-face business relationships and transactions.

This article provides a synoptic view of the key facets of, and terminologies used in, the Central Bank of UAE's ("**CBUAE**") recently issued 'Guidance for Licensed Financial Institutions on Digital Identification for Customer Due Diligence' ("**Guidance**").

Regulatory impetus

The proliferation of digital customer onboarding channels has prompted regulators to lay down guidelines and regulatory requirements of varying granularity. While some regulators lay down in-depth requirements regarding the capabilities of digital ID applications (e.g., biometrics and MRZ recognition), others permit eKYC with a general overview of compliance expectations.

The Central Bank of Bahrain and the Financial Services Regulatory Authority of Abu Dhabi Global Market both made amendments to their regulations in 2021 and 2022 respectively. The amendments introduced specific requirements for digital onboarding and clarified regulatory expectations for the use of technology in a manner that mitigates inherent risks.

CBUAE's regulatory framework for digital IDs

UAE's regulatory framework for AML has always been tech-agnostic. Given the ubiquity of digital onboarding, and in order to elaborate upon the interplay between digital ID systems and regulatory requirements, the Guidance was issued. It is majorly based upon FATF's 'Guidance on Digital ID'.

Digital ID systems have been broadly defined therein as electronic methods of verifying and proving a person's identity. These systems can facilitate remote transactions and non-face-to-face business interactions. They have two main components;

(a) identity proofing and enrollment, and
(b) authentication and identity lifecycle management.

An optional third component is portability and interoperability mechanisms that allow for digital ID credentials to be used across various entities without the need for additional verification (e.g., in Europe, the eIDAS Regulation enables cross-recognition of digital ID systems, and digital ID wallets are expected shortly).

The subsequent sections of the article dive into the nuances of the Guidance and CBUAE's standards for compliance. This includes the necessary components of a digital ID system and the potential risks that emanate therefrom.

COMPONENTS OF A DIGITAL ID SYSTEM

Identity proofing and enrollment

Identity proofing and enrollment is the first stage of a digital ID system, which is directly relevant to customer identification and verification obligations under Article 8 of Cabinet Decision No. (10) of 2019 ("**Implementing Regulations**"). Identity proofing is made up of three actions:

a. Collection and resolution involves obtaining attributes, evidence and

conducting de-duplication by ensuring that the identity attributes and evidence relate to a unique person (in order to prevent duplicate enrolment). The Implementing Regulations require financial institutions ("FIs") to collect various identity attributes pertaining to natural persons, including, name, nationality and address. Evidence of such attributes can take the form of physical, purely digital or digital representations of physical documents (e.g., Emirates IDs or passports). This is generally accomplished through filling an online form, sending a selfie photo and uploading photos of documents such as passport, Emirates ID, etc.

b. Validation involves establishing the genuineness of attribute evidence and ensuring the accuracy of information such evidence contains. It is the process of checking identity information and evidence against a reliable source to confirm that it is accurate. FIs are required to check for any physical or digital abnormalities in the evidence to determine whether it is genuine or forged. This is often done by thoroughly analysing (manually or with the help of software and online databases) the documents uploaded. Many FIs leverage third party solutions that offer document liveness checks. The Guidance expressly requires FIs to use ICP's online validation gateway, the UAE Pass Application, or other government-supported solutions for validating and verifying Emirates IDs in particular.

c. Verification is the process of confirming that the identity evidence provided is related to the individual being identity-proofed. This can be done through biometric solutions like facial recognition or liveliness detection. This is typically done by comparing the facial features of customers, captured through live selfies, to the photos present on the identity proof.

d. Enrollment is the process of registering the person and establishing their identity account by linking their verified identity to an authenticator controlled or possessed by them (also known as "credentialing"). An authenticator is used to confirm or "authenticate" that the applicant is the

> “Many regulated FIs in the UAE use digital onboarding systems with biometrics and ID proofing functionalities. The use of NFC technology, which extracts information from embedded chips of physical IDs, is a recent development in this space.”

individual to whom a credential was issued and is the actual accountholder. Account passwords and OTPs for mobile phone number or email-based accounts are typically used for this purpose.

Authentication

Authentication is the process of verifying that the person seeking access to an account or service is the same person who has been previously identified and verified. This is done by using various types of authentication factors, such as something you know (e.g., password), something you have (e.g., OTP on mobile devices) or something you are (e.g., biometrics).

The Guidance states that the strength of authentication processes no longer depends on the number and type of factors used. Instead, it is determined by whether the process is secure against common and evolving attacks (e.g., phishing and man-in-the-middle attacks). Multifactor authentication (“MFA”), which uses multiple independent authenticators from at least two different authentication factors, is generally considered secure. Nowadays, MFA is considered as the bare minimum of authentication mechanisms. The Guidance recommends that the authorisation of high-risk activities (such as high value fund transfers) should be subject to MFA which involves a biometric factor.

The Guidance further states that the new norm is to use continuous authentication, using data points like location, device information, typing patterns, and device angle to verify identity throughout the session, instead of particular points in time (e.g., at log-in).

Portability and interoperability mechanisms

Digital ID systems can have a feature that allows for the portability of proof of identity. This means an individual's digital ID credentials can be used across different private sector or government entities without the need to obtain and verify personal information each time. This can potentially save time and resources for the relying parties and minimise the risk of identity theft. The Guidance states that such mechanisms are not a necessary component for digital ID systems.

RISKS ASSOCIATED WITH DIGITAL ID SYSTEMS AND MITIGATION MECHANISMS

The Guidance provides a macro view of the risks that digital ID systems may be subject to, and provides recommendations for mitigating such risks.

Identity proofing and enrollment risks

The Guidance postulates that Digital ID systems are more susceptible to risks from stolen or counterfeit IDs compared to physical IDs. To mitigate such risks, the Guidance refers to some strategies based off the U.S. National Institute of Standards and Technology (“NIST”) Digital Identity Guidelines. These include, inter-alia, validating security features of IDs (i.e., features that prove that the ID is genuine and has been issued by an official authority, such as, holographic imprints, barcodes, QR codes, etc.) and personal info contained therein with issuers of IDs. Biometrics are effective in combatting stolen IDs. Many regulated FIs in the UAE use digital onboarding systems with biometrics and ID proofing functionalities.

The use of NFC technology, which extracts information from embedded chips of physical IDs, is a recent development in this space. A combination of these functionalities has been recommended.

Authentication and identity lifecycle management risks

The authentication stage of digital ID systems, according to the Guidance, is vulnerable to attacks from malicious actors claiming a legitimate identity to gain unauthorised access to products, services, and data. Risks include phishing, credential stuffing (testing stolen credentials for matches on other platforms), man-in-the-middle middle (intercepting communications between victim and service provider), and PIN code capture and replay (keystroke logging to record PIN codes). Further, MFA based on passwords and OTPs can also be vulnerable to a variety of attacks, including, brute-force login attacks, online data breaches, SIM card swapping and mobile device compromise. Biometric authenticators like fingerprints and iris scans are more cumbersome to overcome, but can still be stolen or spoofed. The Guidance recommends using MFA that is based on biometrics along with phishing-resistant authenticators such as public key encryption, to make the authentication process water-tight.

An example of phishing resistant authenticators is Fast Identity Online Alliance standards. Such protocols work by creating a key pair on registration. The private key is retained by the customer's device. On subsequent log-ins, authentication is done by the customer's device proving possession of the private key. Access to private keys is only permissioned after the customer performs a certain action (e.g., entering pin or biometrics).

Broader issues

The Guidance also discusses overarching issues resulting from the inherent use of technology that may have ramifications relating to the integrity or availability of digital ID systems. In particular, it makes reference to data protection and privacy challenges. It suggests that FIs should observe compliance with UAE's local data protection and privacy obligations, including, inter-alia, the Personal Data Protection Law.

ASSESSING THE RELIABILITY AND INDEPENDENCE OF DIGITAL ID

The Guidance re-iterates CBUAE's stance on the permissibility of FIs adopting digital ID systems of their choosing, as long as they are reliable, independent and produce accurate results. To ensure that the system is reliable, FIs must conduct two assessments.

Assurance level assessment

The first assessment is an assurance level assessment, in which the FI can understand the assurance levels that the digital ID system provides based on its technology, architecture, and governance, and determine its reliability and independence. The FI can conduct the assessment themselves or obtain audit or certification from an expert body. When performing an assessment itself, due diligence on the digital ID service provider should be conducted. When relying upon expert bodies, FIs should ensure that the body applies appropriate and publicly disclosed assurance frameworks and standards.

Appropriateness assessment

In the appropriateness assessment, the FI should make a risk-based determination of whether the digital ID system is appropriately reliable and independent for customer due diligence in light of potential money laundering, terrorist financing, fraud and other illicit financing risks associated with the customers, products and services, geographic areas of operations, and other relevant factors.

CONCLUSION

While many FIs were already leveraging digital ID systems that acknowledge FATF's recommendations to a certain extent, the Guidance draws a clear and comprehensive picture on CBUAE's expectations with regard to AML compliance. It serves as a north-star for any FI seeking to onboard individual customers through remote channels and adds to CBUAE's expansive repository of guidance. Given the express recognition of digital ID systems and regulatory certainty offered, FIs may be less apprehensive in deploying such technology, further contributing towards UAE's digital space.

Text by:
KABIR HASTIR KUMAR,
junior associate, KARM Legal Consultants