ST. KITTS BRANCH
FinancialSERVICES
Regulatory Commission

NewsLetter

March 2020
Issue No. 71

DIGITAL IDENTITY

Digital Identity or Digital ID captures an individual or entity's real identity via a network or the internet when used for identification in online connections or transactions via computers, cell phones or other mobile devices.

Digital technology is growing fast and is becoming a convenient way to communicate and transact business as people become more reliant on smart and mobile devices for different reasons. There is still the requirement to identify and verify customers including beneficial owners using reliable independent source documents, data or information in accordance with Recommendation 10 (Customer Due Diligence) of the Financial Action Task Force's (FATF's) Recommendations. In the digital ID context, the requirement that digital "source documents, data or information" must be "reliable and independent" means that the digital ID system being used to conduct customer due diligence (CDD) relies upon technology, adequate governance, processes and procedures that provide appropriate levels of confidence that the system produces accurate results. Essentially, the digital ID system must assist financial service providers with identifying a customer's or beneficial owner's official identity.

In March 2020, the FATF published Guidance to provide an understanding of the use of Digital Identity and how it works in providing a risk based approach to conducting CDD in accordance with international standards. This newsletter summarizes the information outlined in this Guidance.

> **"Verification"** is part of identity proofing and involves confirming that the validated identity relates to the individual (applicant) being identity-proofed or verified.—FATF

Official Identity

Determining one's identity is fundamental to the CDD requirements of Recommendation 10 of the FATF Recommendations. In order to verify a customer prior to any business relationship, the official identity must be determined. An official identity is specific to a natural person and is based on characteristics (attributes or identifiers) that would establish a person's uniqueness in the population or in a particular context. This official identity is recognized by the state for regulatory and other official purposes (eg. opening a bank account within a financial institution).

Proof of Official Identity

When establishing a business relationship with a regulated entity, the individual's proof of identity must be obtained. The proof of identify must constitute evidence of core attributes (full name, date and place of birth and nationality) to establish and verify official identity. Paragraph 76 of the Financial Services (Implementation of Industry Standards) Regulations, No. 51 of 2011 outlines the personal information which should be collected to verify official identity. Additionally, paragraphs 77—78 of the FSR list the acceptable documents which should be collected as evidence of the official identity. Presently, these are the verification procedures generally used to conduct CDD in a physical (documentary) format.

In the case of digital ID systems, electronic means are used to prove an individual's official identity online and/or in-person environments.

> "**Digital ID systems"** are systems that cover the process of identity proofing/enrolment and authentication. Identity proofing and enrolment can be either digital or physical (documentary), or a combination, but binding, credentialing, authentication, and portability/federation must be digital.—FATF

Digital ID systems may use digital technologies in various ways such as:

⇒ 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

⇒ Biometrics to help identify and/or authenticate individuals, and

⇒ Digital application program interfaces (APIs), platforms and protocols that facilitate online identification/ verification and authentication of identity.

Why Digital Identity?

It can be said that anyone who has initiated online activity may have also started their digital ID. One's digital ID may be patched together from several online services and networks used. Online activities can relate to a person's profession, socialization or personal transactions; hence digital ID can be created from any combination of these. You may begin establishing your digital ID by simply signing up for online banking or using a mobile app for a financial institution. For some, this presents no issues; for others, however, such realisation of mixing the different spheres of their lives can come as quite a surprise. Being aware of the possibilities as well as the implications of what it means to 'be online' is therefore critical. This underscores the importance of authenticity and security of electronic data.

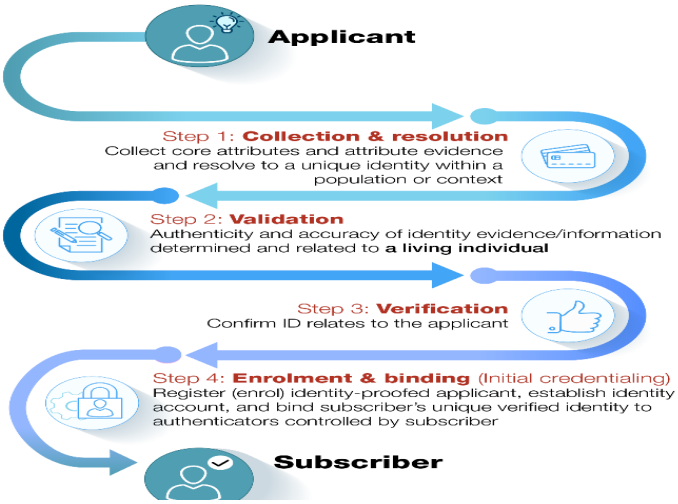
Components of Digital ID systems

Digital ID systems involve three (3) components: two (2) essential and one (1) optional.

Identity proofing and enrolment (with initial binding/credentialing)

The question is: ***Who are you?*** This essential component is directly linked to the verification requirements of Recommendation 10. Figure 1 below illustrates the verification process (identity proofing and enrolment) from the collection of identity attributes (eg. uploading a copy of passport) to establishing an identity account using authenticators (eg. password).

Figure 1



Authentication and identity lifestyle management

This component answers the question: ***Are you the person who has been identified and verified?*** Authentication determines whether the same person accessing the account is the same person whose identity was verified and subsequently enrolled. The process further confirms that this is the person who continues to use the enrolled identity (account). There are three (3) factors which are used to authenticate a person:

⇒ Ownership factors: Something the person possesses

⇒ Knowledge factors: Information the person knows

⇒ Inherent factors: Characteristics of the person

Figure 2 below outlines examples of each factor of authentication.

Figure 2

Recommendation 10 requires regulated entities to conduct ongoing due diligence of its customers during the business relationship. The authentication component can be used for ongoing monitoring as it provides reasonable assurance that the same person who established the identity under the verification procedures is also continuously using the account. It also allows transactions to be digitally tracked during the course of the account's existence. The regulated entities can also use authentication to detect fraud and any misuse of the identity or account.

Components of Digital ID systems (cont'd)

Identity lifestyle management involves any actions taken in response to events that occur during the lifecycle of the account which may affect the use, security and trustworthiness of authenticators. For example, an account may be blocked for numerous use of an incorrect password or theft.

Portability and interoperability mechanisms

This component is optional and allows for the use of a portable identity. It means that an individual's digital ID can be used to establish new business relationships at a unrelated regulated entity. The portability component must be supported by appropriate digital ID architecture and protocols which can be achieved by *federation*.

> "**Federation** refers to the use of federated digital architecture and assertion protocols to convey identity and authentication information across a set of networked systems.—FATF

Risk Based CDD

Recommendation 10 requires regulated entities to apply a risk based approach to determine the level of CDD measures to be applied. The key aspect of digital ID, and in some cases attraction, is the element of *non-face-to-face*. Generally, *non-face-to-face* business and transactions are considered **high risk**. In order to reduce the risk associated with *non-face-to-face* transactions, jurisdictions must develop digital ID assurance frameworks with high 'assurance levels' or 'levels of assurance'.

> **Assurance levels or levels of assurance:** refers to the level of trustworthiness, or confidence in the reliability of each of the three components of the digital ID system.—FATF

Jurisdictions should develop technical standards and guidelines relating to identity, information technology security and privacy which are used to establish the digital ID assurance frameworks with appropriate risk mitigation measures and systems. With these digital ID assurance frameworks, the risk associated with *non-face-to-face* transactions would be reduced which may present a standard, or even, a low level of risk.

Benefits of Digital ID systems

Reliable, independent digital ID systems with appropriate levels of assurance can provide the following benefits:

- Minimizes weaknesses in human control measures by reducing the possibility of human error and judgment
- More efficient, user-friendly experiences for customers during on-boarding and while accessing accounts and transactions
- Assist regulated entities in ongoing and transaction monitoring

Challenges and risks of Digital ID systems

- Data breaches and cyber attacks
- Impersonation/false identity and identity theft
- Credential stuffing
- Phishing

Reference:

- *FATF Guidance—Digital Identity, March 2020*