ST. KITTS BRANCH
Financial Services Regulatory Commission

NewsLetter

June 2023
Issue No. 109

What is Digital Identity ?

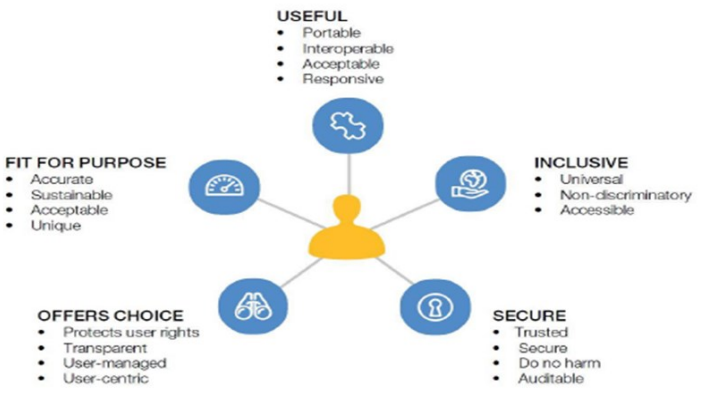
What is a Digital ID System?

According to the Financial Action Task Force (FATF), Digital Identity (ID) Systems use electronic means to prove a person's official identity online at various assurance levels. Assurance levels measure the level of confidence in the reliability and independence of a Digital ID system and its components.

Digital ID Systems use digital technology throughout the identity lifecycle including data capture, validation, storage and transfer; credential management; and identity verification and finally authentication.

What makes a digital ID beneficial to both the user and the institution?

Good Digital ID is identification that is verified and authenticated to a high degree of assurance over digital channels, unique, established with individual consent, protects user privacy and ensures control over personal data.



A Digital ID can be defined as a set of digital records that verify that an individual is who he/she says he/she is.

A Digital ID contains certain unique identifiers that allow systems, services and applications to know who or what they are interacting with. During an in-person transaction, you may show a driver's licence or other government-issued identification to verify your identity. Nonetheless, to verify your identity in the digital world, without human intervention, there needs to be a combination of data and attributes or behaviours that, together, provide a reasonable level of certainty about your authenticity. These attributes may include the following:

- Username
- Password
- Fingerprint or facial scan
- Email address
- Network
- IP address
- Online activities

Benefits of Digital ID Systems for AML/CFT/CPF Compliance

Digital ID systems can improve the reliability, security, privacy, convenience and efficiency of identifying individuals. This includes:

◊ Reducing human errors and subjective judgement;

◊ Improving customer experience and generate cost savings for regulated entities;

◊ Enabling regulated entities to get a better understanding of client behaviour;

◊ Facilitating the identification and reporting of suspicious transactions; and

◊ Reaching populations in remote areas to support secure non– face to face transactions.

Challenges of Digital ID Systems for AML/CFT/CPF Compliance

- Identity proofing and/or authenticating individuals over the Internet can create risks related to cyberattacks and potential large-scale identity theft.
- Risks related to ML/TF/PF include the absence of password and biometric authenticators and unknown risks through changes in technical design and;
- Different types of authenticators/processes may be vulnerable to risks that enable individuals to use another person's legitimate identity to access goods and services.

United Assurance Group of Companies Limited (UAGCL) is one of the Country's leading insurance companies. One of the key reasons behind UAGCL's continuous success is constant innovation and improvement in internal and customer-facing processes. Today, UAGCL is an ecosystem consisting of assurance, insurance and reinsurance companies—all sharing the passion for innovation.

The Challenge

One of the challenges is streamlining AML & KYC Operations while improving onboarding time. While digitalization in the insurance industries open many opportunities for companies and their customers, there is no denying that digitalization opens doors to new types of compliance risks and technological loopholes leading to significant regulatory scrutiny.

This trend was further fueled by restrictions on movement caused by the COVID-19 pandemic. With the onboarding and account opening process being conducted entirely online, financial criminals could use stolen or falsified identity documents or sensitive information to manipulate the system and perform unlawful acts such as account takeovers, money laundering, terrorist financing, etc.

To facilitate the growth of their digital insurance services, the Company was looking for ways to automate and enhance anti-money laundering (AML) and Know Your Customer (KYC) controls in the account opening process, without jeopardizing strict adherence to regulations.

The Solution

Accurate Identity Verification with Digital Footprints

Anti-Money Laundering (AML) and KYC operation teams in insurance services typically rely on numerous data sources to check and clear new customers for matches in sanctions registries, adverse media appearances, political exposure relevance, etc. These tools alone are often not sufficient to screen all relevant AML/KYC aspects, while ensuring speed and scale at onboarding.

As a way to supplement and optimize their existing AML and KYC procedures and validate new customers, UAGCL used Fido's identity scoring algorithm powered by digital footprints. The algorithm combines digital signals from various sources to paint a more complete picture of customer validity and risk level. Fido's powerful identity scoring algorithm can reliably spot irregularities in customer identity by assessing digital signals such as:

Phone number	Email address	Browser detection
Device detection	IP address detection	Associated external service

When collated, these data signals generated a score that UAGCL used to recognize suspicious identities requiring further assessments, thus effectively reducing risks from the identity verification process while complementing standard AML and KYC checks and procedures requested by the regulatory authority.

References

Source: FATF (2020), Guidance on Digital Identity, FATF, Paris, www.fatf-gafi.org/publications/documents/digital-identityguidance.html

Source: www.forgerock.com/what-is-digital-identity