

**Digital Identity and e-KYC Guidelines for the Arab Countries**

Summary



[Date]

[Company name]

[Company address]

**KEY DEFINITIONS**

These definitions are based on the definitions used by World Bank in its paper and the Draft FATF Guidance.

* “Assurance Levels” or “Levels of Assurance” Refers to the level of trustworthiness, or confidence in the reliability of each of the three stages of the Digital ID process.
* “Attributes” A named quality or characteristic inherent in or ascribed to someone or something. In identification systems, common personal identity attributes include name, age, sex, place of birth, address, fingerprints, a photo, a signature, an identity number, date and place of registration, etc.
* “Authentication” Something that establishes that the claimant (customer) who asserts his or her identity to obtain access to the customer’s account is the same person whose identity was obtained, verified, and credentialed during on-boarding.
* “Authenticator” Something the claimant possesses and controls that is used to authenticate (confirm) that the claimant is the individual to whom a credential was issued, and therefore (depending on the strength of the authentication component of the digital identity system) is (to varying degrees of likelihood, specified by the authentication assurance level) the actual subscriber and account holder.
* “Digital ID” A set of electronically captured and stored attributes and/or credentials that uniquely identify a person.
* “Digital ID system” 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 thereof.
* “Identity” A set of attributes that uniquely identify a person.
* “Identification” The process of establishing, determining, or recognizing a person’s identity.
* “Interoperability” Means that an individual’s digital identity credentials can be used to prove official identity for new customer relationships at unrelated private sector or government entities, without their having to obtain and verify personally identifiable information (PII) and conduct customer identification/verification each time.
* “Verification” Means the part of identity proofing and involves confirming that the validated identity relates to the individual (applicant) being identity proofed.

**EXECUTIVE SUMMARY**

Presently, an estimated one billion people globally do not have access to an officially recognizable identity and most of these people reside in developing economies. Absence of a trustworthy identification acts as one of the biggest barriers in accessing a wide range of sociopolitical and economic rights and is a roadblock in achieving the financial inclusion goals. Further, with most transactions moving digital, legacy identification systems (based on physical documents and processes) themselves become a limitation. Technology provides opportunities to reconsider existing systems and build the infrastructure necessary to balance market integrity, financial inclusion and economic growth, while also meeting international financial standards like the UN SDG Goals and FATF recommendations. Financial services can leverage Digital ID systems to increase efficiency, enhance effectiveness and identify new ways of providing services to customers. The analysis is supported by the ‘G20 High-Level Principles of Digital Financial Inclusion’ and the ‘Principles on Identification for Sustainable Development’ developed by the World Bank Group. Digital Identity is a “compilation of electronically captured and stored attributes of a uniquely identifiable persona that can be linked to a physical person.” The attributes can be divided into various categories including birth related information (place of birth, date of birth etc.), descriptive information (height, weight, physical traits etc.), personal identifiers (like social security number) and biometric data (fingerprint, DNA, iris scan etc.). Identity systems may fall into one of the two major categories: foundational (created for general public administration and identification) or functional (created in response to a demand for a particular service or transaction). Specifically, in the case of financial services, irrespective of the nature of identity used as a reliable source of identification, it is necessary that the identity system is legal, unique and digital. The FATF Draft Guidance on Digital Identity (November 2019) identified that to be considered a ‘Digital Identity’ certain components of the identity lifecycle would have to be mandatorily digital. The lifecycle of identity systems includes three major components: TABLE 1- Digital ID Components Component One: Identity proofing and enrolment (with initial binding/credentialing) Process involves collecting, validating and verifying the identity information of an individual, enrolling the individual with an identity account and connecting (or binding) the individual’s unique identity to authenticators possessed and controlled by this person Mandatorily Digital Component Two: Authentication Establishes that the claimant is the same person who has been identity proofed, enrolled, and credentialed (e.g., is the on-boarded customer). Authentication itself could be undertaken utilizing attributes which the person either ‘has’, ‘knows’ or ‘is’. Mandatorily Digital Component Three: Portable Identity Means that an individual’s Digital ID credentials can be used to prove official identity for new customer relationships, without their having to obtain and verify Optional 8 9 Arab Regional Fintech Working Group Digital Identity and e-KYC Guidelines in Arab Countries Arab Regional Fintech Working Group Digital Identity and e-KYC Guidelines in Arab Countries Arab Regional Fintech Working Group – Digital Identity and e-KYC Guidelines in Arab Countries Page 10 of 107 personally identifiable information and conduct customer identification and verification each time Though Digital ID can pave way to eliminate financial exclusion and have a wide range of benefits, it also brings to fore a set of new risks, which are solely related to the technology being used including risks from cybersecurity and data theft. In the light of the risks associated with identity theft, the importance of technical standards and frameworks cannot be harped upon. The FATF Recommendations oblige FIs to conduct CDD using “reliable” information. Therefore, a Digital ID system which complies with the required assurance levels and interoperability standards should be deemed to be a contingent requirement for such information to fulfill the ‘reliability’ test. Various international organizations and agencies are involved in developing standards. However, examples like the eIDAS Regulation are a great example for intergovernmental efforts in this respect. The FATF Recommendations have obligated FIs to adopt a ‘risk-based’ AML principle while undertaking CDD. The ‘risk-based’ principle requires assessment of the risks associated with illicit activities (such as money laundering and terrorist financing). To achieve this objective, FIs are required to implement control measures reasonably deploy corresponding resources to limit or control the effects of such risks, as and when they occur. KYC is an inherent part of the CDD process and may be undertaken through: • Tiered CDD models (with basic CDD, simplified CDD or enhanced CDD being used based on the risks associated with the CDD); and • e-KYC models that allow approved entities to query a national identity system to authenticate or verify customers’ identities and, in some cases, to retrieve basic attributes about them, which attributes may be stored electronically or digitally. Developments in technology have brought about various technology solutions, often referred to as ‘KYC utilities’ which act as a single repository of customer identity data which is utilized for facilitating easier KYC process. By pooling resources, reducing duplicative efforts, and digitizing processes through KYC utilities, FSPs can shorten the time required for identity checks and verification, reduce CDD compliance costs and potentially improve the quality and reliability of customer data. Governments, may either develop such technologies and repositories themselves or consider the use of specialized private sector players as well as the co-operation of financial service providers for developing such a central repository. With the intention of understanding the development of Digital ID and e-KYC programmes among the Arab countries, a questionnaire was circulated to the Central Banks of the Arab Countries. Based on the findings of the survey, it is noted that Digital ID system are still in nascent stages, though there are systems in most countries for a government issued national identity system. Most countries are still following physical KYC structure with face-to-face interactions (or equivalent) and physical documents being the basis for client on-boarding and verification models. Bahrain and UAE appear to be the frontrunners in the implementation of an e-KYC model. Based on the findings of the survey, a range of action items have been proposed to Arab Countries: 10 11 Arab Regional Fintech Working Group Digital Identity and e-KYC Guidelines in Arab Countries Arab Regional Fintech Working Group Digital Identity and e-KYC Guidelines in Arab Countries Arab Regional Fintech Working Group – Digital Identity and e-KYC Guidelines in Arab Countries Page 11 of 107 • Establishment of a unique, legal, interoperable, Digital ID with an ‘identity first’ focus that collects minimal information for creation of an identity • Support the Digital ID framework by adoption of policies, rules and regulations addressing the risks or concerns associated with the use of Digital ID • Establish a ‘risk-based’ CDD regime which balances between the AML/CFT objective and financial inclusion objectives • Prioritize integrity of user data and facilitate processes and procedures for minimalistic sharing of the information during CDD • Create benchmarks and standards for use of any ‘non-government’ backed identity systems • Ensure complete, accurate and better integrated databases that can be utilized for customer identification and verification purposes • Implement a strong governance model to manage the Digital ID and CDD regime • Provide regulatory clarity, remove barriers and foster enabling regulatory environment for innovation which may provide newer solutions for CDD. • Collaborate with regional and international bodies and regulators • Formulate transnational frameworks for interoperability and levels of assurance being implemented across Arab countries.

**Importance of Digital Identity**

Identity is a fundamental requirement for most transactions that occur today. Legacy systems utilized identity systems based on physical documents or processes. Physical identity systems were structured for face-to-face transactions. Some of the inherent characteristics of physical identity systems end up acting as a limitation of their use in the digital world. The major characteristics of physical identity documents are as follows:

* Document based – It effectively depends on access or possession to the physical documents like passport, driver’s license and similar identity documents, even if such documents may not have to be submitted in originals. A proof of identity that is based on possession of physical document may not require demonstration of a link between an individual and the documents, enabling use of an entity’s credentials by a different user.
* Siloed: Identity data is held in discrete places that are not interconnected and cannot be aggregated by the entity nor be connected to other applications.
* Inflexible: Identity attributes are collected based on the standardized set of information required for a purpose and such information may not be easily adapted.

The inherent features of physical identity systems would act as limitations for their use for conducting CDD on a digital platform. These concerns are effectively resolved through the development of Digital ID systems that store identity attributes uniquely in a digital or electronic system. However, Digital ID systems bring with them a separate set of concerns or risks (some of which are elaborated subsequently in this report). If appropriately designed, managed and governed in compliance with national and international standards and best practices Digital ID acts as an efficient and effective system capable of handling complex transactions and increased volumes. Technology provides opportunities to reconsider existing systems and build the infrastructure necessary to balance market integrity, financial inclusion and economic growth, while also meeting international financial standards, including the Basel Committee, FATF, the FSB and the UN SDG. These aspects are discussed below.

The availability of a reliable, digitally authenticated identity system can strongly support financial competitiveness. Some of the key aspects of a Digital ID that may facilitate financial competitiveness is:

* Biometrics-linked Digital ID may make it easier for the unbanked to obtain financial accounts by simplifying the documentation requirements required at account opening;
* It may help the FIs to comply with the customer identification and verification components of CDD.
* It may also provide more cost-effective ways of onboarding new customers, which could potentially be conducted by agents. Agents can use Digital ID to reliably record customer’s identity and proof of validation which can be verified and used to feed the information from the Digital ID system for the required CDD checks.

**The Principles on Identification for Sustainable Development**

* **Principle 1: Inclusion: Universal Coverage and Accessibility:**

Ensuring universal coverage for individuals from birth to death, free from discrimination.

Removing barriers to access and usage and disparities in the availability of information and technology.

There are many different barriers to the adoption of identity systems, for example:

* + Socio-cultural barriers such as the culture of distrust, the loss of anonymity, religious or cultural practices hindering the collection of data;
  + potential economic barriers such as increased transaction costs or the high investment costs associated;
  + technical barriers such as the information technology disparities, existing proprietary standards, the lack of interoperability, inherent drawbacks of the technology itself (example would be concerns surrounding biometric accuracy) and the legacy problems.
  + organizational & procedural barriers such as the lack of internal capacity of some government departments,
  + legal barriers such as the multiplication of legal requirements, of corporate ID policies, and of national laws impacting identity

The identification system would have to be designed with special attention to each of the above barriers. It would have to be ensured that the identity system, would in itself, not act as a tool which results infringement of personal or community rights. Access to civil registration or registration of birth and death free of charge should be made available to all, including non-imposition of any direct fees or any indirect costs associated with obtaining identification supporting documents. In a world where most services and amenities are being made available digitally or electronically, the lack of connectivity or a mere preliminary understanding of technology, would also result in denial of identification service. Nations should direct joint efforts to formalize procedures that support the provision of both online and offline infrastructure to provide “last-mile” access and connectivity, particularly for those in remote locations. Countries where a large section of the population has tertiary education also tend to have a population with higher skill levels - confirming that digital literacy cannot be seen separately from traditional literacy at the country level. In other words, individuals with higher levels of education, especially tertiary education or higher, are much more likely to have advanced digital skills. During the creation of an identity system, special attention is to be given to poverty stricken persons or groups, who may be at risk of exclusion for cultural, political or other reasons (such as women, children, rural populations, ethnic minorities, linguistic and religious groups, migrants, the forcibly displaced, and stateless persons), who may not be able to produce any traditional identity evidence. The Draft FATF Guidance highlights that importance of ‘trusted referees’ in such a scenario. Trusted referees may include notaries, legal guardians, medical professionals, conservators, persons with power of attorney, or some other form of trained and approved or certified individual who may, under national legislations and policies, be authorized to certify the identity of persons.

* **Principle 2: Design: Robust, Secure, Responsive and Sustainable**

Establishing a robust—unique, secure, and accurate—identity.

Creating a platform that is interoperable and responsive to the needs of various users’ responsiveness.

Using open standards and ensuring vendor and technology neutrality.

Protecting user privacy and control through system design.

Planning for financial and operational sustainability without compromising accessibility.

To be treated as a trustworthy identity system, the identity database must act as accurate and up to-date information that may assist in identification and verification. However, to be used as a source for authentication, the database or identity system should also have adequate safeguards against tampering (alteration or other unauthorized changes to data or credentials), identity theft and other errors. Identification providers should work to ensure that identification and authentication services are flexible, scalable, and meet the needs of individuals, public agencies and private entities. The technological robustness, scalability and interoperability of the system are key to facilitate competition and innovation. Technology neutrality and diversity should be fostered to increase flexibility. A system design that is not fit for any purpose or suitable to meet policy and development objectives should be avoided. The long-term fiscal and operational stability of the system should be considered while planning and developing identification systems.

* **Principle 3: Governance: Building Trust by Protecting Privacy and User Rights**

Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.

Establishing clear institutional mandates and accountability.

Enforcing legal and trust frameworks through independent oversight and adjudication of grievances.

**High Level Principles for Digital Financial Inclusion**

The G20 High-Level Principles for Digital Financial Inclusion19 are a major driving force for the adoption of digital approaches to achieve financial inclusion goals in the G-20 member states. It states: “‘Digital financial inclusion refers broadly to the use of digital financial services to advance financial inclusion. It involves the deployment of digital means to reach financially excluded and underserved populations with a range of formal financial services suited to their needs, delivered responsibly at a cost affordable to customers and sustainable for providers.”

Principle 7 of the G-20 Principles suggests that as a part of its action plan towards digital financial inclusion, countries should “facilitate access to digital financial services by developing, or encouraging the development of, customer identity systems, products and services that are accessible, affordable, and verifiable and accommodate multiple needs and risk levels for a risk-based approach to customer due diligence.” This principle echoes the need to implement a Digital ID which is “accessible, affordable and verifiable”.

**What is Digital ID?**

Institute of International Finance defines ‘Digital Identity’ as a “compilation of electronically captured and stored attributes of a uniquely identifiable persona that can be linked to a physical person.” The definition places heavy reliance on “attributes” which may be considered as building blocks of digital identity. Attributes can be divided into various categories including birth related information (place of birth, date of birth etc), descriptive information (height, weight, physical traits etc.), personal identifiers (like social security number) and biometric data (fingerprint, DNA, iris scan etc.) . On the other hand, the Draft FATF Guidance defined Digital ID systems “as 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.” As may be noted from a review of the definition provided by FATF, unlike the definition of Digital ID provided above, the requirement will be surrounding the various stages/ components of the identification process to be digital for an identity system to be considered as a Digital ID. In any event, all organizations agree that the material requirement of any identity system, including a Digital ID system will be to prove the “official identity” of a person.

**Identity System Types:**

1. **Foundational identification system**

An identity system created for general public administration and identification—including civil registries, national IDs, and national population registers. They may serve as the basis for a wide variety of public and private transactions, services and derivative identity credentials. These are, hence, mostly official identification documents and typically providers of such identities are national governments who are interested in giving their citizens a means to prove who they are.

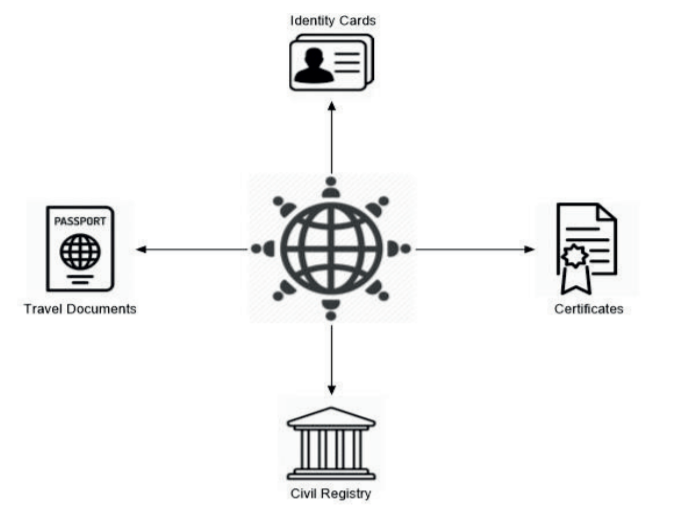


Figure Foundational Identity

1. **Functional identification system**

An identity system created in response to a demand for a particular service or transaction. Though created for a specific purpose, such an identity may be commonly accepted for broader identification purposes but may not always bestow legal identity. The providers of these identity documents may be government or nongovernment players, such as NGOs and private organizations.

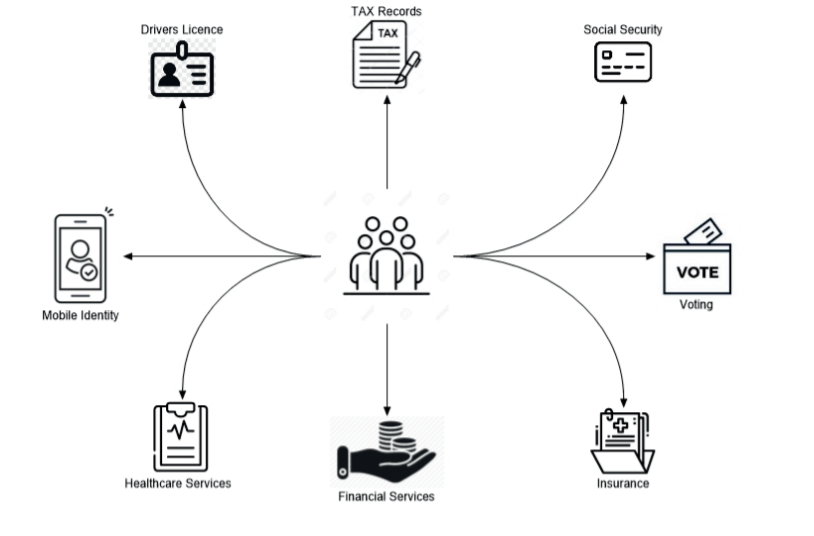


Figure Functional Identity

**Dimensions of Identity System**

Both foundational and functional ID systems vary along multiple dimensions, including the technology they use, whether it establishes a unique model and who they cover in the population.

From a financial services perspective, it is necessary that the identity system is legal, unique and digital. These characteristics are not mutually exclusive, and an identity system can possess one or all of these characteristics to varying degrees.

* **Legal/Official:**  An identity is considered legal if it is recognized as providing proof of legal identity in accordance with a national legislation. ‘Legal Identity’ is defined as “the basic characteristics of an individual's identity. e.g. name, sex, place and date of birth conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth.”
* **Uniqueness:** An identity is considered unique if each individual only has one identity and no two people share the same identity. It also proposes that each identity is claimed only by one person.
* **Digital:** An identity is considered to be digital if an individual’s attributes can be captured and stored electronically and issued on digital credentials that can identify a person. A Digital ID can provide higher levels of security and facilitate the use thereof by the private sector as a platform for providing other services.

Digital ID ecosystems at the national level can be loosely categorized into the following types:

* **Government Issued System:** Under this model, a Digital ID, is issued by the statement and the identity attributes are stored in one or more government owned database(s). UAE’s Emirates ID is a classic example which may be used as the basis for verifying other digital identities, such as banking and mobile phone credentials.
* **Private Sector Initiated and government-endorsed digital identity providers:** In this model a semi-centralized system, individuals are free to choose between multiple trusted identity providers (e.g., banks, mobile operators, etc.) and use these credentials to access a broad range of public and private services via an identity hub or gateway that facilitates authentication across multiple platforms (e.g., Sweden, Finland, UK, Australia).

**Digital ID System Lifecycle**

The lifecycle of identity systems includes three major components:

1. **Component One: Identity proofing and enrolment (with initial binding/credentialing)**

This process involves collecting, validating and verifying the identity information of an individual, enrolling the individual with an identity account and connecting (or binding) the individual’s unique identity to authenticators possessed and controlled by this person.

1. **Component Two: Authentication**

It establishes that the individual seeking access to an account (or other services or resources) - the claimant is the same person who has been identity proofed, enrolled, and credentialed. Authentication itself could be undertaken utilizing attributes which the person either ‘has’ (e.g. cryptographic keys stored in hardware, a OTP in a hardware device, or a software OTP generator installed on a digital device, such as a mobile phone), ‘knows’ (e.g. a shared secret, a personal identification number (PIN), or a response to a pre-selected security question) or ‘is’ (e.g. facial, fingerprint or retinal pattern biometrics).

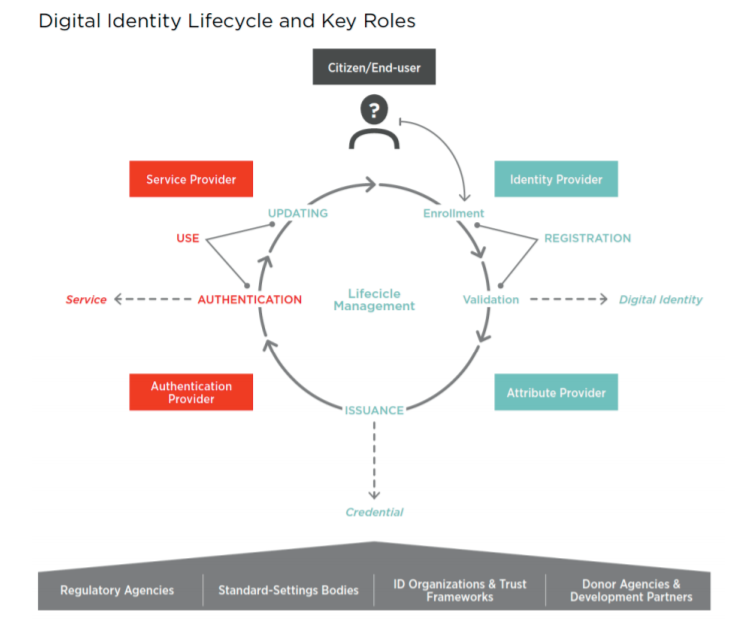


Figure Identity Lifecycle

1. **Component Three: Portability and Interoperability Mechanisms**

Portable identity means that an individual’s digital identity credentials can be used to prove official identity for new customer relationships at unrelated private sector or government entities, without their having to obtain and verify personally identifiable information and conduct customer identification and verification each time. Portability requires developing interoperable digital identification products, systems, and processes. Portability/interoperability can be supported by different Digital ID architecture and protocols.

In accordance with the Draft FATF Guidance, essentially Component One and Component Two would mandatorily be required to be digital for an identity system to be considered as a Digital ID system.

**Technical Standards & System Requirements**

Open standards are a key to solving another major pain point in the introduction of Digital ID systems by regulatory bodies – vendor “lock-in” or technology dependency. Open standards create a framework for developers by defining the components of a system and how they interact with each other. The standards may provide basic parameters for operation of the system without limiting or inhibiting technology providers from protecting their intellectual property and differentiating themselves from the competition, thus continuing to drive innovation. By standardizing what components make up a system and how they communicate, systems become more agile and agnostic. This results in provider and technology neutrality and provides the governments flexibility in choosing between the various technological solutions available. The risk of a wrong decision or choice is significantly reduced because the systems are based on accepted and recognized open standards which are agile and adaptable. Also, governments will be at a lower risk of contractual lock-in because patents and other proprietary issues no longer stand in the way. Ultimately, an open standards approach allows governments to strategically plan and evolve their systems without fear of future compatibility issues – providing a guarantee of consistency and harmonization across government identity ecosystems.

* **Level of Assurance**

When utilizing a technology provider and a related a Digital ID system, it is pertinent to gauge the Level of Assurance provided by the identity system. When a person identifies or authenticates herself using one or multiple identity attributes, the degree of confidence that he/she is who he/she claims to be depends on the degree of security assurance provided and the context in which the information is captured. Higher levels of assurance reduce the risk of a fraudulent identity and increase the security of transactions. However, this can also mean increased the cost to parties concerned including the identity holders and relying agencies indirectly resulting in exclusion. The strength of identification and authentication processes are critical to access control and reducing identity theft.

For identity proofing, the level of assurance depends on the method of identification (e.g., in person vs. remote), the attributes collected, and the degree of certainty with which those attributes are verified (e.g., through crosschecks and deduplication). For authentication, the level of assurance depends on the type of credential(s), the number of authentication factors used (i.e., one vs. multiple), and the cryptographic strength of the transaction.

The eIDAS Regulation defines three different assurance levels (low, substantial and high) depending on the degree of confidence in the claimed or asserted identity of a person.

Table Levels of Assurance -eIDAS

|  |  |  |
| --- | --- | --- |
| Level of Assurance | Identity assurance (identity proofing at registration) | Authentication assurance |
| Low | * Present ID from authoritative source (remote or in-person) | * Single factor (e.g., password or PIN) |
| Substantial | * Present ID (remote or in-person) * ID verification performed by registration authority | * Multi-factor (e.g., mobile phone + PIN) |
| High | * In-person ID proofing at registration authority * ID verification using official government sources and documents | * Multi-factor * Must access private data/keys stored on tamper-resistant hardware token * Cryptographic protection of personally identifying information (PII) |

* **Interoperability of the system**

Interoperability is the ability to transfer and render useful data and other information across systems, applications, or components. Interoperability ensures a common understanding of the exchanged data between systems and across organizations, consequently thereby improving access to eGovernment services, smarter governance and easier access to healthcare, education and other financial inclusion objectives.

The attributes that get recorded as a part of the identity and the method used to capture them have important implications for the trustworthiness of the identity and its interoperability with other domestic and international identity systems. Moreover, a high level of interoperability contributes in reducing operating costs. Implementing the systems based on a unified technical standard would hence be a pertinent requirement for the purposes of creating a universal Digital ID system with a cross-border utility.

**Benefits of Digital ID System**

* Increased use of and access to financial services
* Individuals and institutions can benefit from Digital ID in a range of other interactions – mobile registrations, e-services, employment, healthcare etc.
* Reduce risks of fraud, identity theft and misplacement of documents, and reduce the overall cost of customer verification processes.
* Increased tax collection: a unique identity can be used to de-duplicate tax records and identify individuals who used multiple tax identities to decrease their liabilities.
* Service provider that is connected to the Digital ID system:
  + Improve efficiency: the need to maintain expensive identity and access management systems and support systems such as help desks will be significantly reduced, allowing staff to focus on delivery of services.
  + Minimize the operating costs and reduce the need for many people to verify their identity in person.
  + Improving security and enhancing privacy.

**Risks and challenges in implementing a Digital ID system**

Digital ID tends to be complex and subject to failure to deliver on high expectations. Risks associated with unsuccessful implementation can be mitigated by adopting guidelines that have emerged from the collective experience of Digital ID schemes rollouts around the world. Additionally, in the financial sector, certain risks associated with or related to money laundering or terrorist financing may also have a significant impact on the implementation of a Digital ID system

* **The risk of exclusion**

Demographics, culture and ethical considerations all require attention when defining a Digital ID. An effective Digital ID is inclusive, but there might be certain segments of the population from whom collecting biometric information is difficult, inaccurate or impossible. Such populations might include vulnerable populations (including tribal and ethnic populations or those with unclear migration status) as well as those with low digital literacy or lack of connectivity. Physical features, cultural and religious beliefs, age factors, occupational factors might make fingerprint and iris capture of sufficient detail and quality, problematic. For example, persons working in hard labor occupations or have leprosy likely will be unable to successfully scan their fingerprints. Similarly, changes in age may result in changes in facial features, affecting facial recognition. Legal, procedural, and social barriers to enroll in and use identification systems should be identified and mitigated, with special attention to poor people and groups who may be at risk of exclusion for cultural, political or other reasons (such as women, children, rural populations, ethnic minorities, linguistic and religious groups, migrants, the forcibly displaced, and stateless persons).

* **Political Concerns**

Creating an identity system is a complex political process and issuing legal identity documents involves the complex process of determining who is eligible and has access to particular rights and entitlements. The creation of a national identity system (digital or otherwise) therefore requires a unified vision and approach that can overcome the common fragmentation of identity by ministries, departments, regions, or donor funded projects related to identification.

* **Cost Implications**

Creating a Digital ID system is a costly project that may require extensive investment in building or updating infrastructure and technology.

* **Data Privacy, Protection and Security**

Digital ID systems aim to achieve multiple global development goals at large. Such goals are achievable through empowerment of individuals and facilitating their access to rights, services, and economic opportunities, however – all of which requires proof of identity of such individual(s), all of which raises challenges and risks for digital privacy and data protection.

In identity systems, data privacy means that data should only be accessed, processed, or shared by and with authorized users for pre-determined and specified purposes which have been consented to by the data subject, in advance. Data protection is fundamental to ensuring data privacy - this includes the legal, operational, technical methods/controls for securing information and enforcing rules over access and use. Digital ID involves the collection, safekeeping (as custodian) and processing of an individual’s (data subject’s) personal data. Digital databases that contain identity attributes used for identity proofing may include personally identifiable information and attributes, such as an individual’s name, age, height, date of birth, ID numbers, as well as fingerprints or other biometric information.

In terms of the classification of data, not all types of data merit the same level of protection. Personal data (which is any information relating to an identified or identifiable natural person) and sensitive personal data ( any personal data which is which is particularly sensitive in relation to a data subject) merit specific protection, because of the fact that the processing of such data could create substantial risks to a person’s fundamental rights and freedoms.

Any activity that collects, stores, or processes personal data raises certain risks, including, but not limited to security breaches, unauthorized disclosure, function creep, identity theft, surveillance risk etc. While the above-discussed risks are present in any identity system, Digital ID systems may augment both the risks and the harms beyond traditional, paper-based systems because they enable:

* + Ever-increasing and mass data security breaches through the consolidation of data, while also making such databases more attractive targets.
  + Digitization allows for the easy (or mass) deletion / destruction of data. Without appropriate data safeguards, entire records may disappear
  + Easy copying of digital records, as opposed to the physical copying and subsequent collation of documents.
  + Exposure of “hidden”, but connected personal data: Automatic data processing, as supported through artificial intelligence and machine learning, makes possible discovery of vast arrays of patterns and other information through analytics, by connecting distinct informational pieces about a person from dissimilar sources, or in using metadata about individuals or groups.

Security benefits of digitized systems present various new opportunities and technological means for greater protection. Specifically, Digital ID systems may offer:

* + More accurate identification and authentication in the leveraging of computer processing and advanced technologies, thus offering a higher level of assurance and accuracy than manual, paper-based authentication processes.
  + Improved data integrity through the adoption of adequate data protection measures better assurance of the integrity and use of collected data, in stark contrast to paper-based records systems that can be easily destroyed, damaged, or altered. Furthermore, automated, safeguarded and tamperproof transaction logging provides auditable records of data processing, thereby improving accountability and aiding the addressing of security breaches.
  + Better and more distinctive data privacy guarantees: Digital technology enables new privacy-enhancing features that were previously not possible. Digital technology can help through digital credentials that obscure or selectively present only the data necessary.
  + Increased agency and control: New technologies and design strategies give individuals greater control over their personal data, including access portals that allow users to verify the correctness of their data and monitor the usage of their data, which could automate data breach notifications.

**Conclusion**

In summation, Digital ID systems can offer new possibilities for achieving sustainable development goals if they are inclusive and trustworthy. When designed appropriately, Digital ID systems can be more secure than analogue systems, with stronger, more intelligent, and more easily monitorable data protection measures, which in turn offer better guarantees of data privacy. Taking advantage of these benefits, however, requires purposeful preventative action and an ongoing commitment to identifying and mitigating potential threats. Absence of such officially authenticated identification may pose disadvantages and undermine the financial inclusion of such individuals. The inability to credibly prove one’s identity does not only hinder financial inclusion but may lead to an individual’s political and social exclusion. In the financial services domain, absence of a valid and officially authenticated identification renders inaccessibility to the basic yet most crucial facilities like loans, bank accounts, ATMs etc. National governments play a primary role in enacting measures to facilitate the recording of legal identity for its residents. With increasing digitization, national governments must now focus on implementing robust and digitally enabled identification systems that can increase individual’s access to financial services and more holistic representation in the digital world. Therefore, it is incumbent that countries establish a reliable supervisory model to introduce efficient Digital ID systems. However, such implementation of systems on a nation-wide scale has its own challenges, namely:

* the risk of exclusion
* political concerns
* cost implications
* data privacy, protection and security

The regulators and international agencies may need to recognize and recommend standards which may be adopted and the systems that need to be implemented in this respect. Essentially, for operationalizing financial integrity for FIs, it is not only desirable but, in most cases, mandatory to understand and officially record the identity of their customers. A financial system in which customers are anonymous is one that can easily be abused and corrupted. To foster financial inclusion, tiered and electronic KYC regime may be utilized by the FIs to gain foresight of their customer’s objectives, needs and circumstances or be prepared to say that the client has refused to identify those objectives.