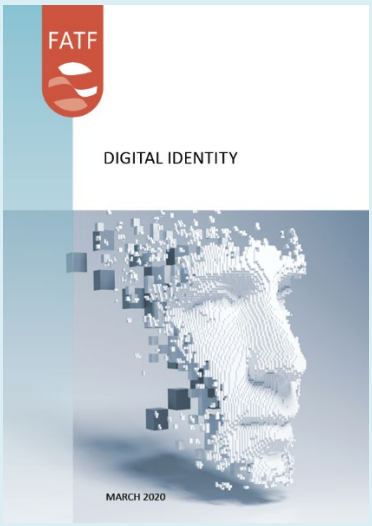
Digital Identity

APPENDIX A:

Description of a Basic Digital Identity System and its participants



Citing reference:

FATF (2020), "Appendix A" in *Guidance on Digital Identity,* FATF, Paris, www.fatf-gafi.org/publications/documents/digital-identity-guidance.html

For more information about the FATF, please visit **www.fatf-gafi.org**

APPENDIX A: DESCRIPTION OF A BASIC DIGITAL IDENTITY SYSTEM AND ITS PARTICIPANTS

This Appendix provides a more detailed explanation of the basic components of a generic digital ID system, expanding on the brief summary set out in Section II. The description is presented at a high level of generality. It provides some examples of technology or process that may be applied for the purposes of illustration for the reader only – it does not encourage or approve the use of any particular identity technology, architecture, or processes, such as biometrics or mobile phone technology. Thus, it applies to a broad range of digital ID systems. This Appendix focuses on the first two components of a digital ID system, because they are most directly relevant to the application of Recommendation 10 requirements for customer identification/verification at on-boarding, and for authenticating customer identity for account access. This appendix is provided to provide context and does not intend to stipulate the technical or organisational requirements for an eligible digital identity within the AML & CTF framework.

Summary of the digital ID process

As reflected in the NIST digital ID standards, the digital ID process involves two basic components and a third optional component:

> **Component One: Identity proofing and enrolment (with initial binding/credentialing)** (essential);
>
> **Component Two: Authentication and identity lifecycle management** (essential); and
>
> **Component Three: Portability and interoperability mechanisms** (optional).

Identity proofing and enrolment may be either digital or documentary, and face-to-face (in-person) or non-face-to-face (remote).[47] In a digital ID system, binding/credentialing, authentication and portability/federation are always, and necessarily, digital.

The terminology used by different jurisdictions and organisations may differ slightly, depending on the system being described. A more detailed description of each of the stages follows.

Component 1: Identity proofing and enrolment

Together, identity proofing and enrolment (with initial binding/ credentialing) constitute the first stage of a digital ID system.

Identity proofing answers the question, "Who are you?" and refers to the process by which an identity service provider (IDSP) collects, validates and verifies information about a person and resolves it to a unique individual within a given population or context.

47 See further explanation of these terms in the Guidance.

The following discussion describes the process flow of identity proofing in three actions: (1) collection/resolution, (2) validation, and (3) verification.

- ***(1) Collection and Resolution*** involves obtaining attributes, collecting attribute evidence; and resolving identity evidence and attributes to a single unique identity within a given population or context(s). The process of resolving identity evidence and attributes to a single unique identity within a given population or context(s) is called **de-duplication.** Some government-provided digital ID solutions include a de-duplication process as part of identity proofing, which may involve checking specific the applicant's biographic attributes (e.g., name, age, and gender); biometrics (e.g., fingerprints, iris scans, or facial recognition images); and government-assigned attributes (e.g., driver's license and/or passport numbers or taxpayer identification number) against the identity system's database of enrolled individuals and their associated attributes and identity evidence to prevent duplicate enrolment.
  - **Attribute evidence** may be either physical (documentary) or purely digital, or a digital representation of physical attribute evidence (e.g., a digital representation of a paper or plastic driver's license). Traditionally, identity evidence has taken a physical form, such as (for natural persons) a government-issued document (preferably, for reliability, bearing a photograph and hologram or similar safeguards)—e.g., a birth certificate; national identity card; driver's license; or passport. Also, traditionally, documentary identity evidence has been physically presented by the claimant to the IDSP. With the development of digital technology, identity evidence may now be generated digitally (or converted from physical to digital form) and stored in electronic databases, allowing the identity evidence to be *obtained remotely* and/or identity attributes and other information to be *remotely verified and validated against a digital database(s).*
  - Attributes may also be inherent—i.e., based on an individual's personal biometric (biological or behavioural) characteristics.[48] Biometrics has rapidly evolved, from static to dynamic, giving rise to distinct types of biometric identity technology, with varying reliability and privacy risks. In order of technological maturity and scale of commercial adoption—as well as the severity of potential privacy threats—digital ID systems may include the use of:
    - Biophysical biometric attributes, such as fingerprints, iris patterns, voiceprints, and facial recognition—all of which are static.
    - Biomechanical biometric attributes, such as keystroke mechanics, are the product of unique interactions of an individual's muscles, skeletal system, and nervous system —all of which are dynamic.

48 It is important to distinguish the use of biometrics as identity attributes from biometrics for identification or deduplication (i.e., as used to establish an individual's identity and uniqueness) versus their use as authenticators. The digital identity technical standards (e.g. NIST standards) support only limited use of biometrics for authentication purposes and impose rigorous requirements and guidelines for this use to address a variety of concerns.

  - Behavioural biometric attributes, based on the new computational social science discipline of social physics, consist of an individual's various patterns of movement and usage in *geospatial temporal data streams*, and include, e.g., an individual's email or text message patterns, mobile phone usage, geolocation patterns, and file access log (including expected log-in channels, geolocation, timing; frequency and type of usage (account balance and activity review vs. transaction).[49]

- The required (core) official identity attributes vary by jurisdiction but could include: full official name; date of birth; place of birth; home address and a unique government-issued identity number. However, governments have considerable flexibility in determining the attributes and evidence required to prove official identity in the jurisdiction. A government's approach to determining required identity attributes may change over time, with the evolution of technology and the related confidence in the trustworthiness of various types of identity attributes.[50] In addition, governments may consider country context and financial inclusion goals in establishing required identity attributes. For example, especially in developing countries with significant itinerate or homeless populations and people without formal addresses, the government may decide to not require address as a core identifier for proving official identity.

- ***(2) Validation*** involves determining that the evidence is genuine (not counterfeit, forged or misappropriated) and the information the evidence contains is accurate by checking the identity information/evidence against an acceptable (authoritative/reliable) source to establish that the information matches reliable, independent source data/records. For instance, the IDSP could (1) check the physical identity evidence (identity document), such as a driver's license and/or passport, or the digital images of the applicant's physical identity evidence, and (a) determine that there are no alterations;; the identification numbers follow standard formats; and the physical and digital security features are valid and intact; and (b) query the government issuing sources for the license and/or passport and validate (confirm) that the information matches.

- ***(3) Verification*** involves confirming that the validated identity relates to *the* individual (applicant) being identity-proofed. For example, the IDSP could ask the applicant to take and send a mobile phone video or photo with other liveness checks; compare the applicant's submitted photo to the photos on the passport identity evidence or the photo on file in the government's passport or license database; and determine they match to a given level of certainty. To

49 See D. Shrier, T. Hardjono and A. Pentland, "Behavioral Biometrics," Chapter 12, *New Solutions for Cybersecurity* (ed. By H. Shrobe; D. Shrier; and A. Pentland (MIT Connection Science and Engineering, MIT Press 2017).

50 For instance, the evolution of Human-Computer Interface (HCI) technology (e.g., combing eye movement and mouse usage) or haptic interfaces may lead some governments eventually to replace reliance on traditional identifiers with reliance on biomechanical attributes. See Section V for a discussion of the evolving role of behavioural biometric attributes in digital identification/verification and authentication.

tie this identity evidence to the actual real-person applicant, the IDSP could then send an enrolment code to the applicant's validated phone number which is tied to the identity; require the applicant to provide the enrolment code to the IDSP; and confirm the submitted enrolment code matches the code the IDSP sent, verifying that the applicant is a real person, in possession and control of the validated phone number. At this point, the applicant has been identity proofed.

Enrolment is the process by which an IDSP registers (enrols) an identity-proofed applicant as a 'subscriber' establishes their identity account. This process authoritatively binds the subscriber's unique verified identity (i.e., the subscriber's attributes) to one or more authenticators possessed and controlled by the subscriber, using an appropriate **binding** protocol. The process of binding the subscriber's identity to authenticator(s) is also referred to as 'credentialing'.

An **authenticator** is something the claimant possess and controls—typically, a cryptographic module, one time code generator or password—that is used to authenticate (confirm) the claimant. More precisely, an **authenticator** is something the claimant possess 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 ID system) is (to varying degrees of likelihood, specified by the authentication assurance level) the actual subscriber and account holder. A **credential** is a physical object or digital structure that authoritatively binds a subscriber's proofed identity, via an identifier/s, to at least one authenticator possessed and controlled by the subscriber. When a digital IDSP (acting as a credential service provider (CSP) issues the authenticator/s and authoritatively binds the authenticator/s to the subscriber's identity, the physical object or digital structure that results is a credential.

Typically, the IDSP issues the authenticator(s) to the subscriber and registers the authenticator(s) in a way that ties them to the subscriber's proofed identity at enrolment. However, the IDSP can also bind the subscriber's account to authenticators provided by the subscriber that are acceptable to the IDSP (acting as a CSP). Moreover, while binding is an essential part of trustworthy enrolment, the IDSP can also bind a subscriber's credentials to additional or alternative authenticators at a later point, as part of identity lifecycle management, discussed below.

Identity proofing can be delivered by a single service provider, or by multiple service providers (see the summary of digital ID system participants, below). In the former case, it is possible that a single entity, process, technique, or technology could conduct each of the identity proofing processes. Similarly, binding the proofed identity during enrolment can be accomplished by a single service provider or by a separate service provider that does not also perform identity proofing.

Figure 5. Identity Proofing and Enrolment

Component 2: Authentication

Authentication answers the question, "***Are you the identified/verified individual?"*** It establishes that the individual seeking to access an account (or other services or resources)--the claimant—is the same person who has been identity proofed, enrolled, and credentialed and has possession and control of the binding credentials and other authenticators, if applicable (e.g., is the on-boarded customer). Authentication can rely on various types of authentication factors and processes, as described below. The trustworthiness of the authentication depends on the type of authentication factors used and the security of the authentication processes.[51]

Authentication factors

Traditionally, there are three basic categories of authentication factors:

- Knowledge factors: Something you know such as: a shared secret (e.g., username, password or passphrase), a personal identification number (PIN), or a response to a pre-selected security question.
- Ownership factors: Something you have, such as: cryptographic keys stored in hardware (e.g., in a mobile phone, tablet, computer, or USB-dongle) or software that the subscriber controls; a one-time password (OTP) generated

[51] When the Guidance describes components of authentication, those are not the same as 'strong customer authentication (SCA)' under the EU's legal framework. What constitutes or does not constitute a valid SCA factor for the purpose of PSDII has to be assessed in accordance with the PSDII and the RTS on SCA+ CSC, rather than FATF guidance.

by a hardware device; or a software OTP generator installed on a digital device, such as a mobile phone.

- Inherence factors: Something you are (biophysical biometrics, such as facial recognition and fingerprint or retinal pattern biometrics; biomechanical biometrics, based on the unique way an individual interacts with digital devices, such as how the individual holds the mobile phone, swipes the screen, keyboard cadence, or uses certain keyboard or gestural shortcuts; and advanced behavioural biometrics).

As discussed below, a given digital ID system will not necessarily use each of these types of factors. For example, although many current digital ID systems use biometrics, it should not be assumed that all digital ID systems do so.

Knowledge authentication factors (something you know) may not actually be secrets. Knowledge-based authentication, in which the claimant is prompted to answer questions that are presumably known only by the claimant, does not constitute an acceptable secret for digital authentication under the NIST standards. Similarly, a biophysical biometric inherence factor does not constitute a secret, and the NIST standards therefore allow the use of biophysical biometrics for authentication only when strongly bound to a physical authenticator.

Importantly, new kinds of technology-based ownership and inherence authenticators (including advanced digital device authenticators, biomechanical biometrics, and **behavioural biometric patterns**), many of which have been or are being developed and deployed primarily for anti-fraud purposes, have significant potential to strengthen digital ID authentication processes for AML/CFT compliance purposes. [52]

Traditionally (and as reflected in the NIST digital ID standards), digital ID authentication is conducted at a particular point in time: when the claimant asserts the customer's/subscriber's identity and seeks authorisation to begin a digital (online session) or in-person interaction to access the customer's account or other financial services or resources. Today, however, many regulated entities, particularly larger financial institutions in developed countries, augment traditional authentication at the beginning of an online interaction with "continuous authentication" solutions that leverage **biomechanical biometrics, behavioural biometric patterns**, and/or dynamic **Transaction Risk Analysis**. Instead of relying on a combination of something the claimant has/knows/is to establish at the beginning of the interaction that the claimant is the on-boarded customer and is in control of the authenticators/credentials issued to that customer, continuous authentication focuses on ensuring that certain data points collected throughout the course of an online interaction, such as geolocation, MAC and IP addresses, typing cadence and mobile device angle—match "what should be expected" during the entire session.

Ways to measure the impact (effectiveness) of continuous authentication technology in mitigating authentication risks have not reached maturity, and the digital ID technical standards, such as the NIST, do not currently address them. The European Commission

[52] As noted in the Guidance itself, digital ID systems also present significant risks (including privacy risks) and opportunities for abuse (e.g., bias or human rights abuse), which are outside the scope of this Guidance but should be effectively addressed.

Delegated Regulation (EU) 2018/389 (RTS on Strong customer authentication and secure communication) under the second Payment Services Directive (PSD2) requires all payment service providers (PSPs) to have transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions for the purpose of implementing the SCA requirements in PSD2 (Art. 2 Regulatory Technical Standards (RTS)). In addition, PSPs that wish to benefit from the "Transaction Risk Analysis" exemption to SCA under Art. 18 RTS need to have in place real time risk monitoring mechanisms in accordance with Art 2 RTS and demonstrate that their fraud rates are below certain thresholds defined in the RTS.[53]

The following discussion applies to static, single-point of time identity authentication methods, addressed by the NIST standards for digital ID.

Authentication processes

Authentication processes are generally categorised by the number and type of authentication factors the process requires, on the understanding that the more factors an authentication process employs, the more robust and trustworthy the authentication system is likely to be. As authentication technology/processes have evolved, that notion is being revised and augmented by a more modern, outcomes-based approach, in which multi-factor authentication is assumed, but the strength of the authentication component does not depend on *how many* factors and types of factors it uses, but rather, on whether its authentication processes are resistant to comprise by commonly executed and evolving attacks, such as phishing and man-in-the-middle attack vectors. (This more holistic, outcomes-based approach should better accommodate the emergence of continuous authentication.)

Types of authentication protocols/processes by increasing levels of security include:

- **Single-factor authentication (1FA)** uses only one authenticator to authenticate a person's identity.
- **Multi-factor authentication (MFA)** uses two or more independent authenticators from at least two different authentication factor categories (knowledge/possession/inherence) to authenticate the claimant's identity. For example, when a claimant seeks to log into an online bank account, using a knowledge-based authenticator (e.g., username and password), the claimant would also need to enter an additional authentication factor from a different authentication factor category in order to successfully access the account. The claimant might use an ownership authentication factor, such as a private key generated in the FIDO-certified authenticator embedded in their mobile phone for this purpose. MFA may be implemented by using either multiple authenticators that in combination present authentication factors from a different categories directly to the verifier, or a single authenticator that provides more than one type of factor, as is the case when an authenticator

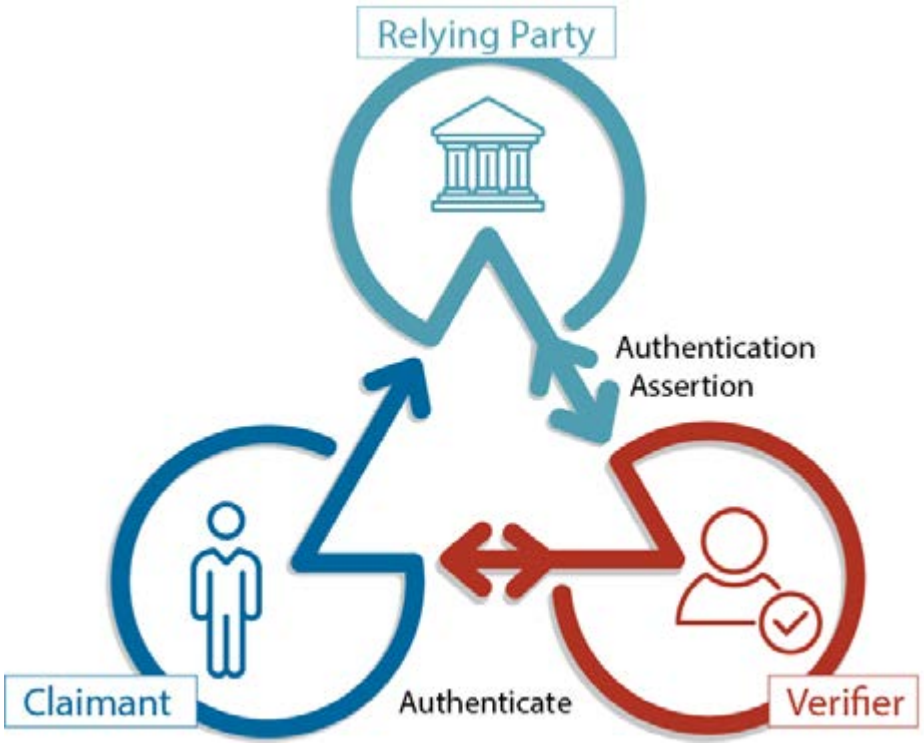
[53] The text of the RTS is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389.

uses one or more factors to protect another type of factor, which in turn is presented directly to the verifier. [54]

The figure below illustrates the authentication process, using the example of a typical financial transaction. In this diagram, an existing customer wants to initiate a financial transaction and must first prove, via one or more authenticators, that he/she is who he/she claims to be—i.e., is the account owner. The customer (claimant) proves his/her possession and control of authenticators by communicating with the IDSP (verifier) over a secure authentication protocol. The verifier confirms the validity of (verifies) the authenticators with the CSP and provides an authentication assertion to the financial institution, which is the RP in the illustrated scenario. NB: the CSP, verifier, and RP may be the same entity (simple, two-party authentication, consisting only of claimant and RP).

Figure 6. Digital authentication

NB: the CSP, verifier, and RP may be the same entity (simple, two-party authentication, consisting only of claimant and RP



54 Under the NIST standards, strong authentication requires either two factor authentication or MFA that uses two or more mutually independent authentication factors of different types, at least one of which is non-reusable and non-replicable and cannot be surreptitiously stolen via the internet. Under the EU PSD2, and as reiterated in the RTS, 'strong customer authentication' is defined as an 'authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data. See Appendix E for a more detailed discussion of the technical standards.

Traditionally, and as reflected in the NIST standards, digital ID authentication is conducted at a particular point in time – when the claimant asserts an identity and seeks authorisation to begin a digital (online session) or in-person interaction and access an account or other financial services. Today, however, many regulated entities, particularly larger financial institutions in developed countries, augment traditional authentication at the beginning of an online interaction with "continuous authentication" solutions that leverage biomechanical biometrics, behavioural biometric patterns and/or "Transaction Risk Analysis".

Identity Lifecycle management

Identity lifecycle management refers to the actions IDSPs should take in response to events that can occur over the lifecycle of a subscriber's authenticator that affect the use, security and trustworthiness of the authenticator. These events could include: issuing and binding authenticators to credentials, either at enrolment or post-enrolment, loss, theft, unauthorised duplication, expiration, and revocation of authenticators and/or credentials.

The attributes associated with an identity may change from year to year. Analytics systems may uncover risk signals suggesting an identity is being used in a manner consistent with fraud or account compromise (as noted previously, in the discussion of "continuous authentication"). Some commercial identity management systems are building in capabilities that analyse whether and how an identity evolves over the course of its lifecycle.

The discussion below uses the function-based term, CSP, in describing the actions that should be taken in response to a specific type of authenticator lifecycle event even though a single IDSP may undertake authenticator lifecycle management, as well as identity proofing and enrolment, and/or authentication.

- **Issuing and recording credentials:** The CSP issues the credential and records and maintains the credential and associated enrolment data in the subscriber's identity account throughout the credential's lifecycle. Typically, the subscriber possesses the credential, but the CSP/verifier may also possess credentials. In all cases, the subscriber necessarily possesses the authenticator/s, which, as discussed above, is used to claim an identity when interacting with a relying party.
- **Binding (a.k.a. credentialing or credential issuance):** Throughout the digital ID lifecycle, the CSP must also maintain a record of all authenticators that are, or have been, associated with the identity account of each of its subscribers, as well as the information required to control authentication attempts. When a CSP binds (i.e., issues credentials that bind) a new authenticator to the subscriber's account post-enrolment, it should require the subscriber to first authenticate at the assurance level (or higher) at which the new authenticator will be used.
- **Compromised Authenticators—Loss, Theft, Damage, Unauthorised Duplication**: If a subscriber loses (or otherwise experiences compromise of) all authenticators of a factor required for MFA, and has been identity proofed at IAL2 or IAL3, the subscriber must repeat the identity proofing process, confirming the binding of the authentication claimant to previously proofed

evidence, before the CSP binds a replacement for the lost authenticator to the subscriber's identity/account. If the subscriber has MFA and loses one authenticator, the CSP should require the claimant to authenticate, using the remaining authentication factors.

- **Expiration and Renewal**: CSPs may issue authenticators that expire and are no longer usable for authentication. The CSP should bind an updated authenticator before an existing authenticator expires, using a process that conforms to the initial authenticator binding process and protocol, and then revoke the expiring authenticator.
- **Revocation (a.k.a. Termination):** CSPs must promptly revoke the binding of authenticators when an identity ceases to exist (e.g., because the subscriber has died or is discovered to be fraudulent); when requested by the subscriber; or when the CSP determines that the subscriber no longer meets its eligibility requirements.

Component Three: Portability and interoperability mechanisms (optional)

Digital ID systems can—but need not--include a component that allows proof of official identity to be portable. Portable identity means that an individual's digital ID 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. Portability requires developing interoperable digital identification products, systems, and processes. Portability/interoperability can be supported by different digital ID architecture and protocols.

Federation is one way of allowing official identity to be portable. Federation refers to the use of federated digital architecture and assertion protocols to convey identity and authentication information across a set of networked systems. Federated identity architecture provides interoperability across separate networks—i.e., it provides the infrastructure that links separate systems into an interoperable network. APIs that do not use federated architecture and assertion protocols are another way of achieving portability.

Federated digital ID architecture and protocols are also being developed and adopted in various jurisdictions to enable interoperability and portable identity across many national-level limited-purpose identity systems.

Trustworthy federation and other approaches to enabling portable private sector digital ID systems could provide many significant benefits. For example, portability/interoperability could potentially save relying parties (e.g., financial institutions and government entities) time and resources in identifying, verifying, and managing customer identities, including for account opening and authorising customer account access. Federation or API-based portability solutions could also potentially save customers the inconvenience of having to prove identity for each unrelated financial institution or government service, and reduce the risk of identity-theft stemming from the repeated exposure of PII.

For example, the interoperability framework under the eIDAS Regulation ensures cross-border cooperation and interoperability of national digital ID systems. The interoperability infrastructure set by the eIDAS framework created technical interfaces relying on eIDAS nodes that play a central role in the interconnection between the relying parties and different national digital ID schemes connected to the nodes.

Participants in a digital ID system

As noted above, digital ID systems can involve different operational models, with different roles for the government and private sector in developing and operating the system and/or providing specific components or sub-components or processes.

The following table describes the basic participants and their roles in a generic digital ID system. Although the table describes each type of participant by its specific function, it should be understood that in government-provided general-purpose or limited-purpose digital ID systems, the government directly conducts (or has another entity(ies) undertake on its behalf) all of the fundamental provider/operator functions. Similarly, for private-sector digital ID systems, a single entity or multiple entities may play all or some of the provider/operator roles.

Table 2. Participants in digital ID systems

IDENTITY SERVICE PROVIDERS	
Identity Service Provider (IDSP)	Generic umbrella term that refers to all of the various types of entities involved in providing and operating the processes and components of a digital ID system. IDSPs provide digital ID systems to users and relying parties. As noted above, a single entity can undertake the functional roles of one or more IDSPs
Identity Verification Service Provider (IVSP)	Entity that conducts identity proofing (validation of evidence and verification linking validated evidence to the applicant).
Identity Provider (IDP)	Entity that manages a subscriber's primary authentication credentials and issues assertions derived from those credentials to RPs. An IDP is usually also the Credential Service Provider (CSP), but may rely on a third party for identity proofing and credentialing.
Credential Service Provider (CSP)	Entity that issues and/or registers authenticators and corresponding electronic credentials (binding the authenticators to the verified identity) to subscribers. The CSP is responsible for maintaining the subscriber's identity credential and all associated enrolment data throughout the credential's lifecycle and for providing information on the credential's status to verifiers. A CSP typically also acts as a Registration Authority (RA) and a Verifier, but may delegate certain enrolment, identity proofing, and credential/authenticator issuance processes to an independent entity, known as a RA or an Identity Manager (IM)—i.e., CSPs can be comprised of multiple independently operated and owned business entities. A CSP may be an independent third-party provider, or may issue credentials for its own use (e.g., large financial institution or a government entity). A CSP may also provide other services, in addition to digital ID services, such as conducting additional CDD)/KYC compliance functions on behalf of a Relying Party (RP).
Registration Authority (RA) (or Identity Manager)	The entity that is responsible for enrolment. The RA registers (enrols) the applicant and the applicant's [credentials and] authenticators after identity proofing.

IDENTITY SERVICE PROVIDERS	
Verifier	Entity that verifies the Claimant's identity to a Relying Party (RP) by confirming the claimant's possession and control of one or more authenticators, using an authentication protocol. The verifier confirms that the authenticators are valid by interacting with the Credential Service Provider (CSP) and provides an assertion over the authentication protocol to the RP. The assertion communicates the results of the authentication process and optionally, information about the subscriber to the RP. To confirm the claimant's possession and control of valid authenticators, the verifier may also need to confirm that the credentials linking the authenticator(s) to the Subscriber's account are valid. The verifier is responsible for providing a mechanism by which the RP can confirm the integrity of the assertion it communicates to the RP. The verifier's functional role is frequently implemented in combination with the CSP, the RP, or both.
USER	
User	The unique, real-life individual who is identity proofed, enrolled, credentialed, and authenticated by a digital ID system and uses it to prove his/her (legal) identity. Users are typically referred to by different names at different stages in a digital ID system, depending on their activities-based role with respect to each of the three components of a digital ID system, as set out below.
Applicant	Person to be identity proofed and enrolled. Applicant refers to the person undergoing the processes of identity proofing and enrolment/binding (credentialing) and applies to the user from the point the user applies for a digital ID and provides supporting identity evidence until the user's identity has been verified and an identity account established and bound to the authenticator(s), at which point the applicant becomes a SUBSCRIBER
Subscriber (a.k.a. Subject)	Person whose identity has been verified and bound to authenticators (credentialed) by a Credential Service Provider (CSP) and who can use the authenticators to prove identity. Subscribers receive an authenticator(s) and a corresponding credential from a CSP and can use the authenticator(s) to prove identity.
Claimant	A Subscriber who asserts ownership of an identity to a RELYING PARTY (RP) and seeks to have it verified, using authentication protocols. A claimant is a person who seeks to prove his/her identity and obtain the rights associated with that identity (e.g., to open or access a financial account).
Relying Party (RP)	Person (natural or legal) that relies on a subscriber's credentials or authenticators, or a verifier's assertion of a claimant's identity, to identify the Subscriber, using an authentication protocol. An RP trusts an identity assertion based on the source, the time of creation, how long the assertion is valid from time of creation, and the corresponding trust framework that governs the policies and processes of CSPs and RPs. The RP is responsible for authenticating the source of an assertion (i.e., the verifier) and for confirming the integrity of the assertion. A RP relies on the results of an authentication protocol to establish confidence in the identity or attributes of a subscriber for establishing a business relationship (account opening) or authorising account access and/or conducting a transaction. RPs may use a subscriber's authenticated identity, the IAL, AAL, and FAL, metadata, providing information about the trustworthiness of each of the digital ID components and processes, and other factors to make a final identity/verification or authorisation decision. Typical RPs include financial institutions and government departments and agencies.
Trust Framework Provider / Trust Authority	Trusted entity that certifies and/or audits IDSP compliance with technical standards (processes and controls) for identity, authentication, and federation assurance levels (IAL, AAL, and FAL). Trust Framework Providers may also be responsible for setting technical standards for these assurance levels. Trust Framework Providers may be government entities (e.g. EU/ eIDAS) or a trusted industry organization, such as Open Identity Exchange (OIX); FIDO (Fast Identity Online) Alliance (specifications and certifications for hardware- mobile- and biometrics-based authenticators that reduce reliance on passwords and protect against phishing, man-in-the-middle and replay attacks using stolen passwords); Kantara; or GSMA (for mobile communications devices).