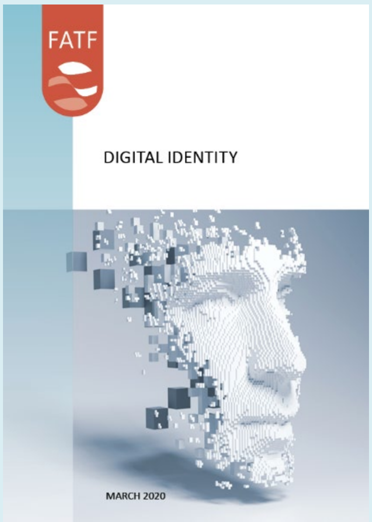
Digital Identity

APPENDIX E:

Overview of US and EU Digital Assurance Frameworks and Technical Standards



Citing reference:

FATF (2020), "Appendix E" 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**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Photocredits coverphoto ©Getty Images

APPENDIX E: OVERVIEW OF US AND EU DIGITAL ASSURANCE FRAMEWORKS AND TECHNICAL STANDARDS

NIST – United States

- Identity Assurance Level (IAL) refers to the reliability of the ID proofing process, as determined by the technical digital ID requirements it requires. The assurance levels for ID proofing, in order of increasing reliability, are IAL1; IAL2; and IAL3;
- Authentication Assurance Level (AAL) refers to the reliability of the authentication process. The assurance levels for authentication (and credential life cycle management), in order of increasing reliability, are AAL1; AAL2; and AAL3; and
- Federation Assurance Level (FAL) (if applicable) refers to the reliability of the federated network—i.e., to the reliability (strength) of an assertion used to communicate authentication results and ID attribute information in a federated environment. The assurance levels for federation, in order of increasing reliability, are FAL1; FAL2; and FAL3.

Identity proofing

Box 18. Leveraging the NIST Digital ID Technical Standards to Evaluate the Reliability of ID Proofing

IAL1—There is no requirement to link the applicant to a specific real-life identity –i.e., there is no assurance that the applicant is who they claim to be, because no ID proofing is required. This means that:

- No identity attributes are required;
- The applicant may, but need not, self-assert identity attributes.
- If any attributes are provided or collected, they are either self-asserted or treated as self-asserted and are not validated or verified.

IAL2—There is high confidence that the identity evidence is genuine; the attribute information it contains is accurate; and that it relates to the applicant.

- Evidence of identity attributes is collected based on the quality of the evidence (weak, fair, strong and superior) and the number of documents or digital information relied upon.
- The identity evidence is validated as genuine.
- The identity evidence and the identity attributes it contains support the real-world existence of the claimed identity, and

- The identity evidence is verified, confirming that the validated identity relates to the individual (applicant), including address confirmation
- Either remote or in-person identity proofing is permitted. NB: In the NIST Digital ID Standards, "In-person" identity proofing includes **supervised remote interactions with the applicant**, as well as interactions where the applicant and identity service provider are physically present in the same location (see discussion below).
- Biometrics are optional
- In instances where an individual cannot meet conventional identity proofing requirements, such as identity evidence requirements, a trusted referee may be used to assist in identity proofing the applicant.
- Evidence of identity attributes must meet specified evidence quality requirements, permitting various combinations of required numbers of pieces of evidence at given strengths, determined by specified characteristics.

IAL3—There is very high confidence that the identity evidence is genuine and accurate; that the identity attributes belong to a real-world person, and that the claimant is that person and is appropriately associated with this real world identity.

- Identity proofing must be in-person; NB: "In-person" identity proofing includes supervised remote interactions with the applicant, as well as interactions where the applicant and identity service provider are physically present in the same location. (See the discussion of Non-Face-to-Face On-boarding in Section III)
- The identity evidence quality requirements are more rigorous
  - Requires more additional identity evidence at higher strength
  - Biometrics are mandatory. Biometric identity attributes and biometric processes are required to detect fraudulent or duplicate enrolments and as a mechanism for binding the verified identity to a credential
- Identity attributes must be verified by an authorised and trained credential service provider (CSP) representative.

Source: United States NIST standards

Table 4. Summary of Identity Proofing Requirements for IAL 1, IAL2, and IAL 3

Requirement	IAL1	IAL2	IAL3
Presence	No Requirements	In-person and unsupervised remote.	In-person and supervised remote.
Resolution	No Requirements	• The minimum attributes necessary to accomplish identity resolution. • KBV may be used for added confidence.	Same as IAL2
Evidence	No identity evidence is collected.	• One piece of SUPERIOR or STRONG evidence depending on strength of original proof and validation occurs with issuing source, OR • Two pieces of STRONG evidence, OR • One piece of STRONG evidence plus two (2) pieces of FAIR evidence.	• Two pieces of SUPERIOR evidence, OR • One piece of SUPERIOR evidence and one piece of STRONG evidence depending on strength of original proof and validation occurs with issuing source, OR • Two pieces of STRONG evidence plus one piece of FAIR evidence.
Validation	No validation	Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented.	Same as IAL2
Verification	No verification	Verified by a process that is able to achieve a strength of STRONG.	Verified by a process that is able to achieve a strength of SUPERIOR.
Address Confirmation	No requirements for address confirmation	Required. Enrollment code sent to any address of record. Notification sent by means different from enrollment code.	Required. Notification of proofing to postal address.
Biometric Collection	No	Optional	Mandatory
Security Controls	N/A	• Moderate Baseline (or equivalent federal or industry standard).	• High Baseline (or equivalent federal or industry standard).

Box 19. In-person identity proofing and enrolment

As noted above, the technical standards permit in-person identity proofing at IAL2 and *require* it at IAL3. Importantly—including with respect to financial inclusion objectives—in-person identity proofing and enrolment can be conducted either by:

- A physical interaction with the applicant, supervised by an operator; or
- A *remote interaction* with the applicant*, supervised by an operator*, based on specified requirements for remote in-person identity proofing, that achieves comparable levels of confidence and security to in-person (physical interaction) identity proofing.

For either type of in-person identity proofing, the technical standards require that (1) The operator must inspect the biometric source (e.g., fingers, face) for presence of non-natural materials as part of the proofing process; (2) the CSP must collect biometrics in a way that ensures that the biometric is collected from the applicant and not another subject and that all biometric performance requirements set forth in the standards are applied.

Comparability Requirements for Supervised Remote In-Person Identity-Proofing and Enrolment

To establish comparability between supervised remote in-person identity proofing and enrollment, and identity-proofing and enrollment where the applicant is in the same physical location as the CSP, the following requirements must be met (in addition to the IAL3 validation and verification requirements, discussed above):

The CSP must:

- Monitor the entire identity proofing session (e.g., by a continuous high-resolution video transmission of the applicant).
- Have a live operator participate remotely with the applicant for the entirety of the identity proofing session. Operators must have undergone a training program to detect potential fraud and to properly perform a virtual in-process proofing session.
- Have all digital verification of evidence (e.g., via chip or wireless technologies) performed by integrated scanners and sensors.
- Ensure that all communications occur over a mutually authenticated protected channel.
- Employ physical tamper detection and resistance features appropriate for the environment in which the identity-proofing session occurs (e.g., a kiosk located in a restricted area or monitored by a trusted individual requires less physical tamper detection than one located in a semi-public area, such as a shopping mall concourse).

The applicant must remain continuously in (cannot depart from) the monitored identity proofing session and all actions taken by the applicant during the identity proofing session must be clearly visible to the remote operator.

Box 20. Authentication and Life Cycle Management

AUTHENTICATION ASSURANCE LEVELS (AALs) set the technical requirements for (1) authentication protocols and processes (including credential and authenticator issuance and binding) and (2) authenticator lifecycle management (including revocation in the event of loss or theft, and expiration/re-proofing and re-binding). Stronger authentication (a higher AAL) requires malicious actors to have better capabilities and expend greater resources to successfully subvert the authentication process. Authentication at higher AALs can effectively reduce the risk of impersonation, replay, and other attacks that can lead to fraudulent claims of a subject's digital ID attacks. AALs include technical requirements for authenticator types; approved cryptography and secure authentication channels (including compromise detection, impersonation and replay resistance requirements); re-authentication of (extended) subscriber sessions; record retention; cyber-security; and privacy. The AALs also establish requirements for binding authenticators to a proofed identity and for actions to be taken in response to events that can occur over the lifecycle of a subscriber's authenticator that that go to the authenticator's trustworthiness after binding, including loss, theft, unauthorized duplication, expiration, and revocation. Many of these requirements are highly technical and incorporate by reference other highly technical information security standards.

The following summary describes at a high level of generality only some of the requirements for authentication at various AALs. See NIST 800-63(b) for a detailed discussion.

- <u>AAL1</u>: Provides *some assurance* that the claimant (the individual asserting (claiming) identity for account authorization) controls an authenticator(s) bound to the subscriber's account. AAL1 permits a wide range of authentication technologies and authenticator types and information security controls at a *low* baseline. MFA is optional). Biometrics alone may be used as a single-factor authenticator at AAL1.

- <u>AAL2</u>: Provides *high confidence* the claimant controls authenticator(s) bound to the customer/subscriber's account. It requires MFA (either a multi-factor authenticator or two single-factor authenticators), using secure authentication protocol(s) that incorporate specified approved cryptographic techniques, and information security controls at a *moderate* baseline. AAL2 imposes more stringent requirements on authenticator types than AAL1.[62] Biometrics may be used as one authentication *factor*

[62] AAL2 permits use of any of the following multi-factor authenticators: multi-factor OTP device; multi-factor cryptographic software; or multi-factor cryptographic device. When a combination of two single-factor authenticators is used, one authenticator must be a memorized secret authenticator and the other must be possession-based (i.e., "something you have") and use any of the following: look-up secret; out-of-band device; single-factor OTP device; single-factor cryptographic software; or single-factor cryptographic device.

(something you are), with the device authenticated as a second factor (something you have), but cannot serve as the only authenticator type.

- AAL3: Provides *very high confidence* that the claimant controls authenticator(s) bound to the subscriber's account. AAL3 requires MFA that uses both a hardware-based authenticator and an authenticator that provides verifier impersonation resistance (VIR), based on proof of possession of a key through an approved cryptographic protocol.[63] Claimants must prove possession and control of two distinct authentication factors through secure authentication protocol(s), using approved cryptographic techniques. The authenticators must be verifier impersonation resistant, replay resistant and resist relevant side-channel attacks. When a biometric factor is used, the identity service provider (verifier) must make its own determination that the biometric sensor and subsequent processing meet specified performance requirements. The CSP must employ appropriately-tailored security controls at a *high* baseline.

eIDAS – European Union

The eIDAS framework provides for three levels of assurance for electronic identification means delivered in the framework of a notified electronic identification scheme: low, substantial and high. Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 sets the minimal security specifications for each of these levels. International standard ISO/IEC 29115 has been taken into account for the specifications and procedures set out in this implementing act as being the principle international standard available in the domain of assurance levels for electronic identification means., the content of the eIDAS Regulation differs from that international standard, in particular in relation to identity proofing and verification requirements, as well as to the way in which the differences between Member State identity arrangements and the existing tools in the EU for the same purpose are taken into account. If, in an EU/EEA country, a public sector body requires, to access one of its online services, an electronic identification with a substantial or high level or assurance, it also has to accept, to access this online service, all the electronic identification means with the same or a superior level of assurance and relating to a notified identification scheme to the Commission and published on the OJ (Official Journal of the European Union). Furthermore, public sector bodies can decide, on a voluntary basis, to recognise electronic identification schemes with a low level of assurance.

[63] The claimant uses a private key stored on the authenticator to prove possession and control of the authenticator. An IDSP (verifier), knowing the claimant's public key through some credential (typically, a public key certificate) uses an approved cryptographic authentication protocol to verify that the claimant has possession and control of the associated private key authenticator, and asserts the person's verified identity to the RP.

For the purposes of eIDAS, the components of a digital ID system are:

- **Enrolment** insures identification uniquely representing either a natural or legal person, or a natural person representing a legal person. Enrolment involves different steps:
  - Application and registration: (1) Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means. (2).Ensure the applicant is aware of recommended security precautions related to the electronic identification means. (3) Collect the relevant identity data required for identity proofing and verification.
  - Identity proofing and verification, consisting in ID document authenticity and validity verification, and relates to a real person, and verification that that person's identity is the claimed identity.
- **Electronic identification** means management, deals with number and nature of authentication factors, whether the electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs, revocation and renewal of it.
- **Authentication** sets out the requirements per assurance level with respect to the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party.
- **Management and organisation**, all participants providing a service related to electronic identification in a cross-border context shall have in place documented information security management practices, policies, approaches to risk management, and other recognised controls so as to provide assurance to the appropriate governance bodies for electronic identification schemes in the respective Member States that effective practices are in place.

For each of these four stages, three assurance levels are defined, low, substantial and high according to following criteria:

- **Low** – provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;
- **Substantial** – provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;
- **High** – provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

It is presumed that when the electronic identification means issued under a notified electronic identification scheme meets a requirement listed in a higher assurance level then fulfil the equivalent requirement of a lower assurance level.

Table 5. Requirements for authentication under eIDAS Levels of Assurance

ASSURANCE LEVEL	ELEMENTS NEEDED
LOW	• The release of person identification data is preceded by reliable verification of the electronic identification means and its validity. • Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline. • The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.
SUBSTANTIAL	Level low, plus: • The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication. • The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.
HIGH	Level substantial, plus: • The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.