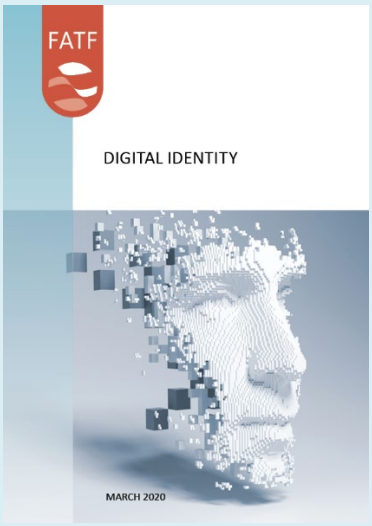
Digital Identity

APPENDIX B:

Case Studies



Citing reference:

FATF (2020), "Appendix B" 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 B: CASE STUDIES

Box 4. India's Unique ID (UID) number

Features of the digital ID system: India's Unique ID (UID) number—or Aadhaar—identity program uses multiple biometrics and biographic information, as well as official identity documentation where it is available, to provide a digital ID to all residents in India, regardless of age or nationality.

The Unique Identification Authority of India (UIDAI) has released a mobile app, m-Aadhaar, which generates a "virtual ID" number, linked to but different than the Aadhaar number, to increase privacy and security. Both the Aadhaar number and Virtual ID can be authenticated online, against the Aadhaar database, or offline, using a QR code.

Financial inclusion measures: The UIDAI Aadhaar enrolment process has flexible identity evidence requirements in order to achieve comprehensive coverage in a jurisdiction where many people lack basic identity documents, and relies on biometrics to establish uniqueness. Enrolment must be in-person but is conducted at authorized registrars located throughout the country (primarily state governments, central ministries, banks and public sector organizations), using software and biometric capture and other equipment prescribed by UIDAI by MOU. Registrars are required to take special measures to enrol women, children, senior citizens, persons with disability, unskilled and unorganised workers, nomadic tribes and all other marginalised/vulnerable groups of individuals who do not have any permanent dwelling.

UIDAI accepts numerous different types of identity documents to verify core attributes at enrolment — 32 types of identity documents containing name and photo; 14 proof of relationship (PoR) documents; 10 date of birth documents; 45 proof of address documents. (see https://uidai.gov.in/images/commdoc/valid_documents_list.pdf).

If an individual does not have any of the "notified" identity documents, the individual can enrol in Aadhaar if a family entitlement document includes his/her name and the Head of Family in the entitlement document enrols in Aaadhar, using required identity Proof-of-Identity and Proof-of-Address documents and introduces the family member while they are enrolling. Where no PoR or other required documents are available, a resident may use Introducers or certifiers, who are individuals notified by the Registrar or regional UIDAI office, who are available at the enrolment centre

Use for CDD: Importantly, under the Amending Aadhaar Act, adopted in July 2019 to comply with the Supreme Court's 26 September 2018 decision that struck down certain provisions of the original Aadhaar Act on privacy grounds, use of Aadhaar remains mandatory for tax purposes and to receive government benefits, subsidies and services financed from the Consolidated Fund of India, but is no longer mandatory to open a bank account (or obtain a mobile phone number). Instead, use of Aadhaar for CDD is strictly voluntary and must be based on the customer's informed consent. Regulated entities may verify the identity of their customers by: (i) authentication or offline verification of Aadhaar, (ii) passport, or (iii) any other documents notified by the central government.

Source: World Bank

Box 5. Peru

Peru's national digital ID system, the National Registry of Identification and Civil Status (Registro Nacional de Identificación y Estado Civil (RENIEC) provides digital ID services to wide range of public and private entities across numerous sectors, enabling them to streamline identity verification and authentication and improve service delivery. In the financial sector, RENIEC serves as the core system for conducting customer identification/verification in compliance with CDD requirements for Peru's e-money and mobile money platform—Billetera Movil (BiM), which was launched in February 2016 and provides services such as cash in/cash out at agents, the ability to check balances, conduct P2P payments and top-up credit to millions of customers.

Source: Wold Bank (2018), *Digital ID On-boarding*

Box 6. Nigeria Bank Verification Numbers (BVN)

Each Nigerian with a bank account is registered in the Bank Verification Number (BVN) system which consists of a biometric-enabled ID database and the e-KYC infrastructure managed by the Nigerian Inter-bank Settlement System (NIBSS). Over 36 Million adults are covered in the BVN database and can use the BVN number to open a new account with another bank, open an online wallet, or apply for a loan. This has lowered onboarding costs and contributes to more robust competition in the financial services market. Customer identification and verification with the BVN is instantaneous and also allows for remote (non-face-to-face) verification through mobile devices. NIBSS has provided Application Programming Interfaces (APIs) allowing for BVN integration to banks and non-bank digital financial service providers, including FinTechs across the country.

Source: World Bank

Box 7. Mexico - High costs in the use of an ID system for CDD purposes

In Mexico, the foundational identification system for individuals is the *Clave Única de Registro Nacional de Población* (CURP), while targeting the entire population and having the potential to use biometrics, is not unique and does not meet the necessary assurance levels for CDD regulatory requirements in Mexico.

On the contrary, the voters card issued by the Instituto Nacional Electoral every ten years includes two forms of biometrics since 2016 (facial recognition and fingerprints) which presents lesser risks of duplications than the CURP. The "general-purpose" nature of the INE for adults in Mexico was created under a temporary legal provision included under the *Ley General de Población* to be used as the primary source of identity for Mexicans until the CURP could provide similar assurance levels to those of INE.

The INE developed a service to allow third parties to verify credentials against the database but the cost of this service – although necessary – is impacting small and medium sized financial institutions as well as Fintech companies willing to operate in the country.

In 2018, the Fintech Law was issued and, conscious at the time of the increasing cases of ID theft in the country, authorities issued measures to mitigate such concerns while meeting FATF recommendations on CDD. Measures issued included the use of the INE as primary source for verification credential for regulated entities and detailed rules regarding the use of biometrics prompting regulated entities to seek adequate Digital ID market solutions to meet the CDD regulatory requirements.

However, the INE was developed to serve as a voters' card and not as a general-purpose identification verifying services and therefore authorities have initiated, in a coordinated manner, an integral reform with regards to digital ID with the objective of having a an official digital ID that can also be used for CDD related purposes .

Source: World Bank

Box 8. UNHCR – Digital ID for refugees

As of the end of 2018, the United Nations Refugee Agency (UNHCR) estimated there were 25.9 million refugees and 3.5 million asylum seekers globally. Countries in developed regions hosted 16% of refugees, while one third of the global refugee population (6.7 million people) were in the World's Least Developed Countries.

Host countries are primarily responsible for issuing proof of official identity to refugees, although this process may be administered by an internationally recognised and mandated authority.

The identity challenges that refugees face are in many ways unique. Many refugees do not possess identity credentials when they arrive in a host State because their credentials were left behind, lost or destroyed during flight. Some refugees may never have had been issued with official identity cards or other credentials, often because they came from fragile or conflict affected areas or faced discrimination preventing registration. At the same time, there is a general principle that prevents contact with the authorities of the country of origin to verify a refugee's identity without the refugee's consent and if there is any risk of harm. International standards therefore indicate that the identity proofing of refugees requires greater reliance on evidence collected during in person applications and interviews, as well as knowledge of the applicant's country of origin, local culture and other local information. Identity assurance increases through regular contact and validation over time to monitor consistency, manage risk and build the refugee's identity in the new context.

UNHCR's digital ID system is used by many host Governments and UNHCR for the registration and identity management of asylum seekers and refugees. By March

2020 over 9 million refugees in 72 countries had been biometrically enrolled in the system.

Features of the digital ID system:

- UNHCR is in the process of strengthening its digital ID system for asylum seekers and refugees. UNHCR's process of identity proofing and enrolment for these individuals is described in UNHCR's Guidance on Registration and Identity Management,[55] Chapter 5.3 "Ascertaining an individual's identity: document review and data collection" and 5.6 "Biometric enrolment and photographs".
- The means of identity authentication provided by UNHCR's digital ID system varies, depending on the country context and the use-cases. The identity credentials issued by the system are mainly used in face-to-face environments. Both asylum seekers' and refugees' identity credentials vary according to host government requirements, but contain facial image and biographic information, which includes a minimum data set and additional attributes that uniquely identify a person. The identity credentials also have a printed bar code or QR code and a unique reference number for the holder.
- UNHCR's digital ID system can support authentication using biometrics, which was initially used for the distribution of humanitarian assistance, including cash transfers (which are termed cash-based interventions). For example, in a number of countries in the Middle East, including Jordan, cash-based interventions are delivered through ATMs with iris scanning equipment to authenticate a user's identity.
- In Malaysia and Indonesia, an Android application is used by the authorities to check the validity of the identity card issued to a refugee by UNHCR and to facilitate verification of the identity of the holder through comparison to a photograph displayed in the application.
- In Uganda, the Office of the Prime Minister (which is responsible for refugee registration and identity and uses UNHCR's digital identification system) in cooperation with the Uganda Communications Commission and UNHCR is establishing a system that will allow for biometric authentication at point of sale by SIM Card vendors. At the time of writing the process was in testing. In Somalia, biometric authentication has been put in place for onboarding for financial services for returning refugees (see below for further details).

Participants in the digital ID system: The roles of participants in UNHCR's digital ID system vary, depending on the country context.

- Where UNHCR is undertaking refugee registration and identity management on behalf of the host Government or in the context of return and resettlement, UNHCR is the sole data controller.
- In other contexts, a hybrid solution is adopted—most commonly where the host State uses UNHCR's system for the registration and identity management of refugees. In these circumstances, UNHCR provides the

55. UNHCR, "Registration and Identity Management Guidance" https://www.unhcr.org/registration-guidancehapter5/registration/

system and the host Government and UNHCR are the joint data controllers, regulated through data sharing agreements.

- In the case of the biometrics system used in Egypt, Iraq, Jordan, Lebanon and Syria, UNHCR works with a private-sector supplier within the context of a data protection protocol.

Use for CDD and relevant regulations: UNHCR's digital ID system and credentials issued by it are allowed to be used for customer identifcation/verification at onboarding in various countries including: Burundi, Malawi, Jordan, Niger and Zambia.[56]

The Central Bank of Somalia has agreed to adopt an approach to CDD for returning refugees who have been biometrically enrolled in UNHCR's system in Kenya and other neighbouring countries. The Voluntary Return Form issued by UNHCR to the returnee prior to departure in the country of asylum, together with biometric authentication of identity using UNHCR's system will be allowed for customer identification/verificationto open a bank account. This solution was tested in December 2018 with accounts opened for two individuals and is expected to be implemented on a wider scale with a Financial Service Provider in 2020.

System's assurance level: The assurance level of UNHCR's system has not been audited against the digital ID trust frameworks and technical standards discussed in this Guidance however at time of writing UNHCR has commissioned external assessments by expert consultants and is evaluating the conclusions.

Financial inclusion: Financial inclusion of refugees is an important component of refugees' protection, self-reliance and resilience. UNHCR distributed 2.4 Billion USD in humanitarian cash-based interventions from 2016-19. To promote financial inclusion, UNHCR aims to deliver cash-based interventions through beneficiaries' bank or mobile money accounts (respecting local regulations), and to give priority to "open loop" systems that leverage local markets and ecosystems, rather than investing in "closed-loop" systems, which only make a limited contribution to financial inclusion. By leveraging digital technology and mobile platforms specifically, UNHCR aims to promote the financial inclusion, which has demonstrated a positive andt tangible impact on the lives of refugees.

Source: UNHCR

Box 9. China - Private sector provided digital ID

Features of, and participants in, the digital ID system: Ant Financial has created a digital ID system, based on the CDD information which has been verified against China's Ministry of Public Security (MPS) as well as other data collected, including face recognition. The customer's name and ID number are verified by the authoritative database held by the MPS to ensure the accuracy of the identity information. Face recognition (matching with avatars on valid documents), multi-channel cross-validation and black list screening is combined with business

[56] UNHCR, "Displaced and Disconnected" (2019) https://www.unhcr.org/innovation/displaced-and-disconnected/

scenarios to complete customer due diligence. Each verification is based on the user's explicit authorisation and confirms the use of the verification service.

Use for financial services: Ant Financial and financial institutions cooperate to provide financial services such as insurance, fund, and microfinance to customers, and also fully use digital ID to provide financial institutions with services such as customer identification and customer risk assessment. Ant Financial's digital ID has been widely accepted in various financial service scenarios, providing more than 3 billion face verification services to hundreds of millions of Alipay users. It is also used in pension inquiry, pension collection, tax declaration and other public services. In addition, Ant Financial provides digital IDs for short term tourists in China who do not have a Chinese bank account but want to make mobile payments. Ant Financial takes special identity verification measures with the Immigration Office to confirm that the passport information is authentic.

System's assurance level: There are no transparent digital ID assurance frameworks and technical standards in China, but it has been suggested that if assessed against the NIST standards, the Ant Financial digital ID system might have identity assurance level 2 (IAL2), authentication assurance level 1(AAL1) and Federation assurance level 2 (FAL2).

Financial inclusion measures:

(1) For residents in rural or remote underdeveloped areas without access to bank accounts or where camera technology is not advanced enough to support facial recognition technologies, Ant Fianncial can verify customer information via the Citizen Identity Information Verification Platform. Limitations are placed on the account (payments cannot exceed 1000 yuan) and cross-border payments are not permitted.

(2) For college students without access to bank accounts, Ant Financial can verify student identities via the China Higher Education Student Information Network, including the student's education status.

Source: China

Box 10. Singapore – National Digital Identity (NDI)

Under the National Digital Identity (NDI), the Singaporean Government is developing a digital identity service stack for Singapore residents and businesses to transact digitally with the Government and private sector in a convenient and secure manner. NDI is built on public key infrastructure (PKI) cryptographic security techniques, and the services have been gradually deployed since 2017 and are expected to be fully operational by 2020.

Features of the digital ID system: There are 4 distinct layers in the NDI stack.

- Trusted data: MyInfo forms the trusted identity data service of NDI and was launched in early 2017. MyInfo includes government-verified data retrieved from various Government agencies and contains more than 100 personal data items. It provides citizens and residents access to and be in control over the sharing of their data. The public are able to auto-fill their government-verified personal information on public and private sector e-

services via a reliable and independent channel upon the individual's consent.

- Trusted identity: A National Certificate Authority (NCA) will be put in place by the Government to issue each resident with a cryptography-based digital identity securely generated and residing within a mobile phone. A digital identity that can be universally trusted by both government and private sector companies. It will supports a multi-tiered identity assurance model, allowing users to conduct more sensitive transactions as their identity assurance level increases.
- Trusted access: NDI will support an open and federated ecosystem of authentication service providers (ASPs). The Government will operate one of the ASPs, but other ASPs may be operated by the private sector, all referencing the same digital identity issued by the Government. In late 2018, SingPass Mobile was launched to enable secure authentication without the need for hardware tokens or SMS-OTPs, which provides greater digital inclusion and ease of access for both public and private sector.
- Trusted services: These are digital services built on NDI's layers. An example is digital signing. Financial institutions can rely on NDI to provide more trusted and high assurance services as well as streamline customer journeys regardless of the boundaries of systems or organisations.

Participants in the Digital ID system: The trusted data and trusted identity layers are provided by the Government. The trusted access layer will support an open and federated ecosystem of authentication and digital signing service providers (ASPs and DSAPs). The Government will operate one of the ASPs.

Use for CDD: Today, more than 60 financial institutions in Singapore leverage MyInfo for over 220 digital services to on-board and perform CDD on customers.

Relevant digital ID-specific AML/CFT regulations: The Monetary Authority of Singapore has issued Guidance on the 'Use of MyInfo and CDD Measures for Non Face-to-Face Business Relations' (AMLD 01/2018).[57] Where MyInfo is used, financial institutions will not be required to obtain physical documents to verify a customer's identity and will also not be expected to separately obtain a photograph of the customer. MAS has clarified that it considers MyInfo to be a reliable and independent source for the purposes of verifying the customer's name, unique identification number, date of birth, nationality and residential address. Financial institutions are required to maintain proper records of data, including data obtained from MyInfo, in accordance with regulatory requirements in Singapore.

System's assurance level: The NDI has used US NIST and EU e-IDAS as reference examples. NDI will be assessing its assurance level against other countries' assurance level as Singapore embarks on bilateral cooperation opportunities. For authentication assurance, it is based on Common Criteria (CC) Evaluation Assurance Level (EAL), with the use of AVA: Vulnerability Assessment (AVA_VAN, from 1 to 5) class.

57. www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Circular-on-MyInfo-and-CDD-on-NFTF-business-relations.pdf

Financial inclusion: The NDI is provided free to all Singapore citizens and residents, and is part of the inclusion programme of the relevant government agencies.

Source: Singapore

Box 11. South Africa

In order to respond to increasing need to mitigate fraud and ID theft, as well as to meet CDD requirements, the South African Banking Risk Information Centre (SABRIC) was established in 2002. Initially composed of the four largest banks, SABRIC now also includes other banks, three Cash-In-Transit and one ATM service provider. In 2007, SABRIC and Department of Home Affairs (DHA) began collaborating to fight identity-related crime. Initially, banks verified customer identity on the basis of a visual inspection of the barcoded green ID book and visual comparison of the photo in it to the appearance of the (prospective) customer. However, the 'manual' method of identity verification had weaknesses. To address them, SABRIC members and the DHA collaborated to enable the verification of customers' identities by matching their fingerprints directly against the DHA's biometric HANIS database, which sends back a 'verified' or 'not verified' response. A secure connection for accessing the DHA database was established in participating bank offices via South Africa's State Information Technology Agency (SITA). The banks pay DHA for verification. The verification process generates an audit trail and the system provides reliable management information. By the end of 2018, seven banks and 4,000 branches were participating in the project. Currently, the number of verifications is about 3 million per month. Queries of the DHA database last typically between 4 and 16 seconds. Between 2 percent to 3.8 percent of e-verifications have been unsuccessful, because the person whose identity was verified lacked a biometric record in HANIS.

Source: World Bank

Box 12. eIDAS interoperability and mutual recognition

Under the eIDAS framework member states can use digital ID for accessing online services. They can also decide to involve the private sector in providing digital ID solutions (means). Under the principle of mutual recognition, member states are obliged to accept notified digital ID means of other member states if they allow the use of digital ID for online access to their public services, and the assurance level of the notified means is equal or higher than the one necessary to access the service. 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.

Source: European Commission

Box 13. Belgium – eCards & ItsMe ®

Belgium's digital ID system includes both public and private-sector components. As explained in greater detail below the government provides general-purpose digital identity credentials, the Belgian Citizen eCard and the Foreigner eCard (together referred to as the Belgian eCards). It also provides the digital identity authentication platform for e-government services. Almost all Belgian citizens and residents have an eCard, which now grants access to a wide range of over 800 eGovernment applications, including Tax-on-Web, social security and eHealth applications, Police-on-web, applications of regional governments, and online portals for municipalities. In addition, a private-sector digital identity authentication service, Itsme®, provides mobile-phone based authentication of identities that are linked to an eCard and a specific mobile phone and SIM card for participating banks and mobile network operators (MNOs). Existing customers can use Itsme® to authenticate their identity in order to log in to their accounts and conduct transactions.

Features of the digital ID system and key participants:

eCards

- Registration for the Belgian e-cards occurs in-person. Municipalities / consulates and embassies are responsible for identity proofing, enrolment, issuance, and delivery of the eCard.
- The Belgian Government provides the Federal Authentication Service (FAS) to authenticate identities for accessing online government services. The FAS platform supports both Internet browser and mobile-phone access, and relies on the IETF TLS standard which provides end-to-end cryptgraphic communications security over networks. FAS authentication involves the following steps:
    - The citizen or foreigner seeks to log into an eGovernment service by entering the PIN code for the individual's eCARD online.
    - The internet browser sends an authentication certificate to the FAS which perhaps the necessary certificate verifications to ensure the integrity, validity and authenticity of the presented TLS client authentication certificate.
    - FAS authenticates the certificate, allowing the individual to complete log-in and access the requested government application.

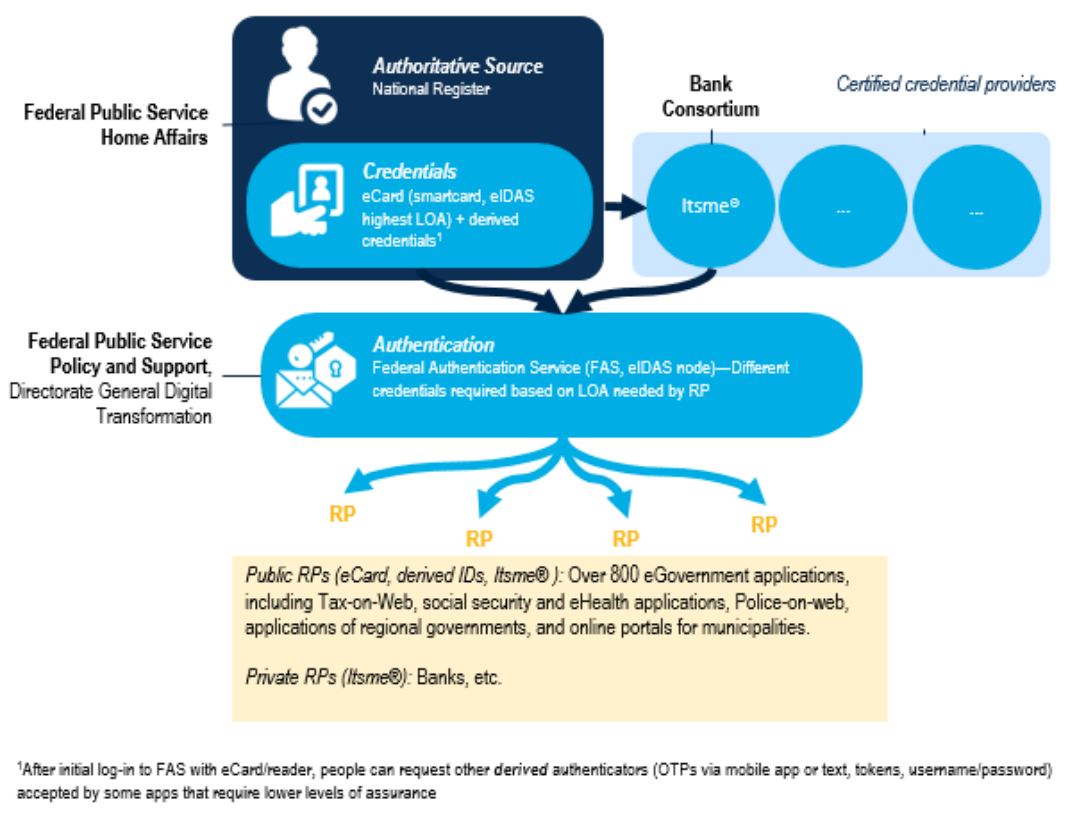
Itsme®

- Itsme® is an initiative of Belgian Mobile iD, a consortium of four leading Belgian banks (Belfius, BNP Paribas Fortis, ING, KBC) and mobile network operators (Orange, Proximus, Telenet). Activation of Itsme® on a mobile device is tied to the Belgian eID card, to assure proof of identity. The authentication flow between the itsme® user and the FAS, using the itsme® App, is based on the OpenID Connect standard (Doc Ref. 1.2.4).

Use in financial services: The Belgian FAS platform is only available to access public services, no financial services are possible at this moment. The itsme® solution is used to authenticate transactions.

Systems' assurance level:

- Belgian eCards provide a High Level of Assurance under eIDAS specifications as confirmed by the eIDAS cooperation network after an in-depth peer review by the Member States.
- Itsme® has undergone a thorough security and governance audit and is recognised by the Belgian government as a valid means of authentication with a 'high' Level of Assurance.



Source: Belgium

Box 14. Sweden – eID Framework and BankID

The Swedish Govenrment, which maintains a central database of the identities of all Swedish citizens and residents, facilitaties digital ID through a public-private partnership. The government provides the federated digital ID architecture (the eID framework - Sweden Connect Technical Framework) and private entities, including banks, act as digital ID service providers, issuing digital ID credentials and providing authentication services.

Features of the digital ID system and key participants: The federation includes both digital ID service providers and relying parties that provide commercial goods or services or government services online. There are currently four digital ID service providers: (1) AB Svenska Pass, (2) BankID, (3) Freja eID, and (4) Telia E-identification—although Telia stopped enrolling individuals for e-idetification in autumn 2017, the e-identification credentials it had issued are valid until they expire.

First launched in 2003 and managed by a consortium of 10 Swedish banks, BankID provides customers with a free digital ID, which can be used to authenticate identity to conduct transactions across the private and public sector. Companies looking to integrate BankID with their services contract with a bank in the BankID network and pay fees for BankID services, which generates a revenue stream for the participating banks. Identity credentials are available in "hard" form—encoded on a smart chip—or "soft" form—available as software on a user's personal computer, tablet, cell phone or other digital device.

Use in financial services: Bank ID can be used for onboarding customers. To obtain a bank ID in the first instance, the individual must undergo documentary CDD by the bank issuing the digital ID. Once obtained, Bank ID can be used to open account with other financial institutions. As at 2016, BankID facilitated 2 billion transactions per year and was used by more than 80 percent of Swedish citizens.

Relevant digital ID-specific AML/CFT regulations: The use of digital ID for customer identification/verification is explicitly provided for in the AML/CFT Act (Ch. 3, s. 7):

"An obliged entity should identify the customer and verify the customer's identity through identity documents or extracts from registers or through other information and documents from an independent and reliable source.

In the application of the first sub-section, instruments for electronic identification and trusted services pursuant to the eIDAS Regulation may be used. Other secure remote or electronic identification processes that are regulated, recognised, approved or accepted by relevant authorities may also be used."

System's assurance level: The Swedish E-Identification Board undertakes checkes of e-identification issuers in accordance with Svensk e-legitimation. Four assurance levels (1 to 4) are defined in the Swedish eID Assurance Framework.[58]

Source: Sweden
References:
https://elegitimation.se/inenglish/howeidentificationworks.4.769a0b711614b669f2953f.html

58 https://docs.swedenconnect.se/technical-framework/mirror/digg/Tillitsramverk-for-Svensk-e-legitimation-2018-158.pdf (in Swedish)

Box 15. Italy - Public System of Digital ID

Features of, and participants in, the digital ID system: Developed under the EU eIDAS Regulation and launched in 2016, the Italian Public System of Digital Identity (SPID),, is a public open digital ID system that allows public and private entities (Identity Providers) accredited by the Agency for Digital Italy (AgID) to offer digital identity registration services to natural persons (citizens and or individuals with residence permits) 18 and older, and to authenticate the SPID digital ID credentials, enabling the identified individual to access public and private services. SPID had about 2.5 million digital identities by March 2018. SPID registration can take place in person, online, or using a mobile device with webcam, depending on the registration procedures offered by a given Identity Provider. To obtain SPID ID credentials, an individual can provide an Identity Provider with a valid identity document (identity card or passport), health card, email address and mobile phone number, or use their digital signature, electronic identity card (CIE), or national service card (CNS).

Use in financial services: The acceptance of SPID is mandatory for the public sector and optional for private sectors (commercial and financial). According to an ABI Lab (Italian Banking Association) survey of Italian banks, 38% of the sample banks planned to use the SPID system for onboarding mobile banking customers and 18% planned to use it for internet banking onboarding by the end of 2019.

Relevant digital ID-specific AML/CFT regulations: The Italian legislation allows obliged entities to use eIDAS compliant digital IDs, like SPID, for customer identification and verification of customers who are natural persons. .

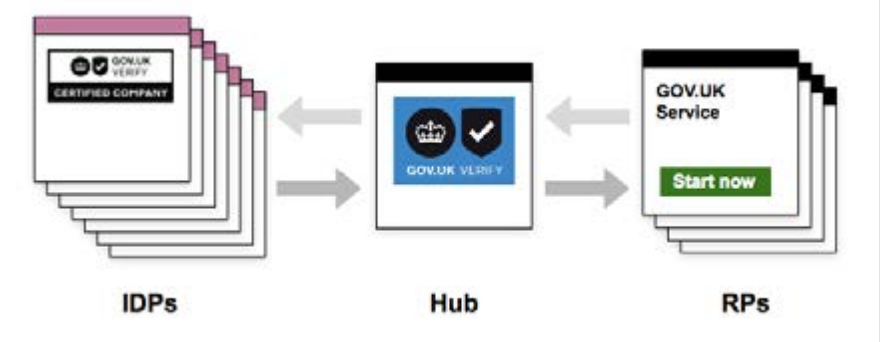
System's assurance level: SPID offers three assurance levels for identity authentication, consistent with standard ISO-IEC 29115. Level 1 allows access to online services, using a user name and password chosen by the user. Level 2, for services that require a higher degree of security, allows access through a user name and password chosen by the user, plus the generation of a temporary access code (one time password), usable through a digital device (e.g., smartphone). Level 3 provides additional security measures, including the use of physical devices (e.g., smart cards) provided by the identity manager. The assurance level required for SPID identity authentication depends on the level of security required by the online service providers.

Source: World Bank, Banca d'Italia and the European Banking Federation

Box 16. UK – GOV.UK Verify

In 2012, the UK Government published a Government Digital Strategy, that introduced the concept of 'Digital by default' – i.e. providing services online and allowing wide access to those who wish to access these services, while not excluding those who cannot or do not wish to access these services in an online channel. As a part of this 'Digital by default' policy, it was recognised that there was a need for a strong digital ID solution that enabled users to prove their identity online, and Government to trust those users are who they say they are.

GOV.UK Verify is a federated digital ID system that enables UK citizens and UK residents to prove their identity online. It uses private sector Identity Providers (IDPs) to identity proof and authenticate the identity of the individual to a specified set of requirements and specifications. IDPs have met government and industry standards to provide identity assurance services as part of GOV.UK Verify.



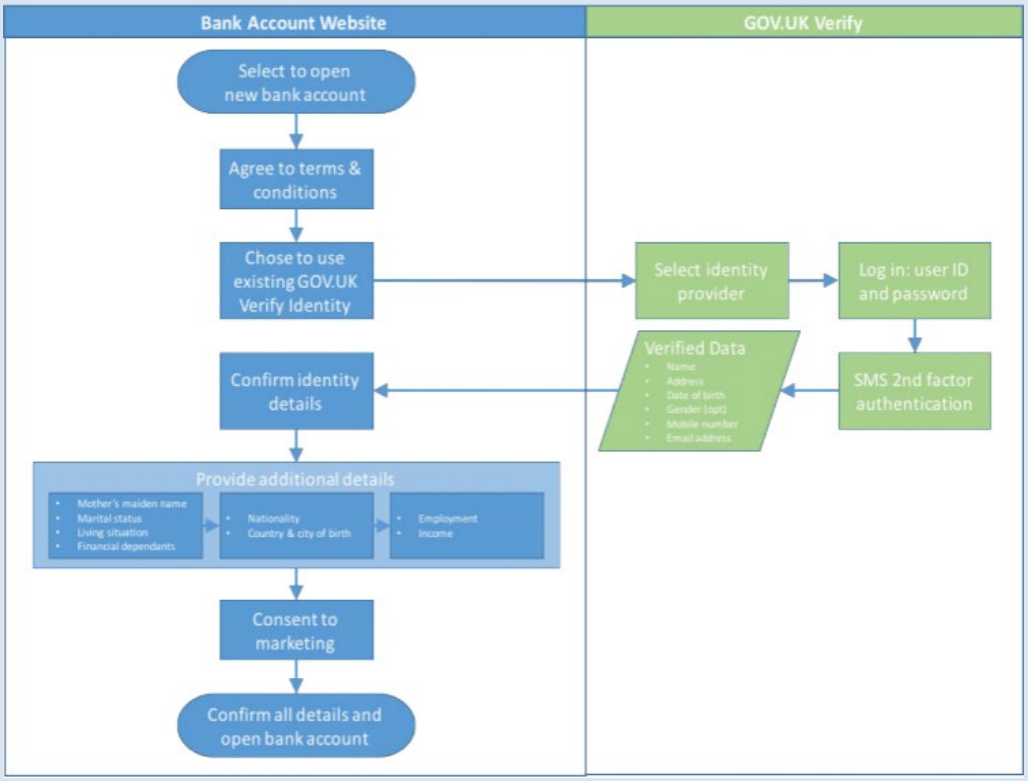
The GOV.UK Verify Hub is the centrally provided infrastructure that manages interactions between users, government services, IDPs, and matching services for the

purpose of authenticating a user to a government service. It also ensures that the required level of identity assurance is requested from an IDP.

A product called the Document Checking Service (DCS) is an API endpoint that allows IDPs to run checks on UK government issued documents against government databases, in support of identity proofing for GOV.UK Verify.

All accounts in GOV.UK Verify require as a minimum 2FA.

The diagram below developed by Open Identity Exchange displays a prototype journey using GOV.UK Verify to open a bank account.



Source: OIX (2017), https://openidentityexchange.org/wp-content/uploads/2017/01/The-value-of-digital-identity-to-the-financial-service-sector-Full.pdf p.13
Source: United Kingdom

Box 17. Estonia

Features of the digital ID system: There are a range of digital ID systems available in Estonia, including:

- ID-cards – the primary identification document in Estonia, are compulsory for all citizens and residents and are the most widely used digital ID option. The ID-card has a photograph and a chip that securely stores personal identity data and digital signature certificates, using public key infrastructure (PKI).
- Mobile-ID is a private sector digital ID service, which can be used via a person's mobile phone. Mobile-ID is issued by a telecom provider in connection to a person's SIM and ID-card. The service needs to be activated on the Police and Border Guard Board's (PPA) website.
- Smart-ID is a private-sector digital ID service that uses the Smart-ID API on a person's mobile phone and the Smart-ID key management server service. Smart-ID can be issued to persons with an Estonian personal identification code. It functions similarly to the ID-card and Mobile-ID in identifying and verifying a customer.

Participants in the digital ID system:

- The Estonian Information System Authority (RIA) coordinates the digital ID authentication solutions. The Police and Border Guard Board issues identity credentials (ID-card, residence card, Digi-ID, and e-resident's Digi-ID) in accordance with the Identity Documents Act. Ministry of Foreign Affairs is responsible for the e-residency programme.
- Two private companies provide technical solutions - Tieto Estonia AS offers user support for the ID-card's basic software and SK ID Solutions AS issues and validates eID certificates.

Use for CDD: Estonian digital ID solutions are used for customer identification/verification at onboarding, as well as for strong customer authentication in compliance with Directive (EU) 2015/2366 (the second Payment Services Directive) and its regulatory technical standards to authorise payment transactions.

Relevant digital ID-specific AML/CFT regulations: In Estonia, a customer can be onboarded face-to-face, via information technology means (video onboarding) and by using two different sources of identity verification. Legislation does not specify what the two verification means should be but the Estonian Financial Supervisory Authority has issued relevant guidance[59] saying that digital ID solutions (i.e. information obtained through authenticating with digital ID) can be one of those sources (point 4.3.1.22), but there should be one additional source of information (point 4.3.1.23) to verify the identity of the customer.

System's assurance level: All the notified Estonian eID schemes have high level of assurance under the eIDAS scheme

Source: Estonia

59. www.fi.ee/sites/default/files/2019-01/FI%20rahapesu%20t%C3%B5kestamise%20juhend%202018%20%28EN%29_pdf.pdf