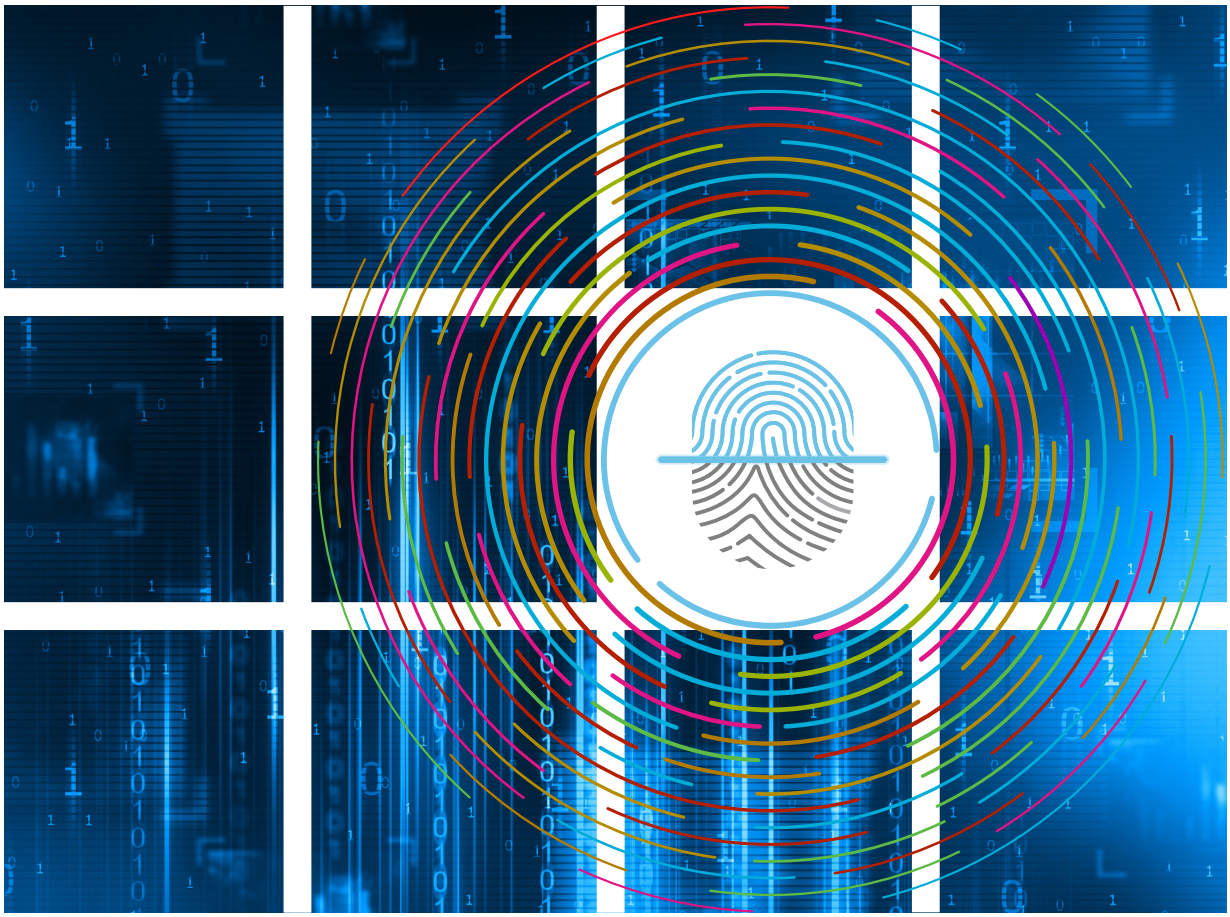
Thematic reports
Regulatory & market environment

ITUPublications

Digital identity in the ICT ecosystem: An overview



Digital identity in the ICT ecosystem: An overview

Acknowledgements

This paper was prepared by Nancy Sundberg, Senior Programme Officer, ITU/BDT/RME, under the direction of Ms Sofie Maddens, Head of the ITU/BDT Regulatory and Market Environment Division (RME) and under the overall coordination of Mr Kemal Huseinovic, Chief of the ITU/BDT Infrastructure, Enabling Environment, and E-Applications Department. The paper was edited by Keith Simpson and Beth Friedmann Peoc'h. The team would like to thank ITU colleagues who provided inputs.

The views expressed in this report are those of the author and do not necessarily reflect the opinions of ITU or its Membership.

ISBN

978-92-61-27961-5 (paper version)

978-92-61-27971-4 (electronic version)

978-92-61-27981-3 (EPUB version)

978-92-61-27991-2 (Mobi version)

Please consider the environment before printing this report.

Table of Contents

List of Tables, Figures and Boxes

Figures

Boxes

Executive Summary

With digital transformation sweeping across sectors and the advent of new electronic identification (eID) technologies, there is a growing trend towards digital identity. In our increasingly digital environment, it is of paramount importance that citizens be in possession of a legal and digital identity if they are to access digital government services and participate fully in the digital economy. In 2018, of the 175 countries with a national ID (foundational or legal identification) system in place, 160 have a system that is at least partially e-ID. However, even in these countries a significant portion of the population still do not have a national ID and over a one billion are still "invisible", lacking all proof of legal identity. In some countries around the world, significant progress is being made to remedy this, building on established practices and often using the Subscriber Identity Module (SIM) registration, "Know-Your-Customer" (KYC) processes and mobile devices as a foundation.

"Digital Identity in the ICT ecosystem: An overview" sets out clearly the different elements in this complex and unfolding landscape. It defines digital identity, provides an overview of the various types of digital identity systems, looks at different approaches taken and the range of challenges being faced, as well as opportunities that arise from using digital identity platforms. These are described in more detail in the next sections.

Making sense of digital identity

Digital identity is defined as mechanisms that assert and verify personal data in the context of digital services and transactions, based on identification, authentication, and authorization processes. Digital identity is classified into three types:

- Foundational: A core digital identity, part of a national identity scheme, based on official documents such as birth records, marriage certificates, and social security documents. Used for example in accessing government services;
- Functional: A digital identity created to address the specific needs of an individual sector, such as healthcare;
- Transactional: A digital identity designed to ease the conduct of financial or other transactions (either face to face or across the Internet) across multiple sectors used for example in making purchases/transactions online but is not treated as a legal identity[1].

Trust remains at the core of all digital identification systems: secured connectivity and access, verification and authentication of digital identity all must underpin online transactions.

Mobile is driving progress, including in remote and rural areas

Today, mobile cellular penetration is approaching saturation than 7.5 billion subscriptions worldwide. The widespread availability of mobile devices coupled with access to the Internet enables individuals in remote and rural areas to enrol, be authenticated, have their identity verified and carry out electronic transactions remotely.

A growing number of countries are following financial Know-Your-Customer (KYC) regulations, requesting mobile service providers to identify their customers – thereby linking a mobile number to a person or an entity, providing a *de facto* means of digitally identifying customers in places where national registration systems are missing. This applies for example to the provision of mobile financial services to unbanked populations, and those who are invisible (i.e., are without an official ID). Mobile numbers can be linked to digital ID numbers to certify and prove that the subscriber is the person s/he claims to be and enable the authenticated person to access e-services using mobile devices. By 2017, 147 countries had adopted SIM registration-KYC rules worldwide.

Challenges to overcome

As we move forward in building digital identities, a number of interlinked issues are emerging:

- The need for a legal framework that addresses data protection, security, privacy and consent. Concerns about online privacy and the possibility of personal data misuse can prevent consumers from participating in the digital economy;
- The need for interoperability between systems. As e-ID systems are used increasingly across sectors of the economy, a coordinated approach is needed to reduce the risk of duplication, and increase efficiencies and veracity in the authentication and verification process. Interoperability would help in building trust, as well as reducing cost and fraud.

Opportunities

There is widespread agreement that that building inclusive, secure, and trustworthy digital identification systems will create opportunities to further development goals, empowering individuals and enhancing their access to rights, services, and the formal economy – opportunities in line with the

[1] Source: ITU-T Focus Group Digital Financial Services: Identity and Authentication.

Sustainable Development Goal (SDG) 16 on promoting peace, justice and strong institutions, whose target 16.9 requires the provision of "legal identity for all, including birth registration by 2030".

Digital identity should be part of an overall digital strategy and collaborative approaches

Digital identity may be required for a number of services and involves collaboration and cooperation between different government agencies, private entities, providers and users across sectors. Although national digital identity systems are generally not developed or overseen by ICT regulators, agencies in charge (typically the national registry) may collaborate with the ICT regulator or the Ministry of ICT when it comes to connectivity issues. Policy-makers should aim to incorporate digital identity into an overall strategy for digital transformation while consulting all the stakeholders to choose the way to arrive at the endpoint of a functioning national digital identity system. Here, the private sector can play a leading role in the verification/authorization process through mobile devices (PIN, SMS, etc.), national identification number, smart cards, etc.

Ongoing ITU work

"Digital Identity in the ICT ecosystem: An overview" is part of ITU's ongoing work in the field of digital identity. Various ITU-T Focus Groups and Study Groups have made recommendations and ITU's Telecommunication Development Bureau (BDT) has launched a project on digital identification for development supporting countries, particularly low- and-middle-income countries, in deploying digital identity initiatives. A Digital Identity Roadmap was developed to provide guidance on the development of a national digital Identity framework implementation plan[2].

[2] See: https://www.itu.int/en/ITU-D/ICT-Applications/Pages/digital-identity.aspx

1 Introduction

Almost half of the world's population is online, and has the capacity to take part in digital society and the digital economy. At the very core of this participation is proof of (legal) identity. Online purchases, making payments, acquiring loans, and accessing e-government services such as passports, tax returns, voting, health records, social benefits and welfare programmes, etc. – all of these require consumers to create accounts, enrol and register before they can take further steps. Furthermore, prior to finalizing the transaction, the service provider has to verify and authenticate the consumer's identity.

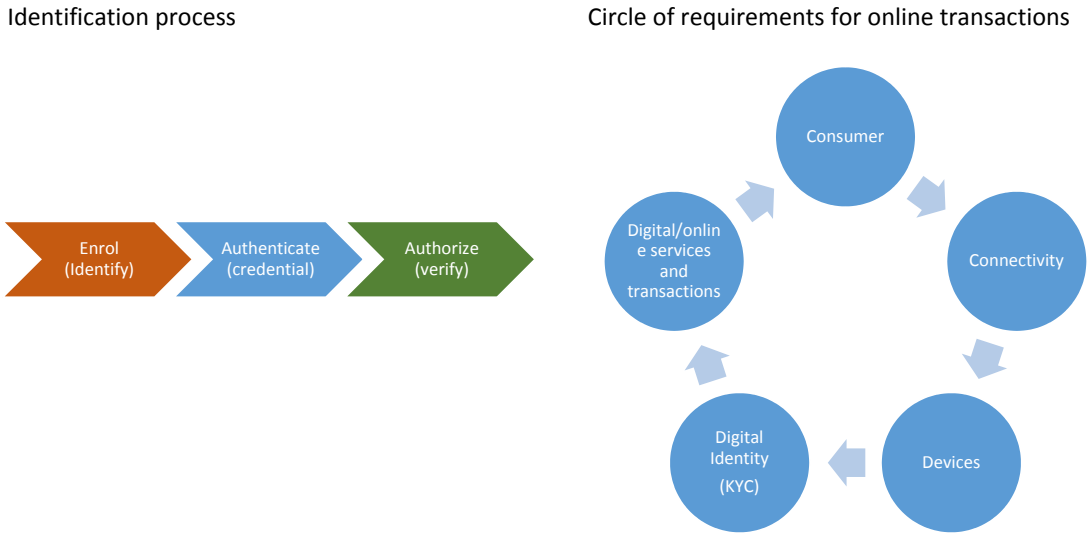
Foundational identity differs from functional identity

There is a distinction between foundational identification systems (for example national ID, civil and population registers) which this paper examines, and functional identification systems that are developed to respond to a demand for a particular service or transaction but importantly may not have the status of a legal identity.

Trend towards digital identity

Consumers may have multiple identities and profiles depending on the service provided, ranging from login and password protected through to 'managed' digital identities – raising security, data control, protection and privacy issues. The range of required shared personal data vary according to the service or transaction but consumers need to trust that their data is secure if the system is to work. In most developed countries, physical paper-based birth certificates and identity documents have been issued to citizens as legal proof of identity, enabling them to carry out official and commercial transactions. Significant progress has also been made in developing countries. However, the World

Figure 1: A three-step approach to digital identification and access to online transactions



Source: ITU.

Bank's ID4D Global Dataset's 2018 edition shows that there are still approximately 1 billion people around the globe (in particular in the developing countries) who lack official identification documents.[1] The lack of formal identification has become particularly problematic in the current refugee crisis. With digital transformation sweeping across sectors and the advent of new electronic identification technologies, digital identity mechanisms for official and commercial transactions is recognized as a solution to enable people around the world to participate in the digital economy.

The way forward: trusted, secured digital identities

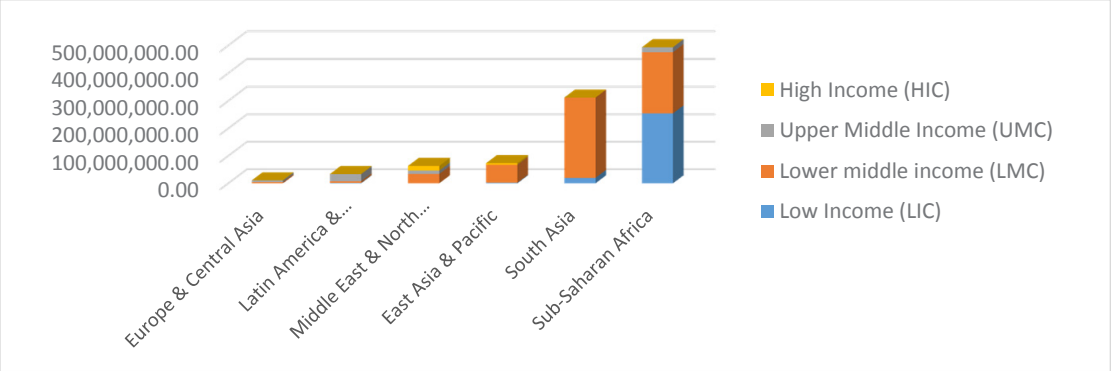
Online users usually have multiple identities with multiple password and login combinations. A 2016 Intel security survey[2] indicated the average user has up to 27 digital identities. Security risks are high these days and the use of username and password is not the most secure way to authenticate identity and often insecurity is increased when the same password is used across multiple identities/ platforms. Governments increasingly recognize that by establishing a system of trusted and secured digital identities that rely on foundational identification (legal identities) can both prevent identity theft and help grow the digital economy. In developing unique identifier systems, countries are following different approaches using individuals' biographic or biometric details. Views on how these digital identities should be used also vary from one country to another – and each approach has its own set of challenges.

One billion people around the world lack proof of legal identity…

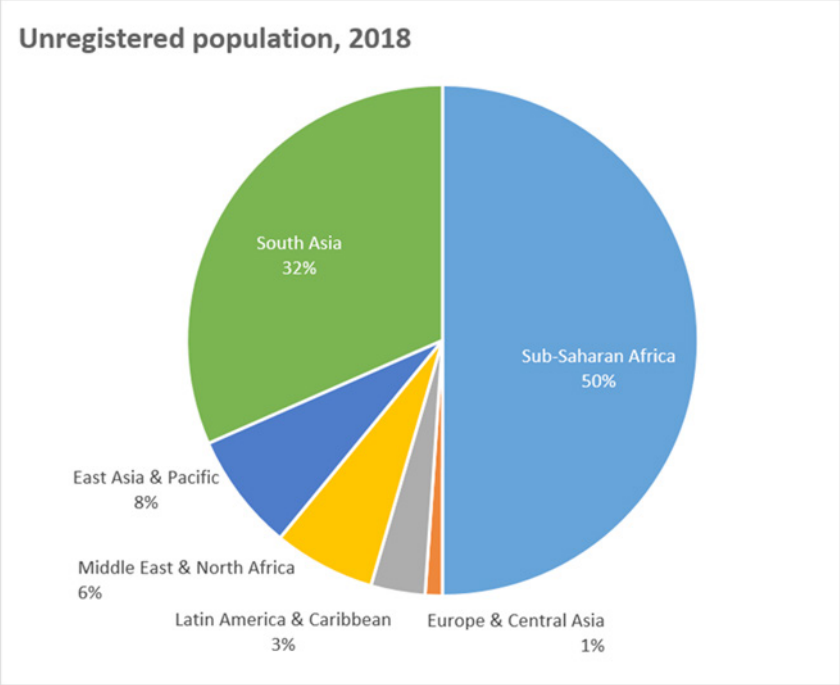
Nearly 988 million people around the world lack proof of legal identity (World Bank ID4D dataset estimates as of April 2018). Progress is nevertheless being made in this area, and digital technologies in general and mobile technologies in particular are an important element in achieving this goal. Electronic identification (eID) systems are increasingly implemented in developing countries. Through the use of biometrics, SIM registration and mobile devices that enroll and authenticate, citizens acquire legal or national foundational identification. The global importance of holding a legal entity was emphasized by including it in the target 16.9 of the UN Sustainable Development Goals (SDGs) that provides for legal identity for all by 2030.

1 http://id4d.worldbank.org/global-dataset
2 http://iphoneeinstein.com/2016/05/survey-says-people-have-way-too-many-passwords-to-remember/

Figure 2: Population lacking identification



Source: World Bank Global ID4D dataset 2018.[3]



Source: World Bank Global ID4D dataset 2018.

According to World Bank data, in 2018, of 175 countries with national, foundational ID system in place, 160 have a system that is at least partially e-ID and 83 collect biometrics data (iris and/or fingerprint). In a digital environment, it is paramount for citizens to be able to prove who they are to fully participate in the digital world. Digital ID is increasingly needed to access not only online commercial and financial services, but to benefit from statutory rights such as the right to claim state benefits.

...But mobile is driving progress in establishing identity – including in remote and rural areas

In 2017, mobile cellular subscription penetration reached more than 7.5 billion subscriptions worldwide. Furthermore, globally, 3.57 billion people were expected to be using the Internet by end 2017, that is 48 per cent of the world's population. Mobile broadband was expected to reach 56.4 per cent penetration by end 2017 and fixed-broadband access more than 979 million subscriptions.[4]

[3] Aggregate figure does not include China due to the lack of publicly available civil registration and national ID coverage data and 10 other countries that do not possess a national ID system and have a birth registration rate of over 95%.

[4] https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf

The widespread availability of connected mobile devices enables individuals in remote and rural areas to enrol, be authenticated, have their identity verified and carry out electronic transactions remotely. It has allowed developing countries in particular to fast-track identification systems and move away from paper-based identification. In addition, a growing number of countries are following financial Know-Your-Customer (KYC) regulation, requesting mobile service providers to identify their customers – thereby linking a mobile number to a person or an entity, providing a *de facto* means to digitally identify customers in places where national registration systems are missing. This applies for example to the provision of mobile financial services to unbanked populations, and those who are "invisible" – i.e., without an official ID. Digital identification across platforms brings opportunities for individuals and businesses but requires security and data protection measures to be in place to foster trust.

Trust is key

This paper addresses a number of issues that arise from building digital identities based on foundational or functional identification systems. These include the need for a legal, data protection framework, security, privacy and consent, interoperability, and the importance of standards. As e-ID systems are used across sectors of the economy, a coordinated stakeholder approach would reduce duplication, avoid conflicting rules, build interoperability and security between technologies and systems, and would build trust in their use. Therefore, trust is at the core: secured connectivity and access, verification and authentication of digital identity must underpin online transactions.

2 Making sense of digital identity

The ITU-T Focus Group on identity and authentication defines digital identity as the various mechanisms of asserting and verifying personal data attributes in the context of digital services and transactions, based on three processes: identification, authentication, and authorization. Digital identity is further classified in three types: foundational, functional and transactional[1] (described in Box 1). Work on digital identity architecture is ongoing in the ITU-T Study Group 3 Question 11/3 which examines digital identify from an economic and policy perspective in international telecommunications services and networks.[2] Further security-related work on identity management and the protection of personally identifiable information among others is currently ongoing in ITU-T Study Group 17.[3]

The ITU's definition of digital identity is provided in Recommendation ITU-T X.1252 "Baseline identity management terms and definitions" as "a digital representation of the information known about a specific individual, group or organization," and issues around the management of identity in data networks are further covered in the following ITU Recommendations:

- Recommendation ITU-T X.1253: "*Security guidelines for identity management systems*", and
- Recommendation ITU-T X.1254: "*Entity authentication assurance framework*".

[1] ITU-T Focus Group Digital Financial Services: *Identity and Authentication:* https://www.itu.int/en/ITU-T/focusgroups/dfs/Pages/default.aspx

[2] https://www.itu.int/en/ITU-T/studygroups/2017-2020/03/Pages/questions.aspx

[3] https://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx

Box 1: Identification process

Proofing (as defined in ITU-T X.1254; often less accurately termed "identification"): This is the process of identifying an individual or organization (as defined in ITU-T X.1252), and formally *establishing* the veracity of that identity. It may involve examining "breeder documents" such as passports and birth certificates, consulting alternative sources of data to corroborate the identity being claimed, and potentially collecting biometric data from the individual.

Authentication (as defined in ITU-T X.1252): This is the process of *validating the assertion* of an attribute associated with an identity previously established during identification. Typically, this involves presenting or using an authentication credential (that was bound to the identity during identification) to demonstrate that the individual (or organization) owns, and is in control of the digital identity being asserted.

Authorization: This is the process of *determining* what actions may be performed or services accessed/provided on the basis of the asserted and authenticated identity.

Digital identity classification:

- Foundational: A core digital identity, usually created as part of a national identity scheme or similar, which is based on the formal establishment of identity through the examination of qualifying (breeder) documents such as birth records, marriage certificates, and social security documents. Such a digital identity typically supports a wide variety of government services, and sometimes extends further.
- Functional: A digital identity which is created to address the specific needs of an individual sector, such as healthcare.
- Transactional: A digital identity which is intended to ease the conduct of financial or other transactions (either face to face or across the Internet) across multiple sectors.

A state-issued eID acts as a strong, reliable foundational identity. However, there are a number of additional use cases that require more flexible or extensible identities, and the functional or transactional identities, derived as they are from the foundational state-issued eID, can fulfil this role.

Source: ITU-T Focus Group Digital Financial Services: Identity and Authentication.

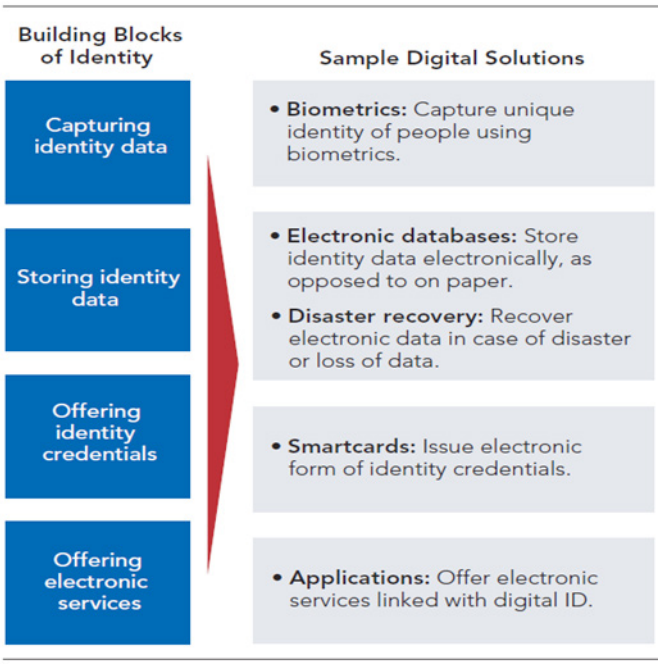
Digital ID is defined by the European Union's (EU) Regulation on electronic identification and trust services for electronic transactions (eIDAS Regulation) as "the process of using personal identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person". The European Union adopted the eIDAS Regulation in 2014 to "ensure that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available; and to create an European internal market for electronic trust services (eTS) – namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication – by ensuring that they will work across borders and have the same legal status as traditional paper-based processes."[4] It requires the electronic identification schemes across EU countries to be interoperable, and provides for the establishment of an interoperability framework.

[4] https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification

2.1 How does digital identity work?

A person's digital identity can be defined by two types of attributes: biographic attributes such as name, age, gender, address; and biometric ones such as fingerprints, iris texture, voice, or facial geometry. As explained by the World Bank, "biometrics can be used to uniquely identify individuals when civil registration systems are lacking, which capture the birth or death of people, or in the absence of official birth certificates in developing countries."[5]

Different types of digital identity platform/ architecture exist, relying on the way technology is used (for registering people or for issuing credentials) or in the way the institutional structure is set-up. The identity provider (controller) can also be a State or private entity.



Source: World Bank analysis.

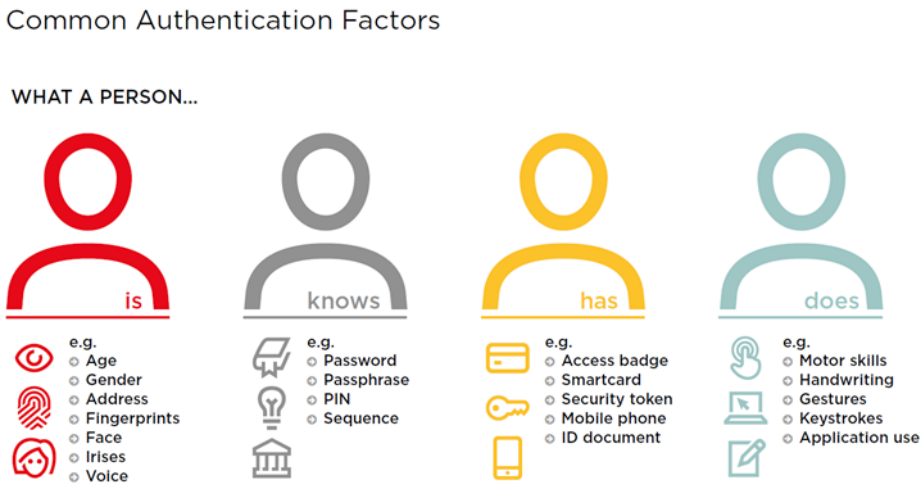
Elements of digital identity

The elements that compose a digital identity platform start with the capture and store of identity data, and the offering of identity credentials and of electronic services that are linked to the registered and authenticated digital identity. The method of capturing the data will impact on its trustworthiness and the interoperability with other identification systems. The government needs to ensure that a minimum set of attributes unique to the individual are provided when setting a legal identity. For example, the EU's eIDAS Implementing Regulation (2015/1501) established that the minimum data set of unique identity attributes for a physical person should include mandatory attributes – the current family name(s), current first name(s), date of birth, and a unique identifier; and additional attributes that are the first and family name(s) at birth, place of birth, current address and gender. Only after the person is registered and credentialed can s/he use his/her digital identity.

[5] World Bank Digital Identity Toolkit, 2014: A Guide for Stakeholders in Africa: https://openknowledge.worldbank.org/bitstream/handle/10986/20752/912490WP0Digit00Box385330B00PUBLIC0.pdf?sequence=1&isAllowed=y

About authentication

As defined by the World Bank and GSMA,[6] authentication can be done based on what a person is, what she knows, what she has and what she does. "It is the process of verifying a person's digital identity using one or more factors or credentials in order to establish that they are who they claim to be. What a person does online, and the records the person leaves behind are part of the person's behavioural identity. Authentication is therefore a process of establishing confidence in a person's digital identity." The common authentication factors define what a person is, knows, has and does providing a good portrait of who a person is of his/her identity. Of course not all of these attributes are required for establishing a national digital identity but they are part of the digital footprint a person leaves online – one that entities collect and may share. A person may want to avoid sharing and keep control of some of these attributes.



Source: "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation".
A joint World Bank Group – GSMA – Secure Identity Alliance Discussion Paper.

Databases and digital identity

Electronic databases can be used to store, reference, validate and authenticate identity data. The database can be a central repository or a distributed system depending on the country and the technology credentials used. Blockchain is a decentralized technology, now being applied to manage digital identities. Information and transactions of interacting participants are recorded in a forgery-proof manner. This is in contrast to centrally organized databases whose contents are controlled by the owner.

Electronic credentials, such as smartcards or mobile phones, offer a way to electronically authenticate the identity of a person for in-person, online, mobile, or offline services. Creating secured and reliable databases to provide trustworthy digital identity credentials is therefore key to ensure privacy and security of digital identity systems.

In Estonia, users are granted a chip-based ID with a personal identification number (PIN) using biographic data as attributes. It differs from the Indian Aadhaar system which is a biometric system that issues a unique 12 digit identification number.

Four types of digital identity ecosystems

Different types of digital identity systems or ecosystems can be found depending on national circumstances and context. Four types of digital identity ecosystems have been identified by GSMA

[6] See: Joint World Bank Group – GSMA – Secure Identity Alliance Discussion Paper: https://openknowledge.worldbank.org/handle/10986/24920

and the World Bank supporting digital transactions and with various degrees of public and private participation:

- *Government-driven centralized system* where one or more databases are owned by the government and where most digital transactions are carried out on the basis of state-issued eID (e.g., Belgium, Germany, Pakistan, Malaysia).
- *Semi-centralized, federated system* in which the individual can choose from multiple trusted identity providers and use these credentials for digital services via an identity hub (e.g., Sweden, United Kingdom, Australia).
- *Decentralized, open identity market* with no national identity schemes, where public and private entities create, own and manage their own digital identity systems (e.g., United States).
- *Self-asserted digital identity* (e.g., Facebook, Google, or other large Internet players) where users choose their own digital attributes and where there is no verification of official identity documents. However, at the time of writing, no examples of countries using this approach exist.

From a consumer or citizen's perspective, no matter what the structure of the system is, security and trust are fundamental. Without trust in the system, consumers will be reluctant to enroll in the digital identification system. Security and trust aspects are addressed later in this paper.

As mentioned above, digital identity may be required for a number of services and involves collaboration and cooperation between different government agencies, private entities, providers and users across sectors. Interoperability of the different systems is key to move from a fragmented approach towards a coordinated approach – requiring the development of technical standards.

Entities in charge of digital identity systems – NIAs (national identity agencies)

Countries have adopted different institutional models for managing foundational digital identity. To provide a broad understanding and based on the World Bank's Digital Identity Toolkit,[7] there are five high-level institutional roles that need to be assigned for collecting (capturing and certifying), storing and using (authenticating and updating) identity data.

The national identity agency (NIA) can be an autonomous body reporting through different structures. For example:

- To a cabinet-level minister (such as the Minister of Interior, Justice or Internal Affairs) such as National Database Registration Authority (NADRA) in Pakistan or
- To the executive as with Unique Identification Authority of India (UIDAI) in India, an autonomous organization governed by an independent board representing the stakeholders, or
- To a directorate within an existing ministry as in Argentina with Registro Nacional de las Personas (RENAPER).

The NIA may have several roles including establishing standards for population enrolment data, operating backend systems and for storing and protecting the consolidated identity information. Enrolling the population can be done by members of the NIA or other registrars such as government agencies, Civil Registry, the Ministry of Health, Ministry of Interior, as part of normal operations. As further explained, "the registrar may collect information broader than the minimum set established by the NIA for its core mission. It could include data for Know Your Customer (KYC) purposes specific to the needs of individual government agencies."

[7] http://documents.worldbank.org/curated/en/147961468203357928/Digital-identity-toolkit-a-guide-for-stakeholders-in-Africa

According to ITU's latest telecommunication/ICT regulatory survey results[8], ICT regulators and Ministry of ICTs have little involvement in foundational digital identification, but play a greater role when linking identification of mobile subscribers to SIM registration – as explained in the next section.

2.2 Linking KYC rules with digital identity

National digital identity systems are generally not developed or overseen by ICT regulators. However, agencies in charge (typically the national registry) may collaborate when it comes to connectivity issues. For example, KYC regulation and enforcement is necessary when providing a national ID, and one of the identification pre-requisites of most, if not all, KYC regulations is to register and activate a SIM. Mobile numbers can be linked to digital ID numbers to certify and prove that the subscriber is the person s/he claims to be and enable the authenticated person access to e-services using mobile devices. A point of sale can also become a means of authentication.

Thailand – voluntary registration of biometric details

In Thailand, the ICT regulator, National Broadcasting and Telecommunications Commission (NBTC), ordered the largest mobile operators to establish service centres for both new prepaid and postpaid mobile SIM card users to enrol their biometric information into a voluntary, online fingerprint ID system. Operator failing to provide fingerprint scanners at service centres face penalties. NBTC is then, encouraging all mobile users to submit their fingerprints into the system designed to improve the security of mobile banking services, online services and to counter potential fraud risks.[9]

Pakistan – building national identity system through mobile registration process

Biometrics solutions can also be used as a standalone solution or as part of a national ID system. In Pakistan, biometric data is verified online during the mobile registration process. Customers must provide their fingerprints along with their national ID reference. The biometric data is validated by the mobile operators against the National ID database, the National Database and Registration Authority (NADRA). NADRA was established in 2000. The Pakistan Telecommunication Authority (PTA) launched the first SIM issuance and activation process whereby mobile cellular operators use biometric verification (authentication) of customers through the NADRA database to activate the SIM card. The validated ID is accepted as meeting the KYC requirement for mobile banking. PTA has worked in close coordination with the National Database and Registration Authority, the telecommunication operators for the implementation of the biometric verification of Subscriber Identity Modules (SIMs). As a result, each SIM operating in Pakistan is mapped to a valid computerized national identity card number that has led to a digital identity system –used for financial inclusion, tax payment, issuing of driving licenses, access to social benefits programmes and more.[10] The government and PTA, the ICT regulator, have encouraged the use of the mobile registration to enable value added services.

The NADRA database stores fingerprints, pictures and family records of citizens, enabling agencies to carry out online verification of identity. In 2013 PTA launched a biometric SIM issuance, verification and identification process that was completed in 2015. This measure applies to all SIMs – both new and those already in use (See Box 2).

India – Unique Identification Authority of India (UIDAI) and the mandatory biometric verification of customers to register new SIMs and to re-verify those already in use

In India, the government has followed a similar approach since 2017 with the setting up the Unique Identification Authority of India (UIDAI) and the mandatory biometric verification of customers to

8 ITU World Telecommunication/ICT Regulatory Database.
9 http://www.biometricupdate.com/201704/thailand-mobile-operators-ordered-to-enroll-customers-fingerprint-id
10 PTA, Pakistan's reply to the Queries on ITU G5 Regulatory Toolkit

register new SIMs and to re-verify those already in use.[11] Similar e-KYC initiatives are in place in other countries such as Peru and Uganda.

Challenges in terms of security, privacy and freedom of choice

The mandatory use of a unique identifier number for people to access welfare schemes and commercial services raises some challenges in terms of security, privacy and freedom of choice. The legal and constitutional validity of linking access to some social and commercial services with the obligation to *de facto* enrol to a national identification system that is voluntary is also an issue in some countries. In August 2017, the Indian Supreme Court declared that privacy is a fundamental right answering concerns over protection of personal data and governmental surveillance issues. On the constitutional validity of the Aadhaar Act and the mandatory linking of Aadhaar (forced enrolment of citizens or not) to access welfare schemes and other commercial services, the Indian Supreme Court, in September 2018, ruled that Aadhaar is constitutional stating that it does not violate the right to privacy. On the mandatory linking of Aadhaar to public and commercial services, the Supreme Court ruled that it could not be made compulsory for bank accounts, mobile connections and school admissions.[12]

Box 2: The process of SIM issuance in Pakistan: towards a digital identity

The Pakistan Telecommunication Authority (PTA) is in charge of regulating the issuance of Subscriber Identity Modules (SIMs) in Pakistan. When mobile cellular services started, the PTA required cellular companies to keep a copy of the subscribers CNIC (Computerized National Identity Card) or ID card. The process was not efficient: the subscriber was issued an inactive SIM, would call the operator's help line, was asked questions (mother's name and place of birth, and so on) and the SIM would be activated. In 2013, a new mechanism was introduced: a SIM card was issued only after online verification of subscriber thumb/fingerprint and CNIC. The process for the issuance of new SIMs through biometric verification was completed in the third quarter of 2014. By May 2015, all SIMs that were already issued were re-verified, and now, all existing SIMs are biometrically verified. As of March 2018, the number of active SIMs in Pakistan reached 149 million out of which 53 million (35.57%) use mobile broadband services. The whole process was audited by a third party firm and the results were found to be satisfactory.

The re-verification process was difficult one but was completed in record time. The PTA along with cellular mobile operators carried out an effective awareness-raising campaign.

Pakistan was the first country in the world to use biometric verification before issuing SIMs –and the first to re-verify existing SIMs. The process was carried out electronically.

SIM as an Identity

In Pakistan, an entity can verify the information it receives (mobile number and CNIC), and can then establish that the SIM belongs to the person who is claiming it.

11 http://dot.gov.in/sites/default/files/Re-verification%20instructions%2023.03.2017.pdf?download=1

12 https://www.ndtv.com/india-news/constitutional-validity-of-aadhaar-top-5-takeaways-from-supreme-courts-verdict-1922376 and https://www.business-standard.com/article/current-affairs/sc-upheld-constitutional-validity-of-aadhaar-card-but-with-caveats-118092700057_1.html

Box 2: The process of SIM issuance in Pakistan: towards a digital identity (continued)

In addition, organizations with no online access to the NADRA database can use the following system: a subscriber can send an empty text message to short code 667. The system will return the name of the person and the CNIC number of the person who is the owner of the SIM currently installed on that phone, which can then be verified by looking at the original CNIC.

This identification system can be used for filing electronic tax returns. More and more organizations, such as the Benazir income support programme providing government subsidies to poor people, use this system coupled with mobile banking. Similarly, the government is also providing smartphones and loans to farmers using this electronic identity verification process.

In Pakistan, most cellular mobile companies also own a branchless bank. Therefore, when a customer wants to buy a SIM, s/he is also offered a Level 1 branchless bank account – with no paper-work involved. The State Bank of Pakistan is also in the process of launching the "Asaan" (meaning easy) Mobile Account scheme allowing individuals to carry out a digital transaction from anywhere, anytime. Currently, branchless banking agents are being trained, government payments digitized, FinTechs funded and interest-free loans being given to small farmers in rural areas via mobile wallets. As a result of these initiatives, m-wallet accounts now number 20 million and close to Rs. 2.097 billion were transacted through mobile banking accounts in 2016.

The SIM is becoming the digital identity for many users in Pakistan.

Source: www.pta.gov.pk – www.nadra.gov.pk

Box 3: India's digital identity infrastructure

The government has initiated an ambitious e-governance project, the Unique Identification (UID), by setting up the Unique Identification Authority of India (UIDAI). The UID aims to provide real-time service for verifying the identity of any Indian resident through biometrics (ten fingerprints, two iris scans, and facial photograph) and demographic information (name, date of birth (verified) or age (declared), gender, address, mobile number (optional) and e-mail ID (optional)) called "Aadhaar". The Aadhaar number is a 12-digit random number issued by the UIDAI. The government has initiated delivery of services and several welfare schemes designed to support the poorest citizens. Governments have been successful in linking the Aadhaar number with several welfare schemes like the LPG subsidy, scholarships to students, pensions and Public Distribution System (PDS), etc. to ensure accurate delivery of benefits to authorized persons only.

Aadhaar enrolment activities are being carried out exclusively by Registrars in each State but they can contract public or private entities to carry out enrolment provided they follow UIDAI's strict technical specifications and regulations. Aadhaar Authentication provides a digital, online identity platform enabling the identity of Aadhaar number holders to be validated instantly anytime, anywhere.

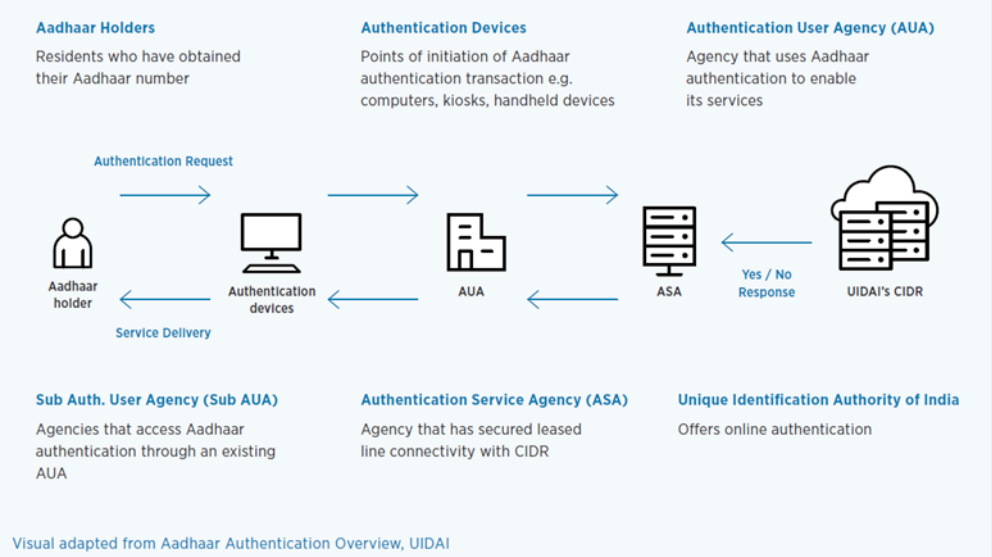
As described on UIDAI's website, there are three approaches for enrolment: *Document based* requiring the submission of one valid Proof of Identity (PoI) document and one valid Proof of Address(PoA) document; *Head of Family (HoF) based* where the head of family may introduce family members by means of documents, which establish the Proof of Relationship (PoR); and *Introducer based* for cases when in the absence of valid Proof of Identity (PoI) document and valid Proof of Address (PoA) document, an introducer's service can be leveraged. An introducer is a person appointed by the Registrar and should have a valid Aadhaar number.

Aadhaar-based authentication is a service that can be requested by entities (government / public and private entities/agencies). This service from UIDAI can be used by requesting entities to authenticate the identity of their customers / employees / other associates (based on the match of their personal identity information) before providing them access to their consumer services / subsidies/ benefits / business functions / premises. The authentication service is provided both online and in real-time by UIDAI through its two data centres i.e., Hebbal Data Centre (HDC) and Manesar Data Centre (MDC) where online services for authentication and other services such as e-KYC are deployed in active-active mode to ensure services are highly available.

As indicated by Dr R. S. Sharma, the TRAI (Telecom Regulatory Authority of India) recommended that the government allow electronic KYC of Aadhaar as one of the valid documents for acquiring a new mobile connection. Consequently, the government issued e-KYC guidelines in August 2016 to make the process of application and authentication faster and simpler for subscribers. e-KYC authentication can only be carried out using One Time Pin (OTP) and/or biometric authentication.

Box 3: India's digital identity infrastructure (continued)

Authentication process



Source: State of Aadhaar Report 2016-2017, http://stateofaadhaar.in/

The Aadhaar identity platform is a key pillar of "Digital India", where every resident of the country is provided with a unique identity. The Aadhaar programme has already achieved several milestones and is by far the largest biometrics-based identification system in the world.

Source: adapted from Dr R. S. Sharma, Chairman, TRAI, India, "E-Governance: The Indian paradigm for citizen friendly governance":
http://www.indembassybern.ch/docs/citizen.pdf and UIDAI's website:
https://uidai.gov.in/authentication/authentication-overview/authentication-en.html

Where no national ID identification systems exist, some countries are using KYC and SIM registration policies to authenticate mobile customers as a means of establishing digital identity. By 2017, 147 countries had adopted SIM registration-KYC rules worldwide.[13]

Important to note and as advised by GSMA – governments should not use mandatory SIM or phone registration policies as substitutes for national identity schemes. These may serve to support government initiatives as a functional registry when such national registration systems are lacking. The purpose of the SIM registration policy is to enable the identification of a person using a mobile service by verifying existing identity documentation. As the identity of the person has been verified through a Know Your Customer process (KYC), and the mobile device/SIM can be attributed to the person, it is then possible to use this information for digital authentication, knowing that the person is who they say they are, and enabling that person access to various services.[14] Mobile is well placed as a digital authentication tool for its widespread use, provided there is robust connectivity, coverage and security measures are in place.

[13] https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/Access-to-Mobile-Services-and-Proof-of-Identity.pdf

[14] https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf

Identity initiatives around the world

In addition to ITU's efforts, several initiatives – both public and private – have been launched to provide digital identity for all. These include:

- The World Bank's Identification for Development (ID4D) initiative designed to help countries realize the transformational potential of digital identification systems and to ensure integration of digital identification systems with civil registration and vital statistics (CVRS).[15]
- The Commonwealth Digital ID initiative which "catalyses progress towards the goal of providing a digitally enabled identity for every woman and girl in the Commonwealth by 2030 with co-funding from the UK and Australia"[16] and support from GSMA.
- The ID4Africa which promotes the responsible adoption of modern digital identity systems as drivers of socio-economic development and provides a platform for African governments to explore how national electronic identity can further socio-economic development in their countries.[17]
- The ID2020 initiative, a public-private partnership founded by Accenture, Microsoft and the Rockefeller Foundation – this is dedicated to solving the challenges of identity for those who are currently lacking one, and is exploring the use of blockchain technology.
- GSMA also launched a Digital Identity programme and Mobile Connect to provide an authentication solution matching a user to their mobile devices.[18]
- The mobile industry is also playing an important role in building digital identity systems in countries like Estonia, Finland, Norway and Switzerland.[19]
- In Oman, the government launched the Electronic Certification (TAM) service provided by the National Digital Certification Center (NDCC) at the Information Technology Authority (ITA)[20] to provide electronic access to government services and transactions using digital authentication. Citizens need to activate TAM on their ID card and can also use their mobile SIM card (the Public Key Infrastructure[21] (PKI) – the SIM card needs to be registered in the name of the person) – and a card reader to access TAM services. Services which citizens can apply to use via their digital identity range from medical appointments to registering as a job seeker and making tax payments. The use of digital identity empowered the government to perform 7.2 million electronic transactions using the ID card and 2.1 million electronic transactions using Mobile ID by end of 2017.[22]
- While no national digital identity system is yet in place in Switzerland, the government is currently working on a draft eID Act that will enable a system to be put in place, through a public-private partnership, and with the government retaining implementation responsibility. The city of Zug in Switzerland announced in July 2017 that it intended to offer digital identities on an app to its citizens using blockchain technology associated with a crypto address. The system is said to be completely decentralized and an app will enable citizens to register their identities while

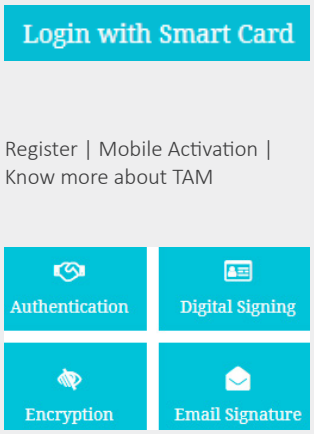
15 http://id4d.worldbank.org/about-us
16 https://senatorcfw.com.au/speech/global-citizen-live-event-commonwealth-heads-government-meeting/
17 http://www.id4africa.com/about/
18 https://www.gsma.com/identity/mobile-connect
19 GSMA case studies such as: Finnish Mobile ID: A Lesson in Interoperability; Estonia's Mobile-ID: Driving Today's e-Services Economy; Norwegian Mobile Bank ID: Reaching Scale through Collaboration; Swisscom Mobile ID: Enabling an Ecosystem for Secure Mobile Authentication: https://www.gsma.com/identity/resources
20 "The Information Technology Authority (ITA) is responsible for implementing national IT infrastructure projects and supervising all projects related to implementation of the Digital Oman Strategy." Source: https://www.ita.gov.om/ITAPortal/Pages/Page.aspx?NID=965&PID=4109&LID=191
21 A public key infrastructure (PKI) uses a dual authentication system in which a digital signature, created through a complex random algorithm using a private key on the card, is checked up against a public key on a database. ITU-T Recommendation X.1122 serves as a guideline for implementing PKI security in mobile systems https://www.itu.int/rec/T-REC-X.1122-200404-I/en
22 Idem.

the town will proceed with the verification using its own identity control procedures.[23] The city conducted an "e-voting" consultation in 2018 using this technology.

- In the European Union, a Cooperation Network has been set up as a mechanism for cooperation between Member States in order to achieve interoperability and security of their eID schemes[24]. It provides a forum with regular meetings, where Member States can exchange relevant information, experience and good practice.

Box 4: Use of digital identity in Oman for government services

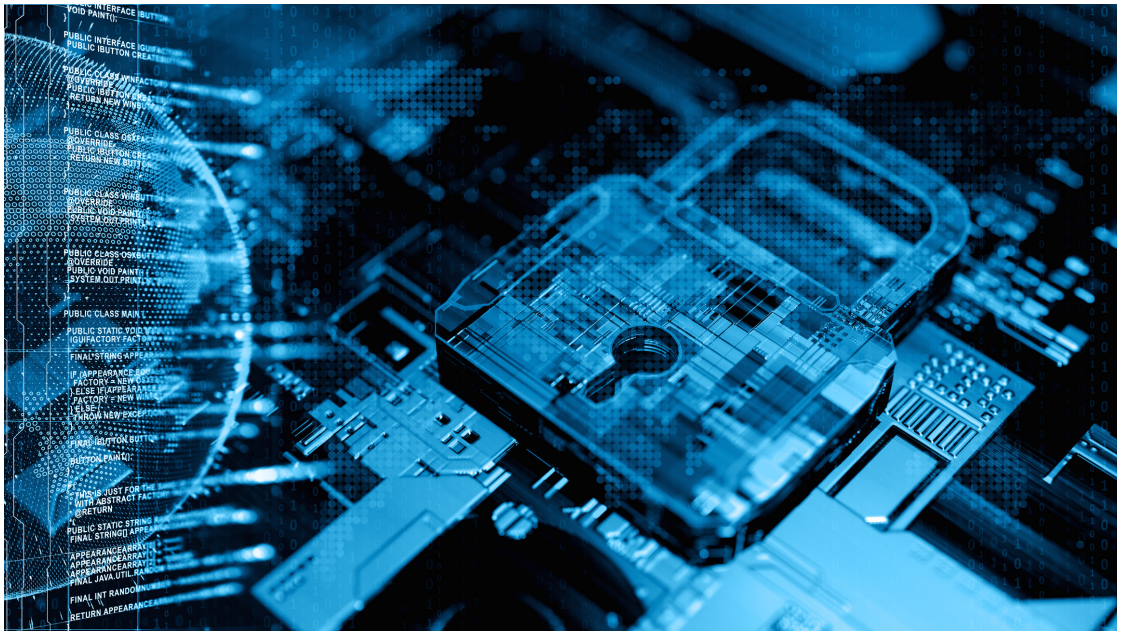
The benefits of your Digital Identity

Entities	Login	Services
Where you can utilize your Digital Identity • Ministry of Commerce and Industry • ROP • Ministry of Health • Ministry of Manpower • Muscat Municipality • Public Authority for Social Insurance • Oman Public Prosecution • National Center for Statistic and Information • Al Rafd Fund • Ministry of Endowments & Religious Affairs (MARA) • Ministry of Environment & Climate Affairs • TRA • Public Authority of Manpower register PAMR • Tender Board • Secretariat General for Taxation (SGT) • Ministry of Information • Ministry of Interior - Election • Oman Post	Please use your National ID or Resident card for login using smart card reader. 	The list of services you can apply for with your Digital Identity • Register a Business • Medical Appointments • Private Clearance • Building Permits • Insurer Details Update • Registering legal complaint • Request for Survey Approval • Request funding from Al Raffd Fund • Declaration processing • Pilgrims e-Registration • Obtain Environmental License • Register as a job seeker • eTendering Registeration • Business or income taxes statement • Municipal Council election • Postal Office Service

Source: Oman eGovernment service portal: http://www.oman.om/wps/portal/index/sso (as of October 2018)

[23] http://www.stadtzug.ch/de/ueberzug/ueberzugrubrik/aktuelles/aktuellesinformationen/?action=showinfo&info_id=383355

[24] In the EU, implementing acts on cooperation between Member States on eID, interoperability framework, assurance levels for eID means and notification have been adopted, with EU Member States being able to notify and recognise, on a voluntary basis, national eID means. As of 29 September 2018 the recognition of notified eID will become mandatory. https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Cooperation+Network+Resources



3 Challenges and opportunities

3.1 Data security

Recorded digital data need to be secured at system and individual level. To ensure security, data protection rules need to clearly define who should be allowed to access personal data and describe precisely when this data can be accessed without the consumer's consent. Unfortunately identity theft is still widespread, as is the release of private information resulting from hacking. Several cases of security and data breaches were reported involving centralized database systems but needed to be verified.[1] The breach of biometric data is particularly serious since such data cannot be replaced as easily as a password, a pin or number – and repercussions on those affected are severe. To prevent such breaches, the implementation of relevant security standards and strong privacy and data protection legal frameworks are required.

Risks associated with centralized systems

A centralized system with the government being the certificate authority can lead to data misuse and the risk of government surveillance of its populace. The risk is reduced when the information is hosted on a decentralized infrastructure, as for example is the case in Estonia with the X-Road (the backbone of e-Estonia) – personal data is scattered and kept in separate databases relying on separate technology stacks. Aall outgoing data from X-Road is said to be digitally signed and encrypted, and all incoming data is authenticated and logged.[2]

Australia: use of decentralized agencies

Australia established a network of decentralized agencies supported by a centralized real-time Document Verification Service. DVS is an online system, rather than a database, and allows organizations to compare a customer's identifying information with government records. The DVS is a

1 https://www.medianama.com/2017/07/223-aadhaar-leaks-government-websites/
2 https://e-estonia.com/solutions/interoperability-services/x-road/

secure system that operates 24/7 and matches key details contained on Australian-issued identifying credentials, providing a "yes" or "no" answer within seconds. The DVS protects customer privacy and stores no personal information. All DVS checks must be done with the informed consent of the person involved.[3] In addition, the Digital Transformation Agency (DTA) is working with other government agencies and main private sector entities on a federated digital identity ecosystem, called the Trusted Digital Identity Framework (TDIF). This ensures all users have a safe, secure way to connect with government services online.[4] A set of requirements were developed that include accreditation, authentication, fraud control, identity proofing, risk management, protective security, usability, and accessibility and privacy. While the TDIF incorporated some parts of the EU General Data Protection Regulation (GDPR), such as consent requirement, there is no intention to enforce the EU GDPR.[5]

Securing personal data

Authentication attributes and sensitive personal data need to be appropriately safeguarded against technology and security risk. In this context, encryption can help mitigate risk. Both companies and individuals have a role to play in safeguarding and protecting personal information. Individuals, can for example maintain up-to-date security programs on their devices, use complex passwords and ensure both PINs and passwords are not shared.

Training staff on maintaining the confidentiality of personal information, protecting it from unauthorized access and disclosure at business and government levels will contribute to enhanced security of data. Training staff is identified as key by the Canadian Privacy Commissioner. In addition, the biometrics is to be handled with caution as described in Box 5.

Box 5: Canada's guidelines for identification and authentication

- Only identify when necessary
- Determine what identity attributes are necessary to authorize a transaction
- Inform individuals and obtain the appropriate form of consent before identification
- Only authenticate when necessary
- Ensure the level of authentication is commensurate with risks
- Ensure employees are properly trained
- Maintain appropriate transaction records
- Continually assess threats and mitigate risks
- Protect personal information
- Rely on trusted identity documents or credentials
- Rely on trusted parties when outsourcing identity management
- Permit individuals to control their identification and authentication information
- Consider the use of biometrics carefully.

[3] https://www.dvs.gov.au/users/Pages/Businesses.aspx
[4] https://www.dta.gov.au/what-we-do/policies-and-programs/identity/
[5] https://www.dta.gov.au/files/identity/tdif-privacy-requirements.pdf

Box 5: Canada's guidelines for identification and authentication (continued)

In regards to biometrics, the guidelines stress that "In their identity management systems, companies should consider whether they are necessary, effective, and proportional to the potential privacy risks, and whether there is a less privacy-invasive way to identify or authenticate an individual".

Although they can be strong identifiers (i.e., a fingerprint is a unique and persistent identifier) they are far from being a panacea. For example, faces change over time, fingerprints can be worn down, and a person's gait can be altered by an accident or injury. Depending on how unique and persistent a biometric is, and how effective the technology used is at data matching, automated recognitions systems may produce false-positives or false-negatives.

Unlike a password, if a biometric is stolen or compromised it is very difficult, if not impossible, to change. If there is a risk that a biometric could be compromised, it should not be used for authentication on its own – it should be used with another authenticator, such as something only the individual has or knows.

When appropriate, biometric information should be locally stored (i.e., on a device) rather than in a central database. Centralized storage heightens the risk of data loss or the inappropriate cross-linking of data across systems. Local storage, such as mobile phones or smart cards, by contrast, gives individuals more control over their personal information.

By its very nature biometric information is sensitive information and should be protected by appropriate safeguards, including for example, encryption."

Source: Guidelines for Identification and Authentication, Office of the Privacy Commissioner of Canada, 2016, available at:
https://www.priv.gc.ca/en/privacy-topics/identity-and-privacy/identification-and-authentication/auth_061013/

The Estonia experience

Following the identification of a security flaw that could make the eID vulnerable to identity theft, the Estonian Government froze the ID card certificates of half of the population in November 2017. Those affected were invited to apply for a new certificate to enable them to carry out their online activities. They had until March 2018 to update their certificates. While no incident was reported, it highlighted the security risks associated with digital identities and how access to online services for citizens can be affected.[6]

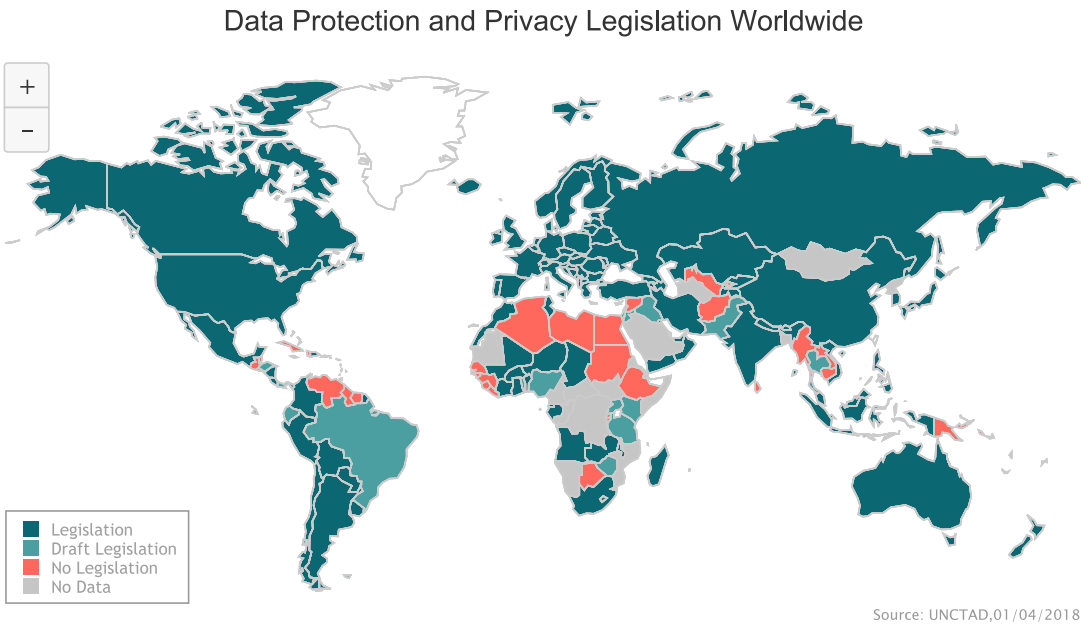
3.2 Privacy, trust and ownership

Trust can make or break deals if one of the parties isn't recognized as a trusted party – and is therefore a central element in the digital economy. As explained in the ITU discussion paper "Maintaining Trust in a Digital Connected Society"[7], the right to data protection, is about empowering "data subjects" and restricting the power of "data controllers" to achieve fairness, balance, transparency and legitimacy – while the right to privacy is about protection against invasion of one's private life. Privacy may be affected by the way in which personal data is collected, stored, used, processed, and disclosed by an increasing range of stakeholders in the digital ecosystem ranging from operators, service or

6 https://www.engadget.com/2017/11/04/estonia-freezes-resident-id-cards-security-flaw/
7 GSR16 Discussion paper on Maintaining Trust in a Digital Connected Society : https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/ITU_MaintainingTrust_GSR16.pdf

application providers, device manufacturers, operating system and other software providers, public entities, etc. Concerns about online privacy and how personal data can be used in ways not anticipated can prevent consumers from participating in the digital economy. In effect, users may often be ignorant of what is being done with their data, who uses it and for what purpose. In the digital economy, sensitive transactions are taking place across many aspects of our daily lives, and with vast amounts of personal data being stored in the clouds and on the Internet – and all without the user knowing where his/her data is located.

According to ITU, at least 109 countries have adopted legislation protecting data or privacy, or both. This is up from 83 countries in 2015[8]. According to data from the United Nations Conference on Trade and Development (UNCTAD) further 10 per cent of countries have draft legislation, while 21 per cent have no legislation in place (UNCTAD, see below).



Source: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Interestingly, Pakistan doesn't have a legislation on data protection and privacy, and in India – although privacy rules do exist as part of the Indian Information Technology Act, 2000, a complaint needs to be made before a Grievance Officer is appointed and the complaint addressed.[9] A data protection law is being drafted by an expert committee.

African Union moving ahead on data protection

Members States of the African Union (AU) took an important step towards data protection by adopting in 2014 the African Union Convention on Cybersecurity and Personal Data Protection. This stresses that data can only be processed for legitimate purposes but fails to define the term "legitimate".

Similar to the EU texts, the AU Convention identifies the following principles:

1. Consent and legitimacy.
2. Lawfulness and fairness.
3. Purpose, relevance and storage.
4. Accuracy.

[8] See ITU ICT Regulatory Outlook Report 2018.
[9] https://www.dlapiperdataprotection.com/index.html?c=IN&c2=&t=data-protection-officers

5. Transparency.
6. Confidentiality and security.

The Convention hasn't yet come into force and awaits ratification by 15 countries.[10] To facilitate the implementation of the Convention, the African Union Commission and the Internet Society in May 2018 developed Guidelines on Privacy and Personal Data Protection for Africa containing some 18 recommendations.[11]

Canada cautions

The Office of the Privacy Commissioner of Canada notes that identification and authentication will result in beneficial exchanges and protection of privacy only if they are appropriately designed. In other words, an organization needs to ensure *it does not collect*, *use, retain or disclose personal information that is not necessary to authenticate a person and authorize a transaction*. In addition, requiring "individuals to unnecessarily go through identification and/or authentication processes, or implementing overly cumbersome processes, can not only be privacy intrusive but can work against mutually beneficial interactions."[12]

EU regulation, May 2018

In the European Union, the General Data Protection Regulation, adopted in 2016 and enforced in May 2018, provides a unified regulatory framework for the protection of personal data across EU countries. Under the GDPR, citizens will have greater control over their personal data stored for identification and any other purposes. Within the GDPR, sensitive personal data such as genetic and biometric data processed to uniquely identify an individual are categorized as "special categories of personal data" (Article 9).

Box 6: How will the GDPR strengthen citizens' rights?

The new regulation will ensure that individuals benefit from the following:

They will have a right to be forgotten. When an individual no longer wants her/his data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted. This is about protecting the privacy of individuals, not about erasing past events or restricting freedom of the press.

They will be informed through easier access to their data. Individuals will have more information on how their data is processed and this information should be available in a clear and understandable way. A right to data portability will make it easier for individuals to transmit personal data between service providers.

They will have the right to know when their data has been hacked. Companies and organisations must notify the national supervisory authority of data breaches which put individuals at risk and communicate to affected individuals all high-risk breaches as soon as possible so that users can take appropriate measures.

---

10 The Convention includes a section on the institutional framework for the protection of personal data that foresees the establishment, in each Member State, of national personal data protection agency. The duties, powers and enforcement measures of the Agency are detailed in the Convention that sets the basic principles governing the processing of personal data and the obligations of the data controller:https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

11 https://www.internetsociety.org/resources/doc/2018/personal-data-protection-guidelines-for-africa/

12 https://www.priv.gc.ca/en/privacy-topics/identity-and-privacy/identification-and-authentication/auth_061013/

Box 6: How will the GDPR strengthen citizens' rights? (continued)

"Data protection by design" and "Data protection by default" are now essential elements in EU data protection rules. These are now a legal requirement. Data protection safeguards will be built into products and services from the earliest stage of development, and privacy-friendly default settings will be the norm – for example on social networks or mobile apps.

There will be stronger enforcement of rules. Data protection authorities will be able to fine companies up to 4% of their global annual turnover if they do not comply with EU rules.

Furthermore, the Regulation recognizes that children deserve specific protection of their personal data. Consent for processing the data of a child must be given or authorized by a parental or guardian. The age threshold is for Member States to define within a range between 13 and 16 years. This provision aims to shield children from pressure to share personal data without fully realizing the consequences.

The Regulation is said to "promote techniques such as anonymization (removing personally identifiable information where it is not needed), pseudonymization (replacing personally identifiable material with artificial identifiers), and encryption (encoding messages so only those authorised can read it) to protect personal data. This will encourage the use of 'big data' analytics, which can done using anonymised or pseudonymized data".

It is also technology neutral, protecting personal data regardless of the technology used or how the personal data is stored.

Companies/organizations processing data will have to explain in clear and plain language why they need the data, how they will be using it, and how long they intend to keep it. It is their responsibility as controller to assess how much data is needed and to ensure that irrelevant data isn't collected. If a security incident occurs and it is likely that the breach poses a risk to an individual's rights and freedoms, the company/organization has to notify the supervisory authority without undue delay, and at the latest within 72 hours after having become aware of the breach. If the data breach poses a high risk to those affected, they should all also be informed.

Source: European Commission Factsheet, Questions and Answers – Data protection reform:
http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm
https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en

The GDPR provides Data Protection Authorities (DPA) with different options in case of non-compliance with data protection rules. In cases of likely infringement, a warning may be issued; in case of infringement, the DPA can impose a reprimand, a temporary or definitive ban on processing and a fine of up to EUR 20 million or 4 per cent of the business's total annual worldwide turnover.

A set of guidelines on the protection of personal data in the Ibero-American[13] region was developed in 2017. Similar to the GDPR, these standards apply to the treatment of personal data contained in physical, automated media, regardless of the form or modality of their creation, type of media, processing, storage and organization (Section 4.1).

World Bank and OECD positions on privacy

The Digital Identity Toolkit of the World Bank stresses that to protect the privacy of people, an eID programme has to institute strong measures, including, but not limited to, appropriate legislation,

[13] http://www.redipd.es/documentacion/common/Estandares_eng_Con_logo_RIPD.pdf

data protection, public notices, an individual's right to consent, design principles for privacy, a documented privacy policy, an independent body for privacy oversight, and the effective enforcement of laws and regulations.

Similar data protection and privacy principles for identity management purposes are considered by the OECD as part of its policies for digital identity management that link practices and requirements with the need for security and privacy.

Box 7: OECD Policies for digital identity management should ensure both security and privacy

The level of assurance regarding the identity of the parties involved should be based on an assessment of the level of risk in the transactions.

To establish trust, digital identity management practices and requirements should be proportionate to the level of risk in the interactions between the parties. The potential impact on privacy of digital identity management practices should be assessed and addressed as appropriate.

Digital identity management practices should respect legal privacy protection requirements. The development and implementation of digital identity management systems should include privacy protection and data security from the outset. Taking advantage of the potential for the technology to support both privacy and security, innovative technical protection measures should reinforce privacy protection requirements wherever possible, including through the use of pseudonyms.

Central registration policies raise privacy issues related to the use of a central population register, unique identifiers and, where relevant, national identity card frameworks. Decentralized registration policy provides each organization or jurisdiction with a high degree of autonomy with respect to the privacy protection measures it establishes. The level of privacy protection provided to individuals when interoperability is implemented depends on the trust agreements between the various participants in the federation. A single technical privacy protection solution cannot be imposed on participants in a decentralized policy framework. Just as for interoperability, participants are more likely to adhere to a set of privacy protection objectives and high level measures than to detailed policy measures or technical mechanisms.

Source: OECD, "DIGITAL IDENTITY MANAGEMENT: Enabling Innovation and Trust in the Internet Economy"
http://www.oecd.org/sti/ieconomy/49338380.pdf

3.3 Interoperability

When different identity systems exist, interoperability becomes a necessity to reduce duplication, increase efficiencies and veracity in the authentication and verification process. Having non-interoperable systems increases fraud-related risks in verification and authentication processes and discrepancies in the data that may arise. Integrated and interoperable systems provide for greater public savings and reduce the cost of identity verification for the private sector. As further noted by the World Bank, enabling private companies to interact with digital identity systems through interoperable querying systems may also contribute positively by reducing transaction costs and increasing the reliability of authentication and verification processes.[14]

[14] World Bank (ID4D), 2018, Private Sector Economic Impacts from Identification Systems: http://pubdocs.worldbank.org/en/219201522848336907/PrivateSectorEconomicImpactsIDSystems-Web.pdf; http://id4d.worldbank.org/research

Furthermore, standards also play an important role in ensuring the effectiveness of interoperable digital identity systems. The lack of common standards may lead to using proprietary technology which in turn results in technology or vendor lock-in in both integrated or multiple digital identity systems.

To implement interoperability, a framework is required that includes minimal technical requirements relating to the connection of nodes of different systems; protection of privacy and confidentiality of data exchanged; storage of data; data integrity; and message formats.[15]

EU requires interoperability across member countries

In the European Union, the 2014 eIDAS Regulation[16] requires that electronic identification schemes across EU countries be interoperable. It provides for the establishment of an interoperability framework that is to be technology neutral that follows international standards, facilitates privacy by-design, ensures personal data is processed in accordance with the Directive 95/46 /EC and addresses accountability, transparency and security requirements of trust service providers. It enables citizens to carry out cross-border electronic transactions.

A cooperation mechanism, called the Cooperation Network has been set up to facilitate cooperation between EU Member States to achieve both interoperability and security of their eID schemes through the exchange of information and adoption of opinions.[17] This cooperation mechanism may provide guiding principles for establishing national and cross-country interoperability frameworks.

Box 8: The EU Interoperability Framework

The framework consists of:

(a) Reference to minimum technical requirements related to the assurance levels under Article 8;

(b) Mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8;

(c) Reference to minimum technical requirements for interoperability;

(d) Reference to a minimum set of person identification data uniquely representing a natural or legal person, which is available from electronic identification schemes;

(e) Rules of procedure;

(f) Arrangements for dispute resolution; and

(g) Common operational security standards.

NOTE: Article 8 foresees three types of levels for the degree of confidence in the claimed or asserted identity of a person: that is low, substantial and/or high.

Source: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

15 http://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2017/August-RR-ITP-2017/S1_Dr_Shahjahan_Mahmood.pdf
16 https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification
17 https://ec.europa.eu/digital-single-market/en/e-identification

4 Turning challenges into opportunities

The World Bank and the Center for Global Development together with other stakeholders, have adopted principles on identification for sustainable development[1] that summarize the issues to be addressed. The principles recognize that building digital identification systems creates opportunities to further development goals, but may also create a number of challenges and risks when data protection laws are absent. Creating inclusive, secure, and trustworthy identification systems can empower individuals and enhance their access to rights, services, and the formal economy. In compliance with SDG Goal 16 on promoting peace, justice and strong institutions, Target 16.9 requires the provision of "legal identity for all, including birth registration by 2030".

The increased adoption of digital technologies will probably contribute to the achievement of this target. These common principles may serve as a basis for stakeholders to address digital identity as part of national digital strategies and agendas. The principles are considered under the following overarching themes:

- Universal coverage and accessibility

  Identification systems should strive for continuous universal coverage from birth to death, free from discrimination, and accessible to all individuals.

  Barriers to access and usage and disparities in the availability of information and technology should be removed.

- Design: Robust, secure, responsive, and sustainable

  Identification systems should be robust, context-appropriate, and interoperable. While they should respond to user demand and long-term needs, they should collect and use only the information necessary for the system's explicit purpose. Open standards and vendor neutrality help to ensure financial and operational efficiency and sustainability.

- Governance: Building trust by protecting privacy and user rights

[1] http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples.pdf

Identification systems must be built on a legal and operational foundation of trust and accountability between government agencies, international organizations, private sector actors and individuals.

People must be assured of the privacy and protection of their data, the ability to exercise control and oversight over its use, and processes for independent oversight and the redress of grievances.

Digital identity – should be part of overall digital strategy

The issue of digital identity should be considered from a broader digital strategy and policy standpoint. Policy-makers should consider incorporating digital identity as part of their digital strategy for digital transformation. Involving all stakeholders in the consultation process is also an important element in the development of a national digital identity strategy. The private sector can play a leading role in the verification/authorization process through mobile devices (PIN, SMS, etc.), national identification number (NIN), smart cards, etc.

The Swedish Government has recognized the importance of digital identity within the context of digital security as part of its 2017 digital strategy.[2] Within the seven pillars of the UK's digital strategy, assuring people's digital identity is foreseen as part of the sixth pillar to digitize the government.[3] In 2016 the government launched GOV.UK Verify, an online identity verification service working with certified companies – this enables citizens to prove their identity online and to access government services such as tax payment.

In Tanzania, the National Identity Agency, established in 2008, developed in 2017 a three-year roadmap (2018-2020) to establish a national identity system, moving away from a fragmented identity ecosystem that integrates the national ID system with civil registration. A taskforce of eight organizations was established to carry out this endeavour and the consultative process involved all stakeholders.

Box 9: Tanzania's Digital ID Ecosystem Roadmap Goals

1. Universal coverage and accessibility
    - By December 2018, all eligible residents will have been registered in the national ID system and issued a national identification number (NIN).
    - By December 2019, all eligible residents will have been issued with their national ID card.
    - By December 2018, District Registration Office (DRO) will be established in every district.
2. Robust design and sufficient capacity
    - By March 2018, NIDA's data centers will be fully operational and secure.
    - By December 2018, NIDA will be technically and financially self-sustaining by charging fees for verification and card replacement.
3. Enabling environment of trust and accountability
    - By September 2018, the national ID system will benefit from a strong legal and regulatory framework that protects personal data and privacy.

---

2 www.government.se/49c292/contentassets/117aec2b9bf44d758564506c2d99e825/2017_digitaliseringsstrategin_faktablad_eng_webb-2.pdf

3 *UK Minister of State for Digital Matt Hancock's address to the Institute of Directors' Digital Strategy Summit, published* on 17 October 2017: https://www.gov.uk/government/speeches/the-seven-pillars-of-the-digital-strategy

Box 9: Tanzania's Digital ID Ecosystem Roadmap Goals (continued)

4. Efficient and reliable verification ecosystem
    - By December 2018, the national ID system will be used for all KYC processes for new customers in financial and mobile services.
    - By December 2018, the national ID system will be integrated into key services and programmes, including tax administration, student loans, civil service payroll, pensions and health insurance.

Source: http://www.id4africa.com/2018_event/Presentations/PS2/1-2-2_Tanzania_Alphonce_Malibiche.pdf

The user's perspective needs to be taken into account when developing digital identity strategy and roadmaps. Simplicity, confidentiality, flexibility and ease-of-use are additional principles that will impact the user's confidence and trust in using the system as well as factors such as reliability, accountability and the integrity of identity data stored and exchanged. Important too for the user/citizen is to be informed of the benefits of adhering to such systems but also to clearly understand their rights and potential risks and vulnerabilities.

While the positive potential of digital identification is widely recognized, implementing and adopting digital identification initiatives still present a challenge due to the complexity of the ecosystem required, the need to ensure robust data protection and security, and the need to interoperate with existing services, systems and identification schemes. Collaboration among agencies is needed to reduce the risk of fragmentation and ensure interoperable systems.

ITU project underway to help deploy digital identity initiatives

In the field of digital identity, many initiatives are underway as mentioned earlier. Leveraging these initiatives, ITU's Telecommunication Development Bureau (BDT) has launched a project to help countries, particularly low- and middle-income countries (LMICs), to deploy digital identity initiatives that add value in most digital economy areas. A Digital Identity Roadmap was developed to provide guidance on the development of a national digital Identity framework implementation plan. ITU has conceived this practical tool to be implementable in a variety of context and environment, independently of the country's level of development[4].

[4] See: https://www.itu.int/en/ITU-D/ICT-Applications/Pages/digital-identity.aspx

Acronyms

AFR	Africa
AU	African Union
BDT	Telecommunication Development Bureau
CNIC	Computerized National Identity Card
CVRS	Civil Registration and Vital Statistics
DPA	Data Protection Authorities
DRO	District Registration Office
DTA	Digital Transformation Agency
DVS	Document Verification Service
EAP	East Asia Pacific
ECA	East & Central Asia
eID	Electronic identification
eIDAS	EU Regulation on Electronic identification and Trust Services for Electronic Transactions
eTS	Electronic Trust Services
EU	European Union
GDPR	General Data Protection Regulation
GSMA	Global System for Mobile Communications Association
HDC	Hebbal Data Centre
HIC	High-Income Country
HoF	Head of Family
ICT	Information and Communication Technology
ID4D	Identification for Development
ITA	Information Technology Authority
ITU	International Telecommunication Union
KYC	Know-Your-Customer
LCR	Latin and Central America Region
LIC	Low-Income Country
LMICs	Low- and Middle-Income Countries
MDC	Manesar Data Centre

MNA	Middle East & North Africa
NDCC	National Digital Certification Center
NIA	National Identity Agency
NADRA	National Database and Registration Authority
NBTC	National Broadcasting and Telecommunications Commission (Thailand)
NIN	National Identification Number
OECD	Organisation for Economic Co-operation and Development
OTP	One Time Pin
PDS	Public Distribution System
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PoA	Proof of Address
PoI	Proof of Identity
PoR	Proof of Relationship
PTA	Pakistan Telecommunication Authority
RENAPER	Registro Nacional de las Personas de Argentina
SAR	South Asia Region
SDGs	Sustainable Development Goals
SIM	Subscriber Identity Module
SMS	Short Message Service
TDIF	Trusted Digital Identity Framework
TRAI	Telecom Regulatory Authority of India
UIDAI	Unique Identification Authority of India
UMIC	Upper Middle Income
UNCTAD	United Nations Conference on Trade and Development

International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Office of the Director
Place des Nations
CH-1211 Geneva 20 – Switzerland
Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Deputy to the Director and Director，Administration and Operations Coordination Department (DDR)
Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5784
Fax: +41 22 730 5484

Infrastructure Enabling Environmnent and e-Applications Department (IEE)
Email: bdtiee@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Innovation and Partnership Department (IP)
Email: bdtip@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Project Support and Knowledge Management Department (PKM)
Email: bdtpkm@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

Africa

Ethiopia
International Telecommunication Union (ITU)
Regional Office
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Ethiopia

Email: itu-addis@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroon
Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroun

Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal
Union internationale des télécommunications (UIT)
Bureau de zone
19, Rue Parchappe x Amadou Assane Ndoye
Immeuble Fayçal, 4e étage
B.P. 50202 Dakar RP
Dakar – Sénégal

Email: itu-dakar@itu.int
Tel.: +221 33 849 7720
Fax: +221 33 822 8013

Zimbabwe
International Telecommunication Union (ITU)
Area Office
TelOne Centre for Learning
Corner Samora Machel and Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Americas

Brazil
União Internacional de Telecomunicações (UIT)
Regional Office
SAUS Quadra 06, Bloco "E"
11º andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasilia, DF – Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados
International Telecommunication Union (ITU)
Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343/4
Fax: +1 246 437 7403

Chile
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Casilla 50484, Plaza de Armas
Santiago de Chile – Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT, 4.º piso
P.O. Box 976
Tegucigalpa – Honduras

Email: ituteguciglapa@itu.int
Tel.: +504 22 201 074
Fax: +504 22 201 075

Arab States

Egypt
International Telecommunication Union (ITU)
Regional Office
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egypt

Email: itucairo@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia and the Pacific

Thailand
International Telecommunication Union (ITU)
Regional Office
Thailand Post Training Center, 5th floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 – Thailand

Mailing address
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thailand

Email: itubangkok@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia
International Telecommunication Union (ITU)
Area Office
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonesia

Email: itujakarta@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322
Tel.: +62 21 380 2324
Fax: +62 21 389 05521

CIS countries

Russian Federation
International Telecommunication Union (ITU)
Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Mailing address:
P.O. Box 25 – Moscow 105120
Russian Federation

Email: itumoskow@itu.int
Tel.: +7 495 926 6070
Fax: +7 495 926 6073

Europe

Switzerland
International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Europe Unit (EUR)
Place des Nations
CH-1211 Geneva 20 – Switzerland
Switzerland
Email: eurregion@itu.int
Tel.: +41 22 730 5111

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-27971-4

9 789261 279714

Published in Switzerland
Geneva, 2018