CATALOG OF Technical Standards for Digital Identification Systems

UPDATED AUGUST 2022

ID4D

WORLD BANK GROUP

© 2022 International Bank for Reconstitution and Development/The World Bank
1818 H Street, NW, Washington, D.C., 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

This work is a product of the staff of The World Bank with external contributions. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent. The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Nothing herein shall constitute or be considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, or of any participating organization to which such privileges and immunities may apply, all of which are specifically reserved.

Rights and Permission

Attribution—Attribution—Please cite the work as follows: Mittal, Anita. 2022. *Catalog of Technical Standards for Digital Identification Systems*, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO)

Translations—If you create a translation of this work, please add the following disclaimer along with the attribution: This translation was not created by The World Bank and should not be considered an official World Bank translation. The World Bank shall not be liable for any content or error in this translation.

Adaptations—If you create an adaptation of this work, please add the following disclaimer along with the attribution: This is an adaptation of an original work by The World Bank. Views and opinions expressed in the adaptation are the sole responsibility of the author or authors of the adaptation and are not endorsed by The World Bank.

Third Party Content — The World Bank does not necessarily own each component of the content contained within the work. The World Bank therefore does not warrant that the use of any third-party-owned individual component or part contained in the work will not infringe on the rights of those third parties. The risk of claims resulting from such infringement rests solely with you. If you wish to re-use a component of the work, it is your responsibility to determine whether permission is needed for that re-use and to obtain permission from the copyright owner. Examples of components can include, but are not limited to, tables, figures, or images.

All queries on rights and licenses should be addressed to World Bank Publications, The World Bank, 1818 H Street, NW, Washington, DC, 20433; USA; email: pubrights@worldbank.org.

Cover images: Shutterstock.

TABLE OF CONTENTS

LIST OF FIGURES

ABBREVIATIONS

AFNOR	Association Française de Normalisation (Organisation of the French Standardisation System)
ANSI	American National Standard Institute
ASN.1	Abstract syntax notation one
BAPI	Biometric Application Programming Interface
CAP	Chip Authentication Program
CBEFF	Common Biometric Exchange Formats Framework
CEN	European Committee for Standards
CITeR	Center for Identification Technology Research
DHS	Department of Homeland Security
DIN	German Institute of Standardization
eID	Electronic Identification Card
EMV	Europay, MasterCard and Visa—Payment Smart Card Standard
EMVCo	EMV Company
FIDO	Fast IDentity Online
GSM	Global System for Mobile Communication
GSMA	The GSM Association
IBIA	International Biometrics and Identification Association
ICAO	International Civil Aviation Organization
ICT	Information and Communication Technologies
ID	Identification
ID4D	Identification for Development
IEC	The International Electrotechnical Commission
ILO	International Labor Organization
INCITS	International Committee for Information Technology Standards
ISO	The International Organization for Standardization
IT	Information Technologies
ITU-T	ITU’s Telecommunication Standardization Sector
JTC	Joint Technical Commission
MRZ	Machine-Readable Zone
NADRA	National Database and Registration Authority (of Pakistan)
NICOP	National Identity Cards for Overseas Pakistanis
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structural Information Standards
OpenID	Open ID Foundation
PSA	Pakistan Standards Authority
PIN	Personal Identification Number

PKI	Public key infrastructure
RFID	Radio-Frequency Identification
RMG	Registration Management Group
SA	Standards Australia
SDGs	Sustainable Development Goals
SIA	Secure Identity Alliance
SIS	Swedish Standards Institute
SNBA	Swedish National Biometrics Association
UIN	Unique Identity Number
UIDAI	Unique Identification Authority of India
WB	The World Bank
WG	Working Group

ABOUT ID4D

The World Bank Group's Identification for Development (ID4D) initiative uses global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification systems to achieve the Sustainable Development Goals. It operates across the World Bank Group with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, legal, among others.

The mission of ID4D is to enable all people to access services and exercise their rights, by increasing the number of people who have an official form of identification. ID4D makes this happen through its three pillars of work: thought leadership and analytics to generate evidence and fill knowledge gaps; global platforms and convening to amplify good practices, collaborate and raise awareness; and country and regional engagement to provide financial and technical assistance for the implementation of robust, inclusive and responsible digital identification systems and with civil registration.

The work of ID4D is made possible through support from the Bill & Melinda Gates Foundation, the UK Government, the French Government, Norad, and the Omidyar Network.

To find out more about ID4D, visit id4d.worldbank.org. To participate in the conversation on social media, use the hashtag #ID4D.

ACKNOWLEDGMENTS

The catalog was prepared by Anita Mittal with contributions from Tariq Malik, Ott Köstner, Flex Ortega De La Tora, Adam Cooper, Ted Dunstone, Seth Ayers, Daniel Bachenheimer, Alastair Treharne, Dr. Narjees Adennebi, Sanjay Dharwadker, Marta Ienco, Stephanie de Labriolle, Julien Drouet, Dr. Adeel Malik, and Anna Metz.

The catalog was presented and discussed during two workshops (September 2017 and March 2018), which informed the content and design. The following organizations participated in these workshops: Accenture; American National Standards Institute; Caribou Digital; Center for Global Development; DIAL; Digital Impact Alliance; Ernst & Young; European Commission; FIDO Alliance; Bill & Melinda Gates Foundation; Government Digital Service; GSMA; ID2020; ICAO; IOM; iSPIRIT; Mastercard; Mercy Corp; Microsoft; National Institute of Standards and Technology; Omidyar Network; One World Identity; Open Identity Exchange; Open Society Foundation; Plan International; PricewaterhouseCoopers; Secure Identity Alliance; Simprints; The World Economic Forum; United Nations Development Program; UNHCR; UNICEF; USAID; Vital Strategies; and WFP.

The catalog was updated in August of 2022.

1. INTRODUCTION

Trusted and inclusive identification (ID) systems are crucial for development, as enshrined in Sustainable Development Goal (SDG) Target 16.9, which mandates countries to provide "legal identity for all, including birth registration." For individuals, proof of legal identity is necessary to access rights, entitlements, and services. Without it, they may face exclusion from political, economic, and social life. For governments, modern identification systems allow for more efficient and transparent administration and service delivery, a reduction in fraud and leakage related to benefits payments, increased security, accurate vital statistics for planning purposes, and greater capacity to respond to disasters and epidemics.

To realize these benefits, many countries are in the process of modernizing their existing identification systems or building new ones. In doing so, most have attempted to capitalize on the promise of new, digital identification technologies, including biometric identification, electronic credentials, such as smart cards and mobile IDs, and online authentication infrastructure.

These advancements, particularly when combined with related digital technologies, such as online and mobile payments systems, have the potential to improve people's lives by making it easier and more secure to access services and transactions. At the same time, the deployment of digital technologies in identification poses several challenges, including with respect to data protection and privacy, ensuring the inclusion of the most vulnerable, and the financial and operational sustainability of different technology options.

Novel approaches, including decentralized and federated ID systems, are emerging rapidly along with new types of virtual and digital credentials. As people are looking to prove who they are in different settings including online and across borders, and service providers look to more efficient and high-assurance verification mechanisms, the need for trusted and interoperable identification system has also intensified. Adherence to technical standards – henceforth "standards" – is one of the core building blocks of optimizing a system's operations and its ability to support service delivery.

Standards establish universally understood and consistent interchange protocols, testing regimes, quality measures, and best practices with regard to the capture, storage, transmission, and use of identity data, as well as the format and features of identity credentials and authentication protocols. Therefore, they are crucial at each stage of the identity lifecycle, including registration, identity proofing, credentialing, and authentication. The choice of standards has implications for a wide range of performance metrics and system capabilities, including the accuracy, quality, and consistency of data collection, the interoperability between ID subsystems, with other domestic systems, and across borders, the level of trust in identities and authentication protocols, system and information security, and vendor- and technology neutrality.

2. OBJECTIVE

Standards are critical for identification systems to be trusted, interoperable and sustainable. The objective of this report is to identify the existing international technical standards and frameworks applicable across the identity lifecycle for technical interoperability. This catalog of technical standards can serve as a reference for stakeholders across the identification ecosystem and support the selection of appropriate standards based on country context and objectives of the system. A decision tree of the technical standards, organized by technology area, is provided to help with the assessment and selection process. The application of the decision tree has been illustrated by country case studies of Estonia, India, Malawi, Pakistan and Peru. In addition, this catalog of existing standards, organized by category and subcategory, may also help to identify areas where standards are missing or where there are competing standards and a choice needs to be made.

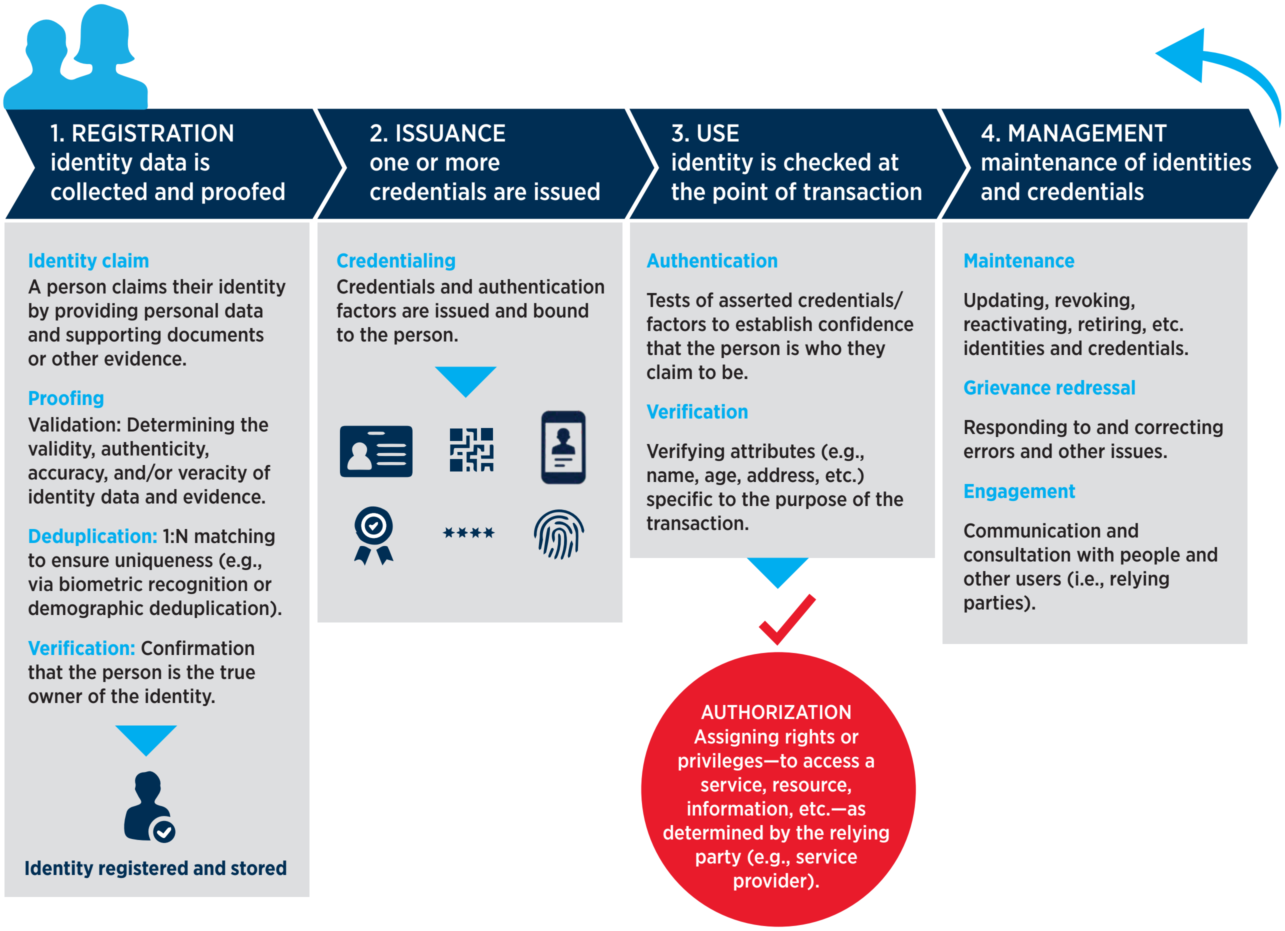
3. SCOPE

Identification systems within and across countries may take a variety of forms, each with different applicable standards. This report focuses only on technical standards that relate to the design and implementation of identity ecosystems in a digital context. More specifically, the standards described in this catalog center around the software and physical hardware components, systems, and platforms, which enable machine-to-machine communication. Major standards to facilitate the technical quality and interoperability of the ID system related to: (1) biometrics, (2) cards, (3) 2D barcodes, (4) digital signatures, and (5) federation protocols. In some cases, standards represent a clear consensus, and are used by a majority of ID systems globally. In other cases, there are competing standards that countries must adjudicate between. Different standards will also apply depending on the general design and goals of the ID system (e.g., whether the ID card will be used for international travel). For a more detailed discussion on standards and how they relate to different layers of an interoperability framework, see the ID4D Practitioner's Guide.[1]

[1] https://id4d.worldbank.org/guide/standards; https://id4d.worldbank.org/guide/interoperability-frameworks.

4. THE IDENTITY LIFECYCLE

FIGURE 1 Identity Lifecycle



1. REGISTRATION identity data is collected and proofed

Identity claim A person claims their identity by providing personal data and supporting documents or other evidence.

Proofing Validation: Determining the validity, authenticity, accuracy, and/or veracity of identity data and evidence.

Deduplication: 1:N matching to ensure uniqueness (e.g., via biometric recognition or demographic deduplication).

Verification: Confirmation that the person is the true owner of the identity.

Identity registered and stored

2. ISSUANCE one or more credentials are issued

Credentialing Credentials and authentication factors are issued and bound to the person.

3. USE identity is checked at the point of transaction

Authentication Tests of asserted credentials/factors to establish confidence that the person is who they claim to be.

Verification Verifying attributes (e.g., name, age, address, etc.) specific to the purpose of the transaction.

AUTHORIZATION Assigning rights or privileges—to access a service, resource, information, etc.—as determined by the relying party (e.g., service provider).

4. MANAGEMENT maintenance of identities and credentials

Maintenance Updating, revoking, reactivating, retiring, etc. identities and credentials.

Grievance redressal Responding to and correcting errors and other issues.

Engagement Communication and consultation with people and other users (i.e., relying parties).

Source: Practitioner's Guide https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

Globally, digital identity ecosystems are increasingly complex, and consist of a wide range of identity models and actors with diverse responsibilities, interests, and priorities. Understanding the processes and technology involved in identification is crucial for identifying the standards which are applicable in a given system. To that end, this section provides a general overview of the digital identity lifecycle (based on Technology Landscape for Digital Identification report 2018). This framework is then used to analyze relevant identification standards in Section 6.

Identities are created and used as part of a lifecycle that includes four fundamental stages: (a) registration, including enrollment and validation, (b) issuance of documents or credentials, and (c) authentication and verification of identity attributes for service delivery or transactions. Identity providers also engage in ongoing management of the system, including updating and revocation or termination of identities/credentials, grievance redress, and public engagement (see Figure 1).

4.1 Registration

The lifecycle begins when an individual first registers their identity, which involves the identity claim and the identity proofing process.

4.1.1 Identity Claim

This process involves capturing and recording key identity attributes from a person who claims a certain identity, such as biographic data (e.g., name, date of birth, gender, address, email), bio-metrics (e.g., fingerprints, face, iris scan). Which attributes and supporting documentation or evidence are captured during this phase, the methods and standards used to capture them, and the resulting data quality have important implications for the inclusivity and trustworthiness of the system and the credentials issued as well as the speed of data collection, program cost, interoperability with other ID systems, and its utility for various stakeholders..

4.1.2 Identity Proofing

Once the person has claimed an identity, this data they provide is then validated. This involves checking the validity, authenticity, and accuracy of the supporting documents or evidence provided and confirming that the identity data is valid, current, and related to a real-life person.

4.2 Issuance

After registration, the identity provider issues one or more credentials and/or authenticators—e.g., cards, certificates, PINs, etc.—that can be used by a person alone or in combination to prove or "assert" the identity that has just been created. For an ID to be considered digital, the credentials issued must store data electronically and/or be usable in a digital environment (e.g., being machine readable and/or usable on the internet).Types of such credentials include 2D bar code cards, smart (chip) cards, and mobile IDs[2].

4.3 Authentication

Once a person has been registered and credentialed, they can then authenticate or "prove" their identity to access the associated benefits and services. The authentication process can involve one or multiple factors—i.e., identity credentials and/or attributes. For example, people may use their username and PIN to login to an e-government portal to pay their taxes, or use their card and photo or fingerprint to prove their identity at a healthcare facility.

4.4 Lifecycle Management

Throughout the lifecycle, identity providers manage identity data and credentials through a dynamic process. This includes updating and re-proofing identity attributes that change over time—e.g., surname, address, facial image, etc.—as well as updating, renewing, revoking, or deactivating credentials. Identity providers also work to correct errors, address grievances, and continuously engage with the public and relying parties.

The identity lifecycle requires technical standards at each stage and sub-stage, as discussed further in Section 6.

4.5 Federation

Federation is the ability of one organization to accept another organization's identity credentials for authentication based on inter-organizational trust. The trusting organization must be comfortable that the other identity provider has acceptable policies, and that those policies are being followed. Federation protocols and assurance and trust frameworks facilitate federation of digital identity between organizations. Federation protocols like SAML (Security Assertion Mark-up Language) and OpenID Connect are used to convey the authentication result by the identity provider to the trusting organization. For federation to be effectively used globally, agreement and mapping with the ISO defined assurance framework and adoption of standards are critical.

Federation can occur at multiple levels:

- A trusting organization can capture and send the credential to the issuing organization (i.e., an identity provider) for verification, to authenticate an identity. After verification of the credential, the issuing organization sends a yes/no confirmation and may, when warranted and consented, send a set of claims giving information about the person, using federation protocols like SAML.
- A trusting organization can accept credentials issued by another organization, but still authenticate and authorize the individual locally. For example, a passport issued one country is accepted as a valid credential by a receiving country (and could be validated, for example, through ICAO's global Public Key Directory or PKD), but the receiving country's immigration office still authenticates the holder and requires a visa to authorize travel.
- A trusting organization can accept specific attributes describing an individual from another organization. For example, a bank can request

[2] For more details on credential and authenticators, see: https://id4d.worldbank.org/guide/types-credentials-and-authenticators.

credit score from a credit bureau, rather than maintaining its own registry of credit information.

- A trusting organization can accept an authorization decision from another organization (i.e., mutual recognition). For example, a driver's license authorizing a person to drive in one location may be accepted by another location.

The identity lifecycle requires technical standards at each stage and sub-stage, as discussed further in Section 6. Importantly, the type of attributes (biometrics, biographic, and others) captured during enrollment and the methodologies used to record them have important implications for the assurance and trust in the identity system as well as its utility and interoperability with other domestic and international identity systems.

5. DIGITAL ID RELATED TECHNICAL STANDARDS

5.1 Why Are Standards Important?

In general, technical standards contain a set of specifications and procedures with respect to the operation, maintenance, and reliability of materials, products, methods, and services used by individuals or organizations. Standards ensure the implementation of universally understood protocols necessary for operation, performance, compatibility, and interoperability, which are in turn necessary for product development and adoption. A lack of standards creates issues for the effective and sustainable implementation of identification systems, including with respect to interoperability, interconnectivity and vendor lock-in.

As digital systems and processes are replacing paper-based systems, the technologies, inter-device communication and security requirements underpinning identification systems have become more complex—increasing the importance of standards for identity management. However, choosing between standards is challenging due to rapid technological innovation and disruption, product diversification, changing interoperability and interconnectivity requirements, and the need to continuously improve the implementation of standards.

5.2 Standards-Setting Bodies

Standards are rigorously defined by organizations that are created and tasked specifically for this purpose. In the case of ICT-related standards, these organizations—with the help of experts—set up, monitor, and continuously update technical standards to address a range of issues, including but not limited to various protocols that help ensure product functionality and compatibility, as well as facilitate interoperability. These standards and related updates are regularly published for the general benefit of the public . According to the International Telecommunication Union's (ITU) Technology Watch, several organizations are actively developing technical standards for digital identification systems, including international organizations such as the United Nations' specialized agencies, industry consortia, and country-specific (national) organizations. Each are described briefly below.

- **International Organizations.** The following prominent international organizations are actively involved in setting relevant technical standards: the International Organization for Standardization (ISO); the International Electrotechnical Commission (IEC); ITU's Telecommunication Standardization Sector (ITU-T); the International Civil Aviation Organization (ICAO); International Labor Organization (ILO); and the European Committee for Standards (CEN), World Wide Web Consortium (W3C), Internet Engineering Task Force (IETF)/Internet Society.

- **National Organizations.** In addition to international organizations, country-specific organizations also develop technical standards based on their needs and systems of measurement. Some important organizations include the American National Standard Institute (ANSI); the U.S. National Institute of Standards and Technology (NIST); the U.S.-based International Committee for Information Technology Standards (INCITS), the U.S. Department of Homeland Security (DHS); the U.S. Department of Defense (DoD); Standards Australia (SA); the Swedish Standards Institute (SIS); the Swedish National Biometrics Association (SNBA); the German Institute of Standardization (DIN); Organization of the French Standardization System (AFNOR); the Dutch Standards Organization (NEN); the Unique Identification Authority of India (UIDAI); the Bureau of Indian Standards (BIS); and the Pakistan Standards Authority (PSA).

- **Industry Consortia.** Finally, industry consortia and some nonprofit organizations are also involved in either developing standards or promoting best practices to meet the needs of their members. Prominent examples include: the U.S. government-sponsored consortium known as the Biometric Consortium; Secure Identity Alliance (SIA), Center for Identification Technology Research (CITeR); IEEE Biometrics

Council; Biometrics Institute, Australia; Smart Card Alliance; International Biometrics and Identification Association (IBIA); Kantara Initiative; Open Identity Exchange; Open Security Exchange; Asian Pacific Smart Card Association (APSCA); Organization for the Advancement of Structural Information of Standards (OASIS); Fast IDentity Online (FIDO) Alliance; and Open ID Foundation.

Among the major-standard setting bodies, this review has found that most prominent countries and industry consortia are connected to and collaborate with ISO (for example, through subcommittees and working groups (WG)) to modify or confirm standards for their requirements. Information on the ISO technical committees, sub committees, and working groups involved with standards relevant to digital identity lifecycle is placed at Appendix A.

5.3 Technical Standards

This section contains a compilation of technical standards identified as relevant for identification systems. Most of them relate to credentials and authentication factors. The Technical Standards are grouped in two tables. Table 1 lists standards which are required for interoperability and the second lists standards which address additional requirements such as security and quality. The standards are continuously revised by the standards organizations. The standards in the table have hyperlinks to the website providing information about the standard. The ISO standards page provides information and link to the newer version of the standard if available.

Technical Standards for Interoperability

The major categories of standards listed below fall into the following areas (Figure 2).

1. **Biometrics:**
   a. Image standard: Multiple competing standards are in use for capturing facial image (PNG, JPEG, JPEG2000 in most of the systems while GIF/TIFF (proprietary standards) may be in use in a few). For fingerprint image JPEG, JPEG2000 and WSQ standards are in use.
   b. Biometric data interchange format standards and biometric interface standards: Both of these standards are necessary to achieve full data interchange and interoperability for biometric recognition in an open systems environment. The biometric data interchange format standards specify biometric data interchange formats for different biometric modalities. Biometric data complying with a biometric data interchange format of ISO 19794 represents the core component of biometric interoperability. Parties that agree on a biometric data interchange format specified in ISO 19794 should be able to decode each other's biometric data. Biometric interface standards support exchange of biometric data within a system or among systems and include ISO 19785 Information technology — Common Biometric Exchange Formats Framework. ISO 19785 specifies the basic structure of a standardized Biometric Information Record (BIR), which includes the biometric data interchange record with added metadata such as when it was captured, its expiry date, whether it is encrypted, etc.
2. **Card/Smart Card:** For countries that issue a card-based credential, standards such as ISO-7810 are relevant to ensure interoperability and interconnectivity. For contact cards, where the chip is embossed on the card, the ISO/IEC 7816 standard is followed globally; for contactless cards, where the chip is embedded inside the card, the ISO/IEC 14443 standard is followed. For cards that can also be used as electronic travel documents—including electronic ID cards, passports, drivers' licenses, or any other machine-readable travel documents (MRTDs) used for crossing borders— compliance with ICAO 9303 should be followed.
3. **Digital Signatures:** Multiple non-competing standards are listed whose applicability depends on the approach taken by the specific

system. The guidance note on the digital signature algorithm provides the pros and cons of the two digital signature algorithms RFC3447 RSA/ EC 25519.

4. **2D bar code:** The guidance note on standards selection column provides the pros and cons of the two commonly used bar code standards, PDF417 and QR code, in ID systems.
5. **Federation protocols:** OpenID Connect and OAuth are being increasingly used for federation while SAML has been used extensively earlier.

The standards applicable to a specific ID system may be selected from all or some of the 5 categories.

A decision tree to support easier selection of applicable standards based on the choice of technologies used as part of an Identification system is diagrammatically presented in figure 3.

1. Start at the top of tree and traverse the tree along each branch further down as long as the technology or standard category mentioned at each node is relevant to the ID system.
2. The standards at the leaf level of the branch of the tree (Selection 4) are the applicable standards based on the selections made about the use of a particular technology or system feature (Selection 1 , 2 and 3).
3. Some of the leaf nodes (Selection 4) feature competing standards. The guidance note in the table of standards provides further information about how to assess and select the appropriate one from the available competing standards.
4. A short description and weblink to the standard is available in the standards catalog table.

FIGURE 2 Standards for Identification System

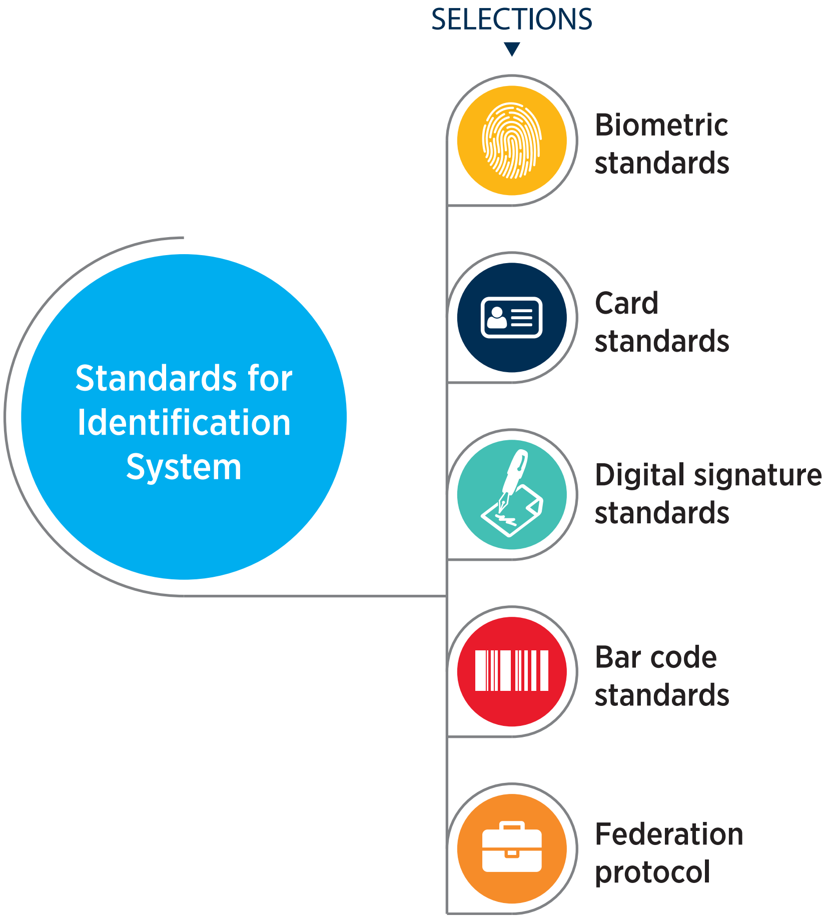
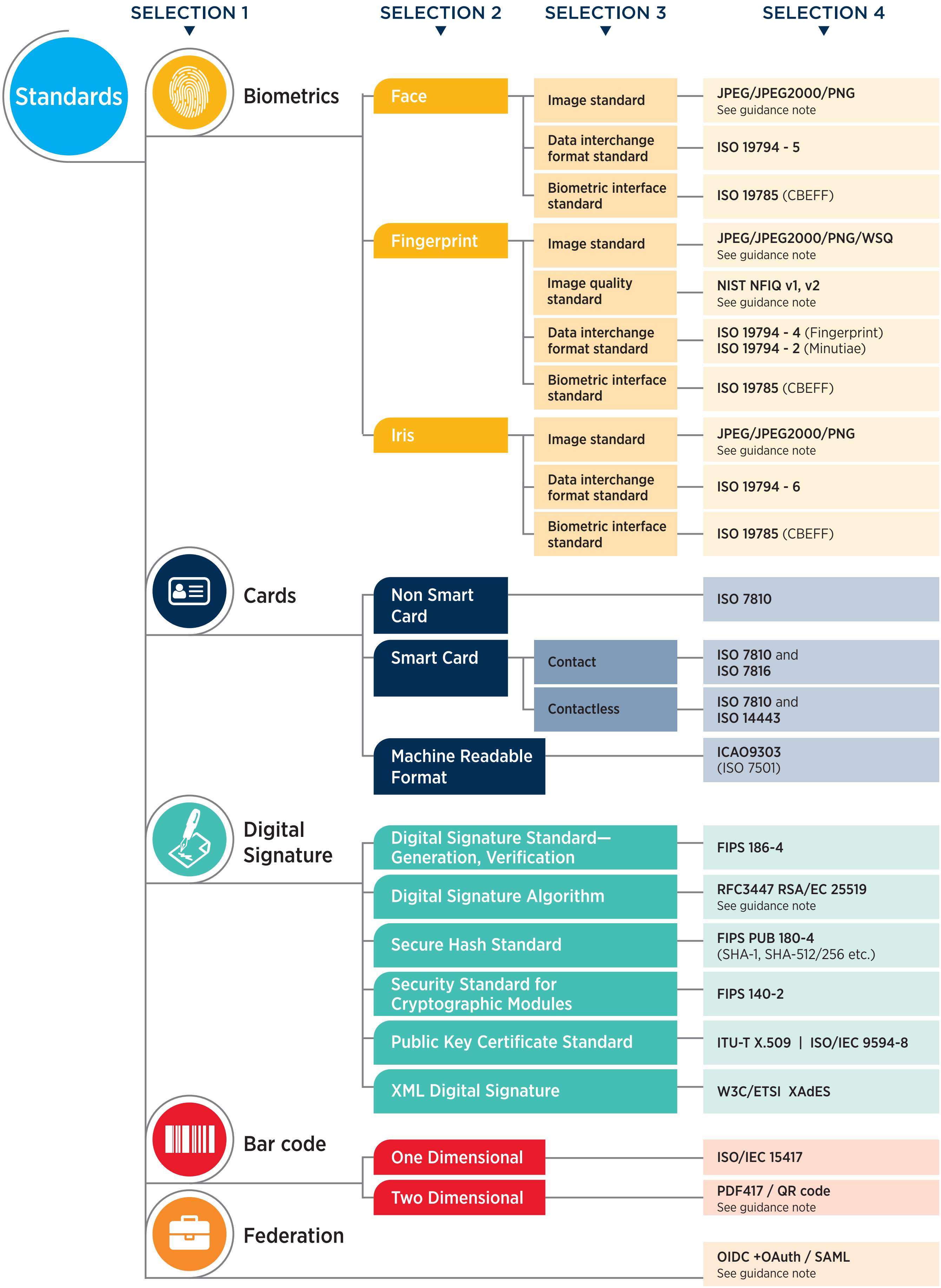


FIGURE 3

DECISION TREE STANDARDS



	SELECTION 1	SELECTION 2	SELECTION 3	SELECTION 4
Standards	Biometrics	Face	Image standard	JPEG/JPEG2000/PNG See guidance note
			Data interchange format standard	ISO 19794 - 5
			Biometric interface standard	ISO 19785 (CBEFF)
		Fingerprint	Image standard	JPEG/JPEG2000/PNG/WSQ See guidance note
			Image quality standard	NIST NFIQ v1, v2 See guidance note
			Data interchange format standard	ISO 19794 - 4 (Fingerprint) ISO 19794 - 2 (Minutiae)
			Biometric interface standard	ISO 19785 (CBEFF)
		Iris	Image standard	JPEG/JPEG2000/PNG See guidance note
			Data interchange format standard	ISO 19794 - 6
			Biometric interface standard	ISO 19785 (CBEFF)
	Cards	Non Smart Card		ISO 7810
		Smart Card	Contact	ISO 7810 and ISO 7816
			Contactless	ISO 7810 and ISO 14443
		Machine Readable Format		ICAO9303 (ISO 7501)
	Digital Signature	Digital Signature Standard—Generation, Verification		FIPS 186-4
		Digital Signature Algorithm		RFC3447 RSA/EC 25519 See guidance note
		Secure Hash Standard		FIPS PUB 180-4 (SHA-1, SHA-512/256 etc.)
		Security Standard for Cryptographic Modules		FIPS 140-2
		Public Key Certificate Standard		ITU-T X.509 | ISO/IEC 9594-8
		XML Digital Signature		W3C/ETSI XAdES
	Bar code	One Dimensional		ISO/IEC 15417
		Two Dimensional		PDF417 / QR code See guidance note
	Federation			OIDC +OAuth / SAML See guidance note

S.No	Inter-operability Area	SubArea	Standard Specification/ (common name)	Standard description	Standards Body	Guidance note for standards selection
A.1	Biometrics	Image Standard	ISO/IEC 15444-1 (JPEG2000)	Image Coding Standard (both lossy and lossless compression)	ISO and IEC	PNG is a lossless image format which is not commonly used in identification systems. The JPEG and JPEG2000 are used in most of the identification systems as image standard for photograph. India has used JPEG2000 as that is considered to be more open than JPEG standard. ICAO 9303 standard permits both JPEG and JPEG2000. JPEG2000 is recommended for EU-Passports because it results in smaller file sizes compared to JPEG compressed images Traditionally WSQ has been used for fingerprint image format. Many identification systems use WSQ as image format. India's ID system uses JPEG2000 as fingerprint and iris image standard format. Most American law enforcement agencies use WSQ for efficient storage of compressed fingerprint images at 500 pixels per inch (ppi). For fingerprints recorded at 1000 ppi, law enforcement (including the FBI) uses JPEG 2000 instead of WSQ.
A.2	Biometrics	Image Standard	ISO/IEC 15948, (PNG)	Technology—Computer graphics and image processing—Portable Network Graphics—lossless compression	W3C	
A.3	Biometrics	Image Standard	ISO/IEC 10918:1994 JPEG	Image Coding Standard—lossy compression	ISO and IEC	
A.4	Biometrics	Image Standard	WSQ	Compression algorithm used for gray-scale fingerprint images	NIST	
B.1	Biometrics	Data interchange—Face	ISO/IEC 19794-5:2011 (Face Image)	Biometric data interchange formats for Face image specifies data scene, photographic, digitization and format requirements for images of faces to be used in the context of both human verification and computer automated recognition	ISO and IEC	In anticipation of the need for additional data elements and in order to avoid future compatibility issues, the ISO/IEC 39794 series are being formulated as the next version to provide biometric data interchange standard formats capable of being extended in a defined way. The adoption of these would need to be monitored before mandating adoption due to wide prevalence of the 19794 series of standards. Another area to watch out for standards would be for contactless biometrics capture and interchange data format standards.
B.2	Biometrics	Data Interchange—Fingerprint	ISO/IEC 19794-4:2011 (Finger print)	Data record interchange format for storing, recording, and transmitting the information from one or more finger or palm image areas for exchange or comparison	ISO and IEC	
B.3	Biometrics	Data Interchange—Iris	ISO/IEC 19794-6:2011 (Iris)	Iris image interchange formats for biometric enrollment, verification and identification system	ISO and IEC	
B.4	Biometrics	Data Interchange—Minutiae	ISO/IEC 19794-2:2011 (Minutiae)	3 data formats for representation of fingerprints using the fundamental notion of minutiae for interchange and storage of this data: a) record-based format, and b) normal and c) compact formats for use on a smart card in a match-on-card application	ISO and IEC	
B.5	Biometrics	Data interchange—Signature	ISO/IEC 19794-7:2014 (Signature)	Data interchange formats for signature/sign behavioral data captured in the form of a multi-dimensional time series using devices such as digitizing tablets or advanced pen systems	ISO and IEC	

(continued)

S.No	Inter-operability Area	SubArea	Standard Specification/ (common name)	Standard description	Standards Body	Guidance note for standards selection
B.6	Biometrics	Biometrics Interface Standard	ISO 19785 :2015 Common Biometric Exchange Format Framework (CBEFF)	The biometric interface standards include ISO/IEC 19785, and ISO/IEC 19784, (BioAPI). These standards support exchange of biometric data within a system or among systems. ISO/IEC 19785 specifies the basic structure of a standardized Biometric Information Record (BIR), which includes the biometric data interchange record with added metadata such as when it was captured, its expiry date, whether it is encrypted, etc	ISO/IEC	
B.7	Biometrics	Fingerprint Image Quality Standard	NIST NFIQ v1, NIST NFIQ v2 NFIQ 2 is included as part of ISO/IEC 29794-4	NIST Fingerprint Image Quality (NFIQ) allows for the standardization needed to support a worldwide deployment of fingerprint sensors with universally interpretable image qualities	NIST	NFIQ 2 is an open source software that links image quality of optical and ink 500 PPI fingerprints to operational recognition performance and serves as a reference implementation of the I ISO/IEC 29794-4 standard . NFIQ 1 (the prior version) had quality range from 1 to 5 with 1 being the best quality where as NFIQ 2 has a range from 0 to 100 with 0 as image of no value and 100 is of highest quality
C.1	Card		ISO/IEC 7810	Identification Cards—Physical Characteristics	ISO and IEC	
C.2	Smart Card		ISO/IEC 7816	e-IDs/Smart Cards—Contact Card Standards	ISO and IEC	
C.3	Smart Card		ISO/IEC 14443	e-IDs/Smart Cards—Contactless Card Standards	ISO and IEC	
C.4	Smart Card		ICAO 9303 adopted as ISO/IEC 7501	Standard for Machine Readable Travel Documents	ICAO ISO and IEC	
C.5	Smart Card		ISO/IEC 24727	Set of programming interfaces for interactions between integrated circuit cards (ICCs) and external applications	ISO and IEC	

(continued)

S.No	Inter-operability Area	SubArea	Standard Specification/ (common name)	Standard description	Standards Body	Guidance note for standards selection
D.1	Bar Code	1 D (D - Dimensional	ISO/IEC 15417 :2012	Automatic identification and data capture techniques -- Code 128 bar code symbology specification	ISO/IEC	1 D codes represent data horizontally using the format of black bars and white spaces. They are suitable for short numbers but beyond 25-30 characters they can become very long. Text and URLs cannot be encoded. 2D bar codes can store over thousand characters, including URLs and images. PDF417 is a stacked barcode that can be read with a sim¬ple linear scan being swept over the symbol. It houses built in error correction capabilities within its high resolution linear rows, so defacement of these types of barcodes is not a large issue. It is displayed as a sleek rectangular shape and hence popular in ID cards. It requires a much higher resolution either when printing these barcodes or displaying them on a device. QR code contains large squares and take up more room than the small, rectangular PDF417. However, QR code has 3-4 times more capacity than PDF 417 code. It's also very straightforward creating QR codes in comparison to PDF417 barcodes. With QR codes, resolution is important but not to the extent of PDF417 barcodes as they use image sensors, not linear scans. Simple mobile applications can easily scan QR codes but it is more challenging to scan PDF417 barcodes, hence needs expensive equipment just to scan these codes. India uses QR code for encrypted and digitally signed data embedded in QR code which is used for offline authentication. Some of the East African Community countries have PDF 417 standard for the barcode on their ID cards.
D.2	Bar Code	2 D	ISO/IEC 18004:2015—Quick Response (QR) code	QR Code symbology characteristics, data character encoding methods, symbol formats, dimensional characteristics, error correction rules, reference decoding algorithm, production quality requirements, and user-selectable application parameters	ISO and IEC	
D.3	Bar Code	2 D	ISO/IEC 15438: 2015—PDF417	Requirements for the bar code symbology characteristics, data character encodation, symbol formats, dimensions, error correction rules, reference decoding algorithm, and many application parameters.	ISO and IEC	
E.1	Digital Signatures/ cryptography	Digital Signature Standard	FIPS 186-4 DSS	This Standard defines methods for digital signature generation that can be used for the protection of binary data (commonly called a message), and for the verification and validation of those digital signatures	NIST	
E.2	Digital Signatures/ cryptography	Digital Signature Algorithm	RFC 3447 RSA (PKCS #1)	The use of the RSA algorithm for digital signature generation and verification	IETF Internet Society	
E.3	Digital Signatures/ cryptography	Digital Signature Algorithm	RFC 7748 Elliptic curves for security/ FIPS 186-5	EC25519 digital signature algorithm and its variants Ed25519 provide digital signature algorithm with small key size 256 bits	IETF	Elliptic Curve 25519 algorithm has smaller key size of 256 bits vs 2048 bits for RSA algorithm. This is seeing increasing adoption especially for secure QR codes which need to be compact but not yet as widely supported in comparison to RSA.

(continued)

S.No	Inter-operability Area	SubArea	Standard Specification/ (common name)	Standard description	Standards Body	Guidance note for standards selection
E.4	Digital Signatures/ cryptography	Secure Hash Standard	SHS (FIPS PUB 180-4)	This Standard specifies secure hash algorithms—SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256	NIST	
E.5	Digital Signatures/ cryptography	Security	FIPS 140-2	Security Requirements for Cryptographic Modules	NIST	
E.6	Digital Signatures/ cryptography	Public Key Infrastructure	ITU-T X.509 | ISO/ IEC 9594-8	The public-key certificate framework defined in this Recommendation | International Standard specifies the information objects and data types for a public-key infrastructure (PKI), including public-key certificates, certificate revocation lists (CRLs), trust broker and authorization and validation lists (AVLs)	ITU-T, ISO and IEC	
E.7	Digital Signatures/ cryptography	XML Advanced Electronic Signatures	XAdES W3C	While XML-DSig is a general framework for digitally signing documents, XAdES specifies precise profiles of XML-DSig making it compliant with the European eIDAS regulation	W3C	
F.1	Federation	Protocol	SAML v2—2005	Security Assertion Markup Language (SAML) defines an XML based framework for communicating security and identity (e.g., authentication, entitlements, and attribute) information between computing entities. SAML promotes interoperability between disparate security systems, providing the framework for secure e-business transactions across company boundaries.	OASIS	SAML was designed only for Web-based applications whereas OpenID Connect was designed to also support native apps and mobile applications in addition to Web applications. OpenId connect is newer and built on the OAuth 2.0 process flow. It is tried and tested and typically used in consumer websites, web apps and mobile apps. Mobile connect and Microsoft's Identity management solutions use this protocols. SAML is its older cousin, and typically used in enterprise settings eg. allowing single sign on to multiple applications within an enterprise using our Active Directory login. The EIDAS framework is based on SAML. Open ID connect is gaining popularity for new implementations as it can support both native apps and mobile apps in addition to web based applications.
F.2	Federation	Protocol	RFC 6749/ OAUTH 2	OAuth 2.0 is the industry-standard protocol for authorization providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices	IETF	
F.3	Federation	Protocol	Open ID connect	OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and Web Services-like manner.	The OpenID Foundation	

Technical Standards for Robust Identity Systems

Table 2. lists standards that provide guidelines on quality-, testing-, privacy- and accessibility-related aspects of identification systems. These can also serve as the basis of relevant operational documents and guidelines. For instance, India's Ministry of Electronics and Information Technology has drafted the "Security Guidelines for use of Biometric Technology in e-Governance Projects" based on the guidelines in the standards ISO 24745, ISO19792, ISO 24714 and ISO 24760.

Biometric sample quality standards are important to ensure that the biometric data collected is usable for automated recognition. Poor sample quality may cause failure to enroll and/or degrade the overall matching performance. The relevant international standards for biometric sample quality include: ISO/IEC 29794-4:2017 (Finger image data); ISO/IEC TR 29794-5:2010 (Face image data); and ISO/IEC 29794-6:2015 (Iris image data). NIST has also published NIST Fingerprint Image Quality (NFIQ) reports and corresponding SDKs which are used globally. The purpose of the BioAPI (ISO 19784) specification is to define an architecture and all necessary interfaces to allow biometric applications to be integrated from modules provided by different vendors. However, these have not been adopted in any known country implementation so far but may find traction in due course of time once the challenges are addressed.

S. No	Area	Standard No	Standard Description
1	Biometrics	ISO/IEC 29794 Series	Biometric Sample Quality—Matching Performance
2	Biometrics	ISO/IEC 29109 Series	Testing Methodology for Biometric Data Interchange
3	Biometrics	ISO/IEC 24745	Security Techniques—Biometric Information Protection
4	Biometrics	ISO/IEC 24761	Authentication Context for Biometrics
5	Biometrics	NIST MINEX	Minutiae Interoperability Exchange Test (MINEX) is a program of NIST to do interoperability testing of minutia template generators and extractors for the United States Government's Personal Identity Verification (PIV) program
6	Biometrics	ISO/IEC 19784-1:2018	BioAPI specification
7	Biometrics	ISO/IEC 24709-1:2017	Conformance testing for the biometric application programming interface (BioAPI – ISO 19784)
8	Biometrics	ISO/IEC 24708:2008	Specifies the syntax, semantics, and encodings of a set of messages (BIP messages) that enable a BioAPI-conforming application to request biometric operations in BioAPI-conforming biometric service providers (BSPs)
9	Biometrics	ISO/IEC 29164:2011	This interface, called Embedded BioAPI provides a standard interface to hardware biometric modules designed to be integrated in embedded systems which can be constrained in memory and computational power.
10	Biometrics	ISO/IEC 29141:2009	Specifies requirements for the use of ISO/IEC 19784-1 (BioAPI) for the purpose of performing a tenprint capture operation.
11	Biometrics	SO/IEC 29197:2015	Evaluation methodology for environmental influence in biometric system performance

S. No	Area	Standard No	Standard Description
12	Biometrics	ISO/IEC 19795 series :2021 ISO/IEC 19795-9:2019 ISO/IEC 19795-10 2019	Multipart standard concerned with “technical performance testing” of biometric systems Part 1: Principles and framework Part 2: Testing methodologies for technology and scenario evaluation Part 3: Modality-specific testing [Technical Report] Part 4: Interoperability performance testing Part 5: Access control scenario and grading scheme Part 6: Testing methodologies for operational evaluation Part 7: Testing of on-card biometric comparison algorithms Part 8: Methodology and tools for the validation biometric methods for forensic evaluation and identification application Part 9 :guidance for testing and reporting methods for biometric systems embedded in mobile devices Part 10: Quantifying biometric system performance variation across demographic groups
13	Biometrics	ISO/IEC 30107-1:2016 ISO/IEC 30107-2:2017 ISO/IEC 30107-3:2017 ISO/IEC 30107-4:2020	Biometric Presentation Attack Detection (PAD) Part 1 describes attacks that take place at the sensor during the presentation and collection of biometric characteristics Part 2 defines data formats for conveying the mechanism used in biometric PAD and for conveying the results of PAD methods. Part 3 principles and methods for performance assessment of PAD mechanisms and classification of attack types Part 4 provides requirements for testing biometric PAD mechanisms on mobile devices with local biometric recognition
14	Biometrics	ISO/IEC 20027:2018	Guidelines for slap tenprint fingerprint capture
15	Biometrics	ISO/IEC 21472:2021	Scenario evaluation methodology for user interaction influence in biometric system performance
16	Biometrics	ISO/IEC 22116:2021	A study of the differential impact of demographic factors in biometric recognition system performance
17	Biometrics	ISO/IEC 24713-1:2008	Biometric profiles for interoperability and data interchange — Part 1: Overview of biometric systems and biometric profiles provides common definitions used within the profile standards
18	Biometrics	ISO/IEC 24741:2018	Biometrics — Overview and application
19	Biometrics	ISO/IEC 24779 series	Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems Part 1 : General Principles Part 4: Fingerprint applications Part 5: Face applications
20	Biometrics	ISO/IEC TR 29156:2015	Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics
21	Biometrics	ISO/IEC 30136:2018	Performance testing of biometric template protection schemes supports evaluation of the accuracy, secrecy, and privacy of biometric template protection schemes. It establishes definitions, terminology, and metrics for stating the performance of such schemes.

S. No	Area	Standard No	Standard Description
22	Biometrics	ISO/IEC TR 29194:2015	Guide on designing accessible and inclusive biometric systems
23	Biometrics	ISO/IEC TR 29196:2015	Guidance for biometric enrolment
24	Biometrics	ISO/IEC TR 30125:2016	Biometrics used with mobile devices
25	Biometrics	ISO 19792:2015	Security techniques—Security evaluation of biometrics
26	Biometrics	ISO 24714:2015	Biometrics—Jurisdictional and societal considerations for commercial applications -- Part 1: General guidance
27	Biometrics	FIDO Biometric Component certification policy: oct 2020	Provides implementation requirements for Vendors and Test Procedures for evaluating the biometric component of a FIDO Authenticator Certification standard
28	Biometrics	Android Compatibility Definition Document (CDD)- Oct 2021 Android 12	Certification standard for the testing of biometric systems that enumerates the requirements to be compatible with the latest version of Android
29	General	NIST 800-63-3 – June 2017	They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions Other parts SP 800-63A,SP 800-63B, SP 800-63C Next version NIST 800-63-4 under review
30	Privacy	ISO/IEC 29100	Privacy framework
31	Privacy	ISO/IEC 27018	Code of practice for PII protection in public clouds acting as PII processors
32	Privacy	ISO/IEC 29190	Privacy capability assessment model
33	Privacy	ISO/ IEC 29184	Guidelines for online privacy notice and consent
34	Management	ISO/IEC 24760 Series	Framework for Management of Identity Information

Standard Name	Standard Description	Standard Body	Comments
ISO/IEC 29115	Entity Authentication Assurance Framework	ISO and IEC	Sets out four levels of assurances for scalable identity management and authentication services
FIDO UAF	Universal Authentication framework	FIDO alliance	Password less authentication experience
eIDAS	Electronic identification and trust services	European Union regulation	Regulation for Identification and trust services for the European union—framework for interoperability of EU identity systems

5.4 Levels of Assurance

A “level of (identity) assurance” is the certainty with which a claim to a particular identity made by some person or entity can be trusted to actually be the claimant's “true” identity. Higher levels of assurance reduce the risk of a fraudulent identity and increase the security of transactions. Assurance levels depend on the strength of the identity proofing process and the types of credentials and authentication mechanisms used during a transaction (Figure 4). For identity proofing, the level of assurance depends on the method of identification (e.g., in-person vs. remote), the attributes collected, and the degree of certainty with which those attributes are verified (e.g., through cross-checks and deduplication). For authentication, the level of assurance depends on the type of credential(s), the number of authentication factors used (i.e., one vs. multiple), and the cryptographic strength of the transaction.

Both eIDAS and ISO/IEC 29115 have developed standards to classify levels of assurance based on these processes and technologies. This framework covers registration, credentialing, and authentication phases and provides guidance for technical as well as organizational and management aspects. The LOAs selected depend on the use case; some sectors and types of transactions will require higher levels of assurance than others.

FIGURE 4 Example levels of assurance

	Low (level1)	Substantial (level2)	High (level3)
Identity assurance level (IAL)	**Self-asserted identity** (e.g., email account creation on web), no collection, validation or verification of evidence.	**Remote or in-person identity proofing** (e.g., provide credential document for physical or backend verification with authoritative source), address verification required, biometric collection optional	**In-person (or supervised remote) identity proofing**, collection of biometrics and address verification mandatory.
Authentication assurance level (AAL)	**At least 1 authentication factor**—something you have, know, or are (e.g., password or PIN)	**At least 2 authentication factors** (e.g., a token with a password or PIN)	**At least two different *categories* of authentication factors** and protection against duplication and tampering by attackers with high attack potential (e.g., embed cryptographic key material in tamper-resistant hardware token + PIN, biometrics with liveness detection + PIN/smart card)
Federation Assurance Level (FAL)	**Permits the relying party to receive a bearer assertion from an identity provider.** The identity provider must sign the assertion using approved cryptography	**FAL1 + encryption** of assertion using approved cryptography	**FAL2 + user to present proof of possession of a cryptographic key** reference in the assertion
Level of risk taken by relying party	mitigated	low	minimal

Source: Practitioner's Guide https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

6. COUNTRY USE CASES

Depending on the country-specific environment, which standards should be adopted? The answer depends on the objectives, scope, and proposed use for the identification system. Examples from Estonia, India, Malawi, Pakistan and Peru are presented below to illustrate the choice of relevant standards by the respective authorities to meet their requirements. These choices depend on a number of factors, including the existing regulatory frame¬works within a country.

Example 1: ID-Kaart in Estonia—Smart Card and Mobile ID

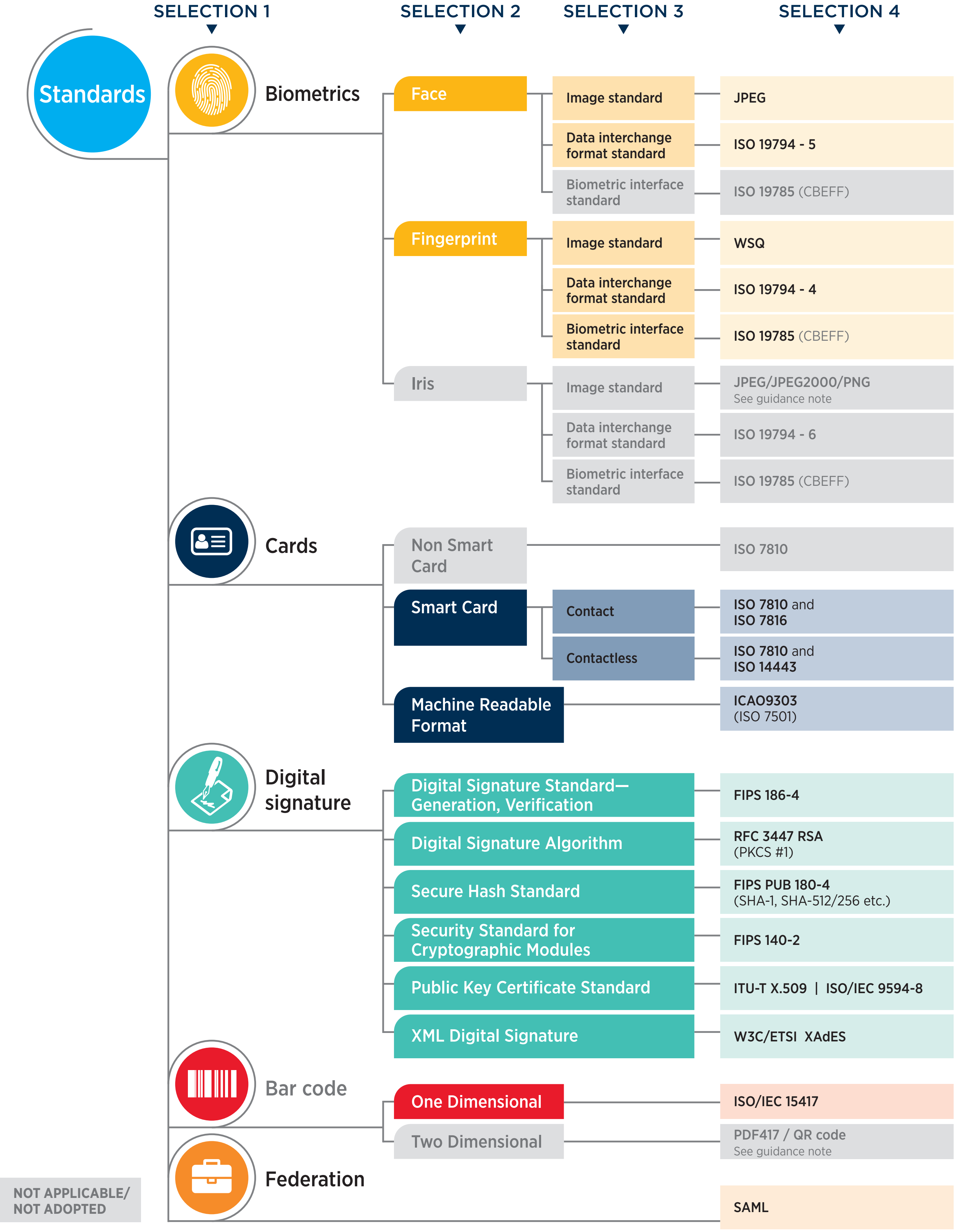
Estonia has a highly developed digital identification system and is one of the most advanced countries in the world when it comes to digital public services. It has issued 1.5 million of smart ID-Kaarts, and boasts over 600,000 users for its smart ID solution as well as 225,000 mobile ID users. These credentials allow their holders to access over 1,000 public services, such as health care, online tax filing, and online voting. Key identifying data such as name, date of birth, unique ID number and digital certificates are stored in the smart card chip or a special mobile SIM card for authentication and digital signing of documents. The access to each of these digital certificates keys is protected by a secret PIN which only the user knows.

The ID-Kaart has advanced electronic functions that facilitate secure authentication and legally binding digital signatures that may be used for nationwide online services. The e-ID infrastructure is scalable, flexible, interoperable, and standards-based. All certificates issued in association with the ID card scheme are qualified certificates conforming with European Directive 1999/93/ EC on the use of electronic signatures in electronic contracts within the European Union (EU). The card complies with the ICAO 9303 travel document standard. Two one dimensional bar codes, based on ISO 15417 standard, are used to encode personal ID number and the document identification number.

The ID-Kaart serves as a trusted credential for accessing public services. To sign a document digitally, a communication model using standardized workflows in the form of a common document format (DigiDoc) has been employed. DigiDoc is based on XML Advanced Electronic Signatures Standard (XAdes), which is a profile of that standard. XAdes defines a format that enables structurally storing data signatures and security attributes associated with digital signatures and hence caters for common understanding and interoperability.

Source: e-Estonia.com and the paper titled ‘The Estonian ID Card and Digital Signature Concept’ Ver 20030307

ESTONIA



	SELECTION 1	SELECTION 2	SELECTION 3	SELECTION 4
Standards	Biometrics	Face	Image standard	JPEG
			Data interchange format standard	ISO 19794 - 5
			Biometric interface standard	ISO 19785 (CBEFF)
		Fingerprint	Image standard	WSQ
			Data interchange format standard	ISO 19794 - 4
			Biometric interface standard	ISO 19785 (CBEFF)
		Iris	Image standard	JPEG/JPEG2000/PNG See guidance note
			Data interchange format standard	ISO 19794 - 6
			Biometric interface standard	ISO 19785 (CBEFF)
	Cards	Non Smart Card		ISO 7810
		Smart Card	Contact	ISO 7810 and ISO 7816
			Contactless	ISO 7810 and ISO 14443
		Machine Readable Format		ICAO9303 (ISO 7501)
	Digital signature	Digital Signature Standard—Generation, Verification		FIPS 186-4
		Digital Signature Algorithm		RFC 3447 RSA (PKCS #1)
		Secure Hash Standard		FIPS PUB 180-4 (SHA-1, SHA-512/256 etc.)
		Security Standard for Cryptographic Modules		FIPS 140-2
		Public Key Certificate Standard		ITU-T X.509 | ISO/IEC 9594-8
		XML Digital Signature		W3C/ETSI XAdES
	Bar code	One Dimensional		ISO/IEC 15417
		Two Dimensional		PDF417 / QR code See guidance note
	Federation			SAML

NOT APPLICABLE/ NOT ADOPTED

Example 2: Aadhaar Identity System of India—Biometric Based

The Unique Identification Authority of India (UIDAI) has issued a unique ID number, known as Aadhaar, to more than 1.3 billion residents. The photograph, fingerprints and irises along with a minimal set of biographic data of each resident are captured before issuing an Aadhaar. It is the world's largest population register that is underpinned by a multimodal biometric database, with nearly the entire population having a digitally recorded and verifiable identity.

UIDAI set up a Biometric Standards Committee in 2009 to provide direction on biometric standards, suggest best practices, and recommend biometric procedures for the system. The committee recommended ISO/IEC 19794 Series (parts 1, 2, 4, 5, 6) and ISO/ IEC 19785 for biometric data interchange formats and a common biometric exchange framework to ensure interoperability. ISO/IEC 15444 (all parts) was selected as a coding system (JPEG 2000 image) for both photo, fingerprint and iris image.

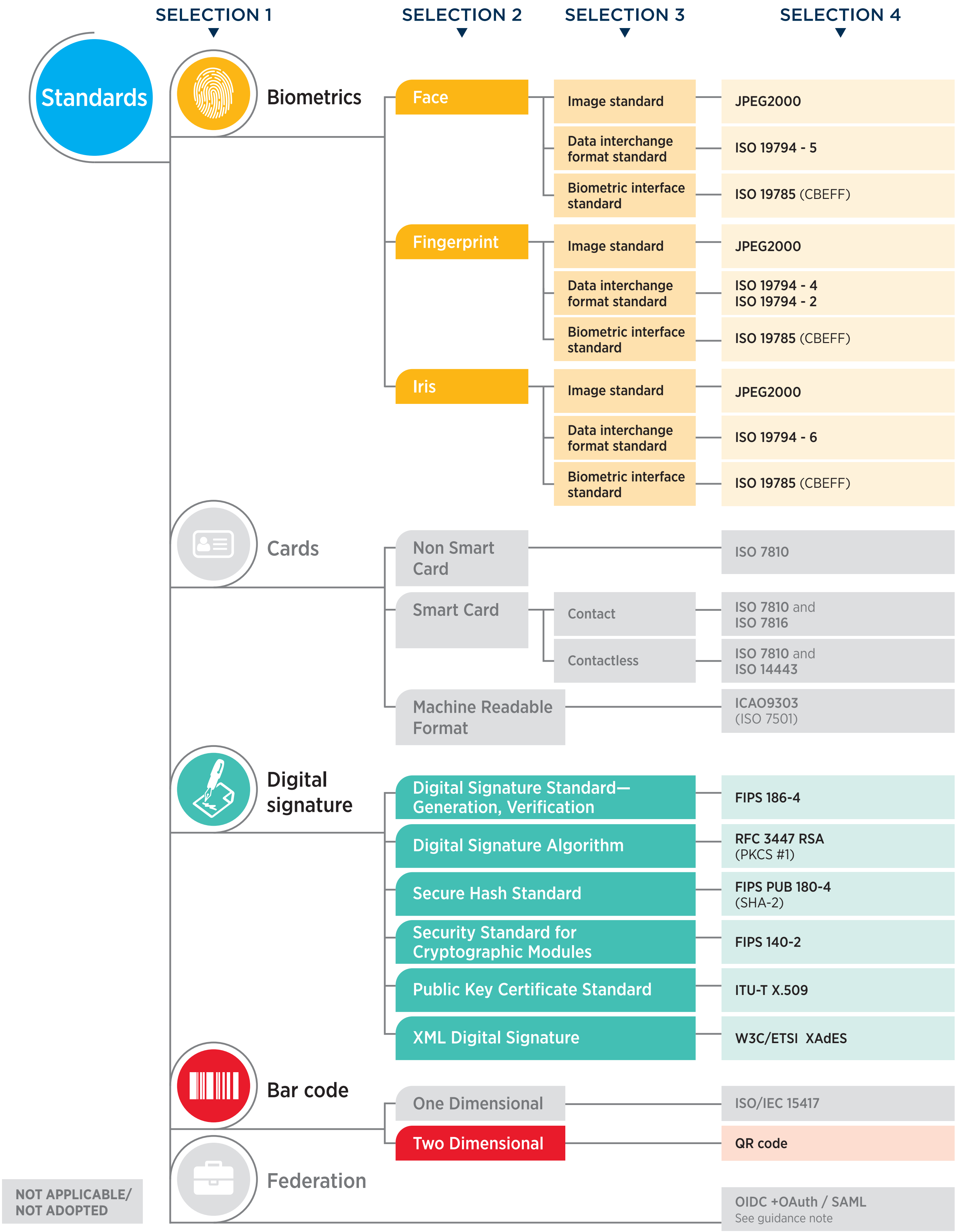
Additionally, UIDAI uses open source software as a principle, which have also been used successfully in the United States and Europe. UIDAI has drafted the "Security Guidelines for use of Biometric Technology in e-Governance Projects" based on the guidelines in the standards ISO 24745, ISO 19792, ISO 24714 and ISO 24760. Data standards for the identity attributes captured during registration and subsequently used for demographic authentication have also been established (demographic standards committee). The Aadhaar system also makes extensive use of PKI/HSM for encryption of data during transmission and storage and for protecting access to the API.

The Aadhaar system does not rely on a physical ID card as the primary means of authentication. The Aadhaar number combined with biometric authentication (1:1 matching) or an OTP can be used to verify a person's identity in a wide variety of settings. In addition, there is a mAadhaar mobile app which allows for electronic storage of demographic data, the Aadhaar number and photograph along with a QR code. A laminated paper ('Aadhaar letter') is also sent to the residents with demographic data, photo and QR code (contains encrypted and digitally signed data). As of 2020, Aadhaar holder can also request a PVC card, which includes the same demographic details and an encrypted QR code. The QR code from these physical credentials and the mAadhaar app is used in some scenarios for offline authentication with the help of a custom application.

Aadhaar Authentication can be performed in one or more of the following modes with yes/no responses:

- Demographic authentication
- Biometric authentication
- One-time PIN mobile based authentication
- Multifactor authentication is a combination of two or three factors listed above
- Source: UIDAI Website & Biometrics Standard Committee Recommendations 2009.

Source: UIDAI Website & Biometrics Standard Committee Recommendations 2009.



Standards

SELECTION 1	SELECTION 2	SELECTION 3	SELECTION 4
Biometrics	Face	Image standard	JPEG2000
		Data interchange format standard	ISO 19794 - 5
		Biometric interface standard	ISO 19785 (CBEFF)
	Fingerprint	Image standard	JPEG2000
		Data interchange format standard	ISO 19794 - 4 ISO 19794 - 2
		Biometric interface standard	ISO 19785 (CBEFF)
	Iris	Image standard	JPEG2000
		Data interchange format standard	ISO 19794 - 6
		Biometric interface standard	ISO 19785 (CBEFF)
Cards	Non Smart Card		ISO 7810
	Smart Card	Contact	ISO 7810 and ISO 7816
		Contactless	ISO 7810 and ISO 14443
	Machine Readable Format		ICAO9303 (ISO 7501)
Digital signature	Digital Signature Standard—Generation, Verification		FIPS 186-4
	Digital Signature Algorithm		RFC 3447 RSA (PKCS #1)
	Secure Hash Standard		FIPS PUB 180-4 (SHA-2)
	Security Standard for Cryptographic Modules		FIPS 140-2
	Public Key Certificate Standard		ITU-T X.509
	XML Digital Signature		W3C/ETSI XAdES
Bar code	One Dimensional		ISO/IEC 15417
	Two Dimensional		QR code
Federation			OIDC +OAuth / SAML See guidance note

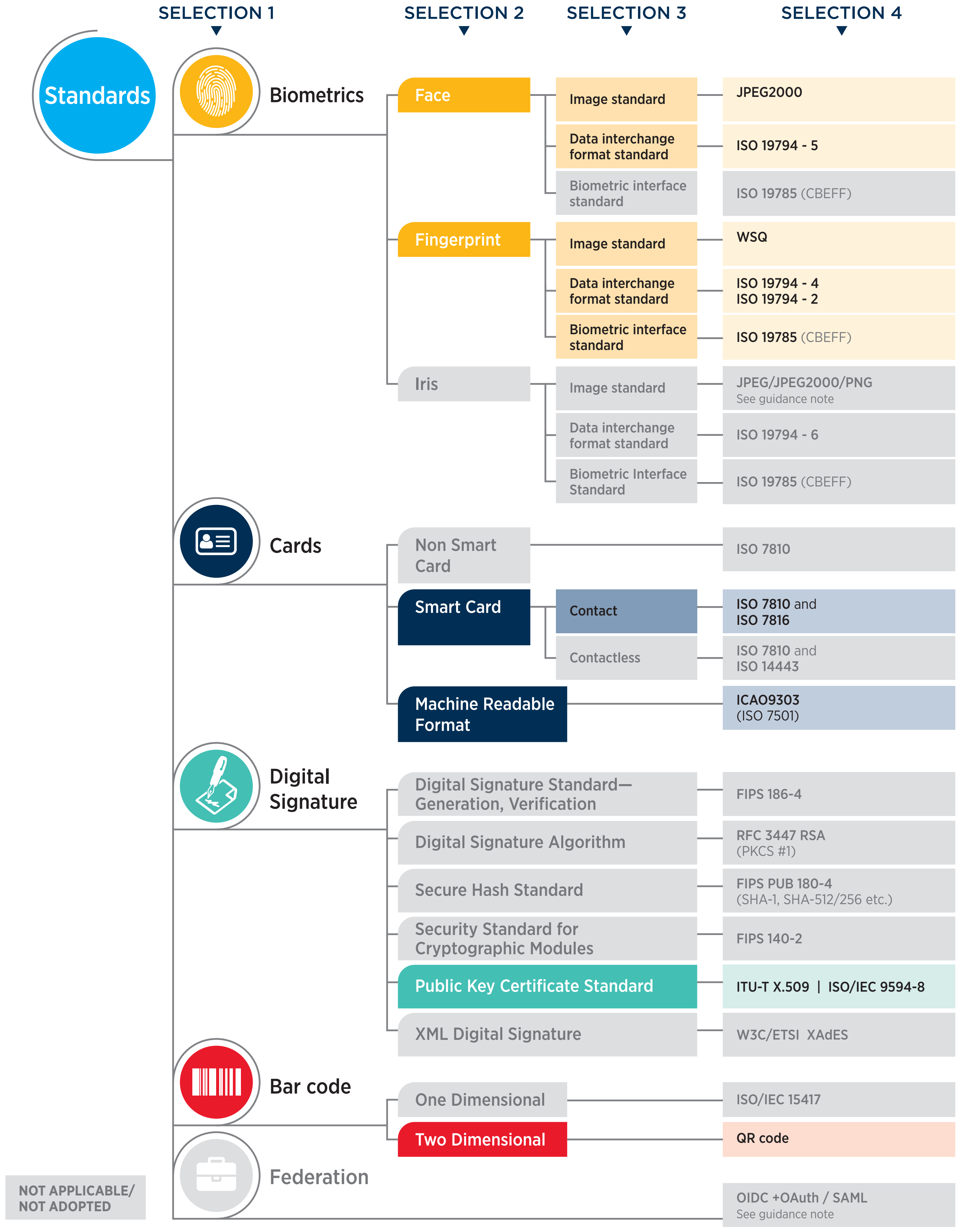
NOT APPLICABLE/ NOT ADOPTED

Example 3: Malawi—Biometrics and Smart Card

The Government of Malawi has achieved high coverage of the adult population through a mass registration and ID issuance effort launched in 2017, which provided more than 9 million people with a national ID card. The identification system is managed by the National Registration Bureau (NRB) under the Ministry of Home Affairs and Internal Security. Malawians age 16 and above are eligible to obtain a national ID card. The registration process captures 10 fingerprints, a digital photograph, and electronic signature. Biometric deduplication is completed before the issuance of a unique ID and smart card.

The ID card is ICAO (9303) and ISO (7816) compliant, with seven built-in security features to prevent forgery and includes a QR code. The chip stores both biometric a biographic information about the holder, including one fingerprint, a facial image, and a copy of their ink signature. Since the card meets international standards, it can, in principle, be used for a wide range of applications including international travel and health insurance (through the CWA 15974 and ISO 21549 standards-compliant eHealth applet). However, while the features are available, they are used only for authentication services by a few service providers, primarily in the financial sector, and have not yet been used in practice for international travel or health.

Source: Malawi's Journey Towards Transformation: Lessons from its National ID Project by Tariq Malik. Center for Global Development 2018



Standards

SELECTION 1	SELECTION 2	SELECTION 3	SELECTION 4
Biometrics	Face	Image standard	JPEG2000
		Data interchange format standard	ISO 19794 - 5
		Biometric interface standard	ISO 19785 (CBEFF)
	Fingerprint	Image standard	WSQ
		Data interchange format standard	ISO 19794 - 4 ISO 19794 - 2
		Biometric interface standard	ISO 19785 (CBEFF)
	Iris	Image standard	JPEG/JPEG2000/PNG See guidance note
		Data interchange format standard	ISO 19794 - 6
		Biometric Interface Standard	ISO 19785 (CBEFF)
Cards	Non Smart Card		ISO 7810
	Smart Card	Contact	ISO 7810 and ISO 7816
		Contactless	ISO 7810 and ISO 14443
	Machine Readable Format		ICAO9303 (ISO 7501)
Digital Signature	Digital Signature Standard—Generation, Verification		FIPS 186-4
	Digital Signature Algorithm		RFC 3447 RSA (PKCS #1)
	Secure Hash Standard		FIPS PUB 180-4 (SHA-1, SHA-512/256 etc.)
	Security Standard for Cryptographic Modules		FIPS 140-2
	Public Key Certificate Standard		ITU-T X.509 | ISO/IEC 9594-8
	XML Digital Signature		W3C/ETSI XAdES
Bar code	One Dimensional		ISO/IEC 15417
	Two Dimensional		QR code
Federation			OIDC +OAuth / SAML See guidance note

NOT APPLICABLE/ NOT ADOPTED

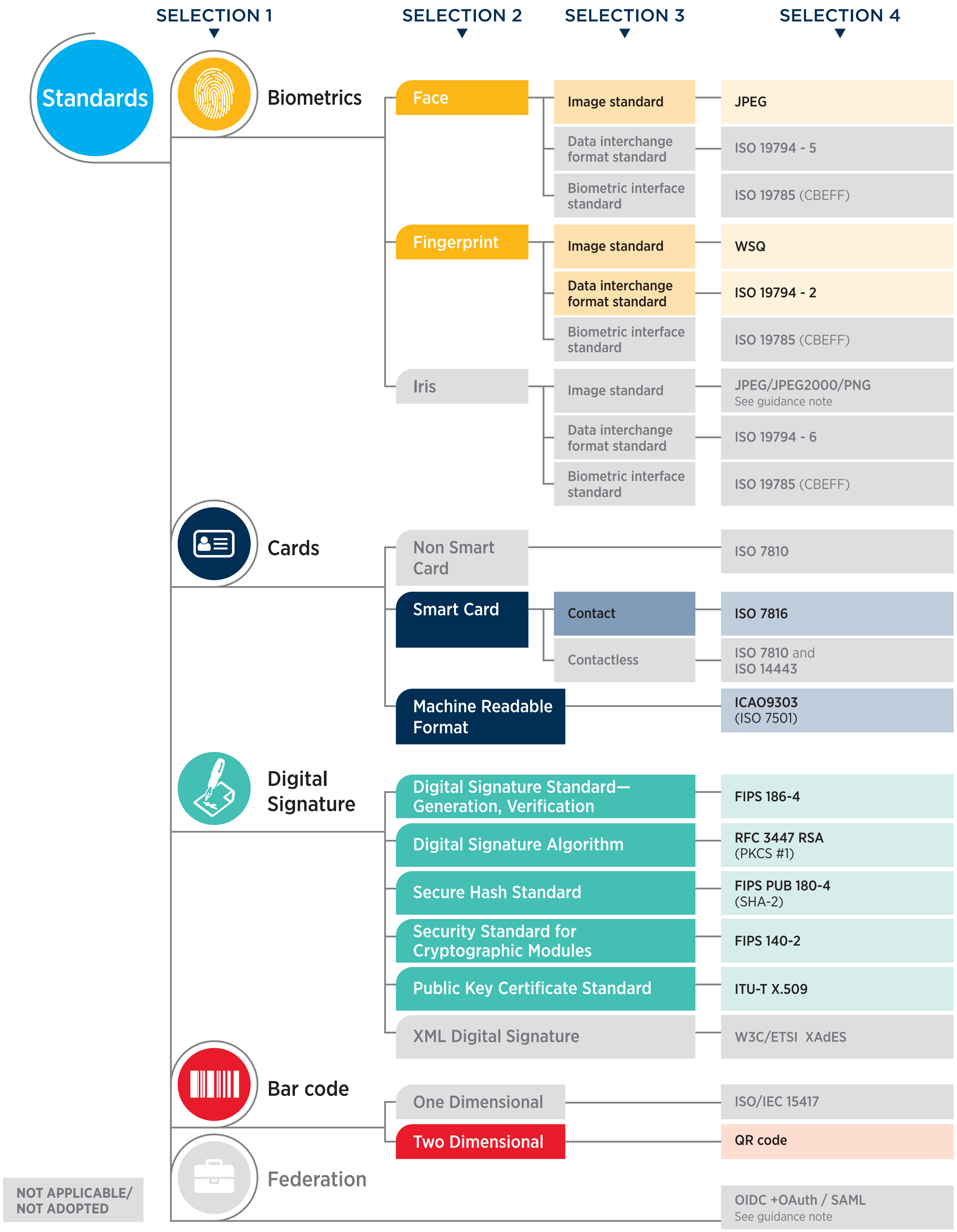
Updated August 2022

Example 4: Smart eID in Pakistan—Biometrics and Smart Card

Pakistan's National Database and Registration Authority (NADRA) has issued over 120 million ID cards and an estimated 88 percent of its adult citizens now have an ID. Over the years, Pakistan's ID card has evolved into a smart eID that contains a data chip and a match-on-card applet. The ID card complies with ICAO standard 9303 part 3 vol. 1 and is also ISO 7816-4 compliant. The smart ID card has more than 20 overt and covert security features to avoid forgery. It also includes QR code and MRZ zone at the back of card.

NADRA uses open source as a guideline/principle for application development. Demographic data is used along with biometric data to improve the deduplication process. NADRA Quality Management and ID Card Production departments are ISO 9001:2000 certified.

Source: Asian Development Bank. 2016. Identity for Development in Asia and the Pacific. Manila: Asian Development Bank.



Standards

SELECTION 1	SELECTION 2	SELECTION 3	SELECTION 4
Biometrics	Face	Image standard	JPEG
		Data interchange format standard	ISO 19794 - 5
		Biometric interface standard	ISO 19785 (CBEFF)
	Fingerprint	Image standard	WSQ
		Data interchange format standard	ISO 19794 - 2
		Biometric interface standard	ISO 19785 (CBEFF)
	Iris	Image standard	JPEG/JPEG2000/PNG See guidance note
		Data interchange format standard	ISO 19794 - 6
		Biometric interface standard	ISO 19785 (CBEFF)
Cards	Non Smart Card		ISO 7810
	Smart Card	Contact	ISO 7816
		Contactless	ISO 7810 and ISO 14443
	Machine Readable Format		ICAO9303 (ISO 7501)
Digital Signature	Digital Signature Standard—Generation, Verification		FIPS 186-4
	Digital Signature Algorithm		RFC 3447 RSA (PKCS #1)
	Secure Hash Standard		FIPS PUB 180-4 (SHA-2)
	Security Standard for Cryptographic Modules		FIPS 140-2
	Public Key Certificate Standard		ITU-T X.509
	XML Digital Signature		W3C/ETSI XAdES
Bar code	One Dimensional		ISO/IEC 15417
	Two Dimensional		QR code
Federation			OIDC +OAuth / SAML See guidance note

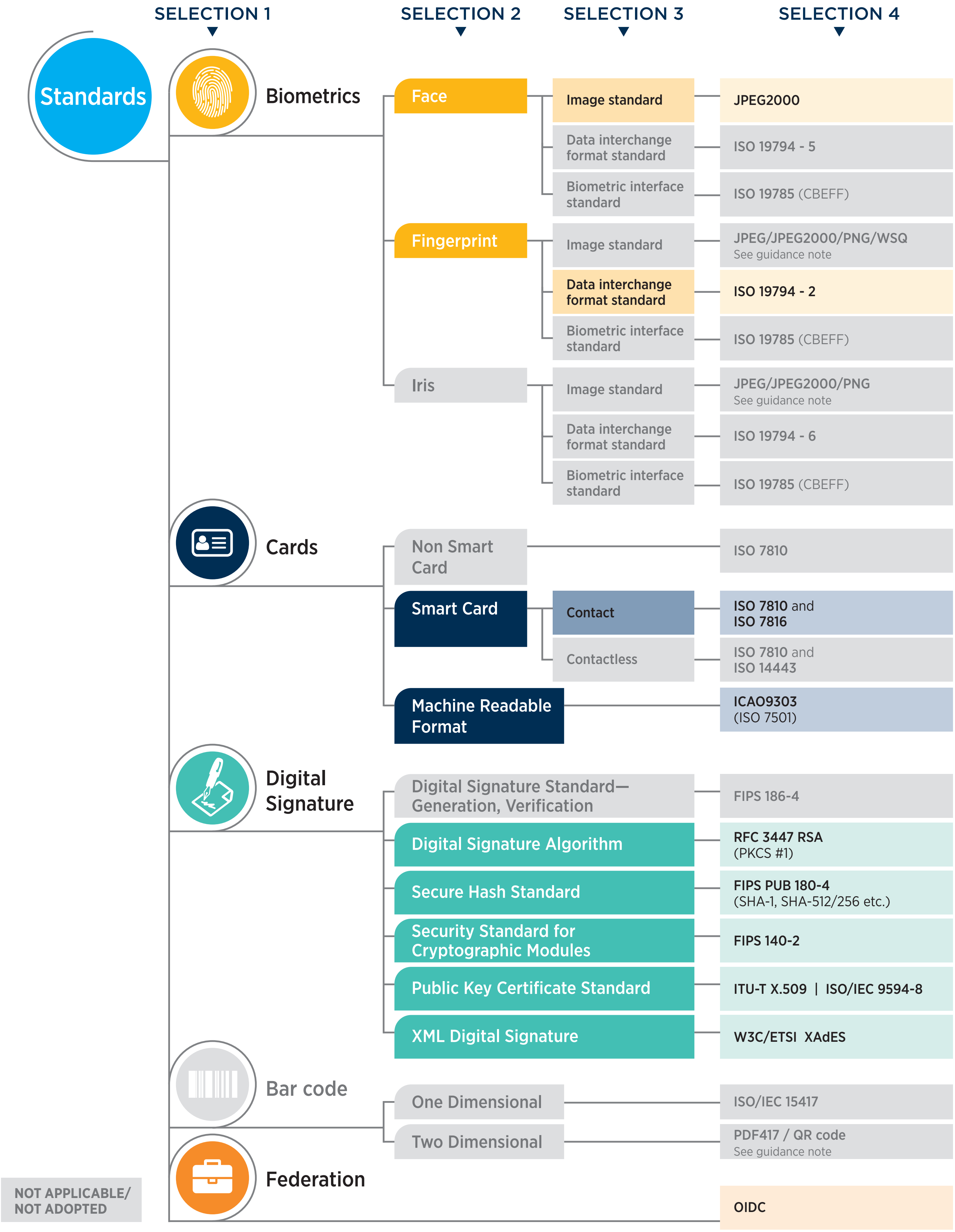
NOT APPLICABLE/ NOT ADOPTED

Example 5: eID with Digital Certificate in Peru

Peru's National Registry of Identification and Civil Status (RENIEC) has introduced an electronic National ID Card (DNIe) to facilitate online transactions and services, alongside its traditional 'blue' ID card, which is used for in-person transactions. RENIEC is an autonomous entity whose mandate includes both civil registration and identification as well as the issuance of digital signatures. It has issued more than 30 million IDs covering almost the entire population of the country. Demand for the electronic ID cards is growing steadily, which now make up about 12 percent of ID requests .

The DNIe provides Peruvian citizens with a digital identity, to facilitate both in-person and remote, online authentication. The DNIe includes two digital certificates, which allows the cardholder to sign electronic documents with the same probative value as a handwritten signature. Peru's eID complies with the ISO/ IEC-7816 standard and its biometrics system follows ISO/IEC 19794. The card also complies with ICAO 9303 and can be used as a machine-readable travel document (MRTD).

Source:Interview with RENIEC official; www.gob.pe website; https://portales.reniec.gob.pe website



Standards

SELECTION 1	SELECTION 2	SELECTION 3	SELECTION 4
Biometrics	Face	Image standard	JPEG2000
		Data interchange format standard	ISO 19794 - 5
		Biometric interface standard	ISO 19785 (CBEFF)
	Fingerprint	Image standard	JPEG/JPEG2000/PNG/WSQ See guidance note
		Data interchange format standard	ISO 19794 - 2
		Biometric interface standard	ISO 19785 (CBEFF)
	Iris	Image standard	JPEG/JPEG2000/PNG See guidance note
		Data interchange format standard	ISO 19794 - 6
		Biometric interface standard	ISO 19785 (CBEFF)
Cards	Non Smart Card		ISO 7810
	Smart Card	Contact	ISO 7810 and ISO 7816
		Contactless	ISO 7810 and ISO 14443
	Machine Readable Format		ICAO9303 (ISO 7501)
Digital Signature	Digital Signature Standard—Generation, Verification		FIPS 186-4
	Digital Signature Algorithm		RFC 3447 RSA (PKCS #1)
	Secure Hash Standard		FIPS PUB 180-4 (SHA-1, SHA-512/256 etc.)
	Security Standard for Cryptographic Modules		FIPS 140-2
	Public Key Certificate Standard		ITU-T X.509 | ISO/IEC 9594-8
	XML Digital Signature		W3C/ETSI XAdES
Bar code	One Dimensional		ISO/IEC 15417
	Two Dimensional		PDF417 / QR code See guidance note
Federation			OIDC

NOT APPLICABLE/
NOT ADOPTED

Updated August 2022

7. CONCLUSION

Standards are key to unlocking the value of identification systems for development and supporting the establishment of interoperable, scalable, secure, and efficient digital identification platforms for service delivery. Understanding the standards landscape and choosing which to adopt can be a challenge for ID practitioners. There are multiple international and national standards-setting bodies, such as ICAO, IEC, ISO, ITU-T, ANSI and NIST, and navigating their catalogs and guidance can at times be challenging. The menu and choice of relevant standards will depend on the purpose, scope, and function of the specific identification system, as also highlighted through the country examples presented earlier. For instance, not all ID systems will use fingerprint or iris biometrics for deduplication or authentication purposes. The format of the credential issued will also vary, with some systems and countries placing more emphasis on physical credentials while others are transitioning to the use of ID numbers and mobile IDs in combination with other authentication factors. Depending on the approach taken, the relevant set of standards will vary. At the same time, ensuring that the features and technologies that are deployed are compliant with international standards is key for its sustainability.

There are several issues that are important to keep in mind when designing an ID system and using standards:

1. **Use open standards when feasible.** Using open standards can help ensure that an ID system is robust, interoperable and technology neutral. However, it is important to consider before using an open standard if the standard is widely used in the market. In some instances, there has been little market uptake of open standards, which may indicate that there is a performance issue or other issue to consider. If a standard is not widely used, then it may be challenging to ensure competition when selecting a prospective product or solution. A full assessment of needs should be completed before selecting solution components. Where an innovative solution is required, wide market adoption will not necessarily exist, particularly if the solution is designed for specific needs or challenges. Equally, in niche applications only few suppliers are likely to exist. In some instances, a solution reliant on a closed standard may offer greater performance than an open standard. In such a case, it would still be important to ensure that the use of a closed standard does not result in vendor lock-in, e.g., by selecting systems components that support open API standards and allow access to system data in portable open data formats (see semantic standards later in this section). This approach will also enable system components to be updated or replaced over time following a modular approach, as vendors change or new, more efficient solutions present themselves.
2. **Technical Standards alone are not sufficient.** In addition to using open technical standards, semantic standards are also important to consider to enable interoperability. Semantic standards define the data formats and metadata for identity attributes like name and date of birth (e.g., the number of characters allowed for a name; order of specifying the first name, middle, name; format of date—date of birth mm/dd/yyyy or dd/mm/yy) to facilitate seamless data exchange across systems. Beyond technical and semantic standards, it is important to adopt strong procurement processes that minimize contractual constraints in the choice of technology and supplier(s) to mitigate the risks of vendor and technology lock-in scenarios. The ID4D procurement guide and checklist provide additional considerations and recommendations on this area. The ID4D Practitioner's Guide offers further guidance on inclusive and trusted ID system design.
3. **Be forward looking.** Standards are not static, and they will evolve over time as new technologies emerge. Therefore, it is important to stay abreast of emerging technologies and standards relevant for ID systems. Some relevant emerging initiatives and standards are the following:

- Verifiable credentials (VCs) are an open standard for digital credentials standard and the data model for verifiable credentials is a World Wide Web Consortium (W3C) Recommendation.

- OSIA is an open standard set of interfaces (APIs) that supports seamless connectivity between all components of the identity management ecosystem – independent of technology, solution architecture or vendor initiative.

- Modular Open Source Identity Platform (MOSIP) provides a vendor neutral and interoperable solution for the implementation of digital, foundational identification systems, designed for easy integration and with security and privacy as key principles.

- The Govstack initiative is defining specifications for an 'identification and authentication' building blocks -i.e., reusable software components that provide key functionality facilitating generic workflows across multiple sectors - along with others as a public good. It is also creating a sandbox for reference implementation and a certification process for checking compliance of solutions with the specifications.

- Trust frameworks for federations e.g., electronic Identification, Authentication and Trust Services (eIDAS- EU) The Pan-Canadian Trust Framework (PCTF- Canada), and the Trusted Digital Identity Framework (TDIF - Australia)

BIBLIOGRAPHY

Ashiq, J. A. *The eIDAS Agenda: Innovation, Interoperability and Transparency.* Cryptomathic, Retrieved 18 March 2016.

ENISA. *Mobile ID Management.* European Network and Information Security Agency, Accessed on April 11, 2016.

Europa.eu. *Regulations, Directives and Other Acts.* The European Union, Retrieved 18 March 2016.

Fumy, Walter, and Manfred Paeschke. *Handbook of eID Security: Concepts, Practical Experiences, Technologies.* John Wiley & Sons, Dec. 13, 2010.

Gelb, Alan, and Julia Clark. *Identification for Development: The Biometrics Revolution.* Working Paper, Washington, DC: Center for Global Development, 2013.

Gomes de Andrade, Norberto Nuno, Shara Monteleone, and Aaron Martin. *Electronic Identity in Europe: Legal Challenges and Future Perspectives (eID 2020).* Joint Research Centre, European Commission, 2013.

GSMA and SIA. *Mobile Identity—Unlocking the Potential of the Digital Economy.* Groupe Spéciale Mobile Association (GSMA) and Secure Identity Alliance, Oct. 2014.

IEEE. *What Are Standards? Why Are They Important?* IEEE, 2011. http://standardsinsight.com/ieee_company_detail/what-are-standards-why-are-they-important.

ITU. *Biometrics and Standards.* Telecommunication Standardization Sector, International Telecommunication Union, Accessed on April 11, 2016.

ITU. *Biometric Standards: ITU-T Technology Watch Report.* International Telecommunications Union, Dec. 2009.

PIRA. *The Future of Personal ID to 2019.* Smithers PIRA International, 06 June 2014.

"Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive." 1999/93/EC.

Turner, Dawn M. *eIDAS from Directive to Regulation—Legal Aspects.* Cryptomathic, Retrieved 18 March 2016.

Turner, Dawn M. *Understanding Major Terms Around Digital Signatures.* Cryptomathic, Retrieved 18 March 2016.

van Zijp, Jacques. *Is the EU Ready for eIDAS?* Secure Identity Alliance, Retrieved 18 March 2016.

Williams-Grut, Oscar. "Estonia wants to become a 'country as a service'." *Business Insider*, 2016.

World Bank. ID4D Practitioner' Guide: Version 1.0. Washington, DC: World Bank, 2019.

APPENDIX A
ISO/IEC JTC SUBCOMMITTEE, WORKING GROUPS AND THEIR MANDATE

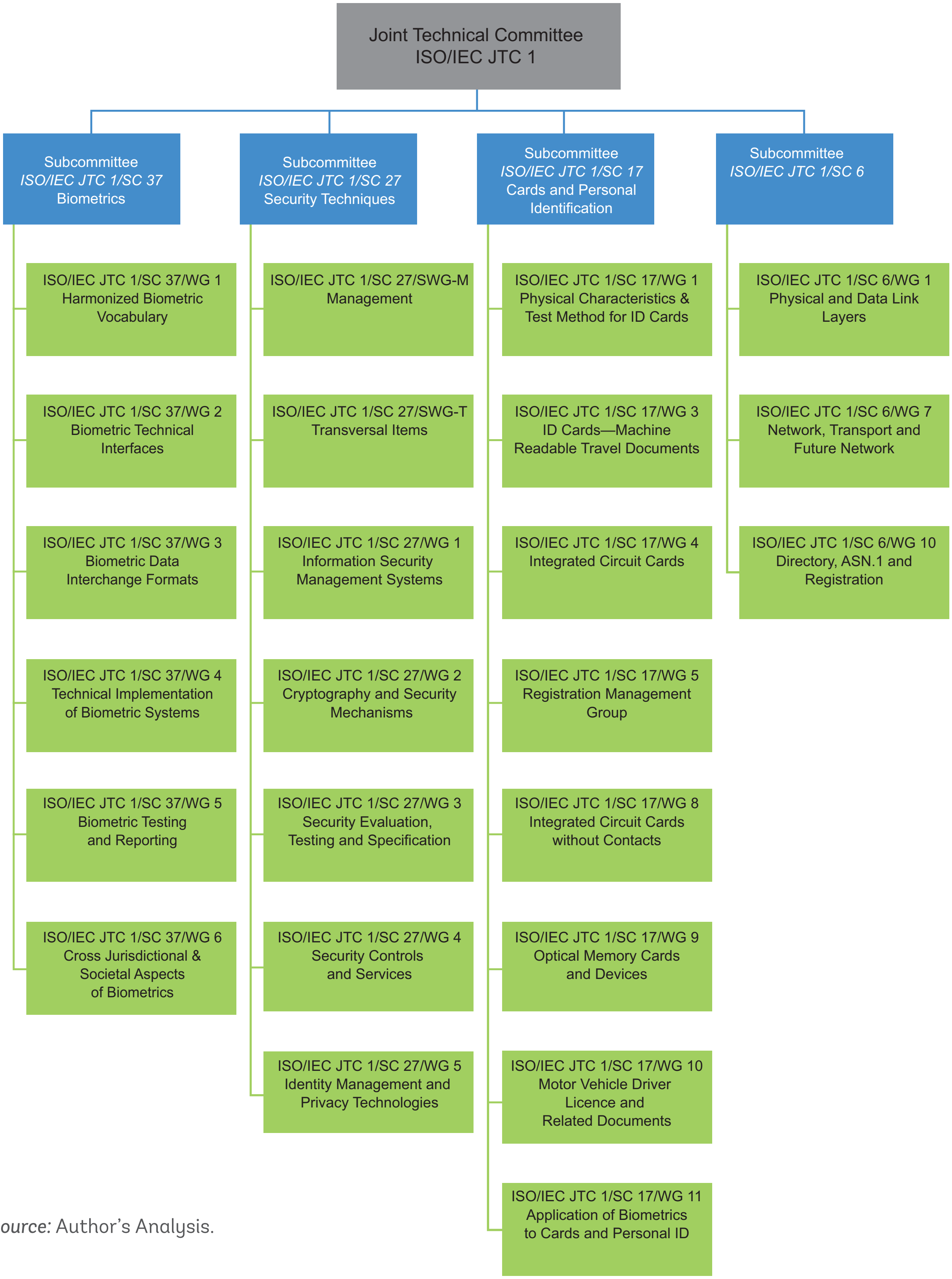
ISO Technical Committees and Working Groups

ISO has established technical committees, subcommittees, and working groups that are in continuous communication with other international and national organizations, as well as industry consortia involved in reviewing or establishing standards. A Joint Technical Committee, ISO/IEC JTC 1, has been formed by ISO and IEC to ensure a comprehensive and worldwide approach for the development and approval of international biometric standards. Within JTC1, subcommittees 37, 27, and 17 are relevant for any country that is planning to undertake a digital identity system. Various working groups within these subcommittees focus on the development and updating of specific standards relevant to the digital identity lifecycle, including:

1. ISO/IEC JTC 1/SC 37: Biometrics
2. ISO/IEC JTC 1/SC 27: IT Security Techniques
3. ISO/IEC JTC 1/SC 17: Cards and Personal Identification
4. ISO/IEC JTC 1/SC 6: Telecommunications and information exchange between systems (standards on digital signature/PKI)

These subcommittees work with other subcommittees within the ISO (liaison committees) as well as external organizations (organizations in liaison), some of whom are also involved in preparation of related standards. The table below identifies the role, scope, and mandate of the technical subcommittees and their subsequent working groups.

FIGURE 5 ISO/IEC Joint Technical Committee 1: Subcommittees and Working Groups for ID Management


Joint Technical Committee ISO/IEC JTC 1
Subcommittee *ISO/IEC JTC 1/SC 37* Biometrics
Subcommittee *ISO/IEC JTC 1/SC 27* Security Techniques
Subcommittee *ISO/IEC JTC 1/SC 17* Cards and Personal Identification
Subcommittee *ISO/IEC JTC 1/SC 6*
ISO/IEC JTC 1/SC 37/WG 1 Harmonized Biometric Vocabulary
ISO/IEC JTC 1/SC 37/WG 2 Biometric Technical Interfaces
ISO/IEC JTC 1/SC 37/WG 3 Biometric Data Interchange Formats
ISO/IEC JTC 1/SC 37/WG 4 Technical Implementation of Biometric Systems
ISO/IEC JTC 1/SC 37/WG 5 Biometric Testing and Reporting
ISO/IEC JTC 1/SC 37/WG 6 Cross Jurisdictional & Societal Aspects of Biometrics
ISO/IEC JTC 1/SC 27/SWG-M Management
ISO/IEC JTC 1/SC 27/SWG-T Transversal Items
ISO/IEC JTC 1/SC 27/WG 1 Information Security Management Systems
ISO/IEC JTC 1/SC 27/WG 2 Cryptography and Security Mechanisms
ISO/IEC JTC 1/SC 27/WG 3 Security Evaluation, Testing and Specification
ISO/IEC JTC 1/SC 27/WG 4 Security Controls and Services
ISO/IEC JTC 1/SC 27/WG 5 Identity Management and Privacy Technologies
ISO/IEC JTC 1/SC 17/WG 1 Physical Characteristics & Test Method for ID Cards
ISO/IEC JTC 1/SC 17/WG 3 ID Cards—Machine Readable Travel Documents
ISO/IEC JTC 1/SC 17/WG 4 Integrated Circuit Cards
ISO/IEC JTC 1/SC 17/WG 5 Registration Management Group
ISO/IEC JTC 1/SC 17/WG 8 Integrated Circuit Cards without Contacts
ISO/IEC JTC 1/SC 17/WG 9 Optical Memory Cards and Devices
ISO/IEC JTC 1/SC 17/WG 10 Motor Vehicle Driver Licence and Related Documents
ISO/IEC JTC 1/SC 17/WG 11 Application of Biometrics to Cards and Personal ID
ISO/IEC JTC 1/SC 6/WG 1 Physical and Data Link Layers
ISO/IEC JTC 1/SC 6/WG 7 Network, Transport and Future Network
ISO/IEC JTC 1/SC 6/WG 10 Directory, ASN.1 and Registration

Source: Author's Analysis.

SubCommittees/Working Group	Scope	Description
ISO/IEC JTC 1/SC 37 Biometrics	Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems	Common file frameworks, Biometric application programming interfaces (BAPI), Biometric data interchange formats, Related biometric profiles, Application of evaluation criteria to biometric technologies, Methodologies for performance testing and reporting and cross jurisdictional and societal aspects
ISO/IEC JTC 1/SC 37/WG 1	Harmonized Biometric Vocabulary	
ISO/IEC JTC 1/SC 37/WG 2	Biometric Technical Interfaces	
ISO/IEC JTC 1/SC 37/WG 3	Biometric Data Interchange Formats	
ISO/IEC JTC 1/SC 37/WG 4	Technical Implementation of Biometric Systems	
ISO/IEC JTC 1/SC 37/WG 5	Biometric Testing and Reporting	
ISO/IEC JTC 1/SC 37/WG 6	Cross Jurisdictional and Societal Aspects of Biometrics	
ISO/IEC JTC 1/SC 27 IT Security techniques	The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects. 1) Security requirements capture methodology; 2) Management of information and ICT security, in particular information security management systems, security processes, security controls and services; 3) Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information; 4) Security management support documentation including terminology, guidelines as well as procedures for the registration of security components; 5) Security aspects of identity management, biometrics and privacy; 6) Conformance assessment, accreditation and auditing requirements in the area of information security management systems; 7) Security evaluation criteria and methodology.	Develops International Standards, Technical Reports, and Technical Specifications within the field of information and IT security. Standardization activity by this subcommittee includes general methods, management system requirements, techniques and guidelines to address both information security and privacy.
ISO/IEC JTC 1/SC 27/SWG-M	Management	
ISO/IEC JTC 1/SC 27/SWG-T	Transversal items	
ISO/IEC JTC 1/SC 27/WG 1	Information security management systems	
ISO/IEC JTC 1/SC 27/WG 2	Cryptography and security mechanisms	
ISO/IEC JTC 1/SC 27/WG 3	Security evaluation, testing and specification	
ISO/IEC JTC 1/SC 27/WG 4	Security controls and services	
ISO/IEC JTC 1/SC 27/WG 5	Identity management and privacy technologies	
ISO/IEC JTC 1/SC 17 for Cards and personal identification	Standardization in the area of: Identification and related documents, cards and, devices associated with their use in inter-industry applications and international interchange	Develops and facilitates standards within the field of identification cards and personal identification

SubCommittees/Working Group	Scope	Description
ISO/IEC JTC 1/SC 17/WG 1	Physical characteristics and test methods for ID cards	
ISO/IEC JTC 1/SC 17/WG 3	Identification cards—Machine readable travel documents	
ISO/IEC JTC 1/SC 17/WG 4	Integrated circuit cards	
ISO/IEC JTC 1/SC 17/WG 5	Registration Management Group (RMG)	
ISO/IEC JTC 1/SC 17/WG 8	Integrated circuit cards without contacts	
ISO/IEC JTC 1/SC 17/WG 9	Optical memory cards and devices	
ISO/IEC JTC 1/SC 17/WG 10	Motor vehicle driver license and related documents	
ISO/IEC JTC 1/SC 17/WG 11	Application of biometrics to cards and personal identification	

Source: ISO http://www.iso.org/iso/home.htm.