

Public Disclosure Authorized



Public Disclosure Authorized



Public Disclosure Authorized



Public Disclosure Authorized



CATALOG OF Technical Standards for Digital Identification Systems

© 2018 International Bank for Reconstruction and Development/The World Bank
1818 H Street NW
Washington DC 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.

Rights and Permissions

The material in this work is subject to copyright. Because The World Bank encourages dissemination of its knowledge, this work may be reproduced, in whole or in part, for noncommercial purposes as long as full attribution to this work is given.

Any queries on rights and licenses, including subsidiary rights, should be addressed to World Bank Publications, The World Bank Group, 1818 H Street NW, Washington, DC 20433, USA; fax: 202-522-2625; e-mail: pubrights@worldbank.org.

TABLE OF CONTENTS

- ABBREVIATIONS** v
- ACKNOWLEDGMENTS** vii
- 1. INTRODUCTION** 1
- 2. OBJECTIVE** 2
- 3. SCOPE** 2
- 4. THE IDENTITY LIFECYCLE** 4
 - 4.2 Registration 4
 - 4.1.1 Enrollment 4
 - 4.1.2 Validation 5
 - 4.2 Issuance 5
 - 4.3 Authentication 5
 - 4.4 Lifecycle Management 6
 - 4.5 Federation 6
- 5. DIGITAL ID RELATED TECHNICAL STANDARDS** 7
 - 5.1 Why Are Standards Important? 7
 - 5.2 Standards-Setting Bodies 7
 - 5.3 Technical Standards 8
 - Technical Standards for Interoperability. 8
 - Technical Standards for Robust Identity Systems. 15
 - 5.4 Frameworks 16
 - 5.4.1 Levels of Assurance 16
- 6. COUNTRY USE CASES** 18
 - Example 1: ID-Kaart in Estonia—Smart Card and Mobile ID. 18
 - Example 2: Aadhaar Identity System of India—Biometric Based 20
 - Example 3: Malawi—Biometrics and Smart Card 22
 - Example 4: Smart eID in Pakistan—Biometrics and Smart Card 24
 - Example 5: eID with Digital Certificate in Peru 26
- 7. CONCLUSION** 28
- BIBLIOGRAPHY** 29
- APPENDIX A ISO/IEC JTC SUBCOMMITTEE, WORKING GROUPS AND THEIR MANDATE** 30

LIST OF FIGURES

- FIGURE 1 INTEROPERABILITY FRAMEWORK—5 BUILDING BLOCKS 3
- FIGURE 2 IDENTITY LIFECYCLE 4
- FIGURE 3 STANDARDS FOR IDENTIFICATION SYSTEM. 9
- FIGURE 4 DECISION TREE STANDARDS10
- FIGURE 5 ISO AND EIDAS AUTHENTICATION LEVELS17
- FIGURE 6 ISO/IEC JOINT TECHNICAL COMMITTEE 1: SUBCOMMITTEES
AND WORKING GROUPS FOR ID MANAGEMENT.31

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, and 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 that are integrated with civil registration.

The work of ID4D is made possible with support from the World Bank Group, Bill & Melinda Gates Foundation, Omidyar Network and the Australian Government.

To learn more about ID4D, visit id4d.worldbank.org.

ACKNOWLEDGMENTS

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

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.

1. INTRODUCTION

Robust and inclusive identification 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 transfers and benefits payments, increased security, accurate vital statistics for planning purposes, and greater capacity to respond to disasters and epidemics.

Despite these benefits, globally, an estimated 1 billion individuals lack proof of identity.¹ In order to close this “identity gap,” many countries have begun to reform existing identification systems and build 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 leapfrog the inefficiencies of paper-based identification systems. At the same time, digital identification poses many challenges related to data protection

and privacy, fiscal sustainability, and the choice and use of different technology options.

Robust Digital ID systems, if developed in an interoperable and scalable manner, can produce savings for citizens, government and businesses. Conversely, disparate initiatives and siloed investments in Digital ID systems are likely to be duplicative and fall short of the far-reaching public and private sector benefits of universal Digital IDs. Pooled approaches and federated ID systems at the regional or sub-regional level can also help strengthening the value proposition of Digital IDs. The robustness and interoperability of an identification system depends on the degree to which it adheres to technical standards—henceforth “standards.”

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 enrollment, validation, deduplication, and authentication. Standards help ensure that the building blocks of identity systems are interoperable and testable, and can meet desired performance targets. The effectiveness of an interconnected and interoperable identification system cannot be ensured without standards.

¹ Estimated by the World Bank ID4D Dataset, 2018.

2. OBJECTIVE

Standards are critical for identification systems to be robust, 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 source of reference for the stakeholders in the identification systems ecosystem. It is envisioned that an analysis of the catalog of existing standards, organized by category and subcategory, would help in a) identification of areas where standards are

missing, b) identify areas where there are competing standards and choice needs to be made and c) assess applicability of standards in a developing country context. This could also help share experiences across countries and avoid reinvention of the wheel by each country/stakeholder. A decision tree of the technical standards organized by technology area is provided to help the selection of technical standards from the catalog. The application of the decision tree has been illustrated in the country case studies of Estonia, India, Malawi, Pakistan and Peru.

3. SCOPE

“Digital identity” is a broad term, with different meanings depending on the context. For this document, we consider digital identity as a set of electronically captured and stored attributes and credentials that can uniquely identify a person. Digital identity systems may take a variety of forms, each with different applicable standards. Within the interoperability framework for digital identification systems there are five main building blocks as outlined in Figure 1. This report focuses only on the Technology

Interoperability building block. The technical standards that are in scope of this report are those that are required to build robust interoperable digital identification systems, which enables the creation of digital identities for individuals after validating their identity through defined processes, issuance of credentials linked to their identity and mechanisms to establish their identity (authenticate) using their digital identity/credentials.

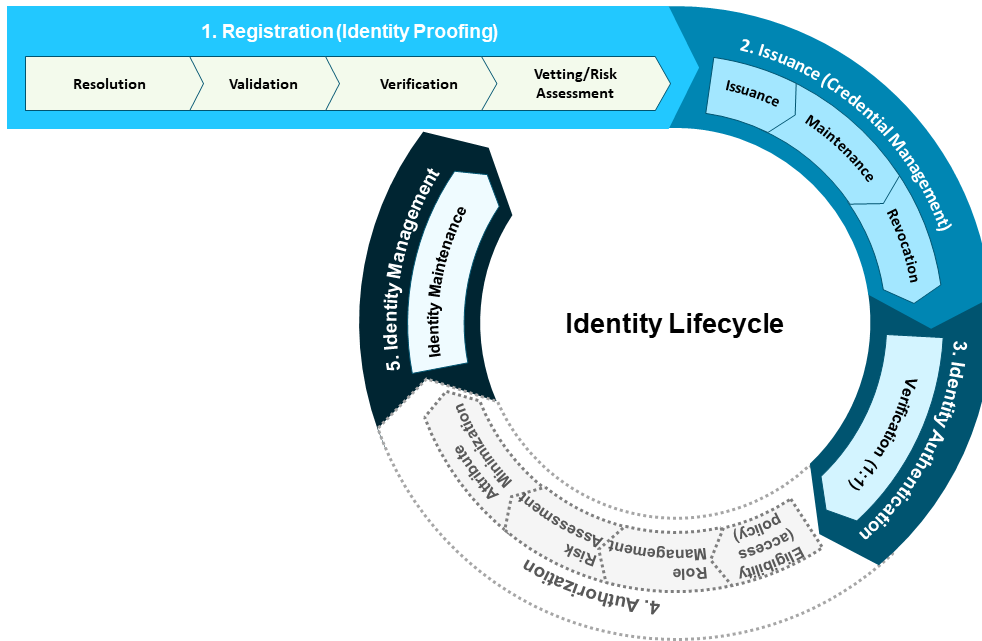
FIGURE 1 Interoperability Framework—5 building blocks

Legal	Legal, policy and regulatory issues related to identity, data privacy and protection
Governance & Management	Usability, security, privacy and performance, including contractual and commercial (e.g. Service Level Agreement—SLA)
Identity Process Interoperability	Process standards around business workflows, trust frameworks and mutual recognition, including federations (e.g. eIDAS)
Semantic Interoperability	Data standards, and data dictionaries ensuring that the meaning of exchange data and information is consistent
Technology Interoperability	Standards around software & physical hardware components, systems & platforms which enable machine-to-machine communication

SCOPE

4. THE IDENTITY LIFECYCLE

FIGURE 2 Identity Lifecycle



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 digital 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.

Digital identities are created and used as part of a lifecycle that includes three fundamental stages: (a) registration, including enrollment and validation, (b) issuance of documents or credentials, and (c) authentication for service delivery or transactions. Identity providers also engage in ongoing management of the system, including updating and revocation or termination of identities/credentials (see figure above).

4.1 REGISTRATION

This is the most important step in creating a digital identity. The process begins with enrollment followed by validation.

4.1.1 Enrollment

This process involves capturing and recording key identity attributes from a person who claims a certain identity, which may include biographical data (e.g., name, date of birth, gender, address, email), biometrics (e.g., fingerprints, iris scan) and an increasing number of other attributes. Which attributes are captured during this phase and the method used to capture them have important implications for the trustworthiness of the identity (see the discussion of levels of assurance below) as well as its utility and interoperability with other domestic and international identity systems.

4.1.2 Validation

Once the person has claimed an identity during enrollment, this identity is then validated by checking the attributes presented against existing data. The

validation process ensures that the identity exists (i.e., that the person is alive) and is claimed by one person (i.e., it is unique in the database). In modern digital identity systems, uniqueness is ensured through a deduplication process using biometric data. Links between the claimed identity and identities in other databases (e.g., civil registries, population registries, and so on) may also be established.

4.2 ISSUANCE

Before a credential can be used to assert identity by a person, a registered identity goes through an issuance or credentialing process, where identity providers may issue a variety of credentials (e.g., identifying numbers, smart cards, and certificates). For an ID to be considered digital, the credentials issued must be electronic, in the sense that they store and communicate data electronically.

Types of electronic credential systems include:

- **Smart cards:** Cards offer advanced security features and record digital cryptographic key and/or biometric on an embedded computer chip. Smart cards can come in the form of a contact/contactless card, or Near Field Communication (NFC)-enabled SIM card. Data stored on a smart card can be accessed offline for authentication where there is no internet connection or mobile network.
- **2D bar code card:** Cards can be personalized with an encrypted 2D bar code containing a person's personal data and biometrics, either instead of or in addition to a chip. The 2D bar code is a cost-efficient mean to provide a digital identity and to authenticate holders by comparing live biometric with that on the card. It has been widely deployed in Africa, Latin America, and the Middle East, including Lebanon, Mali, and Ghana, and more recently in Egypt to authenticate holders during the last elections.
- **Mobile identity:** Mobile phones and other devices can be used to provide portable digital identity and authentication for a variety of online transactions. For example, providers can issue SIM cards with digital certificates or use other mobile network assets that can enable secure and convenient identity and authentication of

users for eGovernment (eGov) services and other public or private platforms.

- **Identity (credential) in a central store/Cloud:** Unlike portable credentials such as smart cards and SIM cards, some systems store certificates and biometrics on a server only. In this case, a physical credential storage device may not be issued. Identity number may be issued in non-electronic form (e.g., India's Aadhaar program issues only a paper receipt). A tamper-resistant environment of cryptographic key generation and management to secure the ID credential in the central store against theft will increase the security and assurance level of the identity system.

4.3 AUTHENTICATION

Once a person has been registered and credentialed, they can use their digital identity to access the associated benefits and services. For example, citizens may use their eID number to pay taxes through an eGov portal, while bank customers can use smart debit cards or mobile financial services to make purchases. In order to access services, the user must be authenticated using one or more factors that generally fall into one of three categories—something you know, something you have, something you are. Authentication using these attributes can occur through various pathways, including

- **Smart cards:** People with smart cards can authenticate their identity using multiple authentication factors for varying levels of assurance. For example, a simple PIN for low risk use cases or a digital signature based on public key infrastructure (PKI) technology for high risk use cases. Fingerprints can be used to establish a non-ambiguous link with the user. Because they store data locally on a chip, smart cards can also be used for offline digital authentication or remote locations where connectivity is limited.
- **Mobile identity:** Using smartphone applications, USSD or SMS-based authenticators, or SIM cards, mobile identity can incorporate multiple authentication factors for varying levels of assurance. For example, a simple PIN for low risk use cases, multiple-factor authentication

solutions (including with the use of biometrics) or a mobile signature based on public key infrastructure (PKI) technology with a secure element (SE) for high-risk use cases. Authentication can be strengthened by using third and fourth factors such as the individual's location or behaviour.

- **ID in the central store/Cloud:** Instead of issuing an identity document or mobile credential, a digital identity system can rely on biometrics for remote authentication. In this case, an identity is asserted and verified via a computer or other device with a biometric reader that connects to the Cloud. A Cloud-based system eliminates the need and cost of physical credentials, but requires robust ICT infrastructure for connectivity and security of the central storage.

4.4 LIFECYCLE MANAGEMENT

Throughout the lifecycle, digital identity providers manage and organize the identity system, including facilities and staff, record keeping, compliance and auditing, and updating the status and content of digital identities. For example, users may need to update various identity attributes, such as address, marital status, profession, etc. In addition, identity providers may need to revoke an identity, which involves invalidating the digital identity for either fraud or security reasons, or terminate an identity in the case of the individual's death.

4.5 FEDERATION

Federation is the ability of one organization to accept another organization's identity. Federation is based on inter-organizational trust. The trusting organization must be comfortable that the trusted organization has similar policies, and that those policies are being followed. Federation protocols and assurance framework facilitate federation of digital identity intra and inter organizations/countries. Federation protocols like SAML (Security Assertion Mark-up Language) are used to convey the authentication result

by the credential provider to the trusting organization. The trusting organization sends captures and sends the credential to the issuing organization for verification. After verification of the credential the issuing organizations sends a set of claims giving information about the user, result of authentication and the strength of the credentials used to authenticate the user. For federation to be effectively used globally, agreement and mapping with the ISO defined assurance framework and adoption of federation protocols as standards are critical.

Federation can occur at multiple levels:

- An organization can accept credentials issued by another organization, but still authenticate and authorize the individual locally:
 - A passport issued by the U.S. Department of State is accepted as a valid credential by a foreign country, but that country's immigration office still authenticates the holder and requires a visa (authorization).
- An organization can accept specific characteristics (attributes) describing an individual from another organization:
 - Your bank will request your credit score from one of the credit bureaus, rather than maintaining that information itself.
- An organization can accept an authorization decision from another organization:
 - A driver's license authorizing you to drive in one state is accepted by another.

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. While the adoption of standards has a positive impact in market penetration and international trade, a lack of standards creates issues for the effectiveness and robustness of an identity system, including problems with interoperability, interconnectivity and vendor lock-in.

As electronic IDs have begun to replace paper-based systems, the technologies, inter-device communication and security requirements underpinning identity 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.²

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

² [IEEE FAQs](#)

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 for identity systems. Most of them relate to the credential to be used for authenticating the user. Technical standards which are applicable to identity applications that are common with any software application (web application/desktop/portal) are not listed/discussed in this report. The Technical Standards are grouped in two tables. The first table lists standards which are required for interoperability of systems and the second table of standards lists standards for robustness of identification systems which address the requirements like security, 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.

1. Biometrics—Image standard—Multiple competing standards are in use for capturing face 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) standard are in use. Comments provide guidelines on selection of image standard for images like face, fingerprint.
2. Biometrics—Biometric data interchange format standards and biometric interface standards are both necessary to achieve full data interchange and interoperability for biometric recognition in an open systems environment. Biometric data complying with a biometric data interchange format of ISO 19794 represents the core component of biometric interoperability. The biometric data interchange format standards specify biometric data interchange formats for different biometric modalities. Parties that agree on a biometric data interchange format specified in ISO 19794 should be able to decode each other's biometric data. The biometric interface standards include ISO 19785 Information technology — Common Biometric Exchange Formats Framework and ISO 19784 Information technology — Biometric application programming interface (BioAPI). These standards support exchange of biometric data within a system or among systems. 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. ISO 19784 specifies an open system API that supports communications between software applications and underlying biometric technology services.
3. Card/Smart Card—For countries that issue a tangible credential such as a physical eID card, standards such as ISO-7810 become 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 eID cards, passports, drivers' licenses, or any other machine-readable travel documents (MRTDs) used for crossing borders—then compliance with ICAO 9303 should be followed. Each identity system would select a card based on various criteria like cost, security features.

4. Digital Signatures—Multiple non-competing standards are listed which are applicable based on the use of digital signature for the identity systems.
5. 2D bar code—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.
6. Federation protocols—Open ID connect and OAuth combination are being increasingly used for federation while SAML has been used extensively earlier.

The list of standards applicable for an ID system would consist of sum of standards selected from each of the 6 categories.

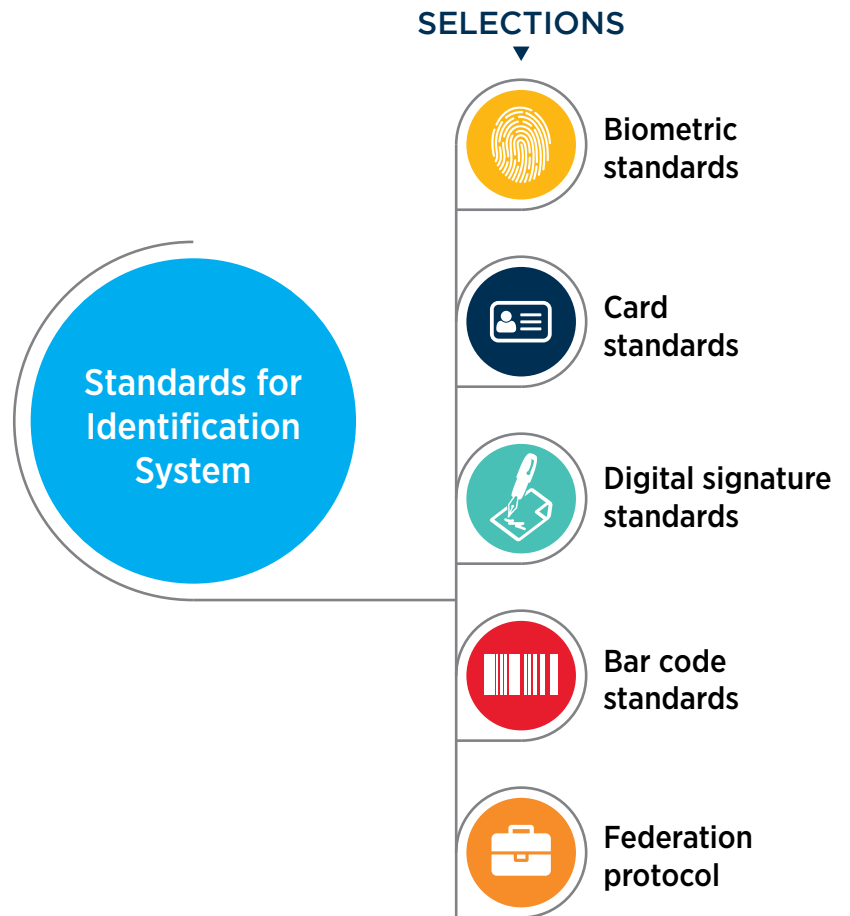
A decision tree which enables selection of applicable standards based on choice of technologies made for the implementation of Identification systems is diagrammatically presented in figure 4.

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 identity system.

Technical Standards for Robust Identity Systems

The table Technical Standards for Robust Identity Systems lists standards which provide guidelines on quality, testing, privacy and accessibility related

FIGURE 3 Standards for Identification System

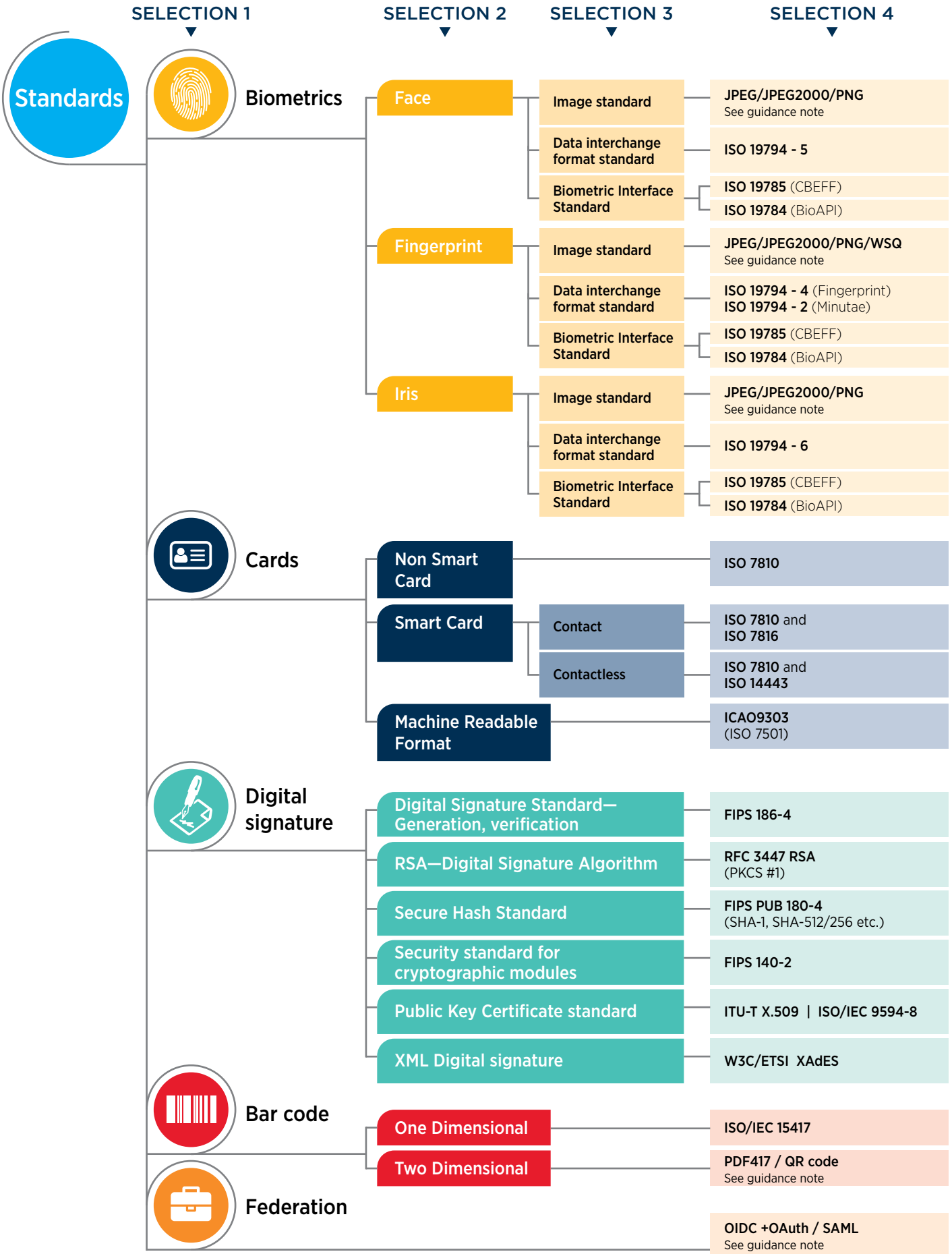











2. The standards at the leaf level of the branch of the tree are the applicable standards for the decisions made in choice of technology and system design.
3. At some of the leaf nodes, one would need to make a selection among competing standards. The guidance note in the table of standards would help in selecting one of the standards from the available competing standards.
4. A short description and weblink to the standard is available in the standards catalogue table.

aspects of identification systems to enhance the robustness of identification systems. The implementers of identification systems can adopt the relevant

FIGURE 4

DECISION TREE STANDARDS









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	<p>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</p> <p>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.</p>
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	
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 	Biometrics Interface Standard	ISO/IEC 19784-1:2018 (BioAPI specification)	Specifies an open system API that supports communications between software applications and underlying biometric technology services.	ISO/IEC	Some nations (e.g. EU, Interpol, Canada, USA) have relied on the core ANSI/NIST-ITL fingerprint and other image exchange format
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.
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	PDF417 is a stacked barcode that can be read with a simple 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.
D.3	Bar Code 	2 D	ISO/IEC 15438:2015—PDF417	Requirements for the bar code symbology characteristics, data character encoding, symbol formats, dimensions, error correction rules, reference decoding algorithm, and many application parameters.	ISO and IEC	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.
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 	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	

(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 	Security	FIPS 140-2	Security Requirements for Cryptographic Modules	NIST	
E.5	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.6	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.
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	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.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	

guidelines and best practices for their identification systems by using these standards. For instance, India's Aadhaar system 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.

5.4 FRAMEWORKS

ISO/IEC 29115 and eIDAS provide assurance levels framework for identity systems. Ideally the National Identity system should conform to the highest level. Further discussion on this would facilitate preparation of guidelines on options for implementation of

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 TR 29194:2015	Guide on designing accessible and inclusive biometric systems
9	Biometrics	ISO/IEC TR 29196:2015	Guidance for biometric enrolment
10	Biometrics	ISO/IEC TR 30125:2016	Biometrics used with mobile devices
11	Biometrics	ISO 19792:2015	Security techniques—Security evaluation of biometrics
12	Biometrics	ISO 24714:2015	Biometrics—Jurisdictional and societal considerations for commercial applications -- Part 1: General guidance
13	Privacy	ISO/IEC 29100	Privacy framework
14	Privacy	ISO/IEC 27018	Code of practice for PII protection in public clouds acting as PII processors
15	Privacy	ISO/IEC 29190	Privacy capability assessment model
16	Privacy	ISO/IEC 29184	Guidelines for online privacy notice and consent
17	Management	ISO/IEC 24760 Series	Framework for Management of Identity Information

Identity systems of the highest assurance levels. Also, guidelines on the different options with their strengths and weaknesses with some example scenarios would help in selecting the appropriate identity system and relevant technical standards.

5.4.1 Levels of Assurance

When a person identifies or authenticates herself using one or multiple identity attributes, the degree of confidence that she is who she claims to be depends on the degree of security assurance provided and the context in which the information is captured, referred

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

to as the level of assurance (LOA). Assurance levels depend on the strength of the identification and authentication processes, and are critical to access control and reducing identity theft. The higher the LOA, the lower the risk is that service providers will rely on a compromised credential during a transaction. For “identity proofing,” the LOA is dependent on the method of identification, including the scope of personal information and attributes collected about an individual during enrollment, and the degree of certainty with which these attributes are ascertained (i.e., have been validated). For example, if personal data are collected during enrollment but not de-duplicated or checked against existing databases for veracity, this would constitute a low LOA because there is no validation of the identity information.

ISO/IEC 29115 provides a framework for entity authentication assurance. Assurance within this Recommendation | International Standard refers to the confidence placed in all the processes, management activities, and technologies used to establish and manage the identity of an entity for use in authentication transactions. This framework also identifies three phases enrollment, credentialing and authentication phases mapping to the three key

activities listed in Identity Lifecycle. It also lists the organizational and management activities which map with Governance phase of Identity and addresses requirements of federation and role of assurance framework in the same without listing it as a separate process.

ISO 29115 sets out four LOA for scalable identity management and authentication services. These levels are shown in Figure 5, along with corresponding definitions from the European Union’s eIDAS framework, and range from weak authentication protocols with extremely high security risk levels, to strong authentication protocols with minimal risk levels. The level of risk is based not only on the credentials and processes used for authentication, but also on the robustness of identity proofing during the registration phase. Depending on the type of application, countries may implement a variety of authentication protocols to meet the standards necessary for the use case.

NIST Digital Identity Guidelines 800-63-3 retire the concept of a LOA as a single ordinal that drives implementation-specific requirements as of 2017. Rather, by combining appropriate business and privacy risk

management side-by-side with mission need, agencies will select IAL, AAL, and FAL as distinct options. While many systems will have the same numerical level for each of IAL, AAL, and FAL, this is not a requirement and agencies should not assume they will be the same in any given system.

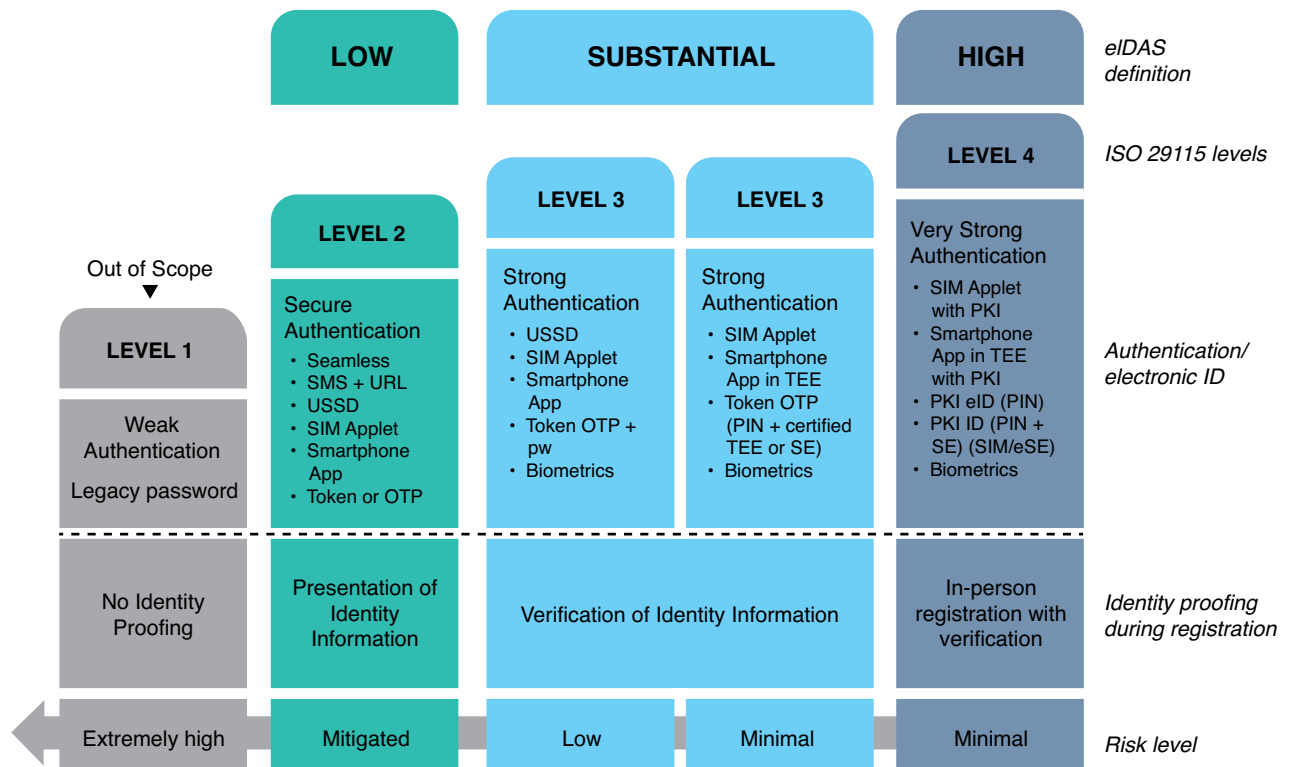
The components of identity assurance detailed in NIST guidelines are as follows:

- IAL refers to the identity proofing process.
- AAL refers to the authentication process.
- FAL refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP).

The separation of these categories provides agencies flexibility in choosing identity solutions and increases the ability to include privacy-enhancing techniques

as fundamental elements of identity systems at any assurance level. For example, these guidelines support scenarios that will allow pseudonymous interactions even when strong, multi-factor authenticators are used. In addition, these guidelines encourage minimizing the dissemination of identifying information by requiring federated identity providers (IdPs) to support a range of options for querying data, such as asserting whether an individual is older than a certain age rather than querying the entire date of birth. While many agency use cases will require individuals to be fully identified, these guidelines encourage pseudonymous access to government digital services wherever possible and, even where full identification is necessary, limiting the amount of personal information collected as much as possible.

FIGURE 5 ISO and eIDAS Authentication Levels



Source: World Bank, 2016.

6. COUNTRY USE CASES

Depending on the country-specific environment, which standards should be adopted and which should be ignored? The answer depends on the objectives, scope, and proposed use for the identity system. Examples of Estonia, India, Malawi, Pakistan and Peru are presented below to illustrate the choice

of relevant standards by respective national governments to meet their requirements. When designing an identification system, however, a priority always to ensure that the choice of technologies and related standards are following existing regulatory frameworks within a country.

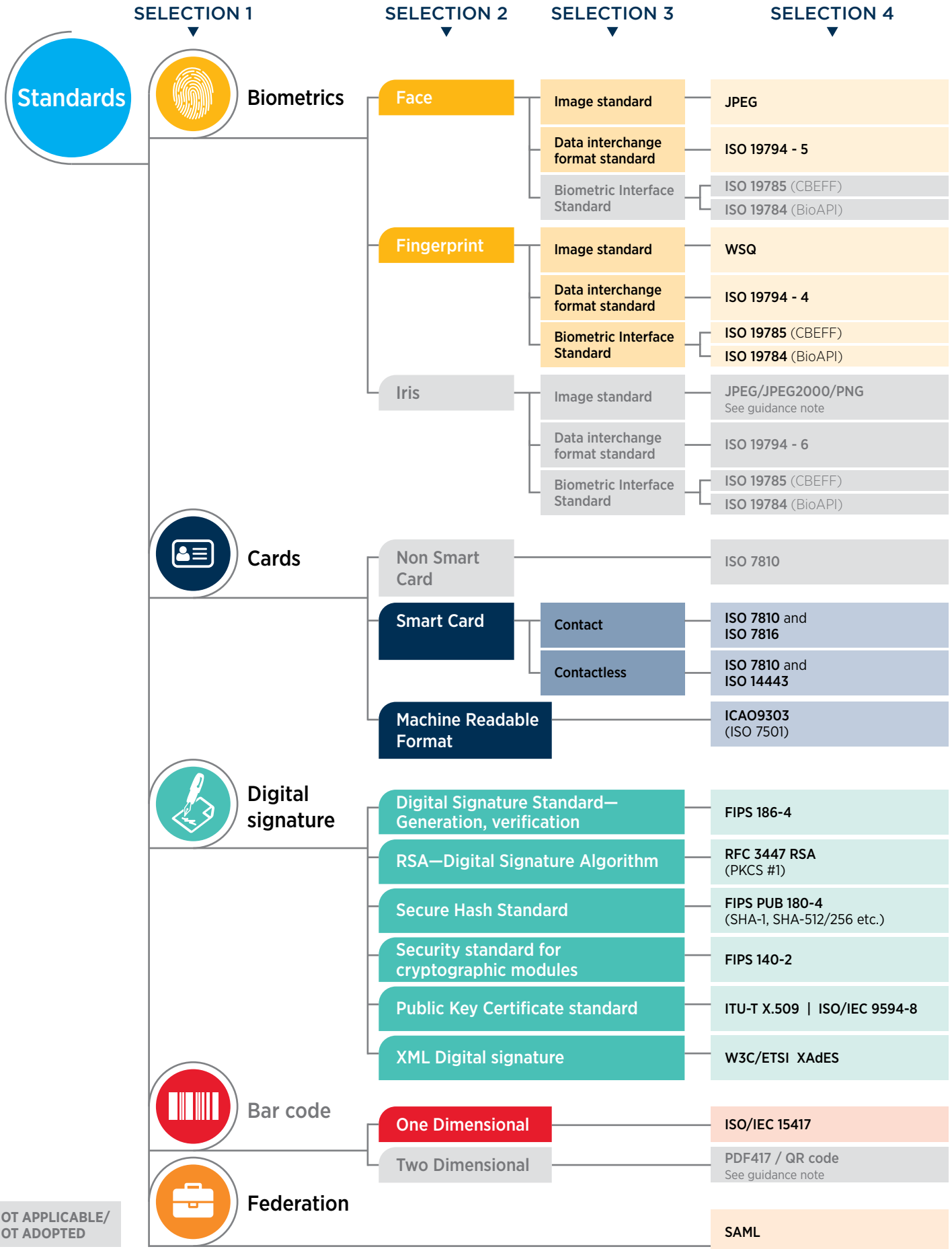
EXAMPLE 1: ID-KAART IN ESTONIA—SMART CARD AND MOBILE ID

Estonia has the most highly developed national ID card system in the world (Williams-Grut 2016). It has issued 1.3 million of its smart ID-Kaarts, each with a unique identifier that allows citizens to access over 1,000 public services, such as health care, online tax filing, and online voting. Estonia is now one of the most digitally advanced nations in the world with regard to public services. It wants to become a “country as a service,” where secure digital identity plays a central role. Key identifying data such as name, date of birth, unique ID number and digital certificates are stored in the smart card chip 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. Estonia does not do biometric deduplication for issuance of unique ID but captures fingerprints at the time of issuance of ID card.

The ID-Kaart is a secure 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



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 billion residents. Photograph, fingerprints and irises of each resident are captured before issuing an Aadhaar. It is the world's largest multimodal biometric database, with nearly the entire population having a digital identity as a result of this system. 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. UIDAI had also come up with standards (demographic standards committee) for the data standards for the identity attributes captured during registration and subsequently used for demographic authentication. Aadhaar system also makes extensive use of PKI/HSM for encryption of data during transmission and storage and for protecting access to API.

Aadhaar system does not issue any physical ID card for authentication. There is a mAadhaar mobile app which allows electronic storage of demographic data, Aadhaar number and photograph along with a QR code. A laminated paper is also sent to the residents with demographic data, photo and QR code (contains encrypted and digitally signed data). The QR code from this paper document or mAadhaar app is also being 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.

Standards

SELECTION 1



Biometrics

SELECTION 2

SELECTION 3

SELECTION 4

Face

Image standard

JPEG2000

Data interchange format standard

ISO 19794 - 5

Biometric Interface Standard

ISO 19785 (CBEFF)

ISO 19784 (BioAPI)

Fingerprint

Image standard

JPEG2000

Data interchange format standard

ISO 19794 - 4

ISO 19794 - 2

Biometric Interface Standard

ISO 19785 (CBEFF)

ISO 19784 (BioAPI)

Iris

Image standard

JPEG2000

Data interchange format standard

ISO 19794 - 6

Biometric Interface Standard

ISO 19785 (CBEFF)

ISO 19784 (BioAPI)



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

RSA—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 universal coverage of the adult population through the recent issuance of biometric national ID card to 9 million people, which is managed by the National Registration Bureau (NRB) under the Ministry of Home Affairs and Internal Security. Only Malawians that are 16 years of age or older are issued a national ID card those under 16 years of age qualify for a national birth certificate. The ID card itself is quite sophisticated. The registration process captures 10 fingerprints, a digital photograph, and electronic signature. Biometric deduplication is done for issuance of a unique ID and smart card. It is ICAO (9303) and ISO (7816) compliant, with seven built-in security features to prevent forgery. The ID card also has a QR code on the card.

The ICAO Identity Applet will allow card holders to use it for all national travel at airports, where card readers can access the data and verify the identity of the holder. It has a digital certificate as well, issued by the NRB. Likewise, the e-Health Applet allows it to become a virtual health insurance card (compliant with European standard CWA15974), so that health offices can use it to verify identity and deliver services for which the holder qualifies. Malawian citizens may not have to carry a separate health card as the main ingredients of a Health insurance card that is compliant with international standards are embedded in National ID card. The national ID card has the capability to be used as a Health Insurance Card but a decision by the Ministry of Health to enable it be used for that purpose is under consideration. These standards are followed by European countries, New Zealand, and Australia. The Public Key Infrastructure applet allows the government to use the card as the basis to roll out, for example, a financial inclusion or social safety net program and verify the identities of beneficiaries. Finally, the e-Driver's License applet can verify whether the holder also has a driving license.

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

Standards

SELECTION 1



Biometrics

SELECTION 2

SELECTION 3

SELECTION 4

Face

Image standard

JPEG2000

Data interchange format standard

ISO 19794 - 5

Biometric Interface Standard

ISO 19785 (CBEFF)
ISO 19784 (BioAPI)

Fingerprint

Image standard

WSQ

Data interchange format standard

ISO 19794 - 4
ISO 19794 - 2

Biometric Interface Standard

ISO 19785 (CBEFF)
ISO 19784 (BioAPI)

Iris

Image standard

JPEG/JPEG2000/PNG
See guidance note

Data interchange format standard

ISO 19794 - 6

Biometric Interface Standard

ISO 19785 (CBEFF)
ISO 19784 (BioAPI)



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

RSA—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



EXAMPLE 4: SMART eID IN PAKISTAN—BIOMETRICS AND SMART CARD

Pakistan's National Database and Registration Authority (NADRA) has issued over 121 million ID cards and hence registered 98 percent of its adult citizens over the age of 18. Over the years, Pakistan's ID card has evolved into a smart eID that contains multi-biometric features to meet the challenges of a digitally connected world. NADRA designed its cards to meet the needs of its citizens living outside the country as well. As a result, its smart eID for overseas Pakistanis, known as the National Identity Card for Overseas Pakistanis (NICOP), complies with ICAO standard 9303 part 3 vol. 1 and is also ISO 7816-4 compliant. An ICAO compliant smart NICOP can be accepted as a form of digital ID in all international airports and at points of entry and departure.

NADRA also 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 also ISO 9001:2000 certified. Smart eID 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.

Source: Author's Analysis.

Standards

SELECTION 1



Biometrics

SELECTION 2

SELECTION 3

SELECTION 4

Face

Image standard

JPEG

Data interchange format standard

ISO 19794 - 5

Biometric Interface Standard

ISO 19785 (CBEFF)
ISO 19784 (BioAPI)

Fingerprint

Image standard

WSQ

Data interchange format standard

ISO 19794 - 2

Biometric Interface Standard

ISO 19785 (CBEFF)
ISO 19784 (BioAPI)

Iris

Image standard

JPEG/JPEG2000/PNG
See guidance note

Data interchange format standard

ISO 19794 - 6

Biometric Interface Standard

ISO 19785 (CBEFF)
ISO 19784 (BioAPI)



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

RSA—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 Electronic ID Card (DNle) is issued by the National Registry of Identification and Civil Status (RENIEC). RENIEC is an autonomous entity with functions, including civil registration, identification, and digital signatures, has issued 30 million eIDs covering almost the entire population of the country.

The DNle provides Peruvian citizens with a digital identity, which can be authenticated physically and virtually. The DNle 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. Because the card is also used as a machine-readable travel document (MRTD), it also complies with ICAO 9303.

Source: Interview with RENIEC official.

Standards

SELECTION 1



Biometrics

SELECTION 2

SELECTION 3

SELECTION 4

Face

Image standard

JPEG2000

Data interchange format standard

ISO 19794 - 5

Biometric Interface Standard

ISO 19785 (CBEFF)
ISO 19784 (BioAPI)

Fingerprint

Image standard

JPEG/JPEG2000/PNG/WSQ
See guidance note

Data interchange format standard

ISO 19794 - 2

Biometric Interface Standard

ISO 19785 (CBEFF)
ISO 19784 (BioAPI)

Iris

Image standard

JPEG/JPEG2000/PNG
See guidance note

Data interchange format standard

ISO 19794 - 6

Biometric Interface Standard

ISO 19785 (CBEFF)
ISO 19784 (BioAPI)



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

RSA—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

7. CONCLUSION

Standards are key to unlocking the value of digital identity for development and supporting an interoperable, scalable, secure, and efficient digital identity platform for service delivery. Without standards, cross-functional systems inter-operability will be difficult to achieve. With so many standards on the horizon, choosing which to adopt is a key issue. It has been observed that because most of the standard bodies involved in developing biometric enrollment, authentication, issuance and management of identity contribute to the Technical Committees and Working Groups of ISO, its standards are widely accepted. However, the precise choice of relevant standards depends on the purpose, scope, and function of the national identification system as demonstrated through the country examples presented earlier. Some countries use their national ID for multiple functions, including as a drivers license, travel document and health insurance. For these countries, their national ID would need to comply with standards required by each of the functions. As an example, see the Malawi country description in Section 6.

In summary, 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 will be able to exist due to market forces. Also, in some instances, a closed solution may offer greater performance than an open

standard. In this case, the closed solution may be the preferred option but if so, be sure that the closed solution does not result in vendor lock-in 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 switched in and out of the identity system over time as vendors change or new, more efficient solutions present themselves. In addition, for some functions of an ID system, which are self-contained and do not require interoperability, such as deduplication, the use of a closed solution may be preferred assuming vendor lock-in is not a concern.

- 2. Technical Standards alone are not sufficient.** In addition to using open technical standards, there are semantic standards, which are important to consider when developing an ID system 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 interoperable data exchange across systems. Also, in addition to technical and semantic standards, there are many other considerations that need to be taken into account when designing a robust, sustainable and inclusive ID system. ID4D has developed a range of tools, including an ID system costing model, that can assist in thinking through the design of a system. These tools will be summarized in a forthcoming operational guide that will be published on the ID4D website (id4d.worldbank.org).
- 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. This is also important to keep in mind when designing an ID system to avoid investing in a system, which may quickly become outdated or is more costly to upgrade as new technologies emerge.

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. *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*. ID4D. 2016.
- World Bank. *Technology Landscape for Digital Identification*. ID4D. 2018)

APPENDIX A

ISO/IEC JTC SUBCOMMITTEE, WORKING GROUPS AND THEIR MANDATE

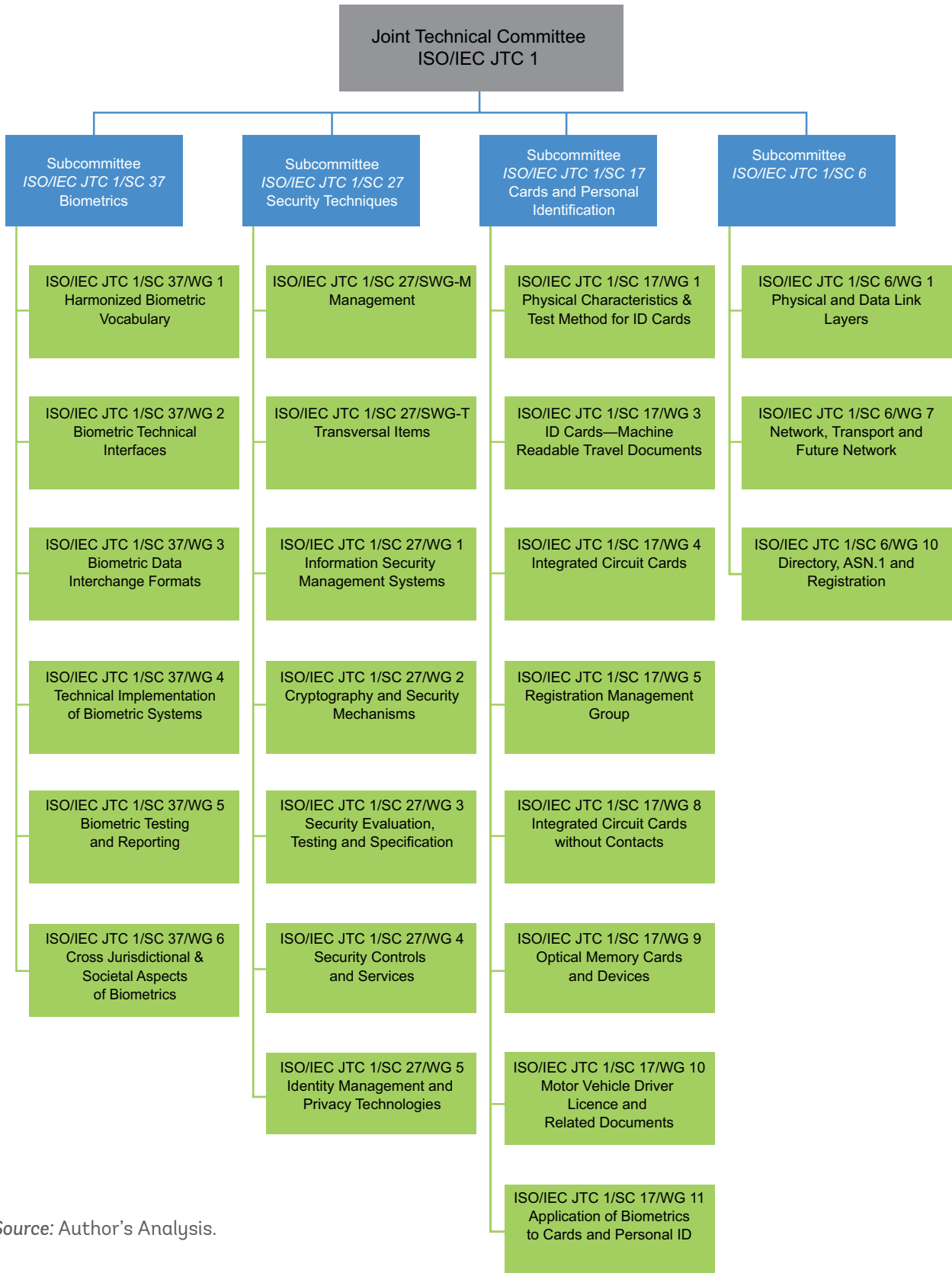
ISO Technical Committees and Working Groups

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



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>.

