Technical Standards for Digital Identity

DRAFT FOR DISCUSSION

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

Cover photo: © Digital Storm.

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
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

ACKNOWLEDGMENTS

This report was prepared by the Identification for Development (ID4D) initiative, the World Bank Group's cross-departmental effort to support progress towards identification systems using 21st century solutions. The report was prepared by Tariq Malik and Anita Mittal with inputs from Julia Clark, Vyjayanti Desai, Samia Melhem and Yasin Janjua. The team also wishes to thank the reviewers who offered helpful suggestions, including Dr. Narjees Adennebi (ICAO), Daniel Bachenheimer (Accenture), Sanjay Dharwadker (WCC Group), Marta Ienco (Mobile-Connect/GSMA), Flex Ortega De La Tora (RENIEC), Stephanie de Labriolle (SIA), Waleed Malik (World Bank), and Dr. Adeel Malik (Oxford University).

This report was presented and discussed with the following organizations in September 2017: American National Standards Institute (ANSI); Center for Global Development; Digital Impact Alliance; European Commission; FIDO Alliance; Bill & Melinda Gates Foundation; Government Digital Service; GSMA; ICAO; IOM; National Institute of Standards and Technology (NIST); Omidyar Network; One World Identity; Open Identity Exchange; Open Society Foundation; Plan International; The World Economic Forum; UNDP; UNHCR; UNICEF; USAID; and WFP.

1. INTRODUCTION

Robust, 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.[1]

Despite these benefits, however, some 1.1 billion individuals around the world lack proof of identity.[2] In order to close this "identity gap," many countries have therefore 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 including 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 a highly 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 wasteful and duplicative, detracting from the far-reaching public and private sector implications 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 programs. Trust in data security will be critical to achieving tangible results. 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.[3] They are therefore 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.

However, the standards used for identification systems can vary significantly by country and economic region or trading bloc. This diversity presents a significant challenge with respect to interoperability and compatibility both within countries and across borders (Gomes de Andrade, Nuno, Monteleone and Martin 2013). Without a common set of standards, countries with underdeveloped identification systems may not know which standards to follow, and may end up using sub-par technologies, and/or proprietary technology that results in vendor lock-in. The lack of a set of standards therefore poses a challenge for countries, as well as development partners who support country identification systems and provide technical assistance.

2. OBJECTIVE

Standards are critical for Identification systems to be robust, interoperable and sustainable. Process standards, data standards and technical standards are the three types of standards for ensuring interoperability at the organizational, semantic and technical layers. The objective of this report is to identify the existing international technical standards and frameworks applicable across the identity life cycle. This catalogue of technical standards could serve as a source of reference for the stakeholders in the identification systems ecosystem. This catalogue would also be the first step of a broader multi-stakeholder engagement to convene and explore the possibility of developing a minimal set of core technical standards for identification systems. It is envisaged that an analysis of the catalogue 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.

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 (World Bank, 2016, GSMA and SIA, Oct. 2014). Digital identity systems may take a variety of forms, each with different applicable standards. This report focuses on technical standards; data and process standards are not in scope of this document. The technical standards that are in scope of this report are those that are required to build robust interoperable digital identification systems which enables 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.

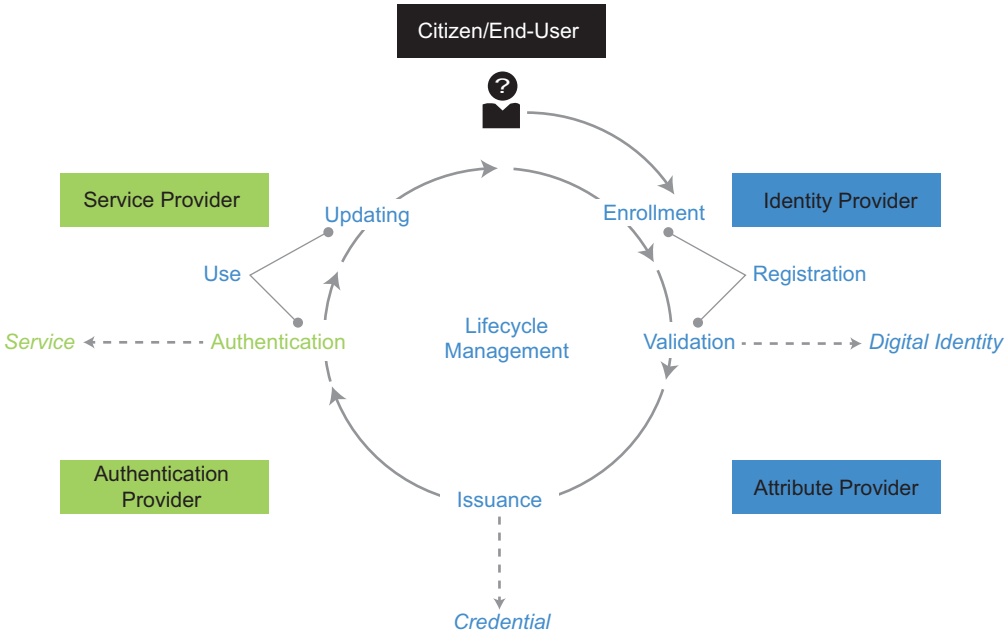
The report is organized as follows:

- Section 4 reviews the identity lifecycle and the processes/stages in this lifecycle to contextualize the relevant technical standards;
- Section 5 then gives an overview of international organizations developing standards and a list of the most commonly used standards for digital identification systems with focus on applicability of standards;
- Section 6 discusses the use case of different identity systems of a few countries;
- Section 7 discusses the issues and challenges to be considered while adopting standards;
- Section 8 provides recommendations for future work on developing minimum technical standards for identification systems to ensure interoperability and avoid vendor lock in;
- The appendices provide details on the standard organization, standards mapping, table giving details on each standard.

4. THE 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.[4] 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 (WB, GSMA and SIA, Oct. 2014) and describes briefly the various stages (WB, GSMA and SIA, Oct. 2014). This framework is then used to analyze relevant identification standards in Section 6.

Digital Identity Lifecycle and Key Roles



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 (WB, GSMA and SIA, Oct. 2014)). The description of the various phases below has been included from the same report (WB, GSMA and SIA, Oct. 2014).

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, certificates, etc.). For an ID to be considered digital, the credentials issued must be electronic, in the sense that they store and communicate data electronically. Common types of electronic credentials used fall into these three categories

- Something you know (for example, a password).
- Something you have (for example, an ID card, mobile phone or a cryptographic key).
- Something you are (for example, a fingerprint or other biometric data).

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, 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.[5]

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. In addition, ISO standards have been followed by most large-scale ID programs and are widely supported and used by industry consortia. As the nucleus of major industry standard contributions, this study therefore focuses on the work of the ISO.

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. Figure 1 identifies the role, scope, and mandate of the technical subcommittees and their subsequent working groups. For detailed description of these subcommittees, see Appendix A.

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

Source: Author's Analysis.

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. For addition of any missing information/standard or correction required to the table of standards/report, please send your feedback to sayers@worldbank.org

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—Data interchange format—ISO standards for different types of biometrics like fingerprint, iris, face are listed. The type(s) of biometrics selected for implementation of identity systems would dictate the standards to be complied with
3. Card/Smart Card—Different standards exist for the different types of card—card with chip and without chip and within chip category we have contact and contactless cards. Each identity system would select a card based on various criteria like cost, features. The standard to be selected depends on the category of card used for the identity system.
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—The standards commonly used PDF417 and QR code are listed. Comments provide guidelines on selection of standard for 2D bar code.
6. Federation protocols—Open ID connect and OAuth combination are being increasingly used for federation while SAML has been used extensively earlier.

S.NO	INTER-OPERABILITY AREA	SUBAREA	STANDARD SPECIFICATION/ (COMMON NAME)	STANDARD DESCRIPTION	STANDARDS BODY	OTHER COMPETING STANDARDS (IF ANY)	COMMENTS
A.1	Biometrics	Image Standard	ISO/IEC 15444-1 (JPEG2000)	Image Coding Standard **(both lossy and lossless compression)**	ISO and IEC	JPEG (Open with some parts having patent issues) PNG (Open) GIF (Proprietary)) TIFF (Proprietary)	Used for face image, finger-print, Iris image. Exchange Format for Restricted Memory Device cases like Smart Cards.
A.2	Biometrics	Image Standard	ISO/IEC 15948, (PNG)	Technology—Com-puter graphics and image processing—Portable Network Graphics—**lossless compression**	W3C	JPEG JPEG2000 GIF, TIFF	Extensible file format for **lossless,** portable, well-compressed storage of raster images. PNG provides a patent-free replacement for GIF and can also replace many common uses of TIFF.
A.3	Biometrics	Image Standard	ISO/IEC 10918:1994 JPEG	Image Coding Standard—**lossy compression**	ISO and IEC	JPEG2000 GIF, TIFF	Graphics—Raster (Lossy Compression)—Exchange Format for Web, Desktop Applications
A.4	Biometrics	Image Standard	WSQ	Compression algorithm used for gray-scale fingerprint images	NIST	JPEG2000, JPEG	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.

(continued)

Continued

S.NO	INTER-OPERABILITY AREA	SUBAREA	STANDARD SPECIFICATION/ (COMMON NAME)	STANDARD DESCRIPTION	STANDARDS BODY	OTHER COMPETING STANDARDS (IF ANY)	COMMENTS
B.1	Biometrics	Data inter-change—Face	ISO/IEC 19794-5:2011 (Face Image)	Biometric data inter-change formats for Face image specifies data scene, photo-graphic, digitization and format require-ments for images of faces to be used in the context of both human verification and computer auto-mated recognition	ISO and IEC		The image compression algorithm can be in any of the following: JPEG2000, PNG, JPEG etc. JPEG2000 or PNG open standards are recommended
B.2	Biometrics	Data Inter-change—Fingerprint	ISO/IEC 19794-4:2011 (Finger print)	Data record inter-change format for storing, recording, and transmitting the information from one or more finger or palm image areas for exchange or comparison	ISO and IEC		JPEG2000, PNG, JPEG, WSQ etc. formats allowed JPEG2000 recommended as it is open standard and allows for both lossy and lossless compression
B.3	Biometrics	Data Inter-change—Iris	ISO/IEC 19794-6:2011 (Iris)	Iris image inter-change formats for biometric enrollment, verification and iden-tification system	ISO and IEC		

(continued)

Continued

S.NO	INTER-OPERABILITY AREA	SUBAREA	STANDARD SPECIFICATION/ (COMMON NAME)	STANDARD DESCRIPTION	STANDARDS BODY	OTHER COMPETING STANDARDS (IF ANY)	COMMENTS
B.4	Biometrics	Data Inter-change—Minutiae	ISO/IEC 19794-2:2011 (Minutiae)	3 data formats for representation of fingerprints using the fundamental notion of minutiae for interchange and stor-age 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 inter-change—Signature	ISO/IEC 19794-7:2014 (Signature)	Data interchange formats for signature/ sign behavioral data captured in the form of a multi-dimen-sional time series using devices such as digitizing tablets or advanced pen systems	ISO and IEC		
C.1	Card		ISO/IEC 7810	Identification Cards—Physical Characteristics	ISO and IEC		Plastic card without chip
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		

(continued)

Continued

S.NO	INTER-OPERABILITY AREA	SUBAREA	STANDARD SPECIFICATION/ (COMMON NAME)	STANDARD DESCRIPTION	STANDARDS BODY	OTHER COMPETING STANDARDS (IF ANY)	COMMENTS
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		
D.1	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	Data Matrix, PDF417	A barcode is a machine-readable optical label that contains information about the item to which it is attached
D.2	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	Data Matrix QR code	PDF417 is a stacked barcode that can be read with a simple linear scan being swept over the symbol. 4 times less capacity than QR code.

(continued)

Continued

S.NO	INTER-OPERABILITY AREA	SUBAREA	STANDARD SPECIFICATION/ (COMMON NAME)	STANDARD DESCRIPTION	STANDARDS BODY	OTHER COMPETING STANDARDS (IF ANY)	COMMENTS
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		PKCS #1 published by RSA laboratories—republished as RFC for internet community
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		
E.4	Digital Signatures/ cryptography	Security	FIPS 140-2	Security Requirements for Cryptographic Modules	NIST		

(continued)

Continued

S.NO	INTER-OPERABILITY AREA	SUBAREA	STANDARD SPECIFICATION/ (COMMON NAME)	STANDARD DESCRIPTION	STANDARDS BODY	OTHER COMPETING STANDARDS (IF ANY)	COMMENTS
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		Estonia Digital ID follows this standard

(continued)

Continued

S.NO	INTER-OPERABILITY AREA	SUBAREA	STANDARD SPECIFICATION/ (COMMON NAME)	STANDARD DESCRIPTION	STANDARDS BODY	OTHER COMPETING STANDARDS (IF ANY)	COMMENTS
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	Open ID connect and OAuth	
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	SAML	Mobile Connect solution providing password less authentication tied to the mobile phone of the user is based on the OpenID Connect & OAuth2

(continued)

Continued

S.NO	INTER-OPERABILITY AREA	SUBAREA	STANDARD SPECIFICATION/ (COMMON NAME)	STANDARD DESCRIPTION	STANDARDS BODY	OTHER COMPETING STANDARDS (IF ANY)	COMMENTS
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	SAML	Mobile Connect solution providing password less authentication tied to the mobile phone of the user is based on the OpenID Connect & OAuth2

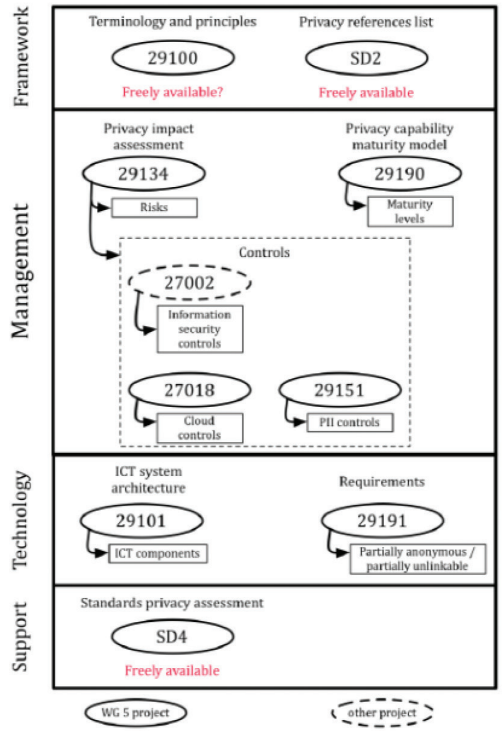
S. NO	STANDARD SPECIFICATION/ (COMMON NAME)	STANDARD DESCRIPTION	STANDARDS BODY	COMMENTS
1	ISO/IEC 29794 Series	Biometric Sample Quality—Matching Performance	ISO and IEC	Quality
2	ISO/IEC 29100	Privacy framework	ISO and IEC	ISO/IEC 29100 provides a privacy framework which: • specifies a common privacy terminology; • defines the actors and their roles in processing personally identifiable information (PII); • describes privacy safeguarding considerations; and • provides references to known privacy principles for IT
3	ISO/IEC 27018	Code of practice for PII protection in public clouds acting as PII processors	ISO and IEC	ISO/IEC 27018 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment
4	ISO/IEC 29190	Privacy capability assessment model	ISO and IEC	ISO/IEC 29190:2015 provides organizations with high-level guidance about how to assess their capability to manage privacy-related processes
5	ISO/IEC 29146	A framework for access management	ISO and IEC	ISO/IEC 29146 defines and establishes a framework for access management (AM) and the secure management of the process to access information and Information and Communications Technologies (ICT) resources, associated with the accountability of a subject within some context
6	ISO/IEC 29134	Privacy impact assessment—Guidelines	ISO and IEC	ISO/IEC 29134:2017 gives guidelines for a process on privacy impact assessments, and a structure and content of a PIA report
7	ISO/IEC 29184	Guidelines for online privacy notice and consent	ISO and IEC	Under development

(continued)

Continued

S. NO	STANDARD SPECIFICATION/ (COMMON NAME)	STANDARD DESCRIPTION	STANDARDS BODY	COMMENTS
8	ISO/IEC 24761	Authentication Context for Biometrics	ISO and IEC	Remote site biometrics authentication
9	ISO/IEC 24760 Series	Framework for Management of Identity Information	ISO and IEC	Protecting Privacy & Security—further discussion needed on use of this standard
10	ISO/IEC 29109 Series	Testing Methodology for Biometric Data Interchange	ISO and IEC	
11	ISO/IEC 24745	Security Techniques— Biometric Information Protection	ISO and IEC	

WG 5 Identity Management & Privacy Technologies Privacy/PII standards in SC 27/WG 5 and elsewhere



Source: https://rm.coe.int/work-and-projects-in-iso-iec-jtc-1-sc-27-wg-5-identity-management-priv/168073ff03

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 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.

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

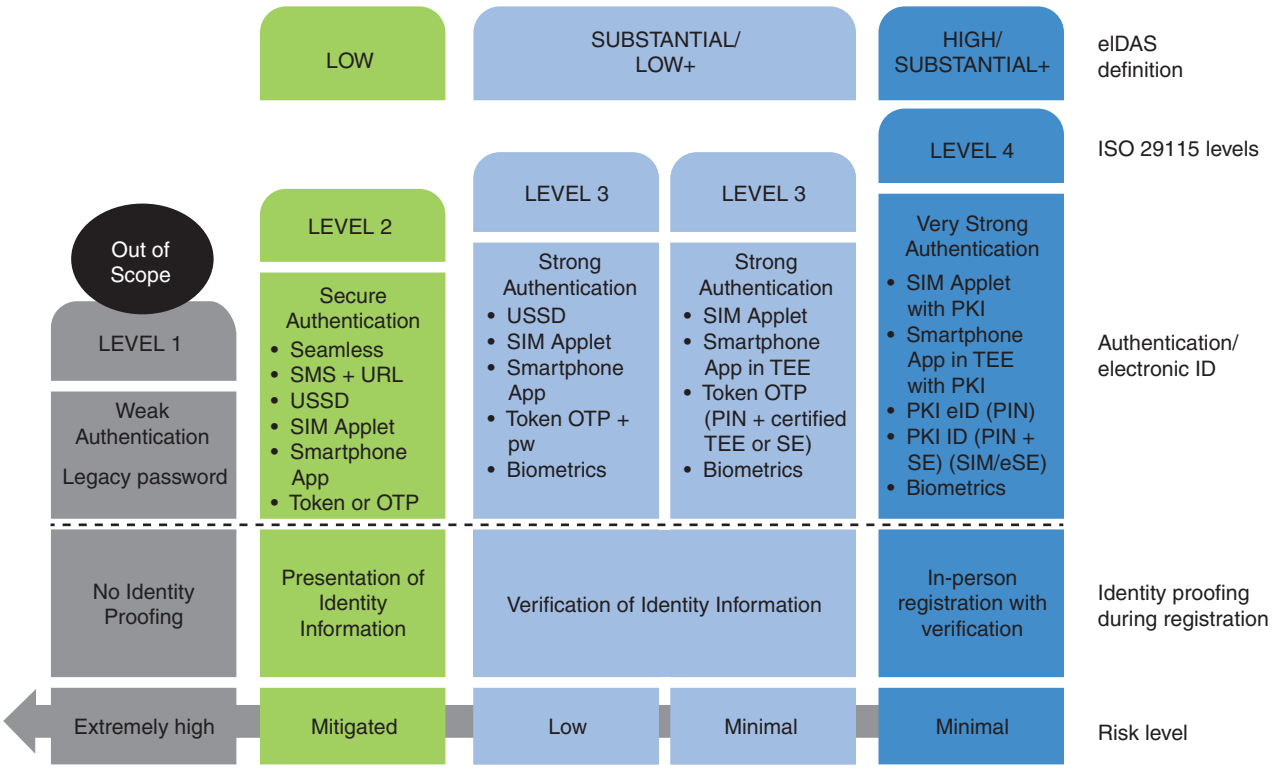
5.4.1 Levels of Assurance

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 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 is the risk 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 levels of assurances for scalable identity management and authentication services. These levels are shown in Figure 2, 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.

FIGURE 2 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 India, Pakistan, Peru, and Estonia are briefly discussed in Boxes 6.1, 6.2, 6.3 and 6.4 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.

Three standards are vital for any legal identification system that involves biometrics: the ISO 19794, 29794 and 29109 series. The ISO 19794 series defines biometric interchange format for various types of biometric data (face image, fingerprint, iris), the ISO/IEC 29794 series refers to biometric quality, and the ISO 29109 series concerns conformance testing that could cover inter alia, testing, surveillance, inspection, audit, certification and accreditation.

ISO 19794 is crucial for **cryptographic protection** in interchange environments as biometric data are sensitive to cyber-attack or identity-theft. Since ID systems are tested rigorously before and after deployment, the use of the ISO 19794 series coupled with ISO/IEC the 29109 series becomes important because the latter describes and specifies conformance-testing methodology for biometric data interchange formats defined in ISO/IEC 19794. It also specifies elements of test assertions and test procedures as applicable to the biometric data interchange format standard.

Box 6.1: 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, and more than 93 percent of Indians now have 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. An important security standard, ISO 24745, which provides guidance for the protection of biometric information for confidentiality and integrity during storage or managing identities, was not implemented due to the complexity of applicable compliance procedures. 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 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.

Box 6.2: 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 is now one of the world's leading suppliers of eID services. It also designed its cards to meet the needs of its citizens living outside the country. As a result, its smart eID, 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.

Source: Author's Analysis.

Any system that uses biometric enrollment and/or authentication is advised to consider these biometric standards. However, for countries that issue biometric-based unique identity numbers without ID cards (e.g., India, see Box 6.1), the standards for creating and managing biometric-based identities are of primary concern.

Smart Cards Related Standards

For countries that issue a tangible credential such as a **physical eID card,** standards such as ISO-7810 to ISO-7813 also 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. In addition, ICAO is developing an international framework of standards for MRTDs as part of their strategy, known as the Travelers Identification Program (TRIP) Strategy, which includes interoperable application standards. For travel ID cards used by seafarers, the guidelines issued by the International Labor Organization (ILO) become relevant.

Box 6.3: eID with Digital Certificate in Peru

Peru's National Electronic ID Card (DNIe), issued by the National Registry of Identification and Civil Status (RENIEC), was considered to be the best ID card in Latin America during the 2015 High Security Printing Latin American Conference in Lima. RENIEC, 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 DNIe provides Peruvian citizens with a digital identity, which can be authenticated physically and virtually. 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. Because the card is also used as a machine-readable travel document (MRTD), it also complies with ICAO 9303.

Source: Interview with RENIEC official.

Box 6.4: 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 signatures are stored in the system alongside a unique number, used by citizens as a unique identifier to sign documents online and verify online identity. 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.

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.

If a Smart card such as an eID is intended to be used as a **bank card,** then EMV standards[6] also become applicable. ISO 8583 defines the physical characteristics such as magnetic strip on the card if it is intended to be used as payment card. In countries where **drivers' licenses** are the primary identity document used to confirm identity, the drivers' license standard known as ISO 18103 is followed. As more functionality is added to an eID card, conforming with all relevant standards may become a complex or difficult task. For example, if an ID-card that is used as payment card *and* an ICAO compliant travel document as well, it may be cumbersome to fit a magnetic strip and ICAO machine readable zone on the card, in addition to a financial institution logo and details necessary for recognition as a valid payment instrument.

7. CONSIDERATIONS WHILE ADOPTING STANDARDS FOR IDENTITY SYSTEMS

The preceding sections highlight relevant standards that have been used for leading digital identification systems in a number of countries. These pioneering countries have spent considerable effort in studying and adopting standards to benchmark and test technology before deploying it, which underscores the value of adopting and implementing specific standards. There are also some lessons to be learnt from other countries which missed adopting standards leading to issues relating to interoperability, robustness and vendor lock-in. As various countries embark on implementation of the digital identification systems for sustainable it would be prudent to identify and advocate a set of minimum technical standards for common good and enable development of robust interoperable identity systems which are not plagued by vendor lock in

In addition, it underscores the need to review new solutions developed by industry consortia, such as Mobile Connect,[7] and new regulations such as eIDAS,[8] which are in the developmental stage and may become standards in near future as more countries adopt them. It is important to benchmark new standards before large-scale implementation to see if these may compromise or hinder scalability, connectivity, interoperability, and compatibility.

Any forthcoming strategy on developing minimum standards for digital identity systems should address the following issues and challenges:

a. Protecting Biometrics from Security Breaches

Digital biometric identification is fast becoming a standard tool to uniquely enroll a population, particularly given the diminishing costs of the technology. Heavy reliance on biometrics poses a challenge in protecting the personal data of citizens, particularly where security infrastructure, technological capacity, and legal protections are weak. Unlike other forms of credentials (passwords and PINs, which can be replaced), breach of biometric data is costly and the consequences may be severe in the case of a hostile attack or hacking. This requires adoption and implementation of relevant security standards and a strong legal framework for privacy and data protection.

b. Single or Multimodal Systems

The choice between using a single or multiple biometric identifiers (fingerprints, iris, face, etc.) may require different standards, and depends on many factors (for example, IT infrastructure cost, and cultural considerations). Multimodal systems have become increasingly popular because they produce more accurate results, as multiple unique attributes are authenticated instead of reliance on a single attribute. They also enable help in deduplication of identities with greater accuracy. This is advantageous in terms of ensuring inclusiveness,[9] which is an important consideration for the development agenda. In low- and middle-income countries, for example, the fingerprints of people involved in manual labor can become worn out and unreadable. The face is the most commonly captured biometric, and is widely used in manual visual verification.

The biggest driver in selecting between a single or multimodal system is accuracy, driven by population size as well as demographic characteristics. In addition, the complexity of various operating systems and technologies in multimodal systems could pose operational challenges. If it becomes cost prohibitive to implement a multimodal system and a country is inclined to implement only part of a complete biometrics system, the risk of biometric failure must be identified and backup procedures for identity authentication (such as validation checks, built-in registration software, or manual examination of authenticity of breeder documents) should be defined.

c. Lack of Biometric Device Standards

The identity lifecycle can only work seamlessly when all IT systems and devices are integrated. Vendor lock-in risks must be mitigated by thoroughly examining previous records of similar implementations. As relevant ISO standards are mainly focused on interchange standards, quality standards and testing methodology standards

(see Section 5.3), there is a lack of standards or certifications regarding devices that read or authenticate biometric information and countries should rely on best practices offered by industry consortia.

d. Modernizing Legacy Identification Systems

Prior to the widespread use of digital biometric technology and databases, some countries had well-established paper-based civil registration systems and national ID systems that relied on collecting limited biometrics (commonly a single fingerprint), that may or may not have been digital. Many countries enhanced these systems by switching to digital capture of biometrics and adding additional attributes (e.g., iris, digital photo). This transition requires standardizing biographic and identity resolution on both biographic and biometric data. Modernizing these systems by incorporating digital biometric technology may also necessitate changes to legal frameworks to modify registration procedures, and upgrading technology and technical skills of staff. These efforts would require adoption and implementation of standards that take into consideration multiple modalities, methodologies and sources for biometrics as well as the management of biographic data.

e. Cost Effectiveness

Digital identification systems are technology based, and new technologies are evolving at an exponential rate. The development of new technologies and equipment may render old technologies obsolete, requiring frequent upgrades that may be costly. For low-income countries, compliance with all proprietary standards may be challenging from a cost perspective, hence the use of open standards is generally recommended. Meeting minimum ISO standards regarding the identity lifecycle for specific applications may be considered in terms of cost effectiveness, as these standards prevent countries from costly corrective actions or revamping identification system. For example, if a country rolls out an ID card which is not ICAO compliant and in future the same is used as travel card, it has to incur unnecessary additional costs to reissue ICAO-compliant cards hence.

f. Interoperability and Interconnectivity

As specified in the European interoperability framework for pan-European eGovernment services document (http://ec.europa.eu/idabc/servlets/Docd552.pdf?id=19529), three aspects of interoperability need to be considered:

- Organisational Interoperability

  This aspect of interoperability is concerned with defining business goals, modelling business processes and bringing about the collaboration of administrations that wish to exchange information and may have different internal structures and processes. Moreover, organizational interoperability aims at addressing the requirements of the user community by making services available, easily identifiable, accessible and user-oriented. Example of an activity with reference to digital ID interoperability across organizations/countries would be to map the identity lifecycle processes of that organization with the ISO Authentication assurance framework levels.

- Semantic Interoperability

  This aspect of interoperability is concerned with ensuring that the precise meaning of exchanged information is understandable by any other application that was not initially developed for this purpose. Semantic interoperability enables systems to combine received information with other information resources and to process it in a meaningful manner. Semantic interoperability is therefore a prerequisite for the front-end multilingual delivery of services to the user.

  Example for digital identity system: Defining the data formats and metadata for identity attributes like name and date of birth would be important to achieve this objective. The format of capturing name and the data type and maximum length of this field is important to ensure correct interpretation and prevent loss of information (length of name, order of specifying the first name, middle name,) format of date—date of birth (mm/dd/yyyy) or dd/mm/yy etc. needs to be agreed upon to ensure correct and complete information/data exchange. For the Aadhaar project in India these standards were defined

in the demographic standard document to enable interoperability of identity data with other systems. This system is being extensively used to provide the Know your Customer (KYC) service based on these standards ensuring data field definition compatibility across various IT systems/applications.

- Technical Interoperability

  This aspect of interoperability covers the technical issues of linking computer systems and services. It includes key aspects such as open interfaces, interconnection services, data integration and middleware, data presentation and exchange, accessibility and security. Example for digital identity system: Identification of standards for biometrics (fingerprints, face image and iris), digital signature standards, federation protocols

  Developing a set of minimum relevant standards for these three layers will therefore help to ensure that identification systems are sufficiently robust and interoperable

g. Foundational Legal Identification Systems

Identity systems developed with the general purpose of identifying individuals and providing proof of ID—may require linking with other functional systems for the provision of services. IT devices from different vendors with varying architectures and operating systems pose interoperability challenges. The development of new technologies also poses challenges regarding interconnectivity. A question arises: should a system be integrated with a central data warehouse, or should a distributed model be implemented? In addition, there is a concern that different biometric devices have their own inherent standards that may result in interconnectivity issues. In addition, multimodal systems create complexity as well, since different vendors offer different biometric solutions. ISO standards should be adopted to ensure interoperability and avoid vendor lock-in.

h. Privacy and Security

It is important to build privacy and security into the architecture of a digital ID system. Privacy challenges arise because the various authorities, agencies, and governmental departments requiring and authenticating identities for service provision and administration may have access to citizens' personal information. Similarly, the systems need to be guarded so that citizens' information is secure and protected. In consequence, privacy- and security-related standards are of central importance.

i. New Standards Compliance

Compliance with new standards may be challenging for the countries who have already registered large populations. With so many competing requirements for identification systems, choosing which standard to implement and which one to relax (for example, to take cultural considerations into account[10]) becomes challenging. For countries that have already collected biometric attributes of large populations, it would be challenging to go back and update their data to implement a *new* standard without recalling all the individuals for re-enrollment. In India, for example, the ISO 24745 security standard—which provides guidance for the protection of biometric information for confidentiality and integrity during storage or managing identities—was not implemented in the rollout of the Aadhaar project due to the complexity of applicable compliance procedures. Although a security standard to ensure the privacy of individuals became available in 2011, when millions had already registered, it would be difficult to implement retroactively in such a large-scale implementation. Hence, compliance with standards should follow a functional or outcome-based approach.

j. Role of Development Partners

Many countries need technical and financial support to implement standards, including support for infrastructure and training. This includes countries that are upgrading legacy identification systems, as well as those building entirely new systems. In addition, development partners can play a role in thought leadership and advocacy for adopting a standards approach to identification systems. This will require a communications strategy to appraise stakeholders on how market driven standards can encourage (a) business growth, (b) public private partnerships, and (c) the inclusiveness of individuals to achieve development benefits at a local level.

An international effort to promote standards will require global coordination and partnership between a variety of actors. Such partnerships should also reach beyond the digital identity sector to include agencies such as the United Nations that work on CRVS, as the standards used for these documents have important implications for identity proofing in digital identity systems.

8. THE WAY FORWARD

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.

A strategic approach to developing a set of global minimum standards should translate into an actionable framework for country governments and their partners. To achieve this, the following next steps are recommended as a potential way forward:

1. Conduct an in-depth analysis of the standards identified in this document to see if a minimum universal set can be recommended.
2. Provide guidelines and options for implementing a high assurance identity system and applicable standards for the option.
3. Identify standards to advocate for on a continuous basis. Provide thought leadership on promoting a common terminology and framework for standards.
4. Support standards development efforts at the international, regional, national, and country levels, in cooperation with a variety of stakeholders, including key international organizations and public-sector partners.
5. Support technical human resource development efforts at the country level to adopt or implement relevant standards.
6. Develop Data Standards and Process standards for semantic and organizational interoperability to achieve a truly interoperable system as described in the Government interoperability framework of various countries.

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.* Washington, DC: World Bank Group, 2016.

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

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.

(continued)

Continued

SUBCOMMITTEES/ WORKING GROUP	SCOPE	DESCRIPTION
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
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.

APPENDIX B STANDARDS DESCRIPTION

STANDARD	DESCRIPTION
ISO/IEC 19785 Information technology—Common Biometric Exchange Formats Framework (CBEFF)	The standard defines a basic structure for standardized biometric information records (BIRs) within the Common Biometric Exchange Formats Framework (CBEFF). This structure consists of three parts: the standard biometric header (SBH), the biometric data block (BDB), and the security block (SB). CBEFF also defines several data elements and their standardized abstract values that can be used in SBHs and SBs (CBEFF treats the BDB as opaque data). CBEFF also establishes mechanisms by which organizations, called "patrons" by CBEFF, can specify and publish BIR format specifications, which are in turn called "patron formats." CBEFF enables patrons to develop BIR specifications that are fully standardized and interoperable, yet are specifically adapted to the requirements of a particular application environment. CBEFF defines rules for BIRs that contain only one BDB (simple BIR) and that contain at least one BDB (complex BIR). CBEFF defines mandatory data elements that identify the format of a BDB and its security attributes (encryption and integrity). All the other CBEFF-defined data elements and abstract values are optional. CBEFF enables patrons to define additional data elements and abstract values as required by the application environment. The standard was updated in 2015. Protection of the privacy of individuals from inappropriate dissemination and use of biometric data is not in the scope of this part of ISO/IEC 19785 but may be subject to national regulation.
ISO/IEC 19794—(Series) Biometric data interchange forms	Framework describes the general aspects and requirements for defining biometric data interchange formats. The notation and transfer formats provide platform independence and separation of transfer syntax from content definition. Data formats for representation of fingerprints using the fundamental notion of minutiae. Relevant for automated fingerprint recognition. Facial recognition formats.
ISO/IEC 15444 (all parts) Information technology—JPEG 2000 image coding system	This standard deal with JPEG 2000 Image coding systems. It deals with Spatial (samples), transformed (coefficients) and Compressed image data. Various elements such as encoder, decoder, code stream, optional file formats with syntax, reconstruction of image data, and guidelines how to implement these processes in practice are explained.

(continued)

Continued

STANDARD	DESCRIPTION
ISO/IEC 29794	Quality metrics are useful for several applications in the field of biometrics. ISO/IEC 29794 defines and specifies methodologies for objective, quantitative quality score expression, interpretation, and interchange. This standard is intended to add value to a broad spectrum of applications in a manner that a) encourages competition, innovation, interoperability and performance improvements; and b) avoids bias towards applications, modalities, or techniques. It presents several biometric sample quality scoring tools, the use of which is generally optional but can be determined to be mandatory by application profiles or specific implementations. It consists of the following parts, under the general title Information technology—Biometric sample quality: • Part 1: Framework • Part 4: Finger image data • Part 5: Facial image data [Technical Report] • Part 6: Iris image data
ISO/IEC 7810	ISO/IEC 7810 is one of a series of standards describing the characteristics of identification cards. The purpose is to provide criteria to which cards shall perform and to specify the requirements for such cards used for international interchange. It takes into consideration both human and machine aspects and states minimum requirements. It defines various sizes (4) of the ID cards, the conditions for conformance, the dimensions and tolerances of the identification cards; the construction and materials of the identification cards; and the physical characteristics of the cards such as bending stiffness, flammability, toxicity, resistance to chemicals, dimensional stability, adhesion or blocking, warpage, resistance to heat, surface distortions, and contamination—all are elaborated in this standard.
ISO/IEC 7811 Series	ISO/IEC 7811 Series standard describes characteristics of identification cards with magnetic stripes. It specifies the embossing, magnetic stripe, location of Read Only magnetic tracks, location of Read/Write Magnetic Tracks, etc.
ISO 7812	ISO/IEC 7812 Identification cards—Identification of issuers was first published by the International Organization for Standardization (ISO) in 1989. It is the international standard that specifies “a numbering system for the identification of issuers of cards that require an issuer identification number (IIN) to operate in international, inter-industry and/or intra-industry interchange,” and procedures for registering IINs. [2] ISO/IEC 7812 have two parts: Part 1: Numbering system Part 2: Application and registration procedures

(continued)

Continued

STANDARD	DESCRIPTION
ISO/IEC 7813	ISO/IEC 7813 specifies the standards for cards used for financial transactions. It specifies the data structure and data content of magnetic tracks 1 and 2, which are used to initiate financial transactions. It takes into consideration both human and physical aspects and states minimum requirements of conformity. It references layout, recording techniques, numbering systems, registration procedures, but not security requirements.
ISO/IEC 18013	The ISO/IEC 18013 standard establishes guidelines for the design format and data content of ISO/IEC-compliant driving licenses (IDL) with regard to human-readable features (ISO/IEC 18013-1), machine-readable technologies (ISO/IEC 18013-2), and access control, authentication and integrity validation (ISO/IEC 18013-3). It creates a common basis for international use and mutual recognition of the IDL without impeding individual countries/states from applying their privacy rules and national/community/regional motor vehicle authorities in taking care of their specific needs.
ISO/IEC 7816	ISO/IEC 7816 is a multi-part international standard broken into fourteen parts. ISO/IEC 7816 Parts 1, 2 and 3 deals only with contact smart cards and define the various aspects of the card and its interfaces, including the card's physical dimensions, the electrical interface and the communications protocols. ISO/IEC 7816 Parts 4, 5, 6, 8, 9, 11, 13 and 15 are relevant to all types of smart cards (contact as well as contactless). They define the card logical structure (files and data elements), various commands used by the application programming interface for basic use, application management, biometric verification, cryptographic services and application naming. ISO/IEC 7816 Part 10 is used by memory cards for applications such as prepaid telephone cards or vending machines. ISO/IEC 7816 Part 7 defines a secure relational database approach for smart cards based on the SQL interfaces (SCQL).
ISO/IEC 14443	ISO/IEC 14443 is an international standard that defines the interfaces to a "close proximity" contactless smart card, including the radio frequency (RF) interface, the electrical interface, and the communications and anti-collision protocols. ISO/IEC 14443 compliant cards operate at 13.56 MHz and have an operational range of up to 10 centimeters (3.94 inches). ISO/IEC 14443 is the primary contactless smart card standard being used for transit, financial, and access control applications. It is also used in electronic passports and in the FIPS 201 PIV card.
ICAO 9303 Standard for Machine Readable Travel Documents	A machine-readable travel document (MRTD) is in fact a travel document with the data on the identity page encoded in optical character recognition format. Many countries began to issue machine-readable travel documents in the 1980s. Most travel passports worldwide are MRPs. They are standardized by the ICAO Document 9303 (endorsed by the International Organization for Standardization and the International Electrotechnical Commission as ISO/IEC 7501-1) and have a special machine-readable zone (MRZ), which is usually at the bottom of the identity page at the beginning of a passport or travel card with basic identity information.

(continued)

Continued

STANDARD	DESCRIPTION
ISO/IEC 8583	ISO 8583 provides a framework for creating protocols for the exchange of financial transaction messages. Typically, these are messages that involve transactions originating from cards of some sort or the other, be they credit or debit cards. It is important to realize that 8583 itself is not a protocol, just as XML is not a file format. XML can be considered a description of how to specify file formats for structured data according to a set of rules. ISO 8583 is a meta-protocol providing a set of rules for the definition of financial transaction protocols. The standard, officially titled "Financial transaction card originated messages—Interchange message specifications" is comprised of three parts: • Part 1: Messages, data elements and code values • Part 2: Application and registration procedures for Institution Identification Codes (IIC) • Part 3: Maintenance procedures for messages, data elements and code values
Europay, Mastercard and VISA (EMV) Standards	EMV is a technical standard for smart payment cards and for payment terminals and automated teller machines that can accept them. EMV (Europay, MasterCard and Visa) cards are smart cards (also called chip cards or IC cards), which store their data on integrated circuits rather than magnetic stripes, although many EMV cards also have stripes for backward compatibility. They can be contact cards that must be physically inserted (or "dipped") into a reader, or contactless cards that can be read over a short distance using radio-frequency identification (RFID) technology. Payment cards that comply with the EMV standard are often called chip-and-PIN or chip-and-signature cards, depending on the exact authentication methods required to use them. EMV stands for Europay, MasterCard, and Visa, the three companies that originally created the standard. The standard is now managed by EMVCo, a consortium with control split equally among Visa, Mastercard, JCB, American Express, China UnionPay, and Discover. There are standards based on ISO/IEC 7816 for contact cards, and standards based on ISO/IEC 14443 for contactless cards (PayPass, PayWave, ExpressPay). Visa and MasterCard have also developed standards for using EMV cards in devices to support card-not-present transactions over the telephone and Internet. MasterCard has the Chip Authentication Program (CAP) for secure e-commerce. Its implementation is known as EMV-CAP and supports many modes. Visa has the Dynamic Passcode Authentication (DPA) scheme, which is their implementation of CAP using different default values.
ISO/IEC 24761 Information technology—Security techniques—Authentication context for biometrics	Specifies the structure and the data elements of Authentication Context for Biometrics (ACBio), which is used for checking the validity of the result of a biometric verification process executed at a remote site. ISO/IEC 24761:2009 allows any ACBio instance to accompany any data item that is involved in any biometric process related to verification and enrollment. The specification of ACBio is applicable not only to single modal biometric verification but also to multimodal fusion. ISO/IEC 24761:2009 specifies the cryptographic syntax of an ACBio instance. The cryptographic syntax of an ACBio instance is based on an abstract Cryptographic Message Syntax (CMS) schema whose concrete values can be represented using either a compact binary encoding or a human-readable XML encoding. ISO/IEC 24761:2009 does not define protocols to be used between entities such as biometric processing units, claimant, and validator. Its concern is entirely with the content and encoding of the ACBio instances for the various processing activities.

(continued)

Continued

STANDARD	DESCRIPTION
Mobile Connect—a new industry mechanism for online identity	Mobile Connect is boasted as a secure universal log-in solution. It is increasingly becoming a new standard in digital authentication. Simply by matching the user to their mobile phone, Mobile Connect allows them to log in to websites and applications quickly without the need to remember passwords and user names. It is generally considered as safe, secure and no personal information is shared without permission. The standard is back by the mobile industry consortium known as Groupe Speciale Mobile Association (GSMA). European Union endorsed the GSM project in 1986. Mobile Connect is available to 2 billion consumers globally. It is becoming popular as it offers a solution by providing citizens with a secure and convenient way to prove who they are, with the device that is always with them: their mobile phone. Mobile Connect can support e-government digital identity authentication for citizens giving access to public services, smart cities, health care, education, cross border public services and voting. Through the in-built privacy protection offered, it can simplify anonymous registration where citizen entitlement does not need to be checked, and reduce the risk of data breaches as well as cut governments' costs to serve. By delivering these benefits to citizens and employees, Mobile Connect has a potential to strengthen trust and uptake of e-government services.
ISO/IEC 24745:2011 Information technology-security techniques—Biometric information protection	Provides guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. Additionally, ISO/IEC 24745:2011 provides requirements and guidelines for the secure and privacy-compliant management and processing of biometric information. • analysis of the threats to and countermeasures inherent in a biometric and biometric system application models; • security requirements for secure binding between a biometric reference and an identity reference; • biometric system application models with different scenarios for the storage of biometric references and comparison; and • guidance on the protection of an individual's privacy during the processing of biometric information. However, does not include measures for physical, environmental security and key management for cryptographic techniques.
FIDO mechanism for security devices and plug-ins	The FIDO (Fast IDentity Online) Alliance is a nonprofit organization formed in July 2012 to address the lack of interoperability among strong authentication devices as well as the problems users face with creating and remembering multiple user names and passwords. The FIDO Alliance plans to change the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services. This new standard for security devices and browser plug-ins will allow any website or Cloud application to interface with a broad variety of existing and future FIDO-enabled devices that the user has for online security. FIDO protocols are based on public key cryptography and are strongly resistant to phishing.

(continued)

Continued

STANDARD	DESCRIPTION
eIDAS Regulation of European Union	eIDAS stands for EU Regulation No 910/2014 on electronic identification and trust services for electronic transactions. eIDAS was published by the European Parliament and the European Council on July 23, 2014. eIDAS oversees electronic identification and trust services for electronic transactions in the European Union's internal market. It regulates electronic signatures, electronic transactions, involved bodies and their embedding processes to provide a safe way for users to conduct business online like electronic funds transfer or transactions with public services. Both the signatory and recipient have access to a higher level of convenience and security. Instead of relying on traditional methods, such as mail, facsimile service, or appearing in person to submit paper-based documents, they may now perform transactions across borders, e.g., using "1-Click" technology. [1][2] eIDAS has created standards for which electronic signatures, electronic seals, time stamps and other proof for authentication purposes provide electronic transactions with the same legal standing as transactions performed on paper.
ISO/IEC 24760 Information Technology-Security Techniques—A framework of Identity Management	Data processing systems commonly gather a range of information on their users, be it a person, piece of equipment, or piece of software connected to them, and make decisions based on the gathered information. Such identity-based decisions may concern access to applications or other resources. To address the need to efficiently and effectively implement systems that make identity-based decisions, ISO/IEC 24760 specifies a framework for the issuance, administration, and use of data that serves to characterize individuals, organizations, or information technology components that operate on behalf of individuals or organizations. For many organizations, the proper management of identity information is crucial to maintain security of the organizational processes. For individuals, correct identity management is important to protect privacy. ISO/IEC 24760 Series specifies fundamental concepts and operational structures of identity management with the purpose to realize information system management so that information systems can meet business, contractual, regulatory and legal obligations.
ISO/IEC 29109	ISO/IEC 29109 defines the concepts of conformance testing for biometric data interchange formats and defines a general conformance-testing framework. It specifies common (modality-neutral) elements of the testing methodology, such as test methods and procedures, implementation conformance claims, and test results reporting. It also provides the assertion language definition and sets forth other testing and reporting requirements, and outlines other aspects of the conformance testing methodology that are generally applicable and not modality specific. As part of the conformance testing methodology, different types and levels of conformance testing are described, as well as their applicability. The conformance testing methodology specified in ISO/IEC 29109-1:2009 is concerned only with data interchange format records and systems that produce or use these records.
ISO/IEC 29115	ISO/IEC 29115:2013 provides a framework for managing entity authentication assurance in a given context. In particular, it: • specifies four levels of entity authentication assurance; • specifies criteria and guidelines for achieving each of the four levels of entity authentication assurance (LoAs); • provides guidance for mapping other authentication assurance schemes to the four LoAs; • provides guidance for exchanging the results of authentication that are based on the four LoAs; and • provides guidance concerning controls that should be used to mitigate authentication threats.

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

Endnotes

[1] For more on the importance of identification for development, see (World Bank 2016, Gelb and Clark 2013).

[2] Estimates by the World Bank ID4D Dataset, as of February 2016. This dataset will be updated annually.

[3] IEEE. What are Standards? Why are they important? IEEE, 2011.

[4] Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, World Bank-GSMA-SIA 2016.

[5] IEE FAQs https://supportcenter.ieee.org/app/answers/detail/a_id/83/~/what-are-standards%3F.

[6] Europay, MasterCard and Visa—Payment Smart Card Standard.

[7] https://mobileconnect.io.

[8] EU Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the European internal market. See also Ashiq, J. A. 2016. "The eIDAS Agenda: Innovation, Interoperability and Transparency." Cryptomathic. 25 January, https://www.cryptomathic.com/news-events/blog/the-eidas-agenda-innovation-interoperability-and-transparency; Turner, Dawn M. "eIDAS from Directive to Regulation—Legal Aspects." Cryptomathic, https://www.cryptomathic.com/news-events/blog/eidas-from-directive-to-regulation-legal-aspects; van Zijp, Jacques. "Is the EU ready for eIDAS?," Secure Identity Alliance.

[9] A multimodal system does not require dependency on just one specific biometric feature.

[10] http://www.eiuperspectives.economist.com/technology-innovation/economic-empowerment-leaders/article/identifying-better-future.

[11] eID cards can be easily carried in a wallet, unlike large legal documents.

[12] Turner, Dawn M. "Understanding Major Terms Around Digital Signatures." Cryptomathic.

[13] According to PIRA, "The global market for Personal ID credentials was valued at $5.3 billion in 2009, and is forecast to reach $9.1 billion by 2019" (PIRA, 2014).

[14] Excerpt from World Bank. 2016. *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation.* Washington, D.C.: World Bank Group, p. 19.

[15] For example, see EU Cross-border Digital Authentication by Gemalto, http://www.gemalto.com/mobile/customer-cases/eu-cross-border-digital-authentication.